2021-12

UNDERWATER COMMUNICATIONS WITH ACOUSTIC STEGANOGRAPHY: RECOVERY ANALYSIS AND MODELING

Strelkoff, Samuel

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/68748

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

UNDERWATER COMMUNICATIONS WITH ACOUSTIC STEGANOGRAPHY: RECOVERY ANALYSIS AND MODELING

by

Samuel Strelkoff

December 2021

Thesis Advisor:	Justin P. Rohrer
Second Reader:	Charles D. Prince

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2021	**3. REPORT TYPE AND DATES COVERED** Master’s thesis

4. TITLE AND SUBTITLE UNDERWATER COMMUNICATIONS WITH ACOUSTIC STEGANOGRAPHY: RECOVERY ANALYSIS AND MODELING	**5. FUNDING NUMBERS**
6. AUTHOR(S) Samuel Strelkoff	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

In the modern warfare environment, communication is a cornerstone of combat competence. However, the increasing threat of communications-denied environments highlights the need for communications systems with low probability of intercept and detection. This is doubly true in the subsurface environment, where communications and sonar systems can reveal the tactical location of platforms and capabilities, subverting their covert mission set. A steganographic communication scheme that leverages existing technologies and unexpected data carriers is a feasible means of increasing assurance of communications, even in denied environments. This research works toward a covert communication system by determining and comparing novel symbol recovery schemes to extract data from a signal transmitted under a steganographic technique and interfered with by a simulated underwater acoustic channel. We apply techniques for reliably extracting imperceptible information from unremarkable acoustic events robust to the variability of the hostile operating environment. The system is evaluated based on performance metrics, such as transmission rate and bit error rate, and we show that our scheme is sufficient to conduct covert communications through acoustic transmissions, though we do not solve the problems of synchronization or equalization.

14. SUBJECT TERMS digital signal processing, equalization, symbol recovery, underwater acoustic communication, steganography	**15. NUMBER OF PAGES** 107
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

UNDERWATER COMMUNICATIONS WITH ACOUSTIC STEGANOGRAPHY: RECOVERY ANALYSIS AND MODELING

Samuel Strelkoff
Lieutenant, United States Navy
BS, United States Naval Academy, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2021

Approved by: Justin P. Rohrer
Advisor

Charles D. Prince
Second Reader

Gurminder Singh
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In the modern warfare environment, communication is a cornerstone of combat competence. However, the increasing threat of communications-denied environments highlights the need for communications systems with low probability of intercept and detection. This is doubly true in the subsurface environment, where communications and sonar systems can reveal the tactical location of platforms and capabilities, subverting their covert mission set. A steganographic communication scheme that leverages existing technologies and unexpected data carriers is a feasible means of increasing assurance of communications, even in denied environments. This research works toward a covert communication system by determining and comparing novel symbol recovery schemes to extract data from a signal transmitted under a steganographic technique and interfered with by a simulated underwater acoustic channel. We apply techniques for reliably extracting imperceptible information from unremarkable acoustic events robust to the variability of the hostile operating environment. The system is evaluated based on performance metrics, such as transmission rate and bit error rate, and we show that our scheme is sufficient to conduct covert communications through acoustic transmissions, though we do not solve the problems of synchronization or equalization.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 Introduction **1**

1.1 Benefit to the Department of Defense 1

1.2 Research Questions 2

1.3 Scope 2

1.4 Approach and Significant Findings 3

1.5 Organization 4

2 Background **7**

2.1 Acoustic Steganography Communication System 7

2.2 Fading 10

2.3 Underwater Acoustic Communication 15

2.4 Data Recovery 19

2.5 Summary 31

3 Methodology **33**

3.1 Theory 33

3.2 Mathematical Refutations 37

3.3 Alternative Solutions 41

3.4 Channel Effects 52

3.5 Implementation 54

3.6 Summary 56

4 Results and Analysis **57**

4.1 Design 57

4.2 Results 58

4.3 Summary 74

5 Conclusions and Future Work **75**

5.1 Key Findings 75
5.2 Recommendations for Future Work 76
5.3 Conclusion 77

List of References **79**

Initial Distribution List **87**

List of Figures

Figure 3.1 Magnitude of Cross-Correlation Peak vs. Delay Offset 38

Figure 4.1 Spectrographs with and without Embedded Symbols. 58

Figure 4.2 Average Root Mean Square Error (RMSE) vs. Symbol Space. . . 59

Figure 4.3 Average Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR) vs. Symbol Space. 61

Figure 4.4 Comparison of Phase Histograms (Least Significant Bit) 62

Figure 4.5 Comparison of Amplitude Histograms (Least Significant Bit) . . 63

Figure 4.6 Comparison of Phase Histograms (Most Significant Bit) 64

Figure 4.7 Comparison of Amplitude Histograms (Most Significant Bit) . . 64

Figure 4.8 Deep Channel Recovery 66

Figure 4.9 Shallow Channel Recovery 69

Figure 4.10 Equalization Assumptions (Deep Channel) 72

Figure 4.11 Equalization Assumptions (Shallow Channel) 73

Figure 4.12 Symbol Recovery vs. Period 74

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

Table 3.1 Equation Variables 42

Table 4.1 Deep Channel Experiment Parameters 66

Table 4.2 Average Deep Channel Recovery Performance 67

Table 4.3 Shallow Channel Experiment Parameters 68

Table 4.4 Average Shallow Channel Recovery Performance 70

Table 4.5 Equalization Assumption Comparison Parameters 71

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

APSK	Asymmetric Phase Shift Keying
BCH	Bose, Chaudhuri, and Hocquenghem
BER	Bit Error Rate
bps	bits per second
BICM	Bit-Interleaved Code Modulation
CCD	Cyclic Coordinate Descent
CDMA	Code Division Multiple Access
CMA	Constant Modulus Algorithm
DFE	Decision-Feedback Equalizer
DFT	Discrete Fourier Transform
DLL	Delay-Locked Loop
DOD	Department of Defense
DPLL	Digital Phase-Locked Loop (PLL)
DSS	Direct-Sequence Spread-Spectrum
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform
HMM	Hidden Markov Model
IDMA	Interleave Division Multiple Access
ISI	Intersymbol Interference
LDPC	Low-Density Parity-Check
LMS	Least Mean Squares
LOS	line of sight
LPI/LPD	Low Probability of Intercept and Detection

LSB	Least Significant Bit
MABW	Multiuser Adaptive Baum & Welch
MAI	Multiple Access Interference
MAP	maximum a posteriori probability
MAV	Multiuser Adaptive Viterbi
MC	Mutual Coupling
MCMA	Modified Constant Modulus Algorithm (CMA)
MLSE	Maximum-Likelihood Sequence Estimation
MMPE	Monterey-Miami Parabolic Equation
MSB	Most Significant Bit
MSE	Mean Square Error
OFDM	Orthogonal Frequency-Division Multiplexing
PAPR	Peak-to-Average Power Ratio
PDF	Probability Density Function
PeCAN	Periodic-correlation CAN
PIC	Parallel Interference Cancellation
PLL	Phase-Locked Loop
PN	Pseudo-Noise
PSNR	Peak Signal-to-Noise Ratio
QPSK	Quadrature Phase Shift Keying
RF	radio frequency
RLS	Recursive Least Squares
RMSE	Root Mean Square Error
RS	Reed-Solomon
SCM	Superposition Coded Modulation
SEI	Super-Exponential Iteration

SIC	Successive Interference Cancellation
SNR	Signal-to-Noise Ratio
SSP	Sound Speed Profile
TDMA	Time Division Multiple Access
UACs	underwater acoustic channels
USN	U.S. Navy
WeCAN	Weighted CAN
ZCZ	Zero-Correlation Zone

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

First, I need to thank my advisor, Dr. Rohrer, and second reader, Charles Prince, without whom none of this would be possible. Thank you for introducing me to this topic, treating me as a peer, maintaining a high standard, and providing much needed guidance and support.

To my wife, I owe an unpayable debt of gratitude. Without her patience, love, support, pragmatism, and sacrifices, I never would have completed this project.

To my mothers, Katherine and Karen—and to all of my family—whose confidence in me usually far outstripped my own: thank you. Thank you for keeping me motivated and believing in the possible. Thank you for supporting me, my spouse, and our children throughout our lives, and especially in this endeavor.

Finally, I am grateful to all my friends and relatives who showed interest in my work, and in ways both large and small, provided moral support. I am humbled by the quality of the people who have graced my life.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

In the modern warfare environment, communication is a critical but not necessarily guaranteed requirement. The evermore sobering reality of communications denied environments highlights the need for communications systems with Low Probability of Intercept and Detection (LPI/LPD). This is doubly true in the undersea environment, where communications and sonar systems can reveal the tactical location of platforms and capabilities, subverting their operational and strategic advantage.

A steganographic communication scheme that leverages existing technologies and unexpected data carriers is a feasible means of increasing assurance of communications, even in denied environments. It is necessary that such a scheme have sufficient throughput and quality to enable effective information sharing.

This thesis explores the ability to improve symbol recovery in the frequency domain steganographic technique developed by LT Ferrao [1], based on Passerieux's time domain work [2], [3]. We seek to expand on the system presented by Ferrao in his thesis by developing techniques to expand the symbol space, mitigate channel effects, and improve symbol recovery. We utilize simulation based experimentation to assess the effectiveness of these techniques.

In this chapter, we describe the benefit of our research to the Department of Defense (DOD), state our objectives, define the scope of our research, present our findings, and outline how this thesis is organized.

1.1 Benefit to the Department of Defense

This study benefits the submarine and special forces of the U.S. Navy (USN), as it will support a means of covert underwater communication that can be applied as a software upgrade to existing equipment. However, benefit extends beyond these specific entities, as the method envisioned could also provide communications in an otherwise denied environment to all manner of aquatic vessels. Current naval subsurface command and control communication systems, as well as obstacle detection and collision avoidance systems, are detectable, interceptable, locatable, and deniable by our adversaries. Any of these four outcomes are undesirable for subsurface platforms, and their very possibility degrades mission capability. Since the research is designed to result in a LPI/LPD communications software system, no new hardware contracts would be necessary, easing adoption across the USN to enhance warfighting capability.

1.2 Research Questions

The principal question we seek to solve with this research is whether we can achieve symbol recovery appreciably better than random guessing within our chosen steganographic underwater communications system. The specific research questions necessary to develop a solution are:

- What effect does the underwater acoustic channel have on transmitted signals? Can equalization techniques reduce the Bit Error Rate (BER) below 10^{-3}?
- What channel equalization techniques can mitigate channel effects and operate within the constrained structure of our steganographic transmission system?
- Does the implementation of symbol recovery techniques and symbol rate improvements to minimize BER maintain the inherent covertness of the scheme in terms of relative distortion, Mean Square Error (MSE), and Peak Signal-to-Noise Ratio (PSNR)?
- Are brute-force methods likely capable of detecting our steganographic system?
- How well does our system perform—in terms of data rate, BER, and PSNR—at various depths, ranges, and acoustic environments?

1.3 Scope

The primary goals of the study are to understand the impediments to symbol recovery and present a technique that maximizes accurate reception under simulated underwater transmission conditions. Additionally, improved symbol rate is pursued. At the conclusion of our research, we make recommendations for subsequent research and relevant applications. In order to reduce complexity sufficiently to progress the state of the art, the following are assumed to be solved or negligible for the purposes of our work and are outside the scope of this thesis:

- Doppler effects in the transmission channel
- Particulars of and compatibility with specific hydrophone and array designs or parameters
- Channel equalization techniques
- Signal detection and receiver synchronization
- System performance in an actual at-sea environment
- Different symbol encoding schemes
- Different steganographic systems and the resistance of our chosen scheme to attack

1.4 Approach and Significant Findings

Our research first analyzes assertions regarding signal synchronization and recovery given by Passerieux in his presentations [2], [3] of this time domain steganographic scheme. Having disproved the assertions, we generate alternatives. We present three potential symbol recovery solutions for the Passerieux-based, frequency domain steganographic system given by Ferrao in his thesis [1]. Our recovery solutions have an additional benefit of increasing the symbol space without changing the modulation technique.

We first derive an analytical recovery method based on the receiver's knowledge of the structure of the received signal and a shared secret key. Secondly, we develop a numerical recovery solution by implementing numerical derivation and integration techniques that attempt to isolate a symbol value that is constant over some fixed number of samples. For our third recovery solution, we present a basic comparative recovery technique based on shared knowledge of the cover signal. While we implement these recovery schemes within the system given by Ferrao [1] that uses a 2048 Hz bandwidth centered around 2500 Hz, our steganographic technique is fundamentally agnostic to the particular bandwidth.

We model the effects of transmission on recovery using two underwater waveguides output by the Monterey-Miami Parabolic Equation (MMPE), then we simulate transmission through a deep water channel and a more adverse shallow channel. We show that our symbol encoding technique does not negatively affect the steganographic properties of our signal. We also show that statistical recovery solutions are unlikely to be successful for our steganographic scheme. We find that because the Discrete Fourier Transform (DFT) generates a point-wise approximation of a continuous Fourier transform, its derivative with respect to frequency is inherently discontinuous, and therefore, a numerical approximation of the indefinite integral of this derivative cannot exit. We successfully demonstrate that a recovery scheme based on locally constant variables can be highly performant in a variety of channels, given an assumption of accurate synchronization and equalization. The assumption of perfect synchronization and equalization results in the unexpected phenomenon of constant recovery performance with distance, so we also show how different assumptions impact performance. Anything other than near-perfect equalization of phase results in recovery performance effectively no better than random guessing.

1.5 Organization

The remainder of this thesis uses the following organization:

Chapter 2: Background

This section provides a survey of existing work related to wireless and acoustic communications. Wireless effects, and their specific application within the underwater acoustic channel are discussed. Existing statistical models of wireless communications are briefly presented to provided context to the existing work on data recovery methods. The bulk of this chapter consists of a discussion on existing data recovery methods.

Chapter 3: Methodology

First, mathematical refutations of assertions from previous works are presented. Then the specific data recovery techniques chosen for analysis are presented and formally described in this section. The theoretical bases, as well as any assumptions or constraints, are discussed. Broadly, this chapter outlines our research goals and the path to achieve them.

Chapter 4: Results and Analysis

The chapter introduces the simulation method along with specific modelling parameters. We present the data collected, describe and apply the models and methods of analysis, and explain the results. Challenges encountered are explained, accompanied by solutions and mitigating factors. Hypotheses for observed trends and anomalies are discussed, and we compare different recovery schemes.

Chapter 5: Conclusions and Future Work

This chapter revisits the research and major findings of the previous chapters. Limitations and remained unanswered questions are discussed. The limitations and gaps, as well as new questions discovered through the research, generate recommendations for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2: Background

The problem of signal detection and synchronization in both the underwater and radio frequency environments is well studied, though not all solutions are relevant to our study. In this chapter, we position our research within the problem domain of existing work. Section 2.1 provides an overview of our chosen steganographic system. Section 2.2 describes various sources and models of fading in the wireless communications channel, while Section 2.3 details the particular challenges and characteristics of the underwater acoustic communications channel. Finally, Section 2.4 surveys existing approaches to detection, synchronization and equalization.

2.1 Acoustic Steganography Communication System

In a recent NPS thesis [1], Ferrao implemented a software-based approach to Passerieux's steganographic method [2], [3] to covertly transmit data through the water via ostensibly natural sounds.

2.1.1 Passerieux's Steganographic Method

Passerieux's novel steganography technique [2], [3] leverages the expected presence of naturally occurring sounds to transmit inaudible and statistically imperceptible data without detection. The method is to add to an unremarkable original signal an auxiliary, low power signal, derived from the same original signal. The covert information is encoded in the phase and amplitude of the auxiliary signal. Through knowledge of the steganographic key and by application of a symmetric operation, a receiver can decode the transmitted data. Using a realistic channel model [4], Passerieux demonstrated the ability to reliably transmit low rate data between moving transponders over a few kilometers.

The method can be divided into two components, the transmitter and the receiver. At the transmitter, a variable-length cover signal is selected and divided into fixed duration intervals. These intervals are contiguous, but non-overlapping, and generally on the order of several tenths of a second. One symbol is encoded into each interval. To encode a symbol, a given interval is further divided into sub-intervals. Passerieux gives two subdivision schemes. In one method, the sub-intervals are divided in the same way as the main intervals—constant length and contiguous, but not overlapping. The second method divides the main interval into an even number of variable length sub-intervals. The sub-intervals are separated by guard periods and symmetrically paired about the halfway point of the interval. Two sub-intervals that are the same distance from the halfway of the main interval have the same length, and sub-intervals that are closer to halfway are longer than those that are farther.

The methods for generating an auxiliary signal are different, though analogous, between the two sub-division schemes. Though the first method has a stronger steganographic key, it breaks down when there is relative motion between the transmitter and receiver. Thus, the interested reader is referred to Passerieux's patent application [3] for a presentation of constant sub-intervals, and we proceed only with the second sub-division scheme here. Pairs of sub-intervals are swapped over the halfway point of the main interval, and then each sub-interval is time-reversed (flipped about its halfway point in the sub-interval). The permuted and time-reversed sub-intervals are each multiplied by a phase-term. The set of phase terms applied across the sub-intervals constitutes the steganographic key. To the edges of the sub-intervals is applied a smoothing function, which minimizes broadband transients at the transitions.

The signal, reconstructed from the guard periods and modified sub-intervals, constitutes the auxiliary signal for the interval. The interval auxiliary signal is multiplied by an amplitude factor and a phase factor. The amplitude factor should be a gain that reduces the amplitude of the auxiliary signal relative to the original signal so as to make it imperceptible. The data symbol is encoded by the combination of the amplitude and phase factors. The full auxiliary signal is thus the compilation of all interval auxiliary symbols. The auxiliary signal is added onto the original signal and the result is then transmitted.

The receiver processes a signal which is a combination of the original signal, the auxiliary signal, and channel effects—such as noise, Doppler spread, multipath, etc. However, if the gain on the auxiliary signal was sufficiently small and the acoustic channel was not excessively adverse, the received signal will approximate the original signal. The receiver then uses the approximate signal as the original signal and completes the same sequence of steps as the transmitter, applying the set of phase-terms on the sub-intervals as the steganographic key. Instead of encoding a symbol, however, the approximate interval auxiliary signal, without gain or phase factors, is used to determine the symbol encoded in the received signal. The cross-correlation between the received signal and the approximate auxiliary signal will have peaks separated by the interval duration when the approximate auxiliary signal is generated with the correct steganographic key. The peaks will be maximized when the approximate auxiliary signal is adjusted by a Doppler compensation term, which is determined iteratively. Between the peaks, the approximate auxiliary signal will have a phase and amplitude proportional to the transmitted symbol.

2.1.2 Masked Underwater Acoustic Communication

In his thesis, Masked Underwater Acoustic Communication [1], Ferrao implemented Passerieux's method in the frequency domain and, using a realistic and accurate model, experimentally determined parameters to optimize the design tradeoffs of the scheme. A frequency domain application of Passerieux's method provides for greater flexibility and reduced computational complexity, though it does modify somewhat the generation of the auxiliary signal and recovery of symbols. As before, the signal is divided into intervals, but then to each interval is applied the DFT, generating the frequency domain representation of the interval. In the frequency domain, the interval is easily partitioned into two components, X1 and X2, where X2 is the frequencies of interest and X1 is the remainder of the signal. Dividing the signal in this way eases recovery and allows optimal frequency selection for desired transmission characteristics.

The auxiliary signal is generated only from X2, which is sub-divided into guard bands and sub-intervals. In lieu of permutation and time-reversal, as in the time domain, frequency domain analogues are applied—complex conjugate and multiplication by a phase term. The steganographic key is then applied across the sub-intervals via multiplication by a complex exponential factor. As in the time domain, a gain and phase factor are applied to the interval to reduce its relative amplitude and encode a symbol. The intervals are added onto the original signal, the inverse transform is applied to the result, and the time domain signal is transmitted.

At the receiver, the signal is received in time domain and transformed to frequency domain via the DFT. Out-of-band frequencies are ignored, and from frequencies in the transmission range are symbols recovered. The auxiliary signal is generated from the received signal—mirroring the process applied to the original signal at the emitter—and then the complex conjugate is taken. The complex conjugate is multiplied by the received signal, and the real terms of the result are proportional to the transmitted signal.

Ferrao tested the frequency domain implementation of Passerieux's technique over two different simulated channels. Using the MMPE acoustic propagation model [5], a benign deep water channel and a challenging shallow water channel were generated. The deep channel consisted of a stationary source and receiver at a depth of 500m and maximum range of 1 km in a 2km deep channel. The shallow channel consisted of a stationary source and receiver at a depth of 60m and maximum range of 3km in a 200m deep channel. In the deep channel, multipath is minimized and spherical spreading dominates in transmission losses. Conversely, the shallow channel is characterized by multipath and cylindrical spreading. The range of detectable transmission was primarily dependent on Signal-to-Noise Ratio (SNR), but the simulations demonstrated adequate symbol recovery from successfully steganographic transmissions at ranges of 1000 meters or better and a bit rate of four bits per second (bps).

Ferrao identified several lines of inquiry for future work, but of particular note are the following:

- Evaluating the algorithm's performance with an even more realistic channel model by implementing spectrum-dependent noise and leveraging MMPE's options and parameters for increased accuracy.
- Developing a method for synchronizing the receiver and estimating data alignment.
- Developing a method to resist or compensate for Doppler effects.
- Improving data rate.

2.2 Fading

Solutions to the channel detection and synchronization problem are well-studied in the radio frequency (RF) environment and are generally classified by their applicability to different fading characteristics and channel models. These have varied relevance to the underwater acoustic channel, but a brief overview of fading and models is warranted to provide context to the state of the art in our area of research.

Sources

In general, all fading can be considered the complex interaction of five source phenomena: diffraction, scattering, reflection, multipath, and Doppler effects.

Diffraction

Diffraction describes the modifications to a wave's propagation path when obstructed by an object larger than the wavelength. The diffraction effect is commonly referenced in the literature as shadowing. Diffraction results in periodic areas of loss and availability given by Fresnel zones. Fresnel zones describe regions where the difference between the diffracted path and the line of sight (LOS) path is a multiple of a half wavelength. Fresnel zones describe diffraction-loss observed as a function of distance from an obstruction, since the signal intensity increases up to the first Fresnel zone, decreases until the second Fresnel zone, etc. [6].

Scattering

Scattering defines the interaction between a wave and a rough surface smaller than (or equal to) the wavelength. A wave is generally scattered in all directions upon interaction with such an object. Scattering results in received power that is less than what would be predicted by reflection and diffraction alone [6]. Additionally, scattering can result in increased noise at the transmitter, which can cause interference if the transmitter is a transducer [7].

Reflection

Reflection is the result of a wave interacting with a smooth surface that is large compared to the wavelength. In such an interaction, various portions of the wave's energy are reflected, absorbed, and transmitted. The proportion of these effects depends primarily on the permittivity, permeability, and conductance of the reflector, which are a function of the material. Inasmuch as the reflector is smooth, (i.e., given a large conductance) the majority of the signal is reflected such that the incidence angle and reflection angle are equal. Any imperfections in the surface result in some scattering of the signal, so that the reflected signal is more diffuse than the arriving signal, but in general, the reflected waves can be considered a single signal. The proportion of the signal that is absorbed is a function of permittivity, and the amount that transmits through the reflector is a function of the permeability. The amplitude of the reflected and transmitted signals is a function of the reflector's material properties and the wave's polarization, wavelength, and arrival angle [6].

While the precise types and locations of reflectors and scatters cannot be determined or anticipated, signals will certainly encounter both effects. Together, they result in variations in amplitude, phase, and time delay, which are random since the distribution and characteristics of the obstructions in the channel are random [6]. Of note, interaction with high conductance reflectors is the primary source of multipath signals.

Multipath

Multipath describes the phenomenon wherein multiple copies of the same signal arrive at the receiver by different propagation paths. Most commonly, the primary path will be the direct, straight-line path from emitter to receiver, and the additional paths will be longer and so the signals will arrive at the receiver after some time delay. The most common source of multipath is reflection (e.g., off the ground), though scattering and refraction (where stratified media have different propagation speeds, causing the signal to bend) can also contribute. Since each path is different, each arrival will not only have a different time delay, but different phase and amplitude fluctuation [6]. The interaction of these arriving signals can be either constructive or destructive. Multipath causes significant fading and Intersymbol Interference (ISI), where previously transmitted encodings corrupt the current signal [8].

Doppler Effects

Doppler effects are most commonly caused by relative motion between the transmitter and the receiver, though motion of the medium can also result in Doppler effects [9]. Divergent motion results in expansion of the signal and an apparent down-shift in carrier frequency. Closing motion causes the signal to compress and generates an apparent increase in carrier frequency. The greater the speed of the relative motion compared to propagation speed, the greater the Doppler effect, though each path in a multipath arrival will have a different Doppler shift, since the angle of arrival affects the Doppler shift [6]. The shift in frequency can cause intercarrier, or interchannel, interference in a frequency division system. Even in the absence of interference, Doppler shifts negatively affect carrier demodulation and data decoding.

2.2.1 Models

In general, there are two types of channel models—large scale and small scale. Large scale models describe general signal characteristics within a wide area, and are typically a function of distance between emitter and receiver. Small scale models are generally more complicated, and attempt to describe the signal variations arising from minor environmental fluctuations or changes in position as small as half a wavelength [6].

Large-Scale Models

There are two foundational large-scale models, the Free-Space model and the Lognormal Path Loss model. The Free-Space propagation model describes unimpeded LOS transmissions as a frequency-selective function of transmitted power, antenna gains, wavelength, and distance, where the only losses are due to spherical spreading. The Lognormal Path Loss propagation model describes transmission losses independent of transmitter power, antenna gains, or the presence of a direct transmission path. The lognormal path loss is a function of the distance between the transmitter and receiver divided by a reference distance and raised by a path loss exponent. Reference distances and the path loss exponents have been experimentally determined for a number of different media and environments [6].

In addition, there are models that designed around specific large-scale phenomena. The 2-Ray Ground Reflection model describes RF communications with exactly two paths: the direct path and a single round reflection. The 2-Ray Ground Reflection model is valid when the distance between the transmitter and receiver is much greater than the square root of the product of their heights. The Knife-Edge Diffraction Model describes losses in the shadow of a single building, hill, or similar obstruction by modelling it as a single knife edge with infinite width. Various versions of the Multiple Knife Edge model also exist. Finally, the Bistatic Radar Equation models losses due to a single large scatterer via the object's Radar Cross Section, which is effectively the reflected signal strength relative to the signal that would be reflected off of a perfect sphere with a volume of about 0.75 m^3. The Bistatic

Radar Equation is valid when the scattering object is between, and sufficiently far from, both the transmitter and receiver [6].

Many models have been designed to described transmissions in common outdoor environments, but particularly common ones include the Longley-Rice model, the Okumara model, the Walfisch-Bertoni model, and the wideband model. The Longley-Rice model describes point-to-point transmissions in the 40 MHz to 100 GHz range over various terrains, and has been extended to include attenuation factors for urban environments. The Okumara model is a set of experimentally determined frequency and distance vs. attenuation curves along with frequency-dependent correction factor curves, and is among the most popular urban models. The Okumara model is valid from 150 MHz to 2 GHz and out to about 100 km. The Walfisch-Bertoni model is based on the Free-Space Path Loss model, but includes loss factors for diffraction and scattering due to buildings and considers the effects of multiple rows of buildings. The wideband model operates based on the determination that the 2-Ray Ground Reflection model is sufficient for LOS transmissions and the Lognormal Path-Loss propagation model holds for obstructed environments [6].

Small-Scale Models

In small-scale models, channels are typically either flat or frequency selective and slow or fast. In a flat-fading channel, all multipath propagations arrive during the period of a single symbol, so there is no intersymbol interference, and transmission characteristics are preserved. Conversely, frequency-selective channels are characterized by intersymbol interference and the channel effects are frequency-dependent. Flat versus frequency selective channels are dictated primarily by the position in the channel of the transmitter and receiver, and the static or slowly varying channel characteristics. Slow versus fast fading channels are determined by the dynamic properties of the transmitter, receiver, and channel itself. Movement of the channel, emitter, and receiver generate Doppler spread. When the Doppler spread is smaller than the channel bandwidth, channel characteristics are approximately constant over several symbol periods, and the channel is considered to be slowly fading. Conversely, the channel is considered fast when the symbol period is longer than the amount of time the channel stays approximately constant [6]. Fast fading induces a lower-bound error rate, increases the error rate overall, and degrades coherent detection schemes [10]. A frequency-selective, fast channel (which usually describes the underwater environment) is the most adverse, wherein each multipath component arrives at different times and with different phase and amplitude [6].

The Rayleigh and Rician models are the most commonly used models for small-scale fading. The Rayleigh model most accurately describes flat multipath channels that do not include a direct path. In this case, the strength of the received signals follows a Rayleigh distribution. The Probability Density Function (PDF) of a Rayleigh distribution is $\frac{x}{\sigma^2}e^{\frac{-x^2}{2\sigma^2}}$, where x is the signal strength and σ^2 is the signal variance. When the channel is flat, but there is a direct path, then it is modeled by the Rician distribution. The direct path is modeled as a continuous transmission onto which is added random fluctuations that are primarily caused by multipath. The Rician distribution is a generalization of the Rayleigh model: when the direct path component is set to zero, the Rician distribution reduces to Rayleigh [6]. Another common small-scale model, the Nakagami model or m-distribution, is a further generalization of the Rician distribution. When the m parameter is one, the Nakagami model reduces to the Rayleigh model, and when m is between one and two, the Nakagami distribution matches the Rician. Lower m values (e.g., $0.5 \leq m \leq 1$) describe higher-frequency, highly-fading channels, and as m goes to infinity, fading tends to zero [11].

Equalization and synchronization solutions are often designed given the assumption of a particular small scale fading model. The review of common models is valuable in order to contextualize the background research.

2.3 Underwater Acoustic Communication

While there is applicability, RF fading models tend to break down when applied to the underwater environment. Since our study is specific to the underwater environment, it is important to discuss the differences between terrestrial RF and underwater acoustic channels (UACs), as well as the specific challenges that make the underwater acoustic environment unique.

2.3.1 Differences between RF and UACs

Acoustic communications and RF systems share similarities, but transmission power limitations, low transmission rate, large propagation losses, and time delays create additional difficulties in UACs [12]. Compared to RF, underwater acoustic communications are forced into a narrow bandwidth and are subjected to significant latency and very complex multipath propagation, resulting in large error rates [13]. Two factors contribute primarily to the differences between RF channels and UACs: propagation speed and variability of the medium.

The ocean fluctuates more rapidly than the atmosphere, and this effect is amplified by the comparatively slow symbol rate in underwater communications [14]. Channel characteristics vary over the long term due to macro-oceanographic effects and seasonal changes. Small scale changes in the short term result of minor perturbations in the environment, causing phase and amplitude variations within a single symbol and adjusting the statistics of received signals. Short-term variations in the wave guide adjust the sound speed profile, which results in multipath propagation and non-constant levels of coherence between receptions in the same location. Additionally, relative velocities of the emitter and receiver caused by surge, sway, yaw, roll, and changes in depth cause path variations that can potentially have effects within a symbol signal [15].

Electromagnetic waves travel at the speed of light, which is five orders of magnitude faster than the speed of sound [16]. Additionally, acoustic wave propagation speed is variable—dependent on temperature, salinity, and pressure—which can change drastically over short distances in the underwater environment [13]. Comparatively, the speed of light is effectively constant [17]. As a result, Doppler effects are more significant in the underwater channel than for RF communications [18], since the propagation speed is closer to the velocities of the transmitter, receiver, waves, and currents. In RF channels, Doppler shifts cause rotation in the received phase and a carrier frequency shift, but in UACs, symbol duration expansion or compression (depending on the direction of the relative motion) occurs as well [18], [19]. Just as the speed of sound amplifies Doppler effects, multipath is also more severe. The relatively slow propagation speed increases the multipath due to the transmission geometry and also increases the severity of the effect by lengthening reverberation times [14]. As a result, multipath can affect tens to hundreds of symbols in UACs, while in RF channels, interference usually extends to less than five symbols [20]. Finally, there is often less correlation between separate receivers receiving the same signal in the underwater environment compared to RF communications [21].

2.3.2 Underwater Acoustic Channel Effects

Frequency selectivity, varying multipath, latency, and severe Doppler shift rank UACs among the most adverse communications media [22]. While underwater acoustic communications are affected by the carrier frequency, varying sound speed profile, sea state, ocean depth and bottom, and configuration and dynamics of the communication elements [23], the primary detractors for underwater acoustic communications are transmission loss, noise, multipath, and Doppler shift [22].

Transmission Loss

Transmission loss has two primary culprits: signal attenuation and spreading. Attenuation is mainly caused by the absorption of acoustical energy by seawater and the conversion of that energy into heat [21]. These losses are strongly positively correlated with both frequency and range [24]. Spreading is the dispersion of acoustical energy as the wavefront expands, which increases with distance [21]. Commonly, a direct path assumption is made, and spreading is modeled as spherical, so losses are proportional to path length squared. Carrier frequency determinations and available bandwidth are strongly influenced by transmission losses [24].

Noise

Noise inhibits signal reception, and high-intensity, short-duration impulsive noises can entirely mask incoming signals [25]. Noises arise from both natural and man-made environmental sources and from the platform on which the receiver is mounted. This latter phenomenon is termed self-noise. Environmental noise is dependent on frequency and location, since noise emitters are generally narrowband, and near-shore, shallow environments are more congested and noisier [24]. Man-made noise thus dominates in littoral regions, while in a deep environment, natural noises dominate [22]. Man-made noise sources include machinery, (such as pumps, gears, and engines) ship traffic, (such as propeller cavitation and hull noises) and industrial work (such as pile driving, grinding, and explosions) [21], [26]. Natural noise sources include wind and sea state, bubbles (though these can have non-natural sources as well), precipitation and sea spray, seismic events, and biological emitters [26].

Self-noise is generated by the platform on which the receiver is mounted (e.g., by the propeller or on-board machinery), and is transmitted to the receiver through the water or through the platform's structure. Additionally, self-noise can be generated by the turbulence that results from the motion of the platform or receiver relative to the water. While all turbulence, including that resulting from currents, causes noise, that noise is generally low compared to ambient noise. However, the pressure changes caused by turbulence are significantly greater than the radiated acoustical energy, so a pressure-sensitive hydrophone may be affected by self-noise due to turbulence, even if there is little radiated noise [26]. Self-noise positively correlates with speed, so at sufficiently slow speeds, ambient noise becomes the limiting factor [7].

Noise is often assumed to be white and Gaussian, but the frequency and position dependence of noise, as well as the prevalence of multipath in the underwater acoustic environment, undermines the validity of this assumption [11].

Multipath

The two main fundamental causes of multipath are reflection and refraction. Which multipath method is dominant depends on water depth, transmission frequency, and communication range, though the shallow-versus-deep distinction (generally delimited by about 100 meters of depth or the termination of the continental shelf) is the main determiner of the principle multipath mechanism [22]. In shallow water, reflections are the primary source of multipath, while refraction is the dominant mechanism in deep water [24]. In the shallow water case, an increase in transmitter gain does not necessarily improve reception, and indeed, may have a deleterious effect [27]. In both cases, the causal reflectors and/or refractors are dynamic, so each multipath component is time-variant, resulting in severe, highly spatially dependent, and rapidly fluctuating fading [15].

In general, channel geometry and knowledge of the communication environment allows for prior calculation of, and compensation for, deterministic macro-multipaths [22]. Additionally, there are random micro-multipaths, which cause increased time-spreading variability. In some cases, the micro-multipath effects can be modeled statistically [20]. Oceanic multipath results in severe, varying, and spatially-dependent intersymbol interference, phase distortion, and time-spreading of the received signal, with this latter effect also being called reverberation in the literature. The spatial dependence of ocean channel effects further complicate transmission reception in mobile systems [24].

Doppler Effects

Doppler shift describes the apparent change in carrier frequency caused by relative motion between the transmitter and receiver or of the propagation medium. This effect is deterministic if the relative motion and sound speed are known a priori. However, this information is not generally precisely known, and compensation is even more difficult when the relative velocities are non-constant [28].

The multiple multipath previously described also has an effect on the signal, causing Doppler spread. First, different incidence angles at the receiver due to each multipath component result in differing relative velocities. Additionally, the various Sound Speed Profiles (SSPs) along the different paths adjust the speed of each path [22]. Finally, motion of the reflectors and scatterers causing the multipath will induce their own Doppler variability. The result is differential Doppler and time-scaling [9].

Multipath-induced Doppler is independent of the relative motion of the transmitter/emitter [29]. However, Doppler spread is dependent on frequency—as frequency increases, so does Doppler spread. Conversely, multipath spread increases with range, which is usually related to frequency such that higher frequency implies shorter range. Overall, the combined effect of multipath and Doppler generally decreases in severity as range increases [22]. UACs are considered doubly spread because of this combined time-spread and Doppler spread that occur.

2.4 Data Recovery

There are three main components of existing approaches to resolve data transmitted in the presence of the adverse effects previously described: detection, synchronization, and equalization. In general, successful accomplishment of one component is a prerequisite for the next. Broadly, equalization aims to determine and cancel out the channel's effects on the signal, detection is the process of differentiating transmissions from background noise, and synchronization seeks methods that align receivers to variable signals. Supporting these schemes are compensation techniques, such as interference cancellation, Doppler compensation, phase tracking, beamforming, spatial diversity, and coding.

2.4.1 Detection

Signal arrival detection is a critical first step for communication systems. Detection provides coarse synchronization and prevents wasted computation on signal-less acoustic energy. Furthermore, improved detection algorithms reduce the necessary SNR for communication, which improves system range and/or follow-on algorithm performance [30]. This step is yet more important in UACs, since the hostile doubly spread channel increases the difficulty of detection, equalization, synchronization, and data recovery [31]. The goal of detection methodologies is to maximize accurate detection and minimize false alarms, but in general, these two outcomes are not jointly optimizable [32]. Common detection methods are envelope detection, matched filtering, binary hypothesis testing, and change detection.

A simple digital transmitter designed by Woodward and Sari [33] band-filters received energy to narrow the detection range to the desired frequencies, and then applies an envelope detector to determine signals of sufficient acoustic energy. Locke and White [34] apply a matched filter via a fractional Fourier transform to detect linear frequency modulated narrow-band signals. In [30], Austin expands the matched filter technique to coded wideband signals with good autocorrelation and low cross-correlation properties such as Welch-Costas and Gold codes. In [35], Ling et al. also review waveforms that have the desired auto- and cross-correlation characteristics, commonly called Zero-Correlation Zone (ZCZ) sequences, such as Frank sequences, for covert applications. Many of these ZCZ sequences have a fixed length, making them brute-force detectable, so the authors recommend flexible waveforms synthesized by the Weighted CAN (WeCAN) or Periodic-correlation CAN (PeCAN) algorithms. Aparicio and Shimura [31] apply the matched filter technique to multiuser (Direct Sequence Code Division Multiple Access (CDMA) [CDMA]) system through the use of a sliding window and a preamble consisting of a common Zadoff-Chu sequence and user-specific complementary set of sequences. Loham [32] and Howland [36] discuss detection methods for Orthogonal Frequency-Division Multiplexing (OFDM) packets, which include a short-long preamble structure. Detection is achieved only on the short preamble using hypothesis testing on the correlation properties of multiple samples, the threshold for which is determined based on a likelihood ratio test (for estimable probabilities) or the Neyman-Pearson test (for a given false alarm probability constraint). Goh et al. [37] present the use of both a second-order matched filter and a third-order correlation zero-lag matched filter, each with hypothesis testing on different thresholds, to detect deterministic signals.

To avoid the need for a known preamble, Yang et al. [38] discuss a detector for deterministic or non-Gaussian signals in the presence of noise with a symmetrical probability density function by detecting asymmetry in the higher-order statistics. Other change detection techniques keep track of the ambient noise. Hoppe and Roan [39] introduce signal detection in a multi-sensor system using principal component analysis of the covariance between two channels. A single receiver hybrid detection technique is described by Lopatka et al. [40] that starts with a learning period and then applies an adaptive threshold against which four detector techniques are applied: impulse detection, speech detection, variance detection, and histogram detection. The impulse detector is a short-duration envelop detector; the speech detector operates on the peak-valley difference of the signal, the variance detector tracks the time-varying signal components in narrow-band signals, and the histogram detector makes decisions for wideband signals based on the distance metric compared to a background noise model.

2.4.2 Synchronization

Synchronization is a broad term that may refer to the signal frame, carrier frequency, reference phase, or transmitted symbol [32]. Phase synchronization is also known as phase tracking, which will be covered later. Symbol synchronization, or data detection, is central to the discussion on equalizers. Frame and frequency synchronization are critical steps that enable successful data decoding, but variable and large propagation delays and Doppler effects in the underwater environment significantly increase the difficulty [41]. This difficulty is compounded by the multipath characteristics that obscure a principle signal arrival, undermining synchronization and, by extension, equalization [14]. Proper frame synchronization enables accurate sampling of the waveform to determine data symbols. Without a sufficient approximation of the start of the symbol period, the signal cannot be properly demodulated. Improper synchronization results in failed receptions and/or more severe ISI [36].

The simple system designed by Woodward and Sari [33] uses a full-frame synchronization code to align the transmitter and receiver clocks. Catipovic and Freitag [25] expand this concept by setting an extended Delay-Locked Loop (DLL) to a known synchronization waveform that is transmitted at a fixed interval and interpolating frame timing therefrom. Alternatively, Aliesawi et al. [42] perform frame synchronization by using a chirp signal at the start of each packet, as do Yurdakul and Senturk [43], though they recommend a chirp in the same band but with lower-power than the data signal. In [22], Stojanovic advocates the use of a short Barker sequence as a channel probe for frame synchronization. Loham [32] and Howland [36] discuss cross-correlation and autocorrelation methods that use the IEEE standard OFDM preambles for coarse frequency and timing synchronization along with a pilot tone to prevent drift. Kung and Parhi [44] achieve joint timing synchronization and equalization for OFDM using a Pseudo-Noise (PN) sequence as a preamble and maximum-likelihood optimization in a sliding window. Yachil et al. [45] introduce an improved synchronization system for Time Division Multiple Access (TDMA)/Frequency Division Multiple Access (FDMA) RF communications using a preamble to jointly synchronize timing and frequency. Similarly, Grotz et al. [46] use a preamble to jointly synchronize frequency, time, and phase based on a maximum-likelihood optimization for a multi-frequency TDMA system.

The receiver designed by Brady and Catipovic [47] achieves coarse synchronization by maximum peak detection for the correlation of the reception and known packet headers. Phase tracking and fine synchronization is subsequently achieved by the equalization and interference cancellation algorithm. Similarly, in [48], Stojanovic et al. introduce an adaptive, fractionally-spaced Decision-Feedback Equalizer (DFE) with second-order digital Phase-Locked Loop (PLL) and DLL that jointly optimizes synchronization and equalization. Coarse frame synchronization is achieved by means of a pre-defined channel probe. Ali et al. [49] propose three frame synchronization algorithms. An optimal trellis-based maximum a posteriori probability (MAP) algorithm operates on the full signal, while a faster, lower-complexity windowing version is also provided. Additionally, a finite automaton combining header recovery and hypothesis testing is presented to achieve frame synchronization sample-by-sample.

2.4.3 Equalization

Equalization mitigates the channel's influence on the signal, including amplitude fluctuations, phase and frequency shifts, intersymbol interference, and time delay. Equalization techniques commonly use some combination of preambles, pilot tones, coding, and statistical analysis. Without equalization or compensation, most signaling schemes will not work [14]. Equalizers generally fit into six categories: linear, decision feedback, adaptive, blind, turbo, and probabilistic-detection [17].

Linear

A linear equalizer is a filter matched to a specific finite impulse response. Typically, linear equalizers only work in benign channels, since they tend to amplify noise signals [50]. Since the ocean channel varies rapidly, linear equalizers are typically insufficient in this environment. However, they are frequently used as the basis for adaptive algorithms, which update the finite impulse response parameters as the channel changes.

Decision-Feedback

A DFE is an extension of the linear equalizer operating on the principle assumption that the effects of a previously determined symbol can be estimated, detected, and compensated for in future symbols. A DFE is effectively a two-step process. In the first section, a linear feed-forward filter cancels channel effects. In the second section, a feedback filter uses previous symbol decisions to compensate current ISI [15]. In practical applications, pure DFEs are not sufficient to achieve necessary performance requirements, but they are commonly used in adaptive equalizers [23].

DFEs tend to succumb to error propagation, wherein an estimate error propagates and compounds on successive iterations. To combat this, Brady and Catipovic [47] developed a soft-decision-based DFE for a specific multiuser acoustic local area network in which a central receiver is able to track the round-trip transmission durations (which are expected to verily slowly) for all transmitters in the system. In this system, user determination and course synchronization are achieved via user-specific headers, which are followed by a training sequence to initialize the estimated channel parameters. The algorithm uses a soft-decision DFE on the received signal before using soft-decision interference suppression to determine the number of interfering users, and the amplitude, Doppler, delay, and phase of each user. This algorithm has the added benefit of overcoming the near-far problem—valid signals that are masked by nearer or louder transmitters.

Adaptive

Adaptive equalizers are so called because the channel compensation parameters are iteratively updated as the signal is processed. Unlike DFEs, which update the equalizer output based on previous decisions, an adaptive equalizer updates the equalizer itself. Adaptive equalizers are commonly based on gradient (i.e., Least Mean Squares (LMS) [LMS]) or

Kalman (i.e., Recursive Least Squares (RLS) [RLS]) methods. LMS systems are generally simpler and lower complexity than RLS equalizers, though RLS converges faster at the expense of computational and memory costs [51]. Both RLS and LMS algorithms seek to minimize the MSE, but different powers of the difference between the transmitted and received signal can be used as the cost function (e.g., Least Mean Fourth) [52]. Adaptive algorithms usually include known training sequences to learn the communication channel.

Kari et al. [52], developed an adaptive linear equalizer designed to handle the impulsive noises common in shallow environments by minimizing a cost function based on the MSE with an added, regularizing logarithmic term. Youcef et al. [53] and Wang et. al [41] implemented adaptive equalization for OFDM systems in the frequency domain, which is useful when the time-spreading is large compared to symbol duration. In [54], Nott implemented an adaptive DFE with forward error correction for communications with long-loiter ocean surveillance gliders. In [48], Stojanovic et al. showed that equalizer performance is improved when jointly estimated with synchronization parameters, and that spacing equalizer taps narrower than symbol-aligned removes symbol timing estimation requirements. Aliesawi et al. [42] found adaptive chip (vice symbol) DFEs (jointly optimized with phase recovery and coupled with an interference cancellation scheme) to be superior to a similarly modified Rake receiver for Interleave Division Multiple Access (IDMA) multi-user underwater acoustic communication systems. Calvo and Stojanovic [55] designed an adaptive algorithm for multiuser data detection in a CDMA system. Their algorithm is based on Cyclic Coordinate Descent (CCD), wherein symbol estimates, channel parameters, and carrier phase are adapted in turn (while holding the others constant) using the minimum MSE criterion. Song and Badiey [56] implemented a time-reversal DFE, adapted using the matching pursuit algorithm for sparse channels in a multiband system.

Blind

As previously mentioned, adaptive algorithms typically utilize a training sequence of known symbols to achieve initial equalization. In the underwater environment, which is rapidly changing, slow, and bandwidth constraining, training symbols are an inefficient (and potentially infeasible) use of limited resources. Blind algorithms remedy this by performing equalization without training information or prior knowledge of transmitted data or channel characteristics for any user [57]; however, this utilization improvement comes at a cost of slower convergence and reduced robustness to phase rotation [51]. Instead of finding a best-fit solution for comparing a received training sequence to an expected sequence, blind equalization techniques minimize the difference in statistics between equalized received symbols and source sequences [58]. Blind techniques are sometimes used to initialize the channel parameters for decision-directed systems, like DFEs [57]. In general, there are four classifications of blind algorithms: Bussgang, polyspectra-based, cyclostationary, and probabilistic [59]. Blind algorithms of the probabilistic variety combine channel estimation schemes with probabilistic-detection symbol recovery, and as such, they will be discussed under that section.

An RLS-based blind equalizer for Direct-Sequence Spread-Spectrum (DSS) systems was designed by Tseng et al. [60]. This algorithm operates on the orthogonal transform of the received signal (which serves to reduce computational complexity) and minimizes the squared error between the equalized signal and an estimated desired signal. This estimated desired signal assumes clusters with a known variance around constellation points. In [28], Yang et al. preprocess demodulated signals to extend the RLS-based blind equalizer to handle ISI, Multiple Access Interference (MAI), and Doppler effects in a differentially modulated, variably mobile, asynchronous underwater multiuser communications system. In differential modulation, symbols are encoded by change in phase, rather than relative to a reference phase.

A common Bussgang-type equalizer is the Constant Modulus Algorithm (CMA), which minimizes deviations in the modulus, or magnitude, of an equalized signal relative to a fixed reference. CMA is phase-blind, so a Modified CMA (MCMA) has been developed to handle phase-sensitive communication schemes [51]. Rao et al. [58] further modified the MCMA to improve convergence rate and steady-state MSE through an updated cost function that is the sum of the cost functions for the real and imaginary parts of the equalizer output with a coordinate transformation applied to change non-modulus signals into modulus signals. Super-Exponential Iteration (SEI) algorithms are similar to CMA/MCMA, but include the inverse matrix of the signal autocorrelation to whiten the input, increasing convergence rate without sacrificing error rate. In [51], Zhong and Xiao-ling propose a SEI decision feedback blind equalization algorithm which includes a second-order digital PLL to account for phase rotation.

Turbo

Turbo equalizers leverage turbo codes, or other near Shannon-limit codes, to extract extrinsic channel information not explicitly encoded in the transmitted data. By iterating between an equalizer and decoder, equalizer outputs improve soft decoding decisions, which in turn improve channel estimates. Aliesawi et al. [19] use a turbo equalizer in IDMA and CDMA systems to achieve MAI cancellation by iterating between a DFE and a Gaussian Approximation-based interference cancellation decoder for the IDMA/CDMA spreading codes. Liu and Song [23] use irregular low density parity check codes and iterate between an adaptive DFE and a belief propagation decoder. Tong et al. [61] compare Superposition Coded Modulation (SCM) and Bit-Interleaved Code Modulation (BICM) in turbo equalizer structures with a focus on OFDM systems, which can incur harmful Peak-to-Average Power Ratios (PAPRs). They develop a Gaussian Approximation-based soft compensation method to overcome the effects of clipping (to reduce PAPR) with minimal BER increase in SCM systems, and show that SCM achieves reduced computational complexity for approximately commensurate performance compared to BICM.

Probabilistic-Detection

Probabilistic-detection algorithms are of two varieties, Viterbi and MAP. Viterbi equalizers use the Maximum-Likelihood Sequence Estimation (MLSE) criterion to generate an optimal data solution by minimizing the error probability for a symbol sequence. MAP equalizers use the maximum a posteriori (MAP) criterion to optimal detect a symbol by minimizing the BER. Both algorithms require some knowledge of the channel in order to generate the statistics through which symbol decisions are made, so these algorithms are often paired with a channel-estimation algorithm such as those already discussed. Probabilistic-detection algorithms rely on accurate knowledge of the statistical distribution of the noise in the channel, which is often assumed to be additive white Gaussian noise. Since the wrong noise assumption deteriorates performance, and since the computational cost of these algorithms can be excessive (exponential with the number of channel taps), probabilistic-detection equalizers, while optimal, may not always be practical [50].

Feder and Catipovic [14] suggest an iterative maximum-likelihood algorithm for blind joint channel estimation and data recovery on data blocks, where the block size is determined by expected channel stability duration. The algorithm iterates between channel response estimation assuming known data using the Expectation-Maximization algorithm and data recovery assuming known channel parameters using a Viterbi algorithm. Antón-Haro et al. [57], [59], compare two different adaptive probabilistic-detection algorithms (Multiuser Adaptive Baum & Welch (MABW) and Multiuser Adaptive Viterbi (MAV)) coupled with coherence checking for blind joint detection of near-far users in a Direct-Sequence CDMA acoustic communication system. MABW is a MAP algorithm based on Hidden Markov Models (HMMs), while MAV is a Viterbi-based MLSE algorithm. Both algorithms demonstrate similar steady-state performance and robustness in practice, but MABW is slightly more computationally complex with a longer convergence time, and MAV has larger memory requirements and a lower performance guarantee.

2.4.4 Compensation

Compensation techniques support equalization by accounting for specific channel effects, such as multi-user interference, phase rotation, Doppler shift, and spatially dependent fading. Additionally, coding can compensate the residual error after data recovery algorithms are applied.

Interference Cancellation

Interference cancellation algorithms suppress known sources of interference, such as those caused by additional system users or known noise sources. Rather than treating additional users as part of the channel noise, interference suppression techniques leverage the determinism of interference signals to account for them specifically. The simplest methods operate on a bank of matched filters, but optimal performance with near-far resistance can be achieved by a maximum-likelihood detector (at an exponential complexity cost). Parallel Interference Cancellation (PIC) and Successive Interference Cancellation (SIC) achieve the same levels of success, but the processing delay in SIC increases with the number of users, so PIC is often preferred in practical applications [55].

In [22], Stojanovic reports on the ability of an adaptive multichannel receiver to perform both noise and MAI cancellation, while Brady and Catipovic [47] developed a joint equalization and interference suppression algorithm for a single centralized master receiver that initializes the equalizer with a soft interference estimate based on a bank of matched filters for known users. Wang et al. [41] describe an asynchronous multiuser OFDM system that pre-processes overlapped segments of the received signal by consolidating and parameterizing all interference within each segment. Then, interference cancellation is applied on the overlapped segments and iterated with equalization. Antón-Haro et al. [59] perform joint equalization and multiuser interference suppression, improving the results of both, by iterating between an adaptive equalizer and adaptive maximum-likelihood multiuser detection algorithm.

Doppler Compensation

Most Doppler compensation involves first estimating the Doppler effects and then compensating by resampling to account for frequency shift and symbol dilation. At the cost of computation, sampling more frequently than the symbol rate (i.e., at the chip rate) can help mitigate the effects of symbol compression and delay spread [22]. Common Doppler estimation methods are interpolation, where shift is estimated between two known receptions of fixed delay, and correlation, where many different shift values are attempted and the best result is selected.

In [18], Burdinskiy et al. improve on the computational complexity of using a bank of correlators by limiting the number of correlation channels and the number of phase shifts calculated, which comes at a slight cost of noise immunity. In another approach to reduce computational load, Saraswathi and Ravishankar [62] introduce a Doppler compensation algorithm in the frequency domain for OFDM systems that seeks a sufficient normalized correlation of two sliding windows. Sharif et al. [63] combine Doppler-tracking, beamforming, and equalization to simultaneously compensate for multipath and Doppler effects. Either a block open-loop Doppler estimator or an adaptive closed-loop Doppler compensator can be used. The block open-loop estimator compensates for Doppler shift by sampling based on interpolating between a preamble and postamble chirp signal. The adaptive closed-loop compensator estimates the Doppler shift with a decision-directed maximum-likelihood algorithm, with the benefit of not requiring a fixed frame length or frame-duration delay. Similar to the block open-loop method of [63], Aparicio and Shimura [31] achieve Doppler compensation by adding a postamble of a Zadoff-Chu sequence and then resampling based on interpolation between the two correlation peaks. Dhanoa and Ormondroyd [9] leverage SIC to achieve joint Doppler and delay compensation using both a preamble and frame-duration pilot tone. Each reception of the pilot tone indicates a multipath arrival and associated Doppler shift. Using the strongest path and compensating for the frequency shift, correlation is performed on the preamble and maximized to determine the time delay. Successively, the strongest path is removed and the process is repeated. Unlike all other referenced implementations, which require known transmissions, Eynard and Laot [29] demonstrate blind compensation of the Doppler effects on carrier frequency and timing in a multichannel system by leveraging proportionality of the frequency and symbol period.

Phase Tracking

Equalization algorithms can achieve some measure of phase compensation, but it is usually insufficient for adverse UACs, especially given the coherently modulated schemes necessary to maximize efficiency [48]. Thus, additional phase tracking is necessary, with a Digital PLL (DPLL) being the predominate method in the literature. A first-order DPLL has a proportional component only, while a second-order DPLL adds an integral coefficient; both are seen in proposed and applied systems.

Stojanovic et al. [48] propose joint optimization using minimum MSE of a fractionally-spaced adaptive DFE and second-order DPLL, which is experimentally confirmed as the most effective method by Zhong and Xiao-ling in [51]. To circumvent preambles, Antón-Haro et al. [59] present a blind equalizer combined with a blind second-order DPLL, whose update equation is based on the imaginary part of the blind equalizer.

Beamforming

Beamforming leverages steerable receiver arrays to clarify multipath by focusing receptions in certain directions and ignoring unwanted receptions. Spatial diversity can have the same effect, but requires sufficient distance between multiple receivers. Beamforming breaks down as the transmission range increases and can ignore valid signals in multiuser systems [24], and since propagation paths change over time, beamformers must be adaptive.

Howe et al. [8] describe an adaptive beamformer that seeks minimum MSE between a reference PN signal and the beamformer output. This method requires periodic retraining and a preamble that is half the frame. Mutual Coupling (MC) between elements in an array tends to distort beamforming, so Huang and Balanis [64] investigate the extent of the effects of MC on the minimum MSE-based adaptive beamformer. They found that while MC does not affect the lower bound on MSE in the channel dominated by environmental noise, MC compensation also does not improve the minimum MSE in the receiver noise dominated case.

Spatial Diversity

Spatial diversity, or multi-channel, requires increased computational complexity and receivers that are sufficiently far apart to be uncorrelated, but in return, they can significantly decrease error rates by compensating for spatially-dependent fading, clarifying multipath without range restrictions, and reinforcing decision results without an increase in bandwidth or signal energy [65]. An optimal receiver system would combine and jointly optimize beamforming, spatial diversity, and equalization [66]. The key to leveraging spatial diversity is the mechanism of diversity combining, for which there are three primary methods: unweighted summing, maximum output, and reliability weighting. This third method is the most robust, but it is the most difficult to implement, since it requires a metric for the reliability of each channel [65]. Further, the complexity of the reliability weighted combiner increases with number of receivers, but the complexity can be reduced (with no appreciable loss of performance) by selecting only the most significant receptions.

In [66], Stojanovic et al. design a jointly optimized receiver system and show that the combination of beamforming and diversity combining achieves equivalent performance at lower cost compared to pure diversity combining. Catipovic and Freitag [25] reduce the necessary receiver separation by using optimal maximum-likelihood diversity combining. Wibisono and Sasase [67] reduce receiver spacing even more, designing a trellis coded diversity system using weighted sum combining that operates successfully even when the receivers are correlated. Goldfeld and Wulich [68] improve on the optimal diversity reception system (e.g., [66] and [25]) by including erasures-correction by means of a block code and purposefully erasing unreliable bits in each channel. Focusing on highly reverberant shallow channels, Bessios and Caimi [27] developed a jointly optimized CMA-based blind equalizer that incorporates a summed spatial diversity combiner.

In [17], Aydogmus implements an adaptive RLS filter with two-channel diversity such that one channel is used to determine symbols and the other is used to confirm. The CCD multiuser detection strategy employed by Calvo and Stojanovic in [55] can be extended to the multichannel environment for only a linear increase in complexity on the number of receivers. The CCD method is applied to each receiver individually, the outputs of which are optimally combined before symbol decision are made.

Channel Coding

Coding in UACs has several purposes, primarily error correction and user detection. In general, channel codes reduce the number of bits that can be transmitted in a given time, but improve overall performance by increasing the chance that transmitted symbols will be correctly interpreted. For example, Hamming codes and convolutional codes allow error correction, while PN codes in CDMA systems allow multiple users to operate on the same frequency band [16].

Catipovic and Baggeroer [69] demonstrate the use of sequential decoding on long constraint convolutional codes to improve error rate over Rayleigh fading channels, while in [68], Goldfeld and Wulich showed that an erasures-correction block code outperforms forward error correction via cyclic Bose, Chaudhuri, and Hocquenghem (BCH) code in a multichannel system. Müller and Rohling [70] combine a convolutional code and Reed-Solomon (RS) code to achieve Doppler-robust error correction encoding. The convolutional code uses soft-decision decoding (by the Viterbi algorithm, for example) to correct individual bit errors, while the RS accounts for burst errors. In [23], however, Liu and Song optimize irregular Low-Density Parity-Check (LDPC) codes for specific channels and show that LDPC codes can outperform Turbo codes, both of which provided better data recovery than convolution codes and RS codes in underwater channels, at the cost of a high complexity turbo-type equalizer. In general, code performance is proportional to diversity order. Hansson and Aulin [71] improve the diversity order of trellis-coded systems through a bit-interleaved constellation expansion technique termed channel symbol expansion diversity.

2.5 Summary

In this chapter, we first presented Passerieux's steganographic method as implemented in the frequency domain by Ferrao. Then, we introduced the characteristics of wireless communications, including common effects and their sources, and large- and small-scale fading models. Next, we described the peculiarities of the underwater acoustic channel, including the differences between UACs and RF communications and the particular effects that make the underwater environment especially hostile. Finally, we presented an array of methods applied in both the acoustic and RF environments to achieve data recovery at a receiver through signal detection, frame synchronization, and channel equalization. In each case, different classes of solutions were presented, and various implementations were introduced. It should be noted that while certain techniques are well-established or show great promise for practical applications, applicable methods are constrained to those that are interoperable with Ferrao's implementation of Passerieux's system and do not undermine the inherently covert nature of the communications scheme. Thus, change-sensitive detection and blind synchronization and equalization techniques are the most likely candidates. Additionally, we can not necessarily assume the availability of multi-element, beamforming, or spatially diverse receivers. We intend to further explore data recovery methods in the context of steganographic communications and analyze their performance and constraints in realistic environments. Specifically, we intend to thoroughly research the following:

- Assuring that transmission recognition can occur only by application of the steganographic key, and not using knowledge merely of the steganographic system
- Transmission capacity improvement
- Optimal symbol recovery methods for our steganographic system in the underwater acoustic environment
- The performance of the application of these various techniques at different ranges, depths, and acoustic environments.

The remainder of this thesis will describe and analyze methods to achieve reliable data recovery, robust to the effects of a hostile acoustic channel, for our steganographic system—to include comparison of competing techniques—and will provide analysis of the performance results in such a system.

CHAPTER 3:
Methodology

In Chapter 2, we presented Passerieux's technique in the frequency domain, discussed the effects of a channel on signals, and reviewed methods for dealing with those effects. In this chapter, we present the mathematical considerations of symbol recovery. Section 3.1 introduces the basic formulation of our frequency domain discussions. Section 3.2 disproves time domain synchronization and recovery offered by Passerieux. Section 3.3 introduces three novel recovery schemes, an analytical method based on the frequency domain representation of Passerieux's technique, a numerical method using discrete approximations of calculus functions, and recovery assuming a known original signal. Section 3.4 discusses the adverse effects of the transmission environment and the impact on each of the symbol recovery solutions. Section 3.5 presents our implementation modules.

3.1 Theory

Our work builds on Ferrao's frequency domain implementation [1] of Passerieux's steganographic method [2], [3], as described in Chapter 2. Ferrao operates on the premise that the real components of the cross correlation in the frequency domain will tend positive or negative depending on the symbol, which is encoded as a negative or positive amplitude factor. Passerieux contends that when the signal is perfectly synchronized, the symbol (encoded in amplitude, phase, or both) will present in the phase of the cross correlation in the time domain. We demonstrate how both of these systems break down mathematically. Additionally, we notice that both Ferrao and Passerieux utilize a symbol encoding scheme that is constant across each interval m and a key that varies across each sub-interval p. We posit that these two elements are mathematically interchangeable and that bit rate can be improved at the expense of computation by performing a search across all possible symbols. The computational increase is logarithmic with the number of symbols, since each bit can be searched independently.

Ferrao provides a mathematical analysis of the frequency domain translation of Passerieux's time domain technique. While we leverage that work, we will not present it here; the interested reader is referred to Ferrao's thesis [1].

After the DFT is applied to a signal interval, a vector of complex values results, with each complex value representing the presence of a given frequency in the original signal. We represent a generic single frequency value with amplitude A and phase a as Ae^{Ja}; specific frequency components in an array are indicated by subscripts (e.g., $A_k e^{Ja_k}$); and we use brackets to indicate the array itself (e.g., $A_{[k]} e^{Ja_{[k]}}$). We also make use of the following formula for phasor addition (given $Ce^{Jc} = Ae^{Ja} + Be^{Jb}$)

$$Ce^{Jc} = \sqrt{A^2 + B^2 + 2AB\cos(b-a)}\, e^{J\left(a + \operatorname{atan2}\left(\substack{B\sin(b-a),\\ A+B\cos(b-a)}\right)\right)} \tag{3.1}$$

which we derive as follows.

First, the definition of the dot product gives

$$Ae^{Ja} \cdot Be^{Jb} = AB\cos(b-a) \tag{3.2}$$

and

$$Ae^{Ja} \cdot Ce^{Jc} = AC\cos(c-a) \tag{3.3}$$

Further, a property of the dot product is

$$Ce^{Jc} \cdot Ce^{Jc} = C^2 \tag{3.4}$$

Substituting the definition of Ce^{Jc} ($Ce^{Jc} = Ae^{Ja} + Be^{Jb}$) into Equation 3.4, we get

$$\begin{aligned} C^2 &= (Ae^{Ja} + Be^{Jb}) \cdot (Ae^{Ja} + Be^{Jb}) \\ &= Ae^{Ja} \cdot Ae^{Ja} + Be^{Jb} \cdot Be^{Jb} + 2Ae^{Ja} \cdot Be^{Jb} \\ &= A^2 + B^2 + 2AB\cos(b-a) \end{aligned}$$

Thus,

$$C = \sqrt{A^2 + B^2 + 2AB\cos(b-a)} \tag{3.5}$$

This gives the magnitude of the sum, but not the angle. The angle can be found by the following series of equations. First, substituting $Ce^{Jc} = Ae^{Ja} + Be^{Jb}$ into Equation 3.3 gives

$$\begin{aligned} AC\cos(c-a) &= Ae^{Ja} \cdot (Ae^{Ja} + Be^{Jb}) \\ &= A^2 + AB\cos(b-a) \end{aligned}$$

Solving for $\cos(c-a)$ gives

$$\cos(c-a) = \frac{A + B\cos(b-a)}{C} \tag{3.6}$$

Recalling that magnitude of the cross product is given by

$$|Ae^{Ja} \times Be^{Jb}| = AB\sin(b-a)$$

then

$$\begin{aligned} |Ae^{Ja} \times Ce^{Jc}| &= |Ae^{Ja} \times Ae^{Ja} + Ae^{Ja} \times Be^{Jb}| \\ &= |Ae^{Ja} \times Be^{Jb}| \\ AC\sin(c-a) &= AB\sin(b-a) \end{aligned}$$

and

$$\sin(c-a) = \frac{B}{C}\sin(b-a) \tag{3.7}$$

Dividing 3.7 by 3.6 and application of the arctangent (specifically the atan2 function, which preserves the quadrant of the solution) solves for the angle, c

$$c = a + \text{atan2}\begin{pmatrix} B\sin(b-a), \\ A + B\cos(b-a) \end{pmatrix} \tag{3.8}$$

Thus, in terms of Ae^{Ja} and Be^{Jb}

$$Ce^{Jc} = \sqrt{A^2 + B^2 + 2AB\cos(b-a)}\,e^{J\left(a + \text{atan2}\left(\substack{B\sin(b-a), \\ A+B\cos(b-a)}\right)\right)} \tag{3.9}$$

Using Equation 3.1, we can describe our steganographic method in terms of a generic frequency component. Recall that the time domain original signal is divided into intervals of length T seconds and the DFT is applied to each T-second interval. Once in the frequency domain, the interval is subdivided into $2M + 1$ subintervals, with data encoded in M subintervals, and $M + 1$ subintervals acting as guard bands. We then represent a generic frequency component in one of the data subintervals of the original signal as $\Omega e^{J\omega}$. The auxiliary signal is built from the time-reversed partner subinterval (e.g., if $\Omega e^{J\omega}$ is in subinterval m, then the partner subinterval is $M - m + 1$.) Due to the symmetry of the DFT, the auxiliary signal component is just the complex conjugate of the original, so $\Omega e^{-J\omega}$. Applying a phase key (a_m), a gain term (α), and a symbol ($be^{J\beta}$), the generic frequency component in the signal to be transmitted ($Te^{J\tau}$) is

$$\begin{aligned} Te^{J\tau} &= Oe^{J\omega} + \alpha bOe^{Ja_m}e^{J\beta}e^{-J\omega} \\ &= \sqrt{O^2 + (\alpha bO)^2 + 2\alpha bO^2\cos(a_m + \beta - 2\omega)}e^{J(\omega + \text{atan2}(\substack{\alpha bO\sin(a_m+\beta-2\omega), \\ O+\alpha bO\cos(a_m+\beta-2\omega)}))} \end{aligned} \tag{3.10}$$

Assuming no transfer function due to transmission effects and perfect receive-side synchronization, the generic received frequency component ($Re^{J\rho}$) is exactly equal to $Te^{J\tau}$. The approximate auxiliary function is then calculated as

$$\hat{\Psi}e^{J\hat{\psi}} = \alpha Te^{-J\tau}e^{Ja_m} \tag{3.11}$$

Finally, the cross-correlation of the approximate auxiliary signal and the received signal is

$$\begin{aligned} Ze^{J\zeta} &= \hat{\Psi}e^{-J\hat{\psi}}Te^{J\tau} \\ &= \alpha Te^{J\tau}e^{-Ja_m}Te^{J\tau} \end{aligned}$$

which, after substituting Equation 3.10 and some basic arithmetic, gives

$$Ze^{J\zeta} = O^2(1 + \alpha^2b^2 + 2\alpha b\cos(a_m + \beta - 2\omega))e^{J(2\tau - a_m)} \tag{3.12}$$

In the real world, channel effects will always be present. These effects are modeled in the frequency domain by a vector of amplitude changes and phase shifts, $H_{[k]}e^{J\theta_{[k]}}$. In terms of a generic frequency component, the received signal after transmission becomes

$$Re^{J\rho} = OH\sqrt{1+\alpha^2b^2+2\alpha b\cos(a_m+\beta-2\omega)}e^{J(\omega+\theta+\text{atan2}(\begin{smallmatrix}\alpha b\sin(a_m+\beta-2\omega),\\ 1+\alpha b\cos(a_m+\beta-2\omega)\end{smallmatrix}))} \tag{3.13}$$

Thus, the approximate auxiliary signal must be computed as

$$\hat{\Psi}e^{J\hat{\psi}} = \alpha Re^{-J\rho}e^{Ja_m} \tag{3.14}$$

giving

$$\begin{aligned} Ze^{J\zeta} &= \hat{\Psi}e^{-J\hat{\psi}}Re^{J\rho} \\ &= \alpha R^2 e^{J\rho}e^{-Ja_m}e^{J\rho} \\ &= \alpha O^2H^2(1+\alpha^2b^2+2\alpha b\cos(a_m+\beta-2\omega))e^{J(2\rho-a_m)} \end{aligned} \tag{3.15}$$

In the methods outlined by Passerieux [2], [3] and Ferrao [1], the gain term (α) is constant across all intervals, the phase key (a_m) varies across intervals and sub-intervals, and the symbol ($be^{J\beta}$) varies from interval to interval but is constant across all sub-intervals. We posit that one can increase the symbol space by using a phase key that varies from interval to interval but is constant through the interval, and a symbol that varies from sub-interval to sub-interval. In this scheme, each interval represents an M-bit symbol, and the magnitude b is a shared secret value that acts as an additional key.

3.2 Mathematical Refutations

In [2], [3], Passerieux asserts that cross-correlation peaks will be maximized when the transmitter and receiver are properly synchronized and Doppler compensated. Further, he states the time domain phase of the cross-correlation will be proportional to the transmitted symbol. We mathematically disprove both claims here.

3.2.1 Synchronization

Proper synchronization is critical to the efficacy of the steganographic method. According to Passerieux [2], amplitude peaks in the time domain cross-correlation will be maximized upon correct application of the steganographic key and proper synchronization. When proper synchronization occurs, the division of the signal into T-second intervals begins at the exact same point in time on the received signal as with the original signal. However, when varying the synchronization delay on a signal with known symbol and key, the magnitude of the time domain cross-correlation peak varies non-monotonically, indicating that the magnitude is not suitable for a synchronization search. Figure 3.1 illustrates this phenomenon. The x-axis is offset from synchronization in seconds, and the y-axis is peak cross-correlation magnitude. Note that if cross-correlation peak were sufficient for synchronization, we would expect an absolute maximum at $x = 0$ (i.e., no delay offset, or perfect synchronization).

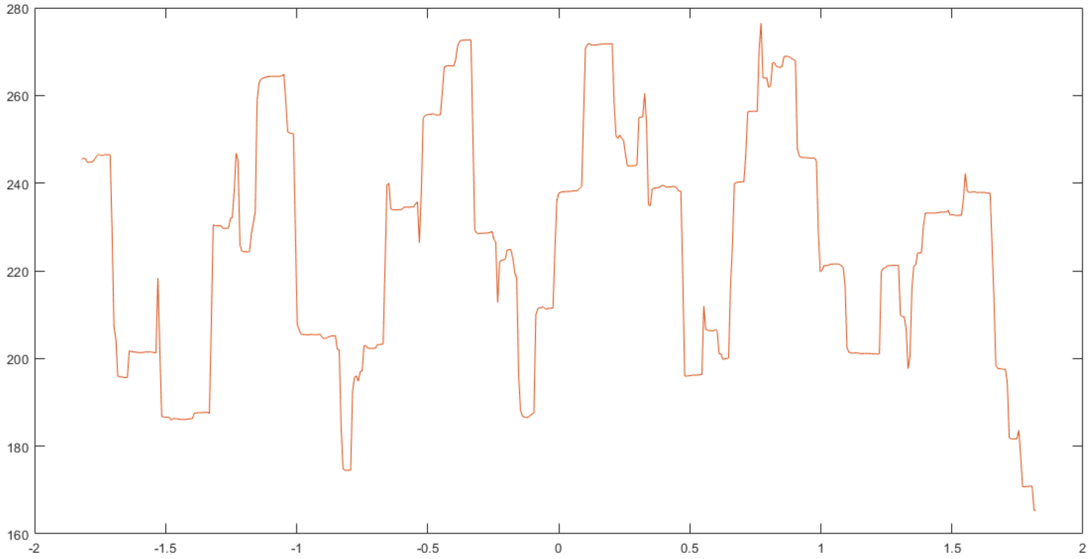

Figure 3.1. Magnitude of Cross-Correlation Peak versus Delay Offset.

We investigate this mathematically by returning to the signal to be transmitted, which in the frequency domain is a vector given by $T_{[k]}e^{J\tau_{[k]}}$ such that

$$T_{[k]} = O_{[k]}\sqrt{1 + \alpha_{[k]}^2 b_{[k]}^2 + 2\alpha_{[k]} b_{[k]} \cos(a_{m_{[k]}} + \beta_{[k]} - 2\omega_{[k]})} \tag{3.16}$$

and

$$\tau_{[k]} = \omega_{[k]} + \text{atan2}\begin{pmatrix} \alpha_{[k]} b_{[k]} \sin(a_{m_{[k]}} + \beta_{[k]} - 2\omega_{[k]}), \\ 1 + \alpha_{[k]} b_{[k]} \cos(a_{m_{[k]}} + \beta_{[k]} - 2\omega_{[k]}) \end{pmatrix} \tag{3.17}$$

(We note that here and throughout, vector operations are element-wise.) When synchronization is off at the receiver (even assuming the absence of channel effects) $T_{[k]}e^{J\tau_{[k]}} = R_{[k]}e^{J\rho_{[k]}}$ does not hold true. When properly synchronized, $R_i e^{J\rho_i}$ is a function of $O_i e^{J\omega_i}$. However, when synchronization is off, the DFT is performed on a different segment of the time domain signal, resulting in an amplitude and phase for the ith frequency component that is completely independent from $O_i e^{J\omega_i}$. In this case, the cross-correlation result is merely

$$Z_{[k]}e^{J\zeta_{[k]}} = \alpha R^2_{[k]} e^{J(2\rho_{[k]}-a_{m_{[k]}})} \tag{3.18}$$

The inverse DFT is defined as

$$x_n = \frac{1}{N}\sum_{k=1}^{N} X_k e^{J\frac{2\pi k(n-1)}{N}} \tag{3.19}$$

Passerieux indicates that one should expect peaks in the time domain cross-correlation spaced at the interval length. This means we should expect a peak at z_1. Setting n to 1 in the inverse DFT equation gives

$$z_1 = \frac{1}{N}\sum_{k=1}^{N} Z_k e^{J\frac{0}{N}} \tag{3.20}$$

which is just the average magnitude of the frequency domain cross-correlation. Thus peak magnitude is a function of the average power in the interval, rather than proper synchronization.

3.2.2 Passerieux's Technique

According to Passerieux, the symbol will be encoded in the phase of the time domain cross-correlation between the T-spaced peaks. To investigate this, we begin with Equations 3.15 and 3.19. We will assume a perfect transmission channel (i.e., $He^{J\theta} = 1e^{J0}$) and perfect synchronization. Equation 3.15 can be generalized to give the frequency domain cross-correlation vector as

$$Ze^{J\zeta} = \alpha^2 O^2_{[k]}(\frac{1}{\alpha} + \alpha b^2_{[k]} + 2b_{[k]}\cos(a_{[k]} + \beta_{[k]} - 2\omega_{[k]}))e^{J(2\rho_{[k]}-a_{[k]})} \tag{3.21}$$

From the definition of the inverse DFT, we can select an arbitrary sample in time (i) between the peaks located at 1 and N (i.e., $1 < i < N$). (Recall that the number of time samples, N, is also the number of frequency domain frequency components.)

$$z_i = \frac{1}{N}\sum_{k=1}^{N} Z_k e^{\jmath\zeta_k} e^{\jmath\frac{2\pi k(i-1)}{N}} \tag{3.22}$$

From Equation 3.18, we can see that for all k, ζ_k is $2\rho_{+}a_k$. Thus, the summation can be rewritten in rectangular coordinates as

$$\begin{aligned} z_i = &\frac{1}{N}\sum_{k=1}^{N}\alpha^2 O_k^2(\frac{1}{\alpha}+\alpha b_k^2+2b_k\cos(a_k+\beta_k-2\omega_k))\cos(2\rho_k+a_k+\frac{2\pi k(i-1)}{N}) \\ &+\jmath\frac{1}{N}\sum_{k=1}^{N}\alpha^2 O_k^2(\frac{1}{\alpha}+\alpha b_k^2+2b_k\cos(a_k+\beta_k-2\omega_k))\sin(2\rho_k+a_k+\frac{2\pi k(i-1)}{N}) \end{aligned} \tag{3.23}$$

The phase of z_i (denoted φ_i) is then

$$\varphi_i = \operatorname{atan2}\begin{pmatrix} \frac{1}{N}\sum_{k=1}^{N}\alpha^2 O_k^2(\frac{1}{\alpha}+\alpha b_k^2+2b_k\cos(a_k+\beta_k-2\omega_k))\sin(2\rho_k+a_k+\frac{2\pi k(i-1)}{N}), \\ \frac{1}{N}\sum_{k=1}^{N}\alpha^2 O_k^2(\frac{1}{\alpha}+\alpha b_k^2+2b_k\cos(a_k+\beta_k-2\omega_k))\cos(2\rho_k+a_k+\frac{2\pi k(i-1)}{N}) \end{pmatrix} \tag{3.24}$$

$$= \operatorname{atan2}\begin{pmatrix} \sum_{k=1}^{N}\alpha^2 O_k^2(\frac{1}{\alpha}+\alpha b_k^2+2b_k\cos(a_k+\beta_k-2\omega_k))\sin(2\rho_k+a_k+\frac{2\pi k(i-1)}{N}), \\ \sum_{k=1}^{N}\alpha^2 O_k^2(\frac{1}{\alpha}+\alpha b_k^2+2b_k\cos(a_k+\beta_k-2\omega_k))\cos(2\rho_k+a_k+\frac{2\pi k(i-1)}{N}) \end{pmatrix} \tag{3.25}$$

Within each of the $2M + 1$ intervals b_k, β_k, and α are constant, and a_k is constant within every subinterval. Then with distribution, we get

$$\varphi_i = \operatorname{atan2}\left(\begin{array}{rl} \alpha \sum_{k=1}^{N} & O_k^2 \sin(2\rho_k + a_k + \frac{2\pi k(i-1)}{N}) \\ + & \alpha^2 b_k \sum_{k=1}^{N} \alpha b_k O_k^2 \sin(2\rho_k + a_k + \frac{2\pi k(i-1)}{N}) \\ + & 2O_k^2 \cos(a_k + \beta_k - 2\omega_k) \sin(2\rho_k + a_k + \frac{2\pi k(i-1)}{N}), \\ \alpha \sum_{k=1}^{N} & O_k^2 \cos(2\rho_k + a_k + \frac{2\pi k(i-1)}{N}) \\ + & \alpha^2 b_k \sum_{k=1}^{N} \alpha b_k O_k^2 \cos(2\rho_k + a_k + \frac{2\pi k(i-1)}{N}) \\ + & 2O_k^2 \cos(a_k + \beta_k - 2\omega_k) \cos(2\rho_k + a_k + \frac{2\pi k(i-1)}{N}) \end{array}\right) \tag{3.26}$$

$$= \operatorname{atan2}\left(\begin{array}{rl} \sum_{k=1}^{N} & O_k^2 \sin(2\rho_k + a_k + \frac{2\pi k(i-1)}{N}) \\ + & \alpha b_k \sum_{k=1}^{N} O_k^2 (\alpha b_k + 2\cos(a_k + \beta_k - 2\omega_k)) \sin(2\rho_k + a_k + \frac{2\pi k(i-1)}{N}), \\ \sum_{k=1}^{N} & O_k^2 \cos(2\rho_k + a_k + \frac{2\pi k(i-1)}{N}) \\ + & \alpha b_k \sum_{k=1}^{N} O_k^2 (\alpha b_k + 2\cos(a_k + \beta_k - 2\omega_k)) \cos(2\rho_k + a_k + \frac{2\pi k(i-1)}{N}) \end{array}\right) \tag{3.27}$$

While one could use trigonometric identities to further factor out the constants $\sin(\beta_k)$ and $\cos(\beta_k)$ and simplify some components of the equation by setting $b_k e^{\jmath\beta_k}$ to 1 in the guard intervals, this does not further clarify the solution. It is sufficient to gather from Equation 3.27 that while φ is a function of the symbol $b_k e^{\jmath\beta_k}$, it is clearly not proportional to the symbol, as Passerieux claims. Moreover, since atan2 is not bijective and φ is a function of multiple variables—with the argument of atan2 primarily driven by $O_{[k]}$—knowledge of the value of φ is not sufficient to resolve the encoded symbol.

We note that if the constant phase key and variable symbol encoding version is used, the discussion is analogous and the conclusions are the same.

3.3 Alternative Solutions

One of the alluring promises of Passerieux's technique is the ability to use any cover signal without relying on shared knowledge of the original signal. We desire to recover signals while maintaining Passerieux's original value proposition. We will assume exact synchronization and a perfect transmission channel initially. Unlike Passerieux and Ferrao, we use a known symbol and unknown phase key.

The various variables used in the equations of this chapter are summarized in Table 3.1.

Table 3.1. Equation Variables.

Variable	**Name**	**Notes**
$Ae^{\jmath a}$	Arbitrary frequency component	Amplitude A and phase a. †
m	Interval	
p	Subinterval	
$Oe^{\jmath\omega}$	Original signal	†
$\hat{O}e^{\jmath\hat{\omega}}$	Approximate original signal	†
a_m	Phase key	Also, a_k for an index, or a_p in a subinterval
α	Gain	
$be^{\jmath\beta}$	Symbol	†
$\Psi e^{\jmath\psi}$	Auxiliary signal	†
$Te^{\jmath\tau}$	Transmitted signal	$Te^{\jmath\tau} = Oe^{\jmath\omega} + \Psi e^{\jmath\psi}$ †
$He^{\jmath\theta}$	Transfer function	†
$Re^{\jmath\rho}$	Received Signal	$Re^{\jmath\rho} = Te^{\jmath\tau}He^{\jmath\theta}$ †
$Ze^{\jmath\zeta}$	Output of cross-correlation	†
$\hat{Z}e^{\jmath\hat{\zeta}}$	Approximate Z and ζ	†
z	$Ze^{\jmath\zeta}$ in the time domain	
φ	Phase of z	
δ	$\delta = \rho - \omega - \theta$	$\delta = \rho - \omega$ when θ is assumed negligible
γ	$\gamma = a_m + \beta - 2\omega$	
K	Symbol ratio	$K = R^2/O^2$
$\hat{K}$	Estimated K	Iterative estimator for K
$\hat{a}_m$	Estimated phase key	Iterative estimator for a_m
ω_g	Guard phase	The received phase in an arbitrary guard interval bin
K_g	Guard ratio	R^2/O^2 in an arbitrary guard interval bin
$\tilde{Z}e^{\jmath\lambda}$	Method 2 cross-correlation	†

† Amplitude and phase commonly decoupled in equations

Continued on next page

Table 3.1 – ***continued from previous page***

Variable	Name	Notes
δ_ω	$\delta_\omega = \hat{\omega} - \omega$	
K_O	$K_O = \hat{O}/O$	
$\hat{\lambda}$	Estimated λ	$\hat{\lambda}$ is the numerically approximated integral of $\frac{\partial\lambda}{\partial f}$
Λ	DFT of λ	
$Ee^{\jmath\varepsilon}$	Estimate error	$Ee^{\jmath\varepsilon} = Oe^{\jmath\omega} - \hat{O}e^{\jmath\hat{\omega}}$ †
f	Frequency	
B, C	Integration equation parameters	In our implementation: $B = \pi/2, C = \gamma_f$
h	Integration equation parameter	$h = \log(\pi\gamma_g N)/(\gamma_g N)$
$\psi(u)$	Exponential transform	$\psi(u) = \frac{\mu}{2}\tanh(\pi\sinh(u))$
$\psi^{-1}(u)$	Transform inverse	$\psi^{-1}(u) = \operatorname{arcsinh}(2\operatorname{arctanh}(u/\mu)/\pi)$
$\psi'(u)$	Transform derivative	$\psi'(u) = \frac{\mu\pi}{2}\operatorname{sech}^2(\pi\sinh(u))\cosh(u)$
$\sigma_{k-\ell}$	Modified sine integral	$\sigma_{k-\ell} = \frac{1}{2} + \frac{\mathrm{Si}(\pi(k-\ell))}{\pi}$, where $\mathrm{Si}(x)$ is the sine integral of x
i, j, k, ℓ	Iterators	
$\mathrm{S}(k,h)(u)$	Normalized sinc function	$\mathrm{S}(k,h)(u) = \sin(\pi x)/(\pi x)$, where x is $(u - kh)/h$
N	DFT size	Also, N_λ in Johnson's derivation technique
N_I	Numerical integration size	
L_λ	Length of λ	In Johnson's derivation technique
μ	Scale factor	
$\alpha_f, \beta_f, \gamma_f$	Integration constraint constants	Also given as α_g, β_g, and γ_g, respectively
$d_f, \varepsilon_d, \varepsilon_c$	Integration constants	d_f also given as d_g

3.3.1 Recovery Directly from Received Signal

The most enticing method for data recovery is to draw the symbol directly from the received signal. In the absence of channel effects, the base equation is Equation 3.10 simplifies to

$$Re^{J\rho} = Te^{J\tau} = O\sqrt{1+\alpha^2b^2+2\alpha b\cos(a_m+\beta-2\omega)}e^{J(\omega+\text{atan2}(\genfrac{}{}{0pt}{}{\alpha b\sin(a_m+\beta-2\omega),}{1+\alpha b\cos(a_m+\beta-2\omega)}))} \tag{3.28}$$

We can readily solve for a_m from the magnitude of the received signal.

$$a_m = \arccos(\frac{R^2}{2\alpha bO^2} - \frac{1}{2\alpha b} - \frac{\alpha b}{2}) - \beta - 2\omega \tag{3.29}$$

However, because we only have two base equations

$$R = O\sqrt{1+\alpha^2b^2+2\alpha b\cos(a_m+\beta-2\omega)} \tag{3.30}$$

and

$$\rho = \omega + \text{atan2}\left(\begin{matrix}\alpha b\sin(a_m+\beta-2\omega),\\ 1+\alpha b\cos(a_m+\beta-2\omega)\end{matrix}\right) \tag{3.31}$$

we can only solve for O and ω in terms of a_m, rendering Equation 3.29 a mere identity.

We cannot solve for a_m unless the values of O and/or ω are known. The simplest mechanism for handling this problem is to use known cover signals, but that would undermine the steganographic intent of our scheme. The alternative is to estimate O or ω with accuracy sufficient to allow proper recovery of a_m. Depending on the values of α, b, a_m, and β, $Re^{J\rho}$ can be a reasonable approximation of $Oe^{J\omega}$. A better approach uses the known values of α, b, and β to make a closer estimation. We leverage the consistency of α, b, a_m, and β across all frequencies in a subinterval to achieve data recovery via an analytical method that retrieves the symbol from the received signal. We will utilize the follow equivalences: $\beta_i = \beta_j, \alpha_ib_i = \alpha_jb_j$, and $a_i+\beta_i = a_j+\beta_j$ for all i and j in a given data subinterval. We will also use the following substitutions for notational simplicity: $\delta_k = \rho_k-\omega_k, \gamma_k = a_m+\beta-2\omega_k$, and $K_k = R_k^2/O_k^2$.

We begin with Equation 3.31. We can rearrange and take the tangent of both sides to get

$$\tan(\rho-\omega) = \frac{\alpha b\sin(a_m+\beta-2\omega)}{(1+\alpha b\cos(a_m+\beta-2\omega))} \tag{3.32}$$

Which we can rearrange and square to get

$$\tan^2\delta(1+\alpha b\cos\gamma)^2 = \alpha^2 b^2 \sin^2\gamma$$

We substitute $1-\cos^2\gamma$ for $\sin^2\gamma$, distribute and expand the multiplications, and rearrange to isolate factors carrying a $\cos\gamma$ term.

$$\frac{\alpha^2 b^2 - \tan^2\delta}{\alpha b\tan^2\delta} = 2\cos\gamma + \alpha b\cos^2\gamma + \frac{\alpha b\cos^2\gamma}{\tan^2\delta}$$

We subsequently solve for $\cos\gamma$ with the following series of algebraic adjustments

$$\frac{\alpha^2 b^2}{\tan^2\delta} - 1 = \alpha b\cos^2\gamma(2\sec\gamma + \alpha b + \frac{\alpha b}{\tan^2\delta})$$

$$\cos^2\gamma = \frac{\frac{\alpha^2 b^2}{\tan^2\delta} - 1}{2\alpha b\sec\gamma + \alpha^2 b^2 + \frac{\alpha^2 b^2}{\tan^2\delta}}$$

$$\cos\gamma = \sqrt{\frac{\frac{\alpha^2 b^2}{\tan^2\delta} - 1}{2\alpha b\sec\gamma + \alpha^2 b^2 + \frac{\alpha^2 b^2}{\tan^2\delta}}} \tag{3.33}$$

From Equation 3.30, we can substitute $2\alpha b/(K-1-\alpha^2 b^2)$ for $\sec\gamma$, and solve for $a_m+\beta$, recalling $\gamma = a_m + \beta - 2\omega$.

$$a_m + \beta = \pm\sqrt{\frac{\cot^2\delta - (\alpha b)^{-2}}{\frac{4}{K-1-\alpha^2 b^2} + 1 + \cot^2\delta}} \tag{3.34}$$

This solution for $a_m + \beta$ is preferred to the more simply derived $\arccos((K-1-\alpha^2 b^2)/(2\alpha b)) + 2\omega$ because it is more forgiving in practice to error in K, which will be affected by application of the transfer function due to channel effects. Note that there are two possible results of Equation 3.34; we select the one that is closest (circularly) to one of the possible values of a_m after subtracting the known β.

If we assume that the values ω_{i-1} and K_{i-1} are known when solving for ω_i and K_i, we can use ω_{i-1} and K_{i-1} to solve for $a_m+\beta$ in iteration i. Since $a_m+\beta$ is now known, we can solve for ω_i iteratively. We iterate from $-\pi$ to π, with the step size determining the precision of our estimated ω_i. We deem thousandths of radians to be sufficiently precise. We select ω_i to be the value of $\hat{\omega}$ that drives the following equation closest to zero.

$$\rho_i - \hat{\omega} - \operatorname{atan2}\begin{pmatrix} \alpha b \sin(a_m + \beta - 2\omega), \\ 1 + \alpha b \cos(a_m + \beta - 2\omega) \end{pmatrix} \tag{3.35}$$

We subsequently solve for K_i iteratively, searching for values of $\hat{K}$ such that $1+\alpha^2 b^2 - 2|\alpha b| \leq \hat{K} \leq \alpha^2 b^2 + 2|\alpha b|$. We select as K_i the $\hat{K}$ that drives the following equation nearest to zero.

$$\tan^2 \delta_i - (2\alpha b - \hat{K} + 1 + \alpha^2 b^2)(2\alpha b + \hat{K} - 1 - \alpha^2 b^2)(\hat{K} + 1 - \alpha^2 b^2)^{-2} \tag{3.36}$$

which is derived from Equations 3.32 and 3.30.

Algebraic operations on Equation 3.30 result in

$$\cos\gamma = \frac{K - 1 - \alpha^2 b^2}{2\alpha b} \tag{3.37}$$

Substituting into Equation 3.32 gives

$$\begin{aligned} \tan\delta &= \frac{\alpha b \sin\gamma}{1 + \frac{\alpha b(K-1-\alpha^2 b^2)}{2\alpha b}} \\ &= \frac{2\alpha b}{2 + K - 1 - \alpha^2 b^2} \\ &= \frac{2\alpha b}{K + 1 - \alpha^2 b^2} \end{aligned} \tag{3.38}$$

We can square both sides and use the trigonometric identity $\sin^2 x = 1 - \cos^2 x$ with Equation 3.37 to get

$$\begin{aligned} \tan^2\delta &= (2\alpha b)^2 \left(1 - (K - 1 - \alpha^2 b^2)^2 (2\alpha b)^{-2}\right)(K + 1 - \alpha^2 b^2)^{-2} \\ &= \frac{4\alpha^2 b^2 - (K - 1 - \alpha^2 b^2)^2}{(K + 1 - \alpha^2 b^2)^2} \\ &= (2\alpha b - K + 1 + \alpha^2 b^2)(2\alpha b + K - 1 - \alpha^2 b^2)(K + 1 - \alpha^2 b^2)^{-2} \end{aligned} \tag{3.39}$$

This iterative method is preferred over a direct calculation of K (for example, $K = 1 + \alpha^2 b^2 + 2\alpha b \cos\gamma$ or $K = 2\alpha b \sin\gamma / \tan\delta - 1 + \alpha^2 b^2$) because these equations for K rely on $\gamma = a_m + \beta - 2\omega$. Since we calculate ω from $a_m + \beta$, any error in $a_m + \beta$ is exacerbated in the direct calculation of K.

For each (K_k, ω_k) pair for all k in a subinterval, we test against all possible values $\hat{a}_m$ from the finite set of keys. We select as the symbol a_m that $\hat{a}_m$ which results in least MSE within the subinterval, where error is defined from Equation 3.30 as

$$\varepsilon = K - 1 - \alpha^2 b^2 - 2\alpha b \cos(\hat{a}_m + \beta - 2\omega) \tag{3.40}$$

The Prerequisite: Finding K_1 and ω_1

The preceding discussion in Section 3.3.1 relies on determination of K_{k-1} and ω_{k-1} for each k in the subinterval, which we define as the (K_{k-1}, ω_{k-1}) pair that gave the smallest $|\varepsilon_{k-1}|$. The critical dependency for this is the ability to first find K_1 and ω_1 from a guard interval frequency bin wherein β is known and a_m is not applied. We determine ω_g in the guard interval iteratively as in Equation 3.35 by setting a_m to 0. We then solve for K_g by rearranging Equation 3.30 into

$$K_g = 1 + \alpha^2 b^2 + 2\alpha b \cos(0 + \beta - 2\omega_g) \tag{3.41}$$

Finally, while $a_g \neq a_m$, β is constant in both the guard and the subinterval, so we leverage $\tan(\beta_g) = \tan(\beta_1)$ in the following way. We begin with Equation 3.32, which we can rearrange to

$$\tan\delta(1 + \alpha b \cos(a_m + \beta - 2\omega)) = \alpha b \sin(a_m + \beta - 2\omega)$$
$$\frac{\tan\delta}{\alpha b \cos(a_m + \beta - 2\omega)} + \tan\delta = \tan(a_m + \beta - 2\omega)$$

$$\text{Since } \tan(A - B) = \frac{\tan(A) - \tan(B)}{1 + \tan(A)\tan(B)} \tag{3.42}$$

$$\frac{\tan(\beta) - \tan(2\omega - a_m)}{1 + \tan(\beta)\tan(2\omega - a_m)} = \tan(\delta)(1 + \frac{1}{\alpha b \cos(a_m + \beta - 2\omega)})$$

$$\tan(\beta) - \tan(2\omega - a_m) = \tan(\delta)(1 + \frac{1}{\alpha b \cos(a_m + \beta - 2\omega)})(1 + \tan(\beta)\tan(2\omega - a_m))$$

$$\begin{aligned}\tan(\beta) = \tan(\delta) + \frac{\tan(\delta)}{\alpha b \cos(a_m + \beta - 2\omega)} + \tan(\delta)\tan(\beta)\tan(2\omega - a_m) \\ + \tan(\delta)\tan(\beta)\frac{\tan(2\omega - a_m)}{\alpha b \cos(a_m + \beta - 2\omega)} + \tan(2\omega - a_m)\end{aligned}$$

$$\begin{aligned}\tan(\beta)(1 - \tan(\delta)\tan(2\omega - a_m) - \tan(\delta)\frac{\tan(2\omega - a_m)}{\alpha b \cos(a_m + \beta - 2\omega)}) = \\ \tan(\delta) + \frac{\tan(\delta)}{\alpha b \cos(a_m + \beta - 2\omega)} + \tan(2\omega - a_m)\end{aligned}$$

$$\begin{aligned}\tan(\beta)(\alpha b \cot(\delta) - \alpha b \tan(2\omega - a_m) - \frac{\tan(2\omega - a_m)}{\cos(a_m + \beta - 2\omega)}) = \\ \alpha b + \sec(a_m + \beta - 2\omega) + \alpha b \tan(2\omega - a_m)\cot(\delta)\end{aligned}$$

$$\tan(\beta) = \frac{\alpha b + \sec(a_m + \beta - 2\omega) + \alpha b \tan(2\omega - a_m)\cot(\delta)}{\alpha b \cot\delta - \alpha b \tan(2\omega - a_m) - \tan(2\omega - a_m)\sec(a_m + \beta - 2\omega)} \tag{3.43}$$

Since $\tan(\beta_g) = \tan(\beta_i)$, and since $2\omega - a_m = \beta - \gamma$, and setting $a_m = 0$ in the guard interval,

$$\begin{aligned}\frac{\alpha b + \sec(\beta - 2\omega_g) + \alpha b \tan(2\omega_g)\cot(\delta_g)}{\alpha b \cot(\delta_g) - \alpha b \tan(2\omega_g) - \tan(2\omega_g)\sec(\beta - 2\omega_g)} = \\ \frac{\alpha b + \sec(\gamma_1) + \alpha b \tan(\beta - \gamma_1)\cot(\delta_1)}{\alpha b \cot(\delta_1) - \alpha b \tan(\beta - \gamma_1) - \tan(\beta - \gamma_1)\sec(\gamma_1)}\end{aligned} \tag{3.44}$$

Notably, γ_1 is the only unknown in Equation 3.44, and we can solve for it iteratively to an arbitrary precision (at the expense of computation) since it is bounded by $(-\pi, \pi]$. With γ_1 known, we solve for K_1 and ω_1 from Equations 3.30 and 3.31, respectively.

$$K_1 = 1 + \alpha^2 b^2 + 2\alpha b \cos(\gamma_1) \tag{3.45}$$

$$\omega_1 = \rho_1 - \operatorname{atan2}\begin{pmatrix} \alpha b \sin\gamma_1, \\ 1 + \alpha b \cos\gamma_1 \end{pmatrix} \tag{3.46}$$

3.3.2 Recovery via Numerical Approximations of Calculus Functions

We attempt a numerical recovery solution by first recalling that the transmitted signal for a generic frequency component is defined by Equation 3.10 as

$$Te^{J\tau} = Oe^{J\omega} + \alpha bOe^{Ja_m}e^{J\beta}e^{-J\omega}$$

and in a perfect transmission scenario, the received signal $Re^{J\rho}$ equals $Te^{J\tau}$. We then estimate the original cover signal and define it as $\hat{O}e^{J\hat{(\omega)}}$, where

$$\hat{O}e^{J\hat{\omega}} \neq Te^{J\tau}$$

and

$$\hat{O}e^{J\hat{\omega}} \neq \alpha bOe^{Ja_m}e^{J\beta}e^{-J\omega}$$

Then $Re^{J\rho} - \hat{O}e^{J\hat{\omega}}$ is just $\alpha bOe^{Ja_m}e^{J\beta}e^{-J\omega}$ plus some residual error. We define this residual as $Ee^{J\varepsilon}$. We then perform a cross-correlation with an estimate of $\alpha bOe^{J\beta}e^{-J\omega}$, giving

$$\begin{aligned}
\tilde{Z}e^{J\lambda} &= (\alpha bOe^{J(a_m+\beta-\omega)} + Eej^{J\varepsilon})(\alpha b\hat{O}e^{J(\beta-\hat{\omega})})^* & (3.47)\\
&= \alpha^2b^2O\hat{O}e^{J(a_m-\omega+\hat{\omega})} + \alpha b\hat{O}Ee^{J(\varepsilon-\beta+\hat{\omega})}\\
&= \alpha b\hat{O}\left(\alpha bOe^{J(a_m-\omega+\hat{\omega})} + Ee^{J(\varepsilon-\beta+\hat{\omega})}\right)\\
&= \alpha^2b^2\hat{O}O\sqrt{1+\left(\frac{E}{\alpha bO}\right)^2+\frac{2E}{\alpha bO}\cos(\varepsilon-\gamma-\omega)}\,e^{J(a_m-\omega+\hat{\omega}+\text{atan2}(\genfrac{}{}{0pt}{}{E\sin(\varepsilon-\gamma-\omega),}{\alpha bO+E\cos(\varepsilon-\gamma-\omega)}))}\\
& & (3.48)
\end{aligned}$$

We use the notation $\tilde{Z}$ for the magnitude of this cross-correlation to differentiate from Z used elsewhere. We then use the definition of $Ee^{J\varepsilon}$ to calculate

$$Ee^{J\varepsilon} = Oe^{J\omega} - \hat{O}e^{J\hat{\omega}} = \sqrt{O^2+\hat{O}^2-2O\hat{O}\cos(\hat{\omega}-\omega)}\,e^{J(\omega-\text{atan2}(\genfrac{}{}{0pt}{}{\hat{O}\sin(\hat{\omega}-\omega),}{O+\hat{O}\cos(\hat{\omega}-\omega)}))} \qquad (3.49)$$

and substitute it into Equation 3.48 to get

$$\tilde{Z} = \alpha b O \hat{O} \sqrt{\alpha b K_O} \sqrt{\begin{aligned} &\frac{1}{\alpha b K_O}(\alpha^2 b^2 + 1 + K_O^2 - 2K_O \cos\delta_\omega) \\ &\quad + 2\sqrt{K_O^{-2} + 1 - \tfrac{2\cos\delta_\omega}{K_O}} \cos(\gamma + \operatorname{atan2}(\genfrac{}{}{0pt}{}{K_O \sin\delta_\omega,}{1+K_O\cos\delta_\omega})) \end{aligned}} \tag{3.50}$$

and

$$\lambda = a_m + \delta_\omega + \operatorname{atan2}\begin{pmatrix} -E\sin(\gamma + \operatorname{atan2}(\genfrac{}{}{0pt}{}{K_O \sin\delta_\omega,}{1+K_O\cos\delta_\omega})), \\ \alpha b O + E\cos(\gamma + \operatorname{atan2}(\genfrac{}{}{0pt}{}{K_O \sin\delta_\omega,}{1+K_O\cos\delta_\omega})) \end{pmatrix} \tag{3.51}$$

where $\delta_\omega = \hat{\omega} - \omega$ and $K_O = \frac{\hat{O}}{O}$.

The phase term vector $\lambda_{[k]}$ can then be considered sample points of a function of the constant (within each subinterval) a_m and values that vary with frequency. When we take the derivative of λ with respect to frequency, then $\frac{\partial a_m}{\partial f} = 0$, while the other terms remain. Subsequently integrating with respect to frequency gives $\hat{\lambda}_{[k]}$, which can be subtracted from $\lambda_{[k]}$ to reveal a_m. This method assumes that a derivative for λ exists and sufficient accuracy from numerical indefinite integration is attainable. We use the derivation technique presented by Steven G. Johnson [72] and the double exponential sinc integration method given by Tanaka et al. [73]. Given the symmetry of the Fast Fourier Transform (FFT), we perform our derivation-integration technique only on the positive frequency bins and negate the result for the negative reflection.

Johnson's derivation technique [72] is fairly straightforward. First, use the FFT to compute Λ from λ, which will have a length N_λ that is even (in our case). For $0 \leq k < N_\lambda/2$, multiply Λ_k by $2\pi k\imath/L_\lambda$, and set Λ_k to zero at $k = N_\lambda/2$. For $N_\lambda/2 < k < N_\lambda$, multiply Λ_k by $2\pi(k - N_\lambda)\imath/L_\lambda$. For our purposes, L_λ is the size of the domain of λ. Finally, take the inverse FFT of the modified Λ_k to compute λ'.

The formula for integration given by Tanaka et al. [73] is

$$\begin{aligned}\int_{-1}^{x} f(t)\mathrm{d}t = \frac{1}{2}[\tanh(B\sinh(C\psi^{-1}(x)))+1]\ \ h\sum_{k=-N_I}^{N_I} f(\psi(kh))\psi'(kh) \\ + h\sum_{k=-N_I}^{N_I}\left[\sum_{\ell=-N_I}^{N_I}\sigma_{k-\ell}\Bigg(f(\psi(\ell h))\psi'(\ell h)\right. \\ \left. - \frac{BC\cosh(C\ell h)}{2\cosh^2(B\sinh(C\ell h))}\ \ h\sum_{k=-N_I}^{N_I} f(\psi(kh))\psi'(kh)\Bigg)\right] \mathrm{S}(k,h)(\psi^{-1}(x)) \\ + O(e^{-\frac{c'_f N_I}{\log(c''_f N_I)}})\end{aligned} \tag{3.52}$$

where $O(e^{-\frac{c'_f N_I}{\log(c''_f N_I)}})$ is an error term, which we can assume to be negligible for sufficiently large N_I (e.g., $N_I \geq 1000$), where N_I is the number of numerical integration iterations. The function $\psi(u)$ is the double exponential transform, for which we use $\mu\tanh(\frac{\pi}{2}\sinh(u))$. For our transform, $\psi'(u)$ is $\frac{\mu\pi}{2}\operatorname{sech}^2(\pi\sinh(u))\cosh(u)$, and $\psi^{-1}(u)$ is $\operatorname{arcsinh}(\frac{2}{\pi}\operatorname{arctanh}(\frac{u}{\mu}))$, as given by Takahasi and Mori [74]. We define μ as a scaling factor, which we set to the maximum modified frequency bin in order to map $(-\infty,\infty)$ to our frequency band. A scaling factor of 1 would map $(-\infty,\infty)$ to (-1,1).

$\mathrm{S}(k,h)(u)$ is an application of the normalized sinc function, $\frac{\sin(\pi x)}{\pi x}$, where x is $\frac{u-kh}{h}$. The function $\sigma_{k-\ell}$ is a modified sine integral, which is usually defined as $\mathrm{Si}(x) = \int_0^x \operatorname{sinc}(t)\mathrm{d}t$, but here is $\frac{1}{2} + \int_0^{k-\ell}\frac{\sin(\pi t)}{\pi t}\mathrm{d}t$, or $\frac{1}{2} + \frac{\mathrm{Si}(\pi(k-\ell))}{\pi}$. Note that $\operatorname{sinc}(0) = 1$ and $\mathrm{Si}(0) = 0$, by definition. MATLAB's implementation of the sine integral is too inefficient for the number of values we have to calculate, so we borrow an implementation from Rowe et al. [75] using the approximation $\mathrm{Si}(x) \approx \frac{\pi}{2} - f(x)\cos(x) - g(x)\sin(x)$, where $f(x)$ and $g(x)$ are approximated by Padé rational functions to a precision on the order of 10^{-16} for $x \geq 4$.

B and C are constants developed from the following constraint:

$$\forall x \in \Re, |f(x)| \leq \alpha_f \exp(-\beta_f \exp(\gamma_f |x|)),\ \text{for some positive numbers } \alpha_f, \beta_f,\ \text{and } \gamma_f. \tag{3.53}$$

We select $\gamma_f = 1/12000, \beta_f = \pi/2 - 10^{-10}$, and $\alpha_f = 10^{39}\max\lambda'$, which maintains the constraint of Equation 3.53. We select a $d_f = 12000\pi$, so that $\gamma_f d_f = \pi/2$, in which case Tanaka et al. [73] give $B = \pi/2, C = \gamma_f, \beta_g = \beta_f, \gamma_g = \gamma_f$, and $d_g = \frac{\pi}{2\gamma_f} - \varepsilon_d$, where ε_d is any positive number such that $d_g > 0$. We set ε_d to 1. Error is minimized when $\gamma_f d_f = \pi/2$ and β_f is as large as possible. The value h is defined by

$$h = \frac{\log(\pi(d_g - \varepsilon_c)\gamma_g N_I/\beta_g)}{\gamma_g N_I}, \text{ where } 0 < \varepsilon_c < d_g \tag{3.54}$$

$$\text{We select } \varepsilon_c = (d_g - \beta_g) \text{ so that } h = \frac{\log(\pi\gamma_g N_I)}{\gamma_g N_I}. \tag{3.55}$$

We compute the numerical indefinite integration technique given by Tanaka et al. for all x such that x equals a frequency in a data interval in order to generate $\hat{\lambda}_{[k]}$. Subtracting $\hat{\lambda}_{[k]}$ from the actual $\lambda_{[k]}$ should give a_m in each of the data intervals, from which we recover the symbols.

3.3.3 Recovery with Known Original Signal

For comparison, if we assume a known original signal (i.e., known $O_{[k]}$ and $\omega_{[k]}$), then symbol recovery is trivial. We refer to this method as comparative. We iteratively select the value γ that drives the following equation closest to zero.

$$R - O\sqrt{1 + \alpha^2 b^2 + 2\alpha b \cos\gamma} \tag{3.56}$$

The symbol value a_m is then $\gamma + 2\omega - \beta$.

3.4 Channel Effects

The previous discussions regarding proposed symbol recovery solutions did not include adverse channel effects, which can be modeled as a factor, $He^{J\theta}$. After transmission through an arbitrary channel, the received signal vector becomes $R_{[k]}e^{J\rho[k]}$ such that

$$R_{[k]} = O_{[k]} H_{[k]} \sqrt{1 + \alpha^2 b^2 + 2\alpha b \cos(a_{[k]} + \beta - 2\omega_{[k]})} \tag{3.57}$$

and

$$\rho_{[k]} = \omega_{[k]} + \theta_{[k]} + \operatorname{atan2}\left(\begin{matrix} \alpha b \sin(a_{[k]} + \beta - 2\omega_{[k]}), \\ 1 + \alpha b \cos(a_{[k]} + \beta - 2\omega_{[k]}) \end{matrix} \right) \tag{3.58}$$

However, we can assume synchronization also provides an initial estimate of $H_{[k]} e^{J\theta_{[k]}}$. In our first symbol recovery scheme, in each subsequent interval we divide the received signal by our estimated transfer function and solve for a_m. We expect that the solved symbol will not exactly equal a canonical value, but we select the closest symbol to the calculated value and update the estimated transfer function. The literature is replete with potential schemes for estimating or updating the transfer function.

We will assume the ability to achieve perfect estimation in interval i in order to validate symbol recovery by dividing $H_i e^{J\theta_i}$ out of $R_i e^{J\rho_i}$.

In the second solution method, the presence of a transfer function affects the calculation of $E e^{J\varepsilon}$. We must now define the residual error as

$$\begin{aligned} E e^{J\varepsilon} &= OHe^{J(\omega+\theta)} + \alpha b OHe^{J(a_m+\beta+\theta-\omega)} - \hat{O} e^{J\hat{\omega}} \\ &= OH\sqrt{1 + \alpha^2 b^2 + 2\alpha b \cos\gamma}\, e^{J(\omega+\theta+\operatorname{atan2}({}^{\alpha b \sin\gamma,}_{1+\alpha b \cos\gamma}))} - \hat{O} e^{J\hat{\omega}} \end{aligned} \tag{3.59}$$

where

$$E = \alpha b OH \sqrt{\frac{2K_O}{\alpha b H}} \sqrt{\begin{matrix} \dfrac{H}{2K_O \alpha b} + \dfrac{2K_O}{\alpha b H} + \dfrac{H \cos\gamma}{K_O} + \dfrac{K_O}{2\alpha b H} \\ - \sqrt{\frac{1}{\alpha^2 b^2} + 1 + \frac{2\cos\gamma}{\alpha b}} \cos(-\delta_\omega + \theta + \operatorname{atan2}({}^{\alpha b \sin\gamma,}_{1+\alpha b \cos\gamma})) \end{matrix}} \tag{3.60}$$

and

$$\begin{aligned} \varepsilon =& \omega + \theta + \operatorname{atan2}({}^{\alpha b \sin\gamma,}_{1+\alpha b \cos\gamma}) \\ & - \operatorname{atan2}\left(\begin{matrix} \sin(-\delta_\omega + \theta + \operatorname{atan2}({}^{\alpha b \sin\gamma,}_{1+\alpha b \cos\gamma})), \\ \frac{H}{K_O} \sqrt{1 + \alpha^2 b^2 + 2\alpha b \cos\gamma} + \cos(-\delta_\omega + \theta + \operatorname{atan2}({}^{\alpha b \sin\gamma,}_{1+\alpha b \cos\gamma})) \end{matrix} \right) \end{aligned} \tag{3.61}$$

Clearly, ε varies with frequency since it is dependent on other frequency-varying variables. Thus, when we differentiate and reintegrate λ with respect to frequency, ε will be included in $\hat{\lambda}$. So when we subtract $\hat{\lambda}$ from λ, we still reveal a_m.

When the original signal is known, determination of $He^{\jmath\theta}$ is trivial. From Equations 3.30 and 3.31,

$$H = \frac{R}{O\sqrt{1 + \alpha^2 b^2 + 2\alpha b \cos(a_m + \beta - 2\omega)}} \tag{3.62}$$

and

$$\theta = \rho - \omega - \operatorname{atan2}\left(\begin{array}{c} \alpha b \sin(a_m + \beta - 2\omega), \\ 1 + \alpha b \cos(a_m + \beta - 2\omega) \end{array} \right) \tag{3.63}$$

3.5 Implementation

In order to test the performance of our symbol embedding and recovery schemes, we implemented a series of modules in MATLAB R2017b [76].

3.5.1 Modules

Two main modules perform the embedding and extraction, while two minor modules simulate transmission and synchronization.

Embedding

The function `stegembed.m` implements the operations described in Section 2.1.2. The inputs to `stegembed.m` are `coverAudio`, `T`, `alpha`, `fl`, `delay`, and `requestedSyms`. The base audio, `coverAudio`, must be in uncompressed .wav format. The float inputs `T`, `alpha`, and `delay`, and positive integer input `requestedSyms` are meta-parameters for the period, auxiliary signal gain, embedding start point, and the number of symbols to encode, respectively. The positive integer `fl` is a helper parameter that defines the lowest frequency for MMPE. The outputs of the embedding function are `x`, `y`, `fs`, `a`, `start_index`, `stop_index`, `s`, `symspace`, and `rstart`. The time domain cover audio, `x`, is returned, which is merely the first channel of the coverAudio input, while `y` is the time domain signal to be transmitted with embedded steganography symbols (the number of embedded bits depends on the `requestedSyms` parameter and the size of `T` relative to the duration of the cover.) `fs` is the sampling frequency, as determined by reading the cover audio, and `rstart` is the `delay` input converted from seconds to number of samples. The matrix outputs a, start_index, stop_index, s, and symspace are the key, data interval starting indices, data interval end indices, embedded symbols (i.e., ground truth), and symbol space, respectively. In our implementation, the symbols are encoded in phase and the symbol magnitude is set to 1. As in Ferrao's implementation [1], stegembed.m always operates on a 2048 Hz band centered about 2500 Hz.

Extraction

We have three extraction functions, one for each of the methods presented in Section 3.3. All three modules have the same output, syms, which is the recovered symbols. The inputs to passerieuxextractMethod1.m are yrc, x, fs, T, alpha, a, symspace, rstart, start_index, stop_index, Hinit, nKeys, and s. As in stegembed.m, T and alpha are float inputs for period and auxiliary signal gain, respectively, while x, fs, a, symspace, rstart, start_index, stop_index, and s are directly the outputs of stegembed.m. The positive integer nKeys is the number of possible symbols, including unique synchronization symbols that are not used for data transmission. yrc is the received time domain signal with embedded symbols after transmission through a simulated channel, while Hinit is the initial estimate of the channel transfer function. passerieuxextractMethod3.m takes exactly the same inputs, while passerieuxextractMethod2.m takes no additional inputs but does not require x, Hinit, or s.

Transmission and Synchronization

We handle transmission via a module that implements the effects on the transmitted signal by the channel simulated using MMPE as well as adding white Gaussian noise with a mean of zero and variance taken from the transmit signal. We do not deviate from Ferrao's implementation, and we refer the interested reader to his thesis [1] for an in-depth discussion thereof.

We make use of a placeholder module for synchronization. Our synch_assume.m function takes as inputs y, yrc, fs, fl, T, start_index, stop_index, and dstart, which are exactly as described elsewhere. The outputs are Hinit, dstart, start_index, and stop_index. A true synchronization function would only require yrc, fs, T, alpha, a, and the known synchronization symbol sequence to generate the outputs.

3.6 Summary

In this chapter, we discussed symbol recovery in Ferrao's implementation of Passerieux's steganographic scheme from a mathematical perspective. We presented basic equations, and disproved the synchronization and recovery solutions asserted by Passerieux. Additionally, we presented three information recovery solutions. The first was an analytical method derived from frequency domain equations. The second was a numerical method built on approximations of derivation and integration from discrete samples. The final method presented was recovery by comparison to a known original signal. We further discussed the effects of an adverse channel on our recovery solutions and described our implementation modules. In Chapter 4, we discuss our design parameters and present our results.

CHAPTER 4:
Results and Analysis

In Chapter 3, we mathematically refuted assumptions and assertions of previous work, developed three alternative methods of symbol recovery, and presented our implementation modules. In this chapter, we describe our experiment design and analyze our results.

4.1 Design

We test our recovery algorithms via two simulated channels—a relatively benign deep water channel and a comparatively adverse shallow channel. We use the same channels as Ferrao [1]. The deep channel has a maximum depth of 1000 m and a maximum range of 1000 m, while the shallow channel has a maximum depth of 100 m and a maximum range of 3000 m. We test recovery every 40 m while permuting through transmitter and receiver depths 1 m, 20 m, and 60 m in the shallow channel and 1 m, 180 m, 500 m depths in the deep channel. For each of the three methods, we assess recovery performance when encoding a symbol space of size 2, 4, 7, 12, 23, 32, and 60, respectively, in each period. Based on Ferrao's results [1], we maintain a period (T) of 0.5 seconds, a gain (α) of 0.32, and SNR of 50 dB.

While a single run of our numerical recovery method (Section 3.3.2) is imperceptably slower than a single run of either the analytical (Section 3.3.1) or comparative (Section 3.3.3) methods, performing the number of iterations necessary to test our second recovery method on the same scale as the others was infeasible in practice. As a result, we modified the experiment design to test recovery every 80 m in both channels for the numerical recovery method. Additionally, in the shallow channel we hold transmitter depth constant at 60m while iterating through receiver depths of 1 m, 20m, and 60 m, and in the deep channel we limit our transmitter and receiver depths to 1 m and 500 m. All other parameters remain unchanged from the other experiments.

4.2 Results

Since we modified the mechanism by which symbols are encoded, it is necessary to first ensure that the steganographic characteristics of the scheme are not degraded. We then present symbol recovery performance. For our analyses, we use the first channel of an uncompressed `.wav` recording of sperm whale vocalizations sampled at 48 kHz, `SpermWhaleNormalClicks.wav` obtained from the National Oceanic and Atmospheric Administration (NOAA) Southwest Fisheries Science Center catalog of cetacean sounds [77].

4.2.1 Steganography Measures

We can establish an initial visual assessment of the quality of the steganography via spectrographs. These heat maps show how the frequency components of a signal vary in amplitude over time. Figure 4.1 shows the spectrograph of the cover signal compared to the spectrographs of our minimum and maximum symbol space.

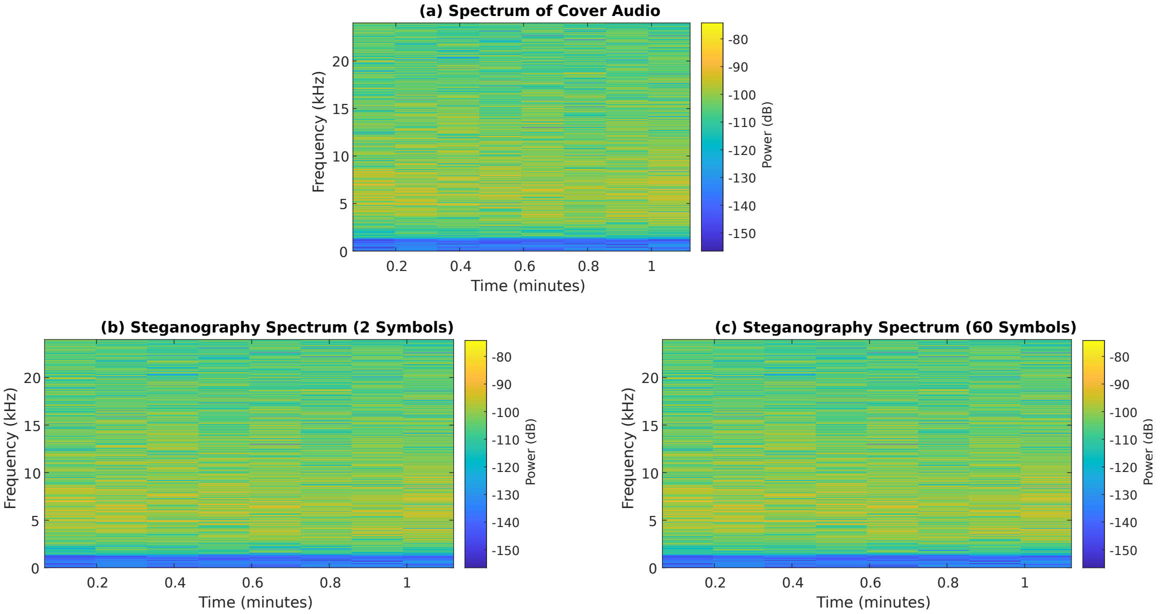

Figure 4.1. Spectrograph of (a) the Unmodified Cover Signal, (b) the Signal with Binary Symbols Embedded, and (c) the Signal with 6-bit Symbols Embedded.

The spectrographs are clearly effectively identical, but we quantify the statistical difference between the signals via common measures of “hiddenness" of a steganographic signal—MSE, Root Mean Square Error (RMSE), SNR, and PSNR.

MSE or RMSE

MSE is a measure of the difference between the steganographic signal and the cover signal, where RMSE is merely the square root of MSE. If the cover signal is given by $y_{[k]}$ and the steganographic signal is given by $x_{[k]}$, both of length N, the MSE is

$$\text{MSE} = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2 \tag{4.1}$$

Figure 4.2 shows how average RMSE varies with the size of the symbol space. Maximum RMSE is $3.474132x10^{-4}$ and RMSE does not increase with symbol space, indicating that our new encoding technique is no less covert than Ferrao’s, nor do we sacrifice covertness for increased symbol transmission.

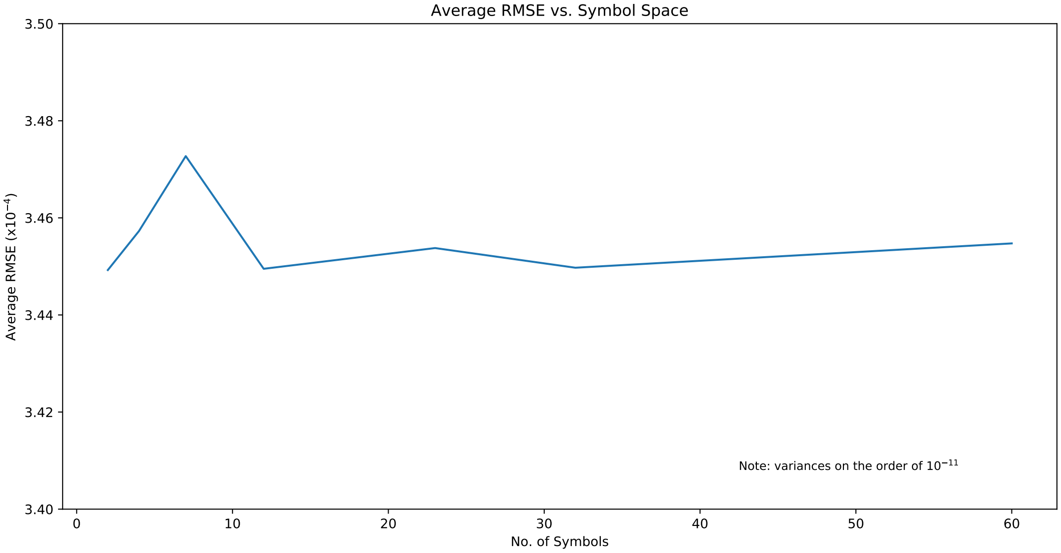

Figure 4.2. Variation of RMSE with the Number of Encodable Symbols.

SNR and PSNR

SNR and PSNR are also variations on MSE, where in this case "Noise" in Signal-to-Noise Ratio is the distortion caused by modifying the signal [78]. Since $y_{[k]}$ is normalized so that the maximum possible amplitude is 1, PSNR is

$$\text{PSNR} = 10 \log_{10} \frac{y_{max}^2}{\text{MSE}} = 10 \log_{10} \frac{1}{\text{MSE}}. \tag{4.2}$$

SNR is defined as

$$\text{SNR} = 10 \log_{10} \frac{\sum_{i=1}^{N} y_i^2}{\text{MSE}}. \tag{4.3}$$

As a rule, we desire SNR to be greater than 30 dB for imperceptible modification, while SNR less than 20 dB risks our method's LPI/LPD characteristics. The primary driver of SNR is the gain term α. Our choice of $\alpha = 0.32$ maintains SNR above 20 dB, but a gain value sufficiently small to raise average SNR above 30 dB ($\alpha \lessapprox 0.18$) undermines symbol recovery [1].

Figure 4.3 shows how average PSNR and SNR vary with the size of the symbol space. As with Figure 4.2, this figure reinforces that our encoding technique maintains comparable covertness to Ferrao's method and enables increased transmission rates without impacting LPI/LPD.

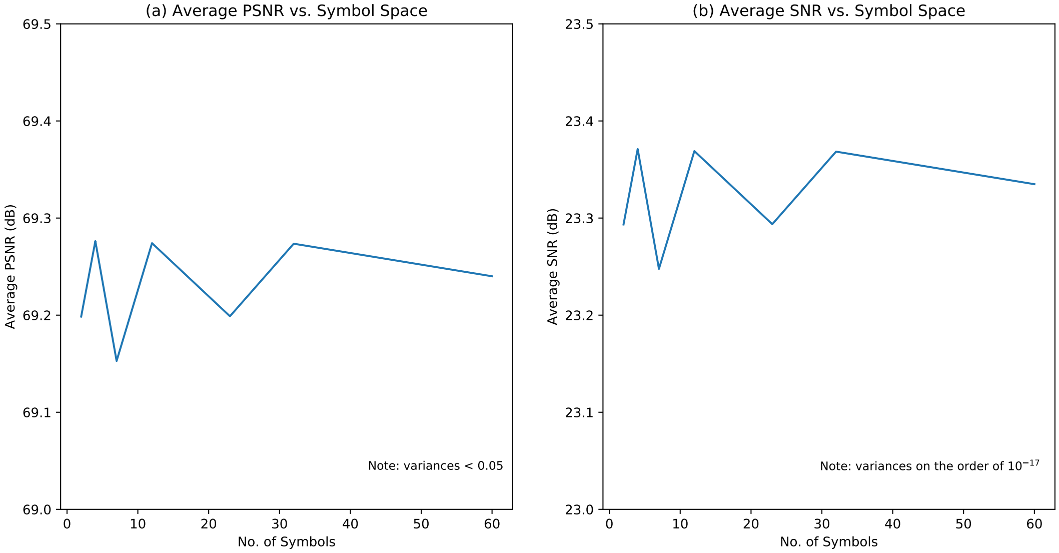

Figure 4.3. Variation of Average SNR and PSNR with the Number of Encodable Symbols.

The traditional steganography metrics in our embedding scheme are on the same order as Ferrao's results, indicating that our technique does not negatively affect the covertness of the system, allowing achievement of increased bit rates without sacrificing LPI/LPD.

Histograms

A histogram of signal phase provides a convenient visualization of the relative frequency with which frequency values appear in the signal, and can provide a "fingerprint" for a given signal or period. For LPI/LPD, we expect the histogram for the steganographic signal to be very similar to the cover signal. Conversely, we would need some uniqueness in the distribution that is mappable to the embedded symbol in order to achieve recovery through statistical means.

Figure 4.4 presents the histograms for the phase within the Least Significant Bit (LSB) subinterval for five arbitrary periods, comparing the original, transmitted, received, and cross-correlation signals. The cross-correlation signal is presented in both the frequency domain and time domain. Each histogram within a row represents the same arbitrary subinterval, period, and channel configuration. The symbol value in the given subinterval is shown by a red vertical line. The dotted vertical blue line gives the mean value in the subinterval, while the dashed vertical blue line displays the mean value for the full period. Phase is bounded by the interval $(-\pi, \pi]$, the histogram bin widths are 0.1323 radians, and the histogram bin heights are normalized so that the maximum possible value is 1.

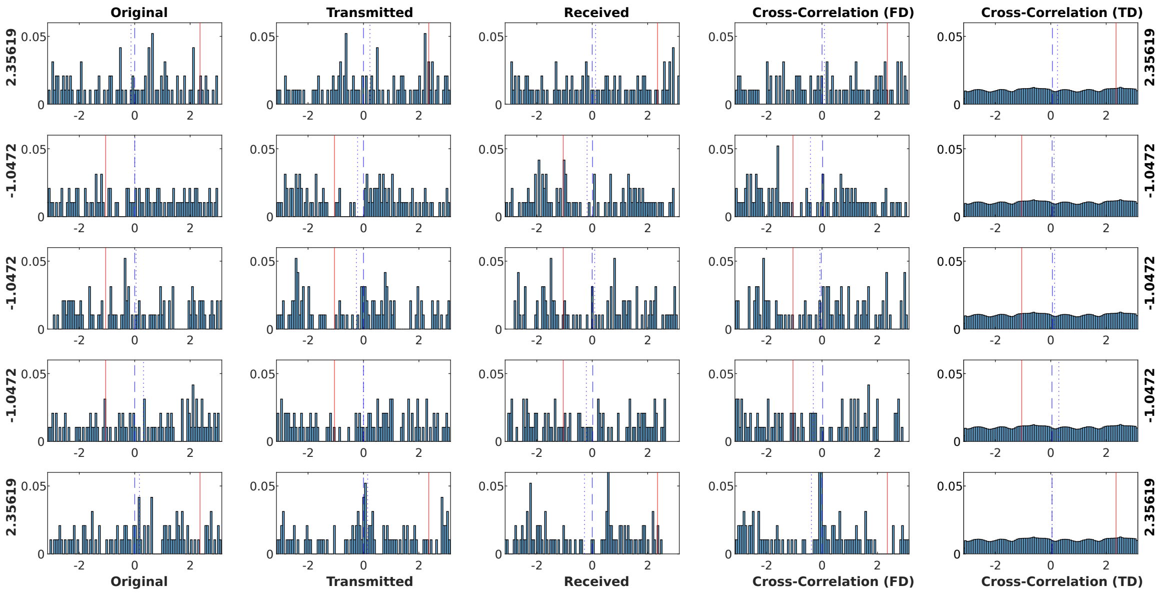

Figure 4.4. Histograms of LSB Phase Values in the Cover, Steganographic, Received, and Cross-Correlated Signals.

Figure 4.5 presents histograms of amplitude within an arbitrary data subinterval for five arbitrary periods of the original, transmitted, received, and cross-correlation signals. As with the histograms of phases, the cross-correlation signal is presented in both frequency domain and time domain, and each histogram within a row represents the same arbitrary subinterval, period, and channel configuration. A dotted vertical blue line gives the mean value in the subinterval, and a dashed vertical blue line displays the mean value for the full period. There is not a convenient analogue of symbol value in signal amplitude, so there is no visual presentation thereof, but the histograms are labeled with their relative symbols. The histogram bin heights are normalized so that the maximum possible value is 1. For ease of comparison, the axis limits are the same across all histograms with the notable exception of the time domain cross-correlation signal. The results for the time domain cross-correlation amplitude histogram are so different in scale that it has a unique set of axis limits.

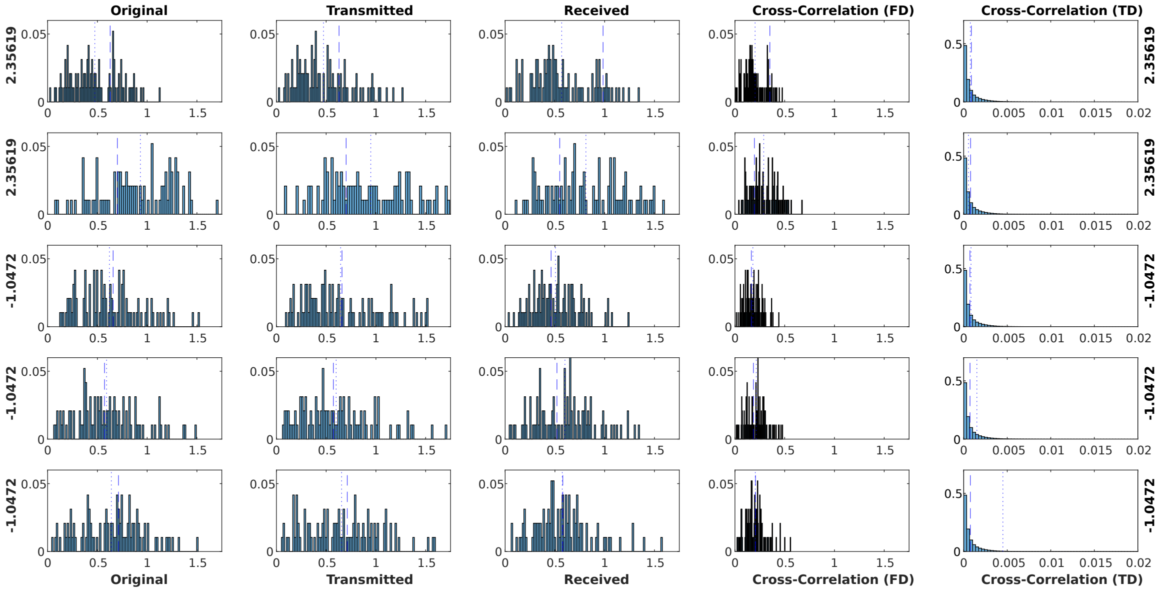

Figure 4.5. Histograms of LSB Amplitude Values in the Cover, Steganographic, Received, and Cross-Correlated Signals.

Figure 4.6 and Figure 4.7 are the same as Figure 4.4 and Figure 4.5, respectively, except that they show the histogram of the Most Significant Bit (MSB) frequency band for a symbol space of 60. There are fewer bins because each successive bit in our system is two-thirds the size of the preceding. This results in more noticeable differences among the histograms, but these differences do not correspond to particular bit values nor do they appear to indicate statistical anomalies that would reveal our steganographic presence.

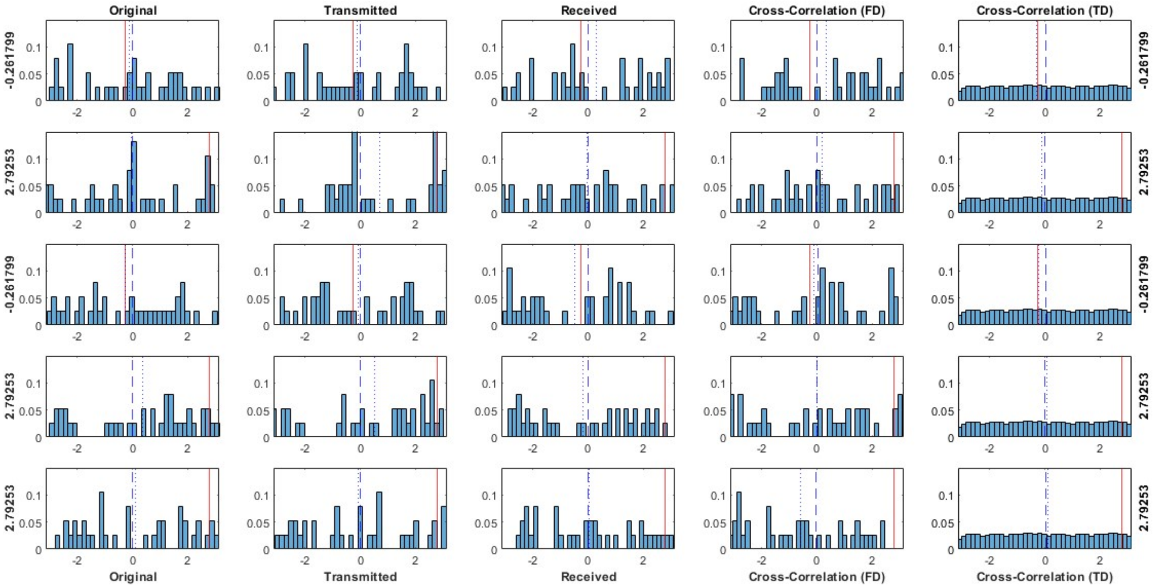

Figure 4.6. Histograms of MSB Phase Values in the Cover, Steganographic, Received, and Cross-Correlated Signals.

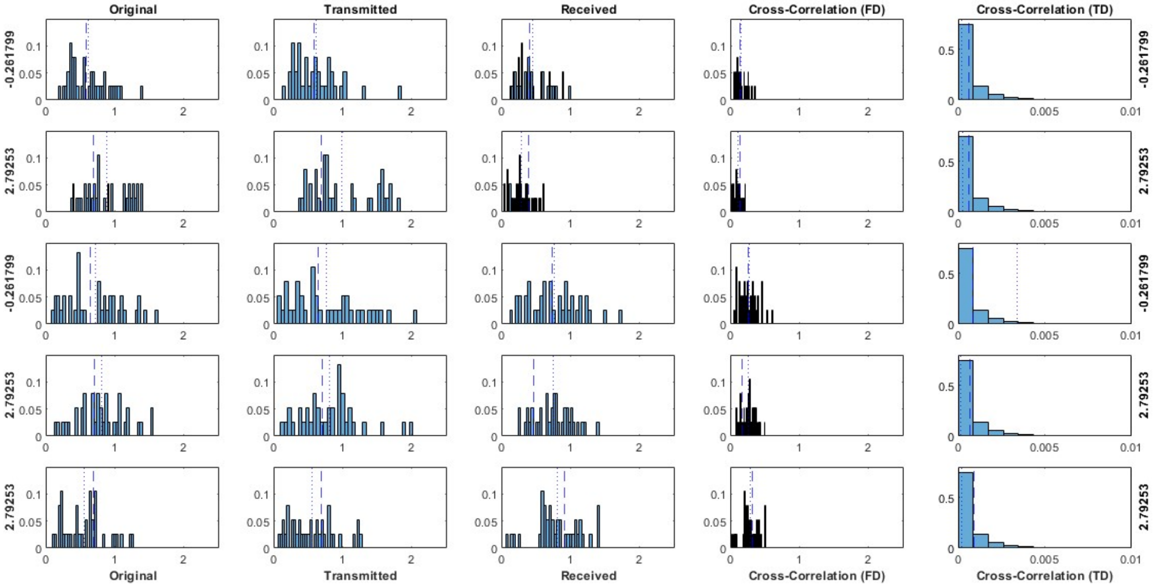

Figure 4.7. Histograms of MSB Amplitude Values in the Cover, Steganographic, Received, and Cross-Correlated Signals.

We highlight in the comparative histograms the relative similarity of the cover, transmitted, and received signals, though effects of the noise floor on the received signal can be seen. The lack of unique characteristics between symbol values (i.e., absence of distinguishing features down a column) demonstrates that statistical recovery or detection methods are unlikely to be successful. Notably, the mean of phase is effectively zero in every case. This is due to the bound on potential phase values—any shift or change in phase affects the interval equally, as values near the edges of the interval circle around to the opposite side of the interval, rather than exceeding the bounds (i.e., modulus 2π with the result shifted by $-\pi$.) Taken together, the lack of distinguishing features among the histograms of amplitude and phase indicate that knowledge of the steganographic scheme alone is highly unlikely to be sufficient to detect the transmission, much less determine the embedded symbols.

4.2.2 Recovery Performance

We assess recovery of embedded symbols after transmission through two underwater channel models generated by the MMPE. We investigate three potential recovery methods in both a deep water channel and a shallow channel, with the specifications for the channels taken from previous work by Ferrao [1]. As in Ferrao's thesis, the channels were built using MMPE's "efficiency" option.

Deep Channel Experiment

The open-ocean model is a 1000 m deep by 1000 m long channel with a flat, moderately reflective bottom and a notional sound speed of 1500 m/s. The channel has a bandwidth of 4096 Hz centered on 2500 Hz. To demonstrate the ability to recover symbols with each of our recovery methods, for each symbol space, transmitter depth, and receiver depth combination, we perform the embedding procedure, simulate the received signal based on the channel characteristics, and then apply extraction with each recovery method. Table 4.1 summarizes the experiment's simulation parameters.

Because we assume an optimal equalization method, neither range nor configuration of the transmitter and receiver appreciably impact recovery. Thus, in Figure 4.8, we average symbol recovery across all transmitter and receiver depths in order to highlight the effect of recovery method and number of encoded symbols on recovery performance. The graph shows recovery percentage vs. range for each transmitter depth. The number of encoded

Table 4.1. Deep Channel Experiment Parameters.

Parameter	**Values**
Symbol Space	2, 4, 7, 12, 23, 32, 60
T, α, SNR	0.5 s, 0.32, 50 dB
Method	Analytical, Comparative
Transmitter Depth	1 m, 180 m, 500 m
Receiver Depth	1 m 180 m, 500 m
Range	1 m to 1000 m, in 40 meter increments
Method	Numerical
Transmitter Depth	1 m, 500 m
Receiver Depth	1 m, 500 m
Range	1 m to 1000 m, in 80 meter increments

symbols is shown by different colors, with each recovery method having a different line style. Table 4.2 summarizes the recovery performances averaged across range.

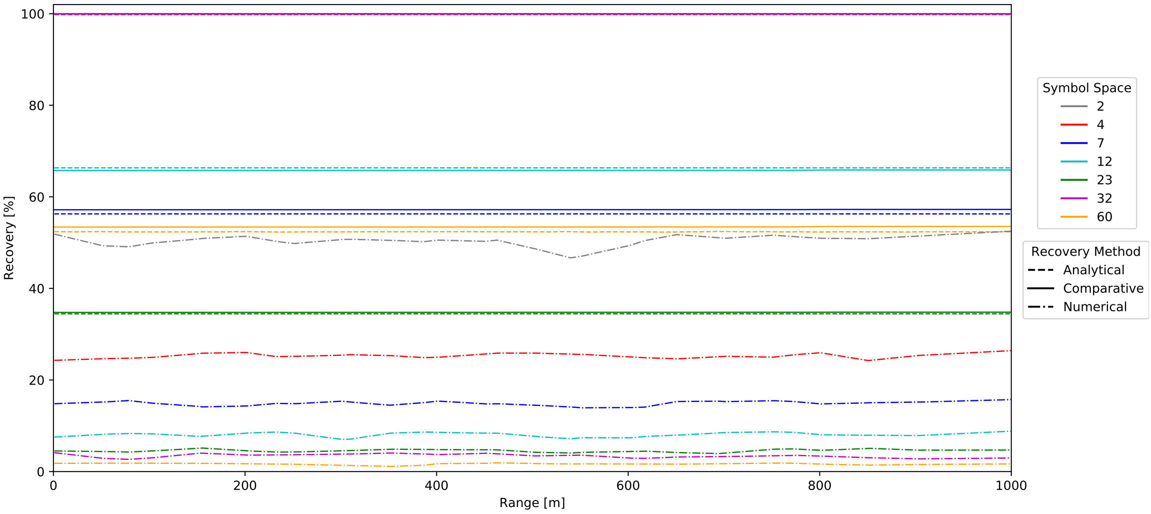

Figure 4.8. Performance of Three Symbol Recovery Methods in a Model Deep Water Channel.

Our analytical recovery method performs within about 1% of the comparative method,

Table 4.2. Average Symbol Recovery Performance in a Model Deep Channel.

Symbol Space	Method	Recovery [%]
2	Analytical	99.99
	Comparative	100.0
	Numerical	50.48
4	Analytical	99.90
	Comparative	100.0
	Numerical	25.29
7	Analytical	56.28
	Comparative	57.20
	Numerical	14.90
12	Analytical	66.34
	Comparative	65.79
	Numerical	8.071
23	Analytical	34.46
	Comparative	34.78
	Numerical	4.567
32	Analytical	99.82
	Comparative	100.0
	Numerical	3.405
60	Analytical	52.37
	Comparative	53.44
	Numerical	1.653

achieving a maximum goodput of 11.73 bps when synchronization and equalization are assumed. The numerical recovery method, on the other hand, on average performs the same as random guessing. Our assumption of perfect knowledge of the transfer function in each period reverses the combined channel effects that normally cause increased signal degradation as a function of distance. As a result, the otherwise expected reduction of symbol recovery performance with distance is not reflected in Figure 4.8.

Shallow Channel Experiment

The shallow channel simulates a 100 m deep by 3000 m long continental shelf with a flat, moderately reflective bottom that generates multipath conditions. As in the open-ocean

Table 4.3. Shallow Channel Experiment Parameters.

Parameter	**Values**
Symbol Space	2, 4, 7, 12, 23, 32, 60
T, α, SNR	0.5 s, 0.32, 50 dB
Method	Analytical, Comparative
Transmitter Depth	1 m, 20 m, 60 m
Receiver Depth	1 m, 20 m, 60 m
Range	1 m to 3000 m, in 40 meter increments
Method	Numerical
Transmitter Depth	60 m
Receiver Depth	1 m, 20m, 60 m
Range	1 m to 3000 m, in 80 meter increments

model, the notional sound speed is 1500 m/s, and the channel has a bandwidth of 4096 Hz centered on 2500 Hz. Identically to the deep channel experiment, for each symbol space, transmitter depth, and receiver depth combination, we perform the embedding procedure, simulate the received signal based on the channel characteristics, and then apply extraction with each recovery method. Table 4.3 summarizes the experiment's simulation parameters.

As with the deep channel model, in Figure 4.9 we average symbol recovery across all transmitter and receiver depths in order to highlight the effect of recovery method and number of encoded symbols on recovery performance. The graph shows recovery percentage vs. range for each transmitter depth. The number of encoded symbols is shown by different colors, with each recovery method having a different line style. Table 4.4 summarizes the recovery performances averaged across range.

Even in the more adverse channel, our analytical recovery method maintains a similar performance to the comparative method, staying within about 10% of comparative recovery. As in the deep channel experiment, the numerical recovery method performs no better than random guessing. Once again, our assumption of perfect equalization negates the factors that normally cause reduction of symbol recovery performance as a function of distance, resulting in nearly constant recovery with range as shown in Figure 4.9.

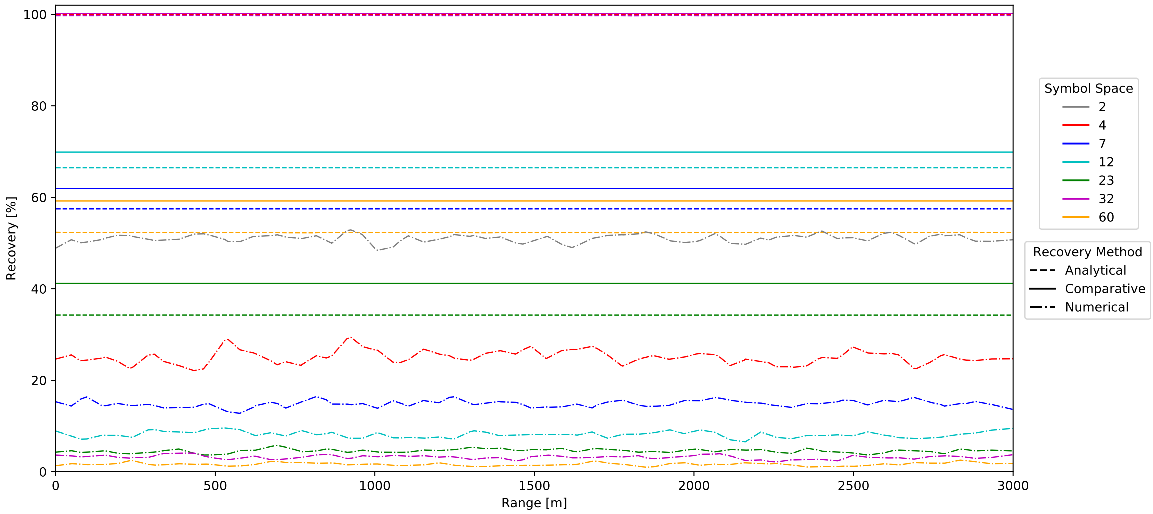

Figure 4.9. Performance of Three Symbol Recovery Methods in a Model Shallow Channel.

When synchronization and equalization are assumed, recovery is apparently dictated by the number of bits per symbol. In our encoding scheme, the MSB is also the smallest interval in the subdivision scheme, and therefore the most prone to error. In general, it seems that as more possible symbols require the most significant bit, performance degrades. (Note: the minimum bits in our scheme is four, and the two additional higher value symbols [e.g., 60 and 61 in the 60-symbol encoding] are generated and reserved for synchronization.) While the assumptions of synchronization and equalization are by no means trivial and will need to be solved for an operational system, our results nonetheless indicate that our analytical recovery method could contribute to a promising steganographic communication scheme.

Equalization Assumptions

Notably, neither Figure 4.8 nor Figure 4.9 show a decrease in recovery performance as range increases. While this behavior would normally be expected, our assumption of perfect equalization counteracts range-dependent adverse channel effects such as scattering, absorption, and spreading. Figure 4.10 and Figure 4.11 show how different equalization assumptions affect recovery in our example deep channel and shallow channel, respectively. For this case study, we use the parameters shown in Table 4.5.

Figure 4.10 shows recovery percentage versus range in the deep channel for each of several

Table 4.4. Average Symbol Recovery Performance in a Model Shallow Channel.

Symbol Space	Method	Recovery [%]
2	Analytical	99.99
	Comparative	100.0
	Numerical	50.99
4	Analytical	99.95
	Comparative	100.0
	Numerical	25.06
7	Analytical	57.47
	Comparative	61.92
	Numerical	14.87
12	Analytical	66.46
	Comparative	69.89
	Numerical	8.144
23	Analytical	34.26
	Comparative	41.20
	Numerical	4.563
32	Analytical	99.73
	Comparative	100.0
	Numerical	3.189
60	Analytical	52.30
	Comparative	59.20
	Numerical	1.643

equalization assumptions. We test the following assumptions:

- no amplitude or phase equalization (None);
- no amplitude equalization, but perfect phase equalization ($e^{\jmath\theta_i}$);
- perfect amplitude equalization, but no phase equalization (H_i);
- no amplitude equalization, but phase equalization using the transfer function from the previous symbol ($e^{\jmath\theta_{i-1}}$);
- amplitude equalization from the previous symbol and no phase equalization (H_{i-1});
- perfect phase equalization, but previous amplitude equalization ($H_{i-1}e^{\jmath\theta_i}$);
- perfect amplitude equalization, but phase equalization from the last symbol ($H_i e^{\jmath\theta_{i-1}}$);

Table 4.5. Equalization Assumption Comparison Parameters.

Parameter	**Values**
Symbol Space, T, α, SNR	4, 0.5 s, 0.32, 50 dB
Method	Analytical
Equalization Assumptions	None, $e^{j\theta_i}$, H_i, $e^{j\theta_{i-1}}$, H_{i-1}, $H_{i-1}e^{j\theta_i}$, $H_ie^{j\theta_{i-1}}$, $H_{i-1}e^{j\theta_{i-1}}$
Channel	Deep Channel
Transmitter Depth	180 m
Receiver Depth	180 m
Range	1 m to 1000 m, in 25 meter increments
Channel	Shallow Channel
Transmitter Depth	60 m
Receiver Depth	60 m
Range	1 m to 3000 m, in 25 meter increments

and

- phase and amplitude equalization based on the transfer function for the previous symbol only ($H_{i-1}e^{j\theta_{i-1}}$).

The effects of each assumption are shown by different combinations of line-style and color.

This shows the importance of correct phase equalization on symbol recovery. While correct amplitude equalization has an almost negligible positive effect on recovery, correct phase equalization is necessary for any successful transmission over appreciable distance. Interestingly, equalization based on the transfer function in the previous period shows a constant poor performance—even under-performing no equalization at all. This behavior is due to the random noise generated as part of the channel simulation, which guarantees that the phases within each period will be different.

Figure 4.11 shows recovery percentage vs. range in the shallow channel for each of our equalization assumptions. We use the same set of assumptions and the same color scheme to graph their affects.

These results validate the importance of equalization on recovery performance—appropriate

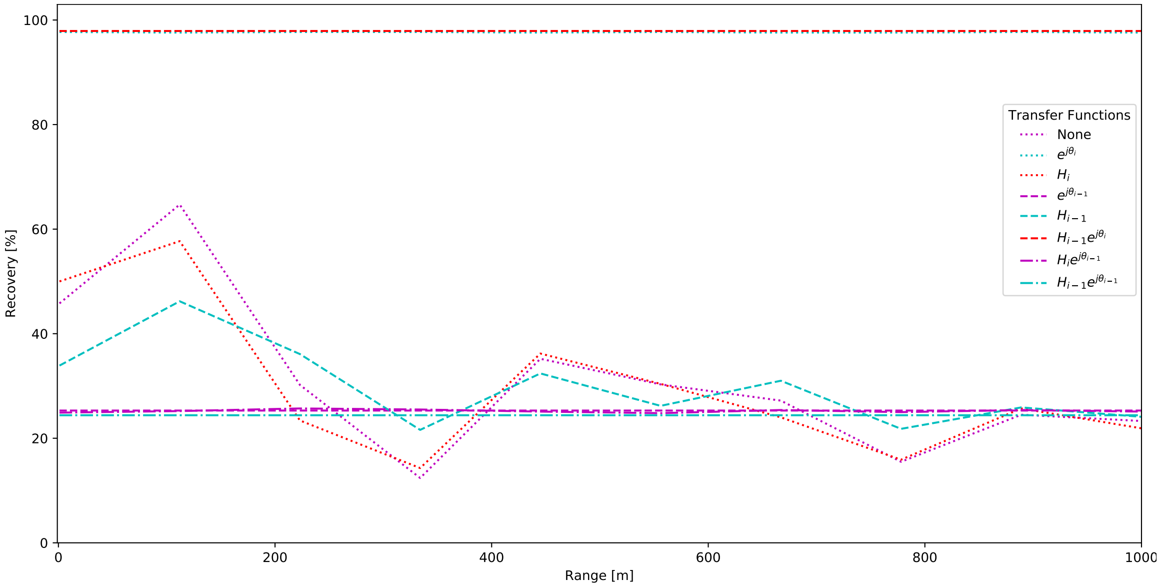

Figure 4.10. Effect of Equalization Assumptions on Symbol Recovery versus Range in a Model Deep Channel.

phase equalization is not merely necessary for adequate performance, but excellent performance over great distance is possible so long as phase equalization is achieved. Moreover, these graphs make visually apparent the increased volatility of the shallow channel versus the deep-water channel.

Bit Rate

The theoretical upper bound on the number of bits (M) in our scheme is given by

$$\lfloor(\lfloor(\frac{2^{B-1}}{3^{B-1}\sum_{k=1}^{B}[(2/3)^k]} * 2048 * T) * 0.25) = 1 \tag{4.4}$$

where B is the number of bits and T is the period duration. This equation ensures that the guard interval is at least of size 1, which gives a maximum bit rate of 12 bps for a 0.5 s period. As we see in our results, the actual bound is lower in practice since we determine the correct bit value by MSE. As the number of bits increases, the size of the smallest data interval shrinks, and recovery performance degrades as the sample size becomes too small to overcome individual errors. However, Equation 4.4 indicates that both data rate and recovery performance theoretically could be improved by increasing the period. Figure 4.12 validates

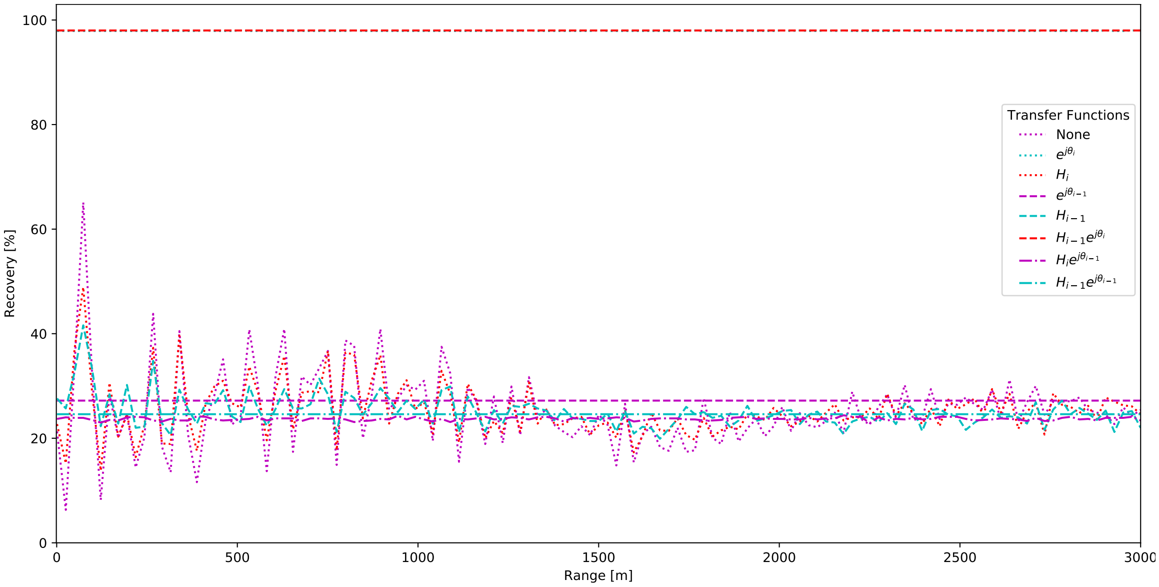

Figure 4.11. Effect of Equalization Assumptions on Symbol Recovery versus Range in a Model Shallow Channel.

this prediction to a degree. The Deep Channel graph gives results using the open-ocean model and the Shallow Channel graph shows results for the shallow channel model. Only the analytical recovery method is used, and different periods are represented by different line styles, with the number of encoded symbols shown by different colors.

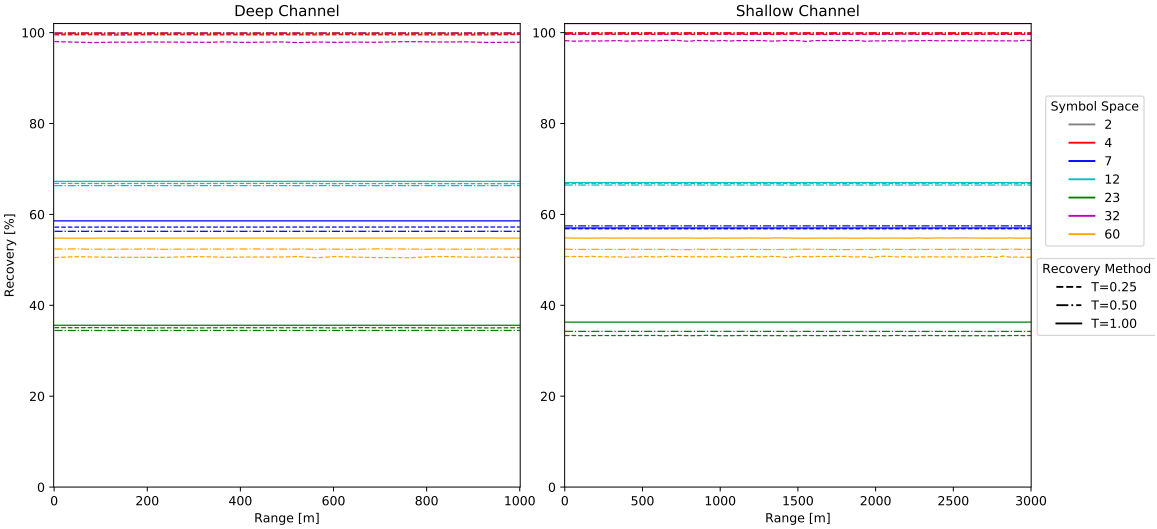

Figure 4.12. Symbol Recovery Performance with Different Periods.

While recovery performance is in general improved by increasing the period, the improvement is insufficient to surmount the loss in overall transmission rate due to decrease in symbol rate.

4.3 Summary

In this chapter, we described the design parameters of our experiments, presented the steganographic security of our embedding scheme, reviewed the results of simulated communications through various model channels, and briefly discussed the effects of equalization assumptions and bit rate considerations in our system. We found that correct synchronization and phase equalization is necessary for adequate performance; however, when synchronization and equalization are achieved, high rates of recovery are possible at long ranges. We also showed that longer periods could theoretically result in higher transmission rates. In Chapter 5, we summarize our findings and present opportunities for future research.

CHAPTER 5: Conclusions and Future Work

In this thesis, we discussed UACs and Ferrao's frequency domain implementation of Passerieux's steganographic technique, and described how a successful steganographic system could improve the operational capabilities of the USN and DOD. We discussed detection, synchronization, and equalization in depth and presented the extant research on these subjects.

This thesis disproved assertions regarding synchronization and recovery made by Passerieux [2], [3] and offered new work based on Ferrao's steganographic scheme [1] that increases bit capacity and provides a means of symbol recovery. We presented the theory and mathematics of three recovery solutions, tested the performance of these solutions in a variety of simulated acoustic channels, and evaluated the steganographic security of our system.

5.1 Key Findings

Passerieux's statement that the transmitted symbol is proportional to the phase of the time domain cross correlation in the period [2], [3] can be refuted by showing the phase is a function of, but not proportional to, the transmitted symbol. Further, peaks in the time domain cross correlation are non-monotonic and merely the average power of the cross correlation period, rebutting Passerieux's statement that synchronization is indicated by peaks in the time domain cross-correlation spaced at the interval length [2], [3].

While correct synchronization and phase equalization is necessary for adequate performance, it is possible to achieve bit rate improvement better than eight bps while maintaining desirable LPI/LPD characteristics—but we did not achieve BER less than 10^{-3}. Once assumptions of synchronization and equalization are applied, we are able to achieve successful recovery approaching 12 bps at ranges of 1 km or more without negatively affecting steganographic covertness, though better bit rates are theoretically achievable by increasing the period.

The idea that the indefinite integral of the numerical derivative of the cross-correlation phase existed and that such an integral could be numerically approximated was not supported by our research. Since the cross-correlation function generates values at equally spaced sample points, the numerical derivative is merely a collection of linear local approximations joined by discontinuities, where the discontinuities are aligned to the sample points. When we integrate numerically, our sample points are the discontinuity points. Moreover, since we are specifically interested in the integral within a finite interval, the integral must necessarily be definite.

5.2 Recommendations for Future Work

Based on our results, we primarily recommend the following areas for additional research focus:

1. Determining a method for signal synchronization (i.e., period alignment), as this is a prerequisite for any recovery solution.
2. Implementing and comparing equalization techniques, as successful equalization is critical for the performance of our recovery technique.
3. Investigating the maximum practical bit rate.
4. Increasing understanding of the communication system's limits via testing in a more realistic simulated channel by improving the MMPE input parameters, using MMPE's "accuracy" option, and implementing spectrum-dependent noise.
5. Improve understanding of the breadth of system applicability by testing with a variety of cover signals.
6. Evaluation of the use of a Viterbi or HMM algorithm, which may be more effective for symbol determination than MSE.

Other areas of recommended future research include:

1. Evaluating performance using other existing models, modeling techniques, and/or simulated channels.
2. Experimenting with various frequency bands to determine performance tradeoffs.
3. Developing a method to directly handle Doppler effects.
4. Determining a division scheme for breaking up the period into data and guard intervals

that maximizes bit rate while maintaining sufficient steganographic covertness.

5. Developing error correction and OSI Layer 2 and 3 protocols to enable interoperability with existing equipment.
6. Modifying the recovery algorithm to encode bits using Quadrature Phase Shift Keying (QPSK) or Asymmetric Phase Shift Keying (APSK), and evaluating the operational and security tradeoffs.
7. Rigorously evaluating the security of our system via steganalysis and information theory techniques.
8. Implementing and testing a complete steganographic system with receiver and transmitter.
9. Performing real-time testing in actual underwater environments.
10. Developing software designed for usability by communications systems operators.

5.3 Conclusion

In this thesis, we showed that recovery of symbols encoded in an LPI/LPD acoustic steganography scheme is possible based on locally constant variables (i.e., without knowledge of the cover signal.) However, the success of our recovery system relies on accurate synchronization and equalization techniques, which we merely assumed. Thus, in order to make this system practical, significant work remains to generate synchronization and equalization solutions.

THIS PAGE INTENTIONALLY LEFT BLANK

List of References

[1] R. Ferrao, "Underwater masked carrier acoustic communication: modeling and analysis," M.S. thesis, Naval Postgraduate School, Monterey, CA, 2018.

[2] J. Passerieux, "Stealth underwater acoustic communications based upon steganography techniques," in *2nd International Conference and Exhibition on Underwater Acoustics*, Rhodes, Greece, 2014, pp. 1199–1206.

[3] J. Passerieux, "Method and system for acoustic communication," U.S. Patent 15/319,703, May 25, 2017.

[4] F. Socheleau, C. Laot, and J. Passerieux, "Concise derivation of scattering function from channel entropy maximization," *IEEE Transactions on Communications*, vol. 58, no. 11, pp. 3098–3103, 2010, https://doi.org/10.1109/TCOMM.2010.091310.090247.

[5] K. Smith, "Convergence, stability, and variability of shallow water acoustic predictions using a split-step Fourier parabolic equation model," *Journal of Computational Acoustics*, vol. 9, no. 1, pp. 243–285, 2001, https://doi.org/10.1142/S0218396X01000401.

[6] P. Barsocchi, "Channel models for terrestrial wireless communications: A survey," CNR-ISTI, Pisa, Italy, Tech. Rep. 2006-TR-16, 2006.

[7] L. Kinsler, A. Frey, A. Coppens, and J. Sanders, *Fundamentals of Acoustics*, 4th ed. Hoboken, NJ: John Wiley & Sons, 1999.

[8] G. Howe, P. Tarbit, O. Hinton, B. Sharif, and A. Adams, "Sub-sea acoustic remote communications utilising an adaptive receiving beamformer for multipath suppression," in *OCEANS CONF REC IEEE*, Brest, France, 1994, vol. 1, pp. 313–316.

[9] J. Dhanoa and R. Ormondroyd, "Combined differential Doppler and time delay compensation for an underwater acoustic communication system," in *OCEANS '02 MTS/IEEE*, 2002, vol. 1, pp. 581–587, https://doi.org/10.1109/OCEANS.2002.1193332.

[10] C. Tellambura and V. Bhargava, "Convolutionally coded binary PSAM for Rayleigh fading channels," *Electronics Letters*, vol. 28, no. 16, pp. 1503–1505, 1992, https://doi.org/10.1049/el:19920955.

[11] S. Joshi, “Coded-OFDM in various multipath fading environments,” in *2010 2nd International Conference on Computer and Automation Engineering (ICCAE)*, Singapore, 2010, vol. 3, pp. 127–131, https://doi.org/10.1109/ICCAE.2010.5452071.

[12] H. Rustad, “A lightweight protocol suite for underwater communication,” in *2009 International Conference on Advanced Information Networking and Applications Workshops*. IEEE Publishing, 2009, pp. 1172–1177, https://doi.org/10.1109/WAINA.2009.173.

[13] D. Marinakis, K. Wu, N. Ye, , and S. Whitesides, “Network optimization for lightweight stochastic scheduling in underwater sensor networks,” *IEEE Transactions On Wireless Communications*, vol. 11, no. 8, pp. 2786–2795, 2012, https://doi.org/10.1109/TWC.2012.052412.110740.

[14] M. Feder and J. Catipovic, “Algorithms for joint channel estimation and data recovery—application to equalization in underwater communications,” *IEEE Journal of Oceanic Engineering*, vol. 16, no. 1, pp. 42–55, 1991, https://doi.org/10.1109/48.64884.

[15] M. Shinego, “Underwater acoustic data communications for autonomous platform command, control and communications,” DTIC, Tech. Rep. 8346749, 2001, www.dtic.mil/dtic/tr/fulltext/u2/a386718.pdf.

[16] J. Proakis, E. Sozer, J. Rice, and M. Stojanovic, “Shallow water acoustic networks,” *IEEE Communications Magazine*, vol. 39, no. 11, pp. 114–119, 2001, https://doi.org/10.1109/35.965368.

[17] M. Aydogmus, “Multireceiver acoustic communications in time-varying environments,” M.S. thesis, Naval Postgraduate School, Monterey, CA, 2014.

[18] I. Burdinskiy, I. Karabanov, M. Linnik, and A. Mironov, “Processing of phase-shift keyed pseudo noise signals of underwater acoustic systems with the Doppler effect,” in *2015 International Siberian Conference on Control and Communications (SIBCON)*. IEEE, 2015, pp. 1–4, https://doi.org/10.1109/SIBCON.2015.7147091.

[19] S. Aliesawi, C. Tsimenidis, B. Sharif, and M. Johnston, “Iterative multiuser detection for underwater acoustic channels,” *IEEE Journal Of Oceanic Engineering*, vol. 36, no. 4, pp. 728–744, 2011, https://doi.org/10.1109/JOE.2011.2164954.

[20] M. Stojanovic, “Recent advances in high-speed underwater acoustic communications,” *IEEE Journal Of Oceanic Engineering*, vol. 21, no. 2, pp. 125–136, 1996, https://doi.org/10.1109/48.486787.

[21] I. Akyildiz, D. Pompili, and T. Melodia, "State of the art in protocol research for underwater acoustic sensor networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 11, no. 4, pp. 11–22, 2007, https://doi.org/10.1145/1347364.1347371.

[22] M. Stojanovic, *Underwater Acoustic Communication*. Hoboken, NJ: John Wiley & Sons, 2015, pp. 1–12. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W5411.pub2

[23] S. Liu and A. Song, "Optimization of LDPC codes over the underwater acoustic channel," *International Journal of Distributed Sensor Networks*, vol. 12, no. 2, pp. 1–10, 2016, https://doi.org/10.1155/2016/8906985.

[24] M. Stojanovic, "Underwater acoustic communications," in *Professional Program Proceedings of Electro/95 International*. IEEE, June 1995, pp. 435–440.

[25] J. Catipovic and L. Freitag, "High data rate acoustic telemetry for moving ROVs in a fading multipath shallow water environment," in *Symposium on Autonomous Underwater Vehicle Technology*, Washington, D.C., 1990, pp. 296–303.

[26] G. Wenz, "Acoustic ambient noise in the ocean: Spectra and sources," *The Journal of the Acoustical Society of America*, vol. 34, no. 12, pp. 1936–1956, 1962, https://doi.org/10.1121/1.1909155.

[27] A. Bessios and F. Caimi, "Multipath compensation for underwater acoustic communication," in *OCEANS CONF REC IEEE*, Brest, France, 1994, vol. 1, pp. 317–322.

[28] G. Yang, Q. Guo, D. Huang, J. Yin, and M. Zheng, "Kalman filter-based chip differential blind adaptive multiuser detection for variably mobile asynchronous underwater multiuser communications," *IEEE Access*, vol. 6, p. 49646–49653, 2018, https://doi.org/10.1109/ACCESS.2018.2868475.

[29] G. Eynard and C. Laot, "Blind Doppler compensation scheme for single carrier digital underwater communications," in *OCEANS 2008*. IEEE, 2008, pp. 1–5, https://doi.org/10.1109/OCEANS.2008.5152066.

[30] T. Austin, "The application of spread spectrum signaling techniques to underwater acoustic navigation," in *Proceedings of the 1994 Symposium on Autonomous Underwater Vehicle Technology, 1994 (AUV '94)*. IEEE publishing, 1994, pp. 443–449, https://doi.org/10.1109/AUV.1994.518658.

[31] J. Aparicio and T. Shimura, "Asynchronous detection and identification of multiple users by multi-carrier modulated complementary set of sequences," *IEEE Access*, vol. 6, p. 22054–22069, 2018, https://doi.org/10.1109/ACCESS.2018.2828500.

[32] K. Lowham, “Synchronization analysis and simulation of a standard IEEE 802.11g OFDM signal,” M.S. thesis, Naval Postgraduate School, Monterey, CA, 2004.

[33] B. Woodward and H. Sari, “Digital underwater acoustic voice communications,” *IEEE Journal Of Oceanic Engineering*, vol. 21, no. 2, pp. 181–192, 1996, https://doi.org/10.1109/48.486793.

[34] J. Locke and P. White, “The performance of methods based on the fractional Fourier transform for detecting marine mammal vocalizations,” *The Journal of the Acoustical Society of America*, vol. 130, no. 4, pp. 1974–1984, 2011, https://doi.org/10.1121/1.3631664.

[35] J. Ling, H. He, J. Li, W. Roberts, and P. Stoica, “Covert underwater acoustic communications: Transceiver structures, waveform designs and associated performances,” in *OCEANS 2010*. IEEE publishing, 2010, pp. 1–10, https://doi.org/10.1109/OCEANS.2010.5663840.

[36] K. Howland, “Signal detection and frame synchronization of multiple wireless networking waveforms,” M.S. thesis, Naval Postgraduate School, Monterey, CA, 2007.

[37] T. Goh, J. Liu, and B. Soong, “Deterministic signal detection: a hybrid approach,” in *Singapore ICCS/ISITA ’92*. Singapore: IEEE publishing, 1992, pp. 385–389, https://doi.org/10.1109/ICCS.1992.254924.

[38] C. Yang, J. Qu, S. Li, and S. Mao, “Signal detection with higher-order statistics,” in *3rd International Conference on Signal Processing, 1996*. IEEE publishing, 1996, pp. 545–548, https://doi.org/10.1109/ICSIGP.1996.567322.

[39] E. Hoppe and M. Roan, “Principal component analysis for emergent acoustic signal detection with supporting simulation results,” *The Journal of the Acoustical Society of America*, vol. 130, no. 4, pp. 1962–1973, 2011, https://doi.org/10.1121/1.3628324.

[40] K. Lopatka, J. Kotus, and A. Czyzewsk, “Detection, classification and localization of acoustic events in the presence of background noise for acoustic surveillance of hazardous situations,” *Multimedia Tools and Applications*, vol. 75, no. 17, pp. 10 407–10 439, 2016, https://doi.org/10.1007/s11042-015-3105-4.

[41] J.-Z. Wang, P.-S. Zhou, P. Catipovic, and P. Willett, “Asynchronous multiuser reception for OFDM in underwater acoustic communications,” *IEEE Transactions On Wireless Communications*, vol. 12, no. 3, pp. 1050–1061, 2013, https://doi.org/10.1109/TWC.2013.011713.120075.

[42] S. Aliesaw, C. Tsimenidis, B. Sharif, and M. Johnston, “Soft Rake and DFE based IDMA systems for underwater acoustic channels,” in *Sensor Signal Processing for Defence (SSPD 2010)*, 2010, pp. 1–5.

[43] S. Yurdakul and S. Senturk, “Performance of a digital data transmission system using matched filter processing of an auxiliary signal for synchronization,” M.S. thesis, Naval Postgraduate School, Monterey, CA, 1979.

[44] K. Kung and K. Parhi, “Optimized joint timing synchronization and channel estimation for OFDM systems,” *IEEE Wireless Communications Letters*, vol. 1, no. 3, pp. 149–152, 2012, https://doi.org/10.1109/WCL.2012.022812.120015.

[45] D. Yachil, J. Davidson, and B. Bobrovsky, “Low complexity multi-channel synchronization for satellite systems with adjacent channel interference,” *International Journal of Satellite Communications and Networking*, vol. 24, no. 1, pp. 1–22, 2006, https://doi.org/10.1002/sat.825.

[46] J. Grotz, B. Ottersten, and J. Krause, “Joint channel synchronization under interference limited conditions,” *IEEE Transactions On Wireless Communications*, vol. 6, no. 10, pp. 3781–3789, 2007, https://doi.org/10.1109/TWC.2007.060099.

[47] D. Brady and J. Catipovic, “Adaptive multiuser detection for underwater acoustical channels,” *IEEE Journal Of Oceanic Engineering*, vol. 19, no. 2, pp. 158–165, 1994, https://doi.org/10.1109/48.286637.

[48] M. Stojanovic, J. Catipovic, and J. Proakis, “Phase-coherent digital communications for underwater acoustic channels,” *IEEE Journal Of Oceanic Engineering*, vol. 19, no. 1, pp. 100–111, 1994, https://doi.org/10.1109/48.289455.

[49] U. Ali, M. Kieffer, and P. Duhamel, “Joint protocol-channel decoding for robust frame synchronization,” *IEEE Transactions On Communications*, vol. 60, no. 8, pp. 2326–2335, 2012, https://doi.org/10.1109/TCOMM.2012.061212.11041.

[50] J. Proakis, “Adaptive equalization techniques for acoustic telemetry channels,” *IEEE Journal Of Oceanic Engineering*, vol. 16, no. 1, pp. 21–31, 1991, https://doi.org/10.1109/48.64882.

[51] L. Zhong and N. Xiao-Ling, “Comparison of equalization algorithms for underwater acoustic channels,” in *2012 2nd International Conference on Computer Science and Network Technology (ICCSNT)*. Rome, Italy: IEEE, 2012, pp. 2059–2063, https://doi.org/10.1109/ICCSNT.2012.652632.

[52] D. Kari, M. Sayin, and S. Kozat, “A new robust adaptive algorithm for underwater acoustic channel equalization,” 2015.

[53] A. Youcef, C. Laot, and K. Amis, “Adaptive frequency-domain equalization for underwater acoustic communications,” in *2011 IEEE OCEANS — Spain*. IEEE publishing, 2011, pp. 1–6, https://doi.org/10.1109/Oceans-Spain.2011.600362.

[54] B. Nott, “Long-endurance maritime surveillance with ocean glider networks,” M.S. thesis, Naval Postgraduate School, Monterey, CA, 2015.

[55] E. Calvo and M. Stojanovic, “Efficient channel-estimation-based multiuser detection for underwater CDMA systems,” *IEEE Journal Of Oceanic Engineering*, vol. 33, no. 4, pp. 502–512, 2008, https://doi.org/10.1109/JOE.2008.2005355.

[56] A. Song and M. Badiey, “Time reversal acoustic communication for multiband transmission,” *The Journal of the Acoustical Society of America*, vol. 131, no. 4, pp. EL283–EL288, 2012, https://doi.org/10.1121/1.3690965.

[57] C. Anton-Haro, J. Fonollosa, Z. Zvonar, and J. Fonollosa, “Blind adaptive multiuser detection with probabilistic algorithms: application to underwater acoustics,” in *1997 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP-97)*. IEEE publishing, 1997, vol. 5, pp. 3889–3892, https://doi.org/10.1109/ICASSP.1997.604750.

[58] W. Rao, W. Tan, Y. Li, and H. Gao, “New modified constant modulus algorithm for underwater acoustic communications,” in *2011 International Conference on Internet Computing & Information Services (ICICIS)*. IEEE publishing, 2011, pp. 563–566, https://doi.org/10.1109/ICICIS.2011.149.

[59] C. Anton-Haro, J. Fonollosa, Z. Zvonar, and J. Fonollosa, “Probabilistic algorithms for blind adaptive multiuser detection,” *IEEE Transactions on Signal Processing*, vol. 46, no. 11, pp. 2953–2966, 1998, https://doi.org/10.1109/78.726809.

[60] C. Tseng, F. Lu, F. Chen, and S. Wu, “Compensation of multipath fading in underwater spread-spectrum communication systems,” in *Proceedings of the 1998 International Symposium on Underwater Technology*. IEEE publishing, 1998, pp. 453–458, https://doi.org/10.1109/UT.1998.670153.

[61] J. Tong, P. Li, and X. Ma, “Superposition coded modulation with peak-power limitation,” *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2562–2576, 2009, https://doi.org/10.1109/TIT.2009.2018224.

[62] K. Saraswathi and S. Ravishankar, “Efficient estimation and compensation of Doppler shift for OFDM signals in underwater communications,” in *2016 Sixth International Symposium on Embedded Computing and System Design (ISED)*. IEEE, Dec. 2016, pp. 137–141.

[63] B. Sharif, J. Neasham, O. Hinton, and A. Adams, “Closed loop Doppler tracking and compensation for non-stationary underwater platforms,” in *OCEANS 2000 MTS/IEEE Conference and Exhibition*. IEEE publishing, 2000, vol. 1, pp. 371–375, https://doi.org/10.1109/OCEANS.2000.881287.

[64] C. Z. Huang and C. Balanis, “The MMSE algorithm and mutual coupling for adaptive arrays,” *IEEE Transactions on Antennas and Propagation*, vol. 56, no. 2, pp. 1292–1296, 2008, https://doi.org/10.1109/TAP.2008.922619.

[65] J. Catipovic and L. Freitag, “Spatial diversity processing for underwater acoustic telemetry,” *IEEE Journal Of Oceanic Engineering*, vol. 16, no. 1, pp. 86–97, 1991, https://doi.org/10.1109/48.64888.

[66] M. Stojanovic, J. Catipovic, and J. Proakis, “Reduced-complexity spatial and temporal processing underwater acoustic communication signals,” *The Journal of the Acoustical Society of America*, vol. 98, no. 2, pp. 961–972, 1995, https://doi.org/10.1121/1.413521.

[67] G. Wibisono and I. Sasase, “Trellis coded PSK modulation with diversity on correlated Rayleigh fading channel,” in *Proceedings of ICUPC - 5th International Conference on Universal Personal Communications*. IEEE publishing, 1996, vol. 2, pp. 538–542, https://doi.org/10.1109/ICUPC.1996.562631.

[68] L. Goldfeld and D. Wulich, “Multichannel system with optimal diversity reception and erasures-correction decoder for Rayleigh fading channels,” *IEEE Transactions on Communications*, vol. 48, no. 12, pp. 1979–1982, 2000, https://doi.org/10.1109/26.891205.

[69] J. Catipovic and A. Baggeroer, “Performance of sequential decoding of convolutional codes over fully fading ocean acoustic channels,” *IEEE Journal Of Oceanic Engineering*, vol. 15, no. 1, pp. 1–7, 1990, https://doi.org/10.1109/48.46830.

[70] T. Müller and H. Rohling, “Channel coding for narrow-band Rayleigh fading with robustness against changes in Doppler spread,” *IEEE Transactions on Communications*, vol. 45, no. 2, pp. 148–151, 1997, https://doi.org/10.1109/26.554360.

[71] U. Hansson and T. Aulin, “Channel symbol expansion diversity-improved coded modulation for the Rayleigh fading channel,” in *Proceedings of ICC/SUPERCOMM ’96 - International Conference on Communications*. IEEE publishing, 1996, vol. 2, pp. 891–895, https://doi.org/10.1109/ICC.1996.541308.

[72] S. G. Johnson. (2011, May). Notes on FFT-based Differentiation. MIT, Dept. of Applied Mathematics. Cambridge, MA. [Online]. Available: https://math.mit.edu/~stevenj/fft-deriv.pdf

[73] K. Tanaka, M. Sugihara, and K. Murota, “Numerical indefinite integration by double exponential sinc method,” *Mathematics of Computation*, vol. 74, no. 250, pp. 655–679, 2005.

[74] H. Takahasi and M. Mori, “Double exponential formulas for numerical integration,” *Publications of the Research Institute for Mathematical Sciences*, vol. 9, no. 3, pp. 721–741, 1973.

[75] B. Rowe, M. Jarvis, R. Mandelbaum, G. Bernstein, J. Bosch, M. Simet, and et al., “Galsim: The modular galaxy image simulation toolkit,” *Astronomy and Computing*, vol. 10, pp. 121 – 150, 2015.

[76] MATLAB, version R2017b. The MathWorks, Inc. [Online]. Available: https://www.mathworks.com

[77] Cetacean sounds. NOAA. [Online]. Available: https://swfsc.noaa.gov/textblock.aspx?Division=PRD&ParentMenuId=148&id=5776

[78] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, UK: Cambridge University Press, 2010.

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California