RF STEGANOGRAPHY TO SEND HIGH SECURITY MESSAGES THROUGH SDRs

A Thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Electrical Engineering

by

MEGAN K. PATRICK
B.S.E.E., Michigan Technological University, 2020

2024
Wright State University

WRIGHT STATE UNIVERSITY
COLLEGE OF GRADUATE PROGRAMS AND HONORS STUDIES

April 17, 2024

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY Megan K. Patrick ENTITLED RF Steganography to Send High Security Messages through SDRs BE ACCEPTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF Master of Science in Electrical Engineering.

Dr. Zhiqiang Wu, Ph.D.
Thesis Director

Dr. Yan Zhuang, Ph.D.
Chair, Electrical Engineering
Department

Committee on Final Examination:

Dr. Xiaodong Zhang, Ph.D.

Dr. Bin Wang, Ph.D.

Dr. Zhiqiang Wu, Ph.D.

Paula Bubulya, Ph.D.
Interim Dean, College of
Graduate Programs & Honors Studies

ABSTRACT

Patrick, Megan, K. M.S.E. E., Department of Electrical Engineering, Wright State University, 2024. *RF Steganography to Send High Security Messages through SDRs.*

This research illustrates a high-security wireless communication method using a joint radar/communication waveform, addressing the vulnerability of traditional low probability of detection (LPD) waveforms to hostile receiver detection via cyclostationary processing (CSP). To mitigate this risk, RF steganography is used, concealing communication signals within linear frequency modulation (LFM) radar signals. The method integrates reduced phase-shift keying (RPSK) modulation and variable symbol duration, ensuring secure transmission while evading detection. Implementation is validated through software-defined radios (SDRs), demonstrating effectiveness in covert communication scenarios. Results include analysis of message reception and cyclostationary features, highlighting the method's ability to conceal messages from hostile receivers. Challenges encountered are discussed, with suggestions for future enhancements to improve real-world applicability.

Contents

List of Figures

Acknowledgment

I extend my deepest gratitude to my boyfriend, whose unwavering support has been crucial over the last few years. Kyle, your willingness to take care of Charlie on weekends and late nights allowed me the invaluable time I needed in the lab. Without your selflessness and understanding, achieving this milestone would have been impossible. Thank you for standing by me during one of the most demanding periods of my life; your love and encouragement have meant everything to me.

I am also grateful to Nicholas and Aaron for their tireless dedication to our work in the lab. Your commitment to putting in long hours, early mornings, and full weekends to ensure the success of our project has been remarkable. Together, we navigated through many challenges, and I am thankful for your collaboration and support.

Additionally, I want to express my gratitude to my coworkers, who have shown me such flexibility and understanding, allowing me to pursue my education and become a stronger member of our team. Your support and encouragement have made all the difference, and I am truly grateful for the opportunity to grow both personally and professionally.

Furthermore, I extend my appreciation to my advisor, Dr. Wu, Dr. Zhou, and the members of my committee for their guidance, encouragement, and the invaluable opportunity to pursue this research. Your expertise, feedback, and unwavering support have been critical in shaping this thesis.

Lastly, to all those who have contributed in ways seen and unseen, thank you for being part of this journey. Your support has been a cornerstone of my success, and I am deeply grateful for each of you.

Dedicated to

Kyle and Charlie

Introduction

1.1 Software-Defined Radios

A Universal Software Radio Peripheral (USRP) Software Defined Radio (SDR) refers to a radio frequency (RF) device that replaces the typical hardware components such as mixers, amplifiers, and modulators with software components of RF architecture to design, prototype, and deploy wireless systems with custom signal processing [4, 5]. National Instruments (NI) provides the NI-2901 USRP, a multi-use, tunable transceiver providing bus connectivity through USB [4, 5]. For the purpose of this thesis, the SDR described will be used as a transmitter and receiver to replicate a joint radar/communication waveform through the novel theory of RF steganography.

1.2 RF Steganography

In military and covert operations, securing RF communication is crucial. Low probability of detection (LPD) waveforms have been commonly used to conceal communications. However, LPD waveforms are susceptible to detection by hostile receivers using an advanced signal detection technique referred to as cyclostationary processing (CSP) [1, 2]. CSP analyzes signals based on their periodic characteristics or modulation patterns, compromising security [6, 7, 8]. To counter the vulnerability of LPD waveforms to CSP, Zhang

et al. propose RF steganography as an alternative approach [1, 2]. RF steganography conceals communication by embedding the intended waveform within another form of RF transmission. Specifically, this method hides digital communication within a radar signal, creating a joint waveform that functions as a radar, while providing concealed communication to intended receivers without generating modulation patterns that can be easily exploited [1, 2].

1.3 Cyclostationary Processing

Cyclostationary processing (CSP) is a fundamental technique in signal processing, particularly in the analysis of RF signals [6]. It exploits cyclostationary features, which are periodic characteristics present in man-made signals over both time and frequency domains [9, 10]. CSP algorithms, such as cyclic autocorrelation and cyclic spectral analysis, are used to extract useful information from signals by analyzing their cyclostationary properties [6].

In RF steganography, CSP plays a crucial role in both the design of covert communication waveforms and the detection of hidden information [1, 2]. By analyzing the cyclostationary features of LFM radar signals, CSP algorithms can distinguish between the radar waveform and the embedded communication signal [8]. This capability allows intended receivers to extract the hidden information while maintaining the LPD characteristics of the overall waveform.

One of the key mathematical tools used in CSP is the cyclic autocorrelation function, denoted by $R_{xx}(\tau, f)$, where τ represents the time lag and f represents the frequency offset [6]. Mathematically, the cyclic autocorrelation function is defined as [6]:

$$R_{xx}(\tau, f) = \lim_{T\to\infty} \frac{1}{T} \int_0^T x(t, \tau) \cdot x^*(t - \tau, f)\, dt$$

Here, $x(t, \tau)$ represents the time-shifted version of the signal $x(t)$ by τ, and $x^*(t-\tau, f)$

represents the complex conjugate of the signal $x(t)$ time-shifted by τ and frequency-shifted by f. The cyclic autocorrelation function provides valuable insights into the cyclostationary properties of the signal, enabling the detection and analysis of hidden communication within RF signals [6].

This work aims to physically realize the theoretical concept RF steganography proposed by Zhang et. al using software-defined radios (SDRs) [1, 2]. The joint radar/-communications waveform integrates variable symbol duration alongside linear frequency modulation. NI-2901 USRPs are used to validate the novel theory of RF steganography through the transmission and reception of these high-security messages [1, 2]. This document reviews the mathematical principles of LFM chirp-based communications with RPSK modulation and variable symbol duration in Section 2. Subsequently, Section 3 discusses the implementation of the RF steganography algorithm using USRPs and summarizes its effectiveness in communication from hostile receivers. Section 4 concludes the document with reflections on the study.

RF Steganography

This section discusses the fundamental mathematics of RF steganography and its significance in establishing secure communication channels. It examines the joint radar and communication concepts' roles in facilitating secure communication techniques. Understanding the RF steganography algorithm's basic components is vital for constructing a secure communication system between a transmitter and its intended receiver. These principles ensure the sensitive information remains confidential, even when facing potential interception by an unwanted receiver.

2.1 LFM Chirp

A linear frequency modulation (LFM) chirp is a signal that linearly increases or decreases its instantaneous frequency, $f_i(t)$, over a given time [11]. An LFM chirp signal is represented mathematically as

$$x(t) = A_c \cos(2\pi f_0 t + 2\pi \frac{k}{2} t^2 + \phi_I) \tag{2.1}$$

where A_c is the amplitude, ϕ_i is the initial phase [11]. The stopping frequency of the LFM chirp signal is represented as $f_i = f_0 + kT$, where f_0 is the starting frequency, k is the chirp rate, and T is the duration of the LFM pulse [2].

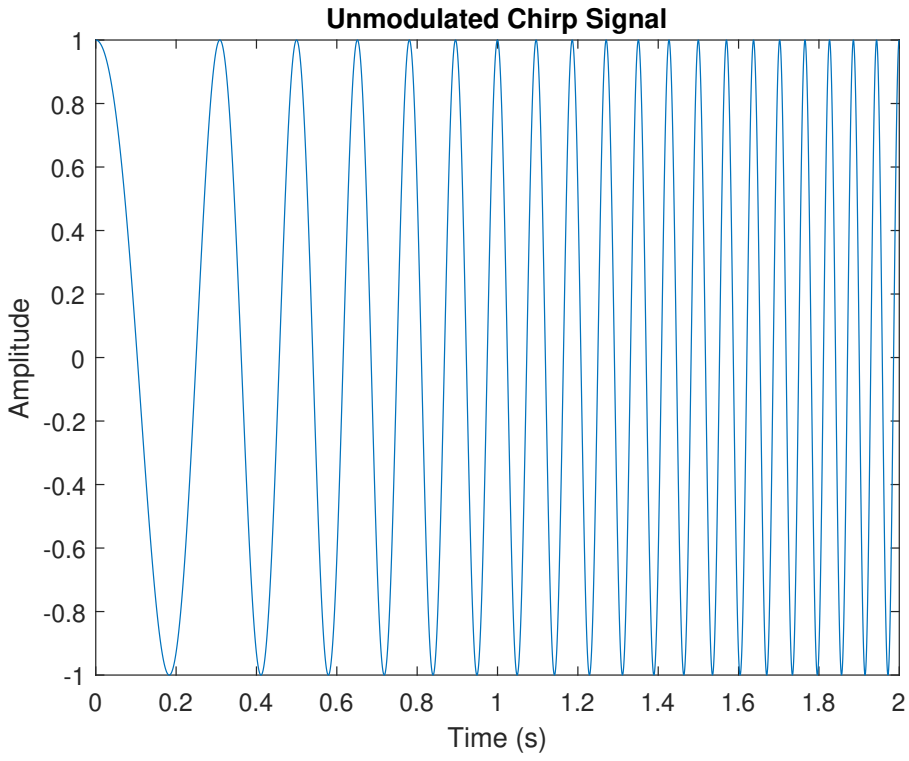

Figure 2.1: Example of an LFM chirp

In RF steganography, the LFM chirp serves as the foundational radar signal and modulation method [2]. Its appeal lies in its ability to reject interference while maintaining low Doppler sensitivity [1, 11]. Initially designed for communications, chirp-modulated signals became integral in concealing communication signals. Zhang et al. discovered that conventional phase-keying methods like BPSK are insufficient for hiding communication signals [1, 2]. Instead, a modified phase-keying method called binary reduced phase shift keying (BRPSK) is required, involving constellation points with a smaller phase difference [1, 2].

2.2 Binary Reduced Phase Shift Keying

Binary reduced phase-shift keying (BRPSK) is an embedded digital modulation scheme proposed by Zhang et. al [1, 2] in which phases such as 0 and π used in the signal constellation plot of a BPSK signal are replaced with signal constellations at a much smaller phase, which is notated ϕ. The BRPSK modulated LFM chirp signal is represented as

$$s(t) = \sum_{i=0}^{N-1} p_i(t - iT_b) \cdot A_c \cos(2\pi f_0 t + 2\pi \frac{k}{2} t^2 + \theta_i + \phi_I) \tag{2.2}$$

where $\theta_i = b_i \cdot \phi$, and $p_i(t)$ is the ith data symbol's pulse with pulse width $T_b i$ [2].

$$p_i(t) = \begin{cases} 1 & if \sum_{i-1}^{l=0} T_b i \leq t \leq \sum_{i-1}^{l=0} T_b i + T_b i \\ 0 & elsewhere \end{cases}$$

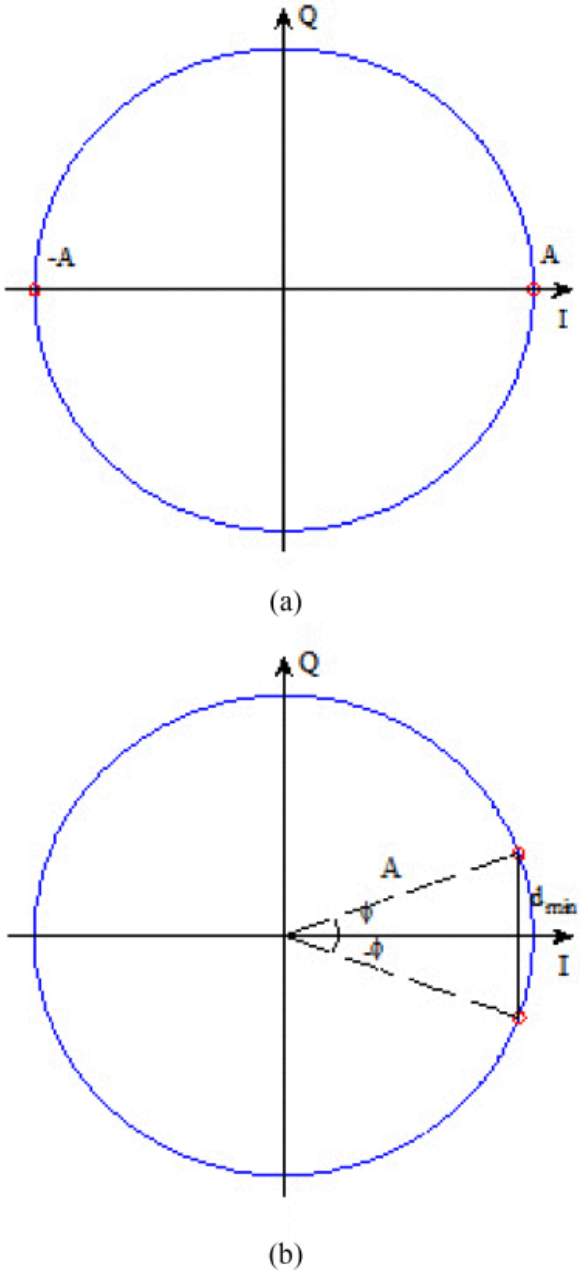

Figure 2.2: Constellation points for BPSK (a) and BRPSK (b) [1, 2]

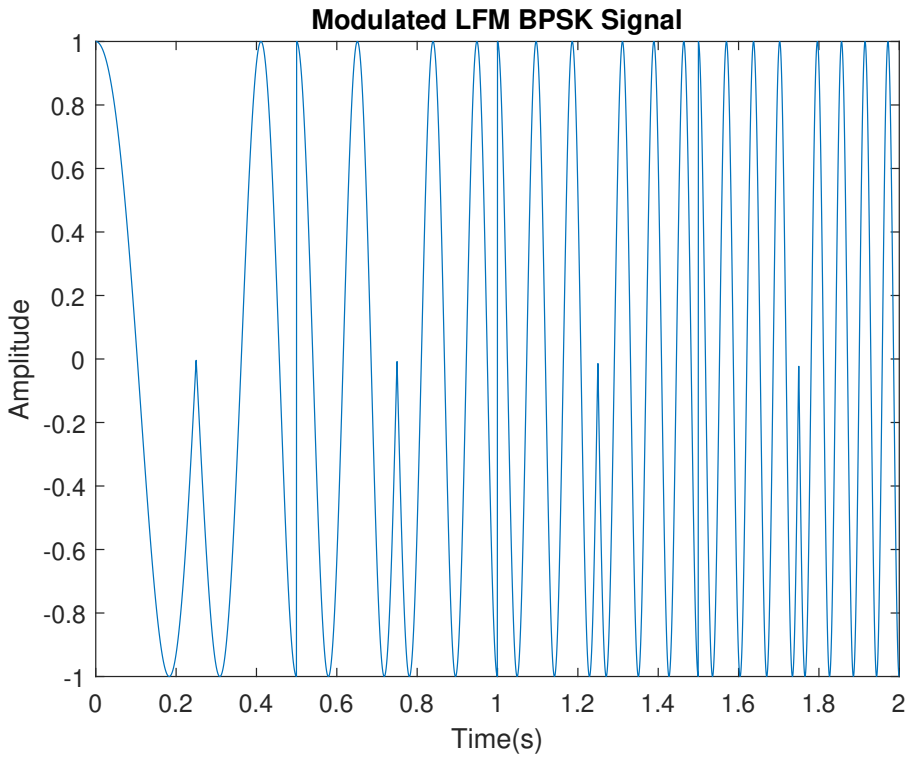

Figure 2.3: Example of LFM with BPSK, phase shifts are obvious

Adding BRPSK to the LFM chirp introduces a small phase difference, ϕ, in the modulation, as shown in Eq. 2.2. This modification aims to make the modulation harder to detect when combined with the digital signal. The resulting modulated chirp signal $s(t)$ closely resembles the original, unmodulated chirp as an effect [1, 2]. Zhang et al. studied methods to make this modulation less detectable by reducing remaining cyclostationary features of BRPSK, introducing a modulation scheme called variable symbol duration (VSD) modulation.

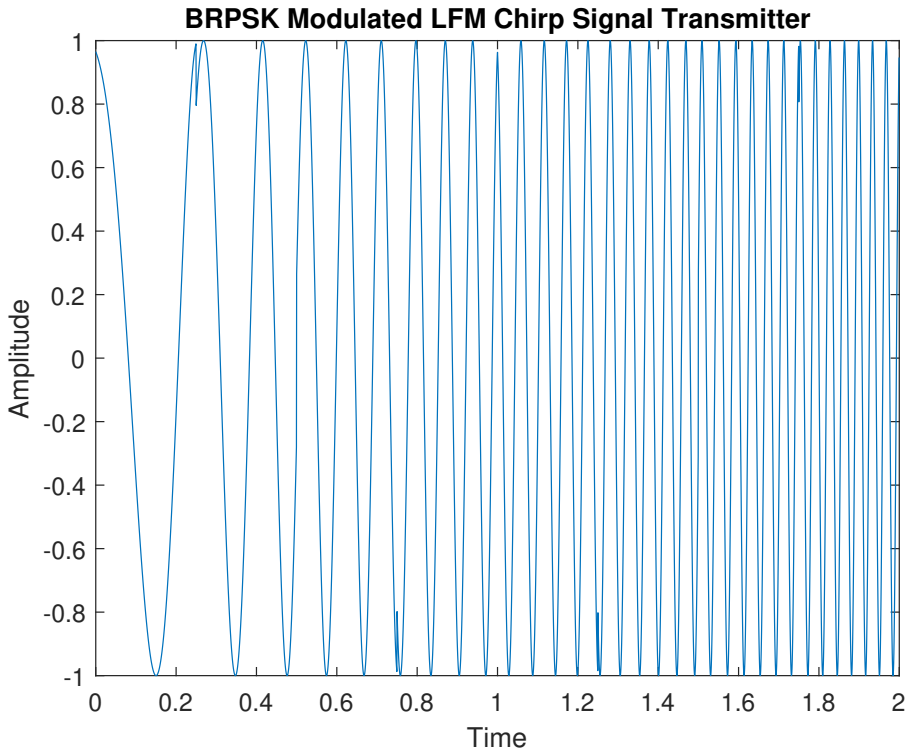

Figure 2.4: Example of LFM with ϕ = 15°BRPSK, phase shifts are less obvious

2.3 Variable Symbol Duration

Variable symbol duration follows a predetermined pseudorandom phase sequence denoted as ϕ_i [1, 2]. This sequence represents a random variable uniformly distributed between low and high angle values ϕ_L and ϕ_H, with a step size of $\Delta\phi$. The duration of each symbol, T_{b_i}, is calculated as follows [1, 2]:

$$T_{b_i} = T_b \frac{sin^2\left(\frac{\phi_L+\phi_H}{2}\right)}{sin^2(\phi_i)} \tag{2.3}$$

Here, T_b represents the symbol duration associated with the mean of the phases $\frac{\phi_L+\phi_H}{2}$. The symbol duration T_{b_i} is normalized to 1 at $E[\phi_i] = \frac{\phi_L+\phi_H}{2}$ [1, 2]. Data symbols with longer durations carry higher energy than shorter symbols, leading to correlating bit error rates (BERs) [1, 2]. Adjusting the phase difference parameter in BRPSK modulation allows

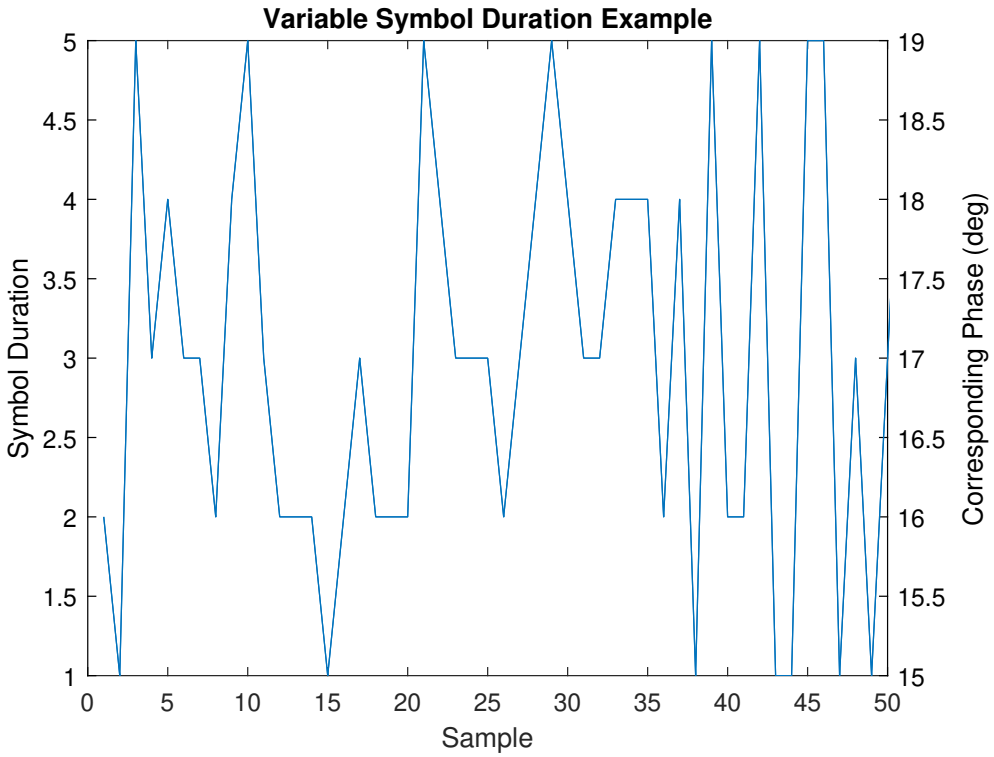

Figure 2.5: Example of random VSD and corresponding phase selection for five variable symbols

for compensation, ensuring a consistent BER despite varying symbol durations.

To avoid exploiting cyclic frequency components, the duration of each symbol is intentionally varied. These durations are chosen to be non-multiples of each other, eliminating a consistent symbol rate [1, 2]. This strategy, combined the LFM chirp, ensures that the radar/communications signal lacks exploitable cyclic frequency components. Only the transmitter and intended receiver know the specific symbol rate being used.

2.3.1 The Importance of Variable Symbol Duration

Expanding on the advantages of using variable symbol duration for RF steganography, it is important to address how this approach mitigates the risk of detection by exploiting cyclic frequency components. By intentionally varying the duration of each symbol in the communication waveform, irregularities are introduced that disrupt the periodicity typically

associated with cyclostationary signals. This deliberate variation ensures that the symbol durations are not multiples of each other, eliminating the presence of a consistent symbol rate [1, 2].

The rationale behind this strategy lies in the nature of CSP, which relies on the detection of periodic characteristics in signals [6]. By introducing variability in symbol durations, a randomness is embedded into the frequency component of the signal structure, creating a signal which lacks exploitable cyclic frequency components. Without a predictable symbol rate, hostile receivers would struggle to discern meaningful patterns or correlations within the signal, reducing the likelihood of detection. This complexity disrupts the patterns typically exploited CSP techniques, reducing the risk of detection by hostile receivers.

This approach aligns with the goal of RF steganography to facilitate covert communication while maintaining LPD characteristics. By leveraging techniques that obscure the cyclostationary features of the transmitted signal, such as VSD, users of RF steganography can enhance the security and resilience of their communication systems against adversarial detection techniques. The deliberate introduction of variability in symbol duration adds another layer of security to the communication process, making the signal more resistant to statistical analysis and pattern recognition algorithms of adversaries. This proactive approach to signal design contributes to the overall effectiveness of RF steganography in achieving covert communication in hostile environments.

Implementing RF Steganography

The goal of these experiments is to transmit a simple communications signal consisting of two 7-bit Barker code headers followed by 10 copies of the message 'Hello.' The messages are to be sent and extracted from embedded 7-bit ASCII codes into the Diagnostic Viewer in Simulink as readable reception of the packets. The functionality of the experimental setup will be confirmed upon reception and decoding of the 'Hello' message using RF steganography.

3.1 Modeling Techniques

Two USRP-2901 SDRs from National Instruments serve as the transmitter and receiver in the experimental setup. The RF steganography algorithm is developed within the MATLAB Simulink environment, integrating signal processing and modulation techniques necessary to replicate the joint radar/communications system. The Communications Toolbox in MATLAB provides essential features for communication system design, including LFM chirp signals for the radar component of RF steganography. The DSP System Toolbox streamlines signal processing tasks through provision of raised cosine filters and spectral analysis for testing.

To interface the Mathworks software using the NI USRP devices, the USRP Hardware Support Package in MATLAB is essential to facilitate real-time data streaming. Compatibility and communication between MATLAB and the SDR platform is achieved using the NI-USRP Configuration Utility. Leveraging these tools enables effective development and testing of the RF steganography system.

3.1.1 Transmitter Architecture

The transmitter consists of five major architectural blocks within Simulink, each corresponding to a different mathematical action required to perform VSD and LFM modulation on a signal. These actions will be expanded on in the following sections, including bits generation, VSD modulation, LFM, square root cosine filtering, and over the air USRP transmission.

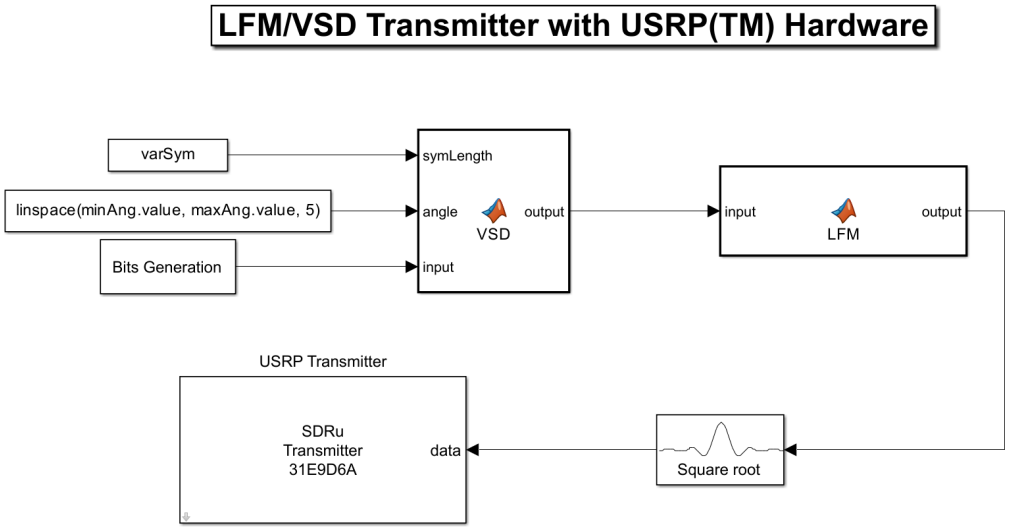

Figure 3.1: Simulink transmitter architecture

Bits Generation

Data frames are formed in the Bits Generation section within the Simulink Model. Each data frame contains two 7-bit Barker code headers for synchronization, concatenated with 10 'Hello' messages converted from 7-bit ASCII to binary values.

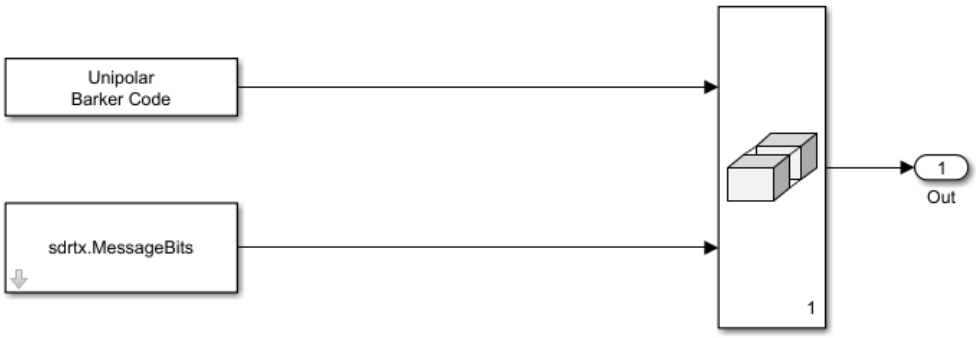

Figure 3.2: Simulink bits generation architecture

The Unipolar Barker Code subsystem takes the bipolar Barker defined in the `sdrtx` transmission initialization file and compares the signal to zero, creating a unipolar code. The `sdrtx.MessageBits` data generates and receives the message bits from the string

'Hello,' which is defined and converted from ASCII to binary data in the initialization script. The sample time is set in the mask parameters of this block as follows:

$$Ts = \frac{1}{P \times T_f} \tag{3.1}$$

The payload length, denoted by P, is determined by:

$$P = N_M \times L_M \times 7 \tag{3.2}$$

Here, N_M represents the number of messages in a frame, and L_M denotes the length of each character message.

The frame time, denoted by T_f, is calculated as:

$$T_f = \left(\frac{R_{samp}}{I}\right) \times (H + P) \tag{3.3}$$

R_{samp} refers to the front end sample rate of the USRP, H is the length of the header code, and the interpolation factor is denoted as I. These calculations ensure that the data is correctly processed through the subsequent signal processing blocks with the appropriate data lengths, preventing loss of information. The 14-bit header message with one "Hello" is displayed in the figure below.

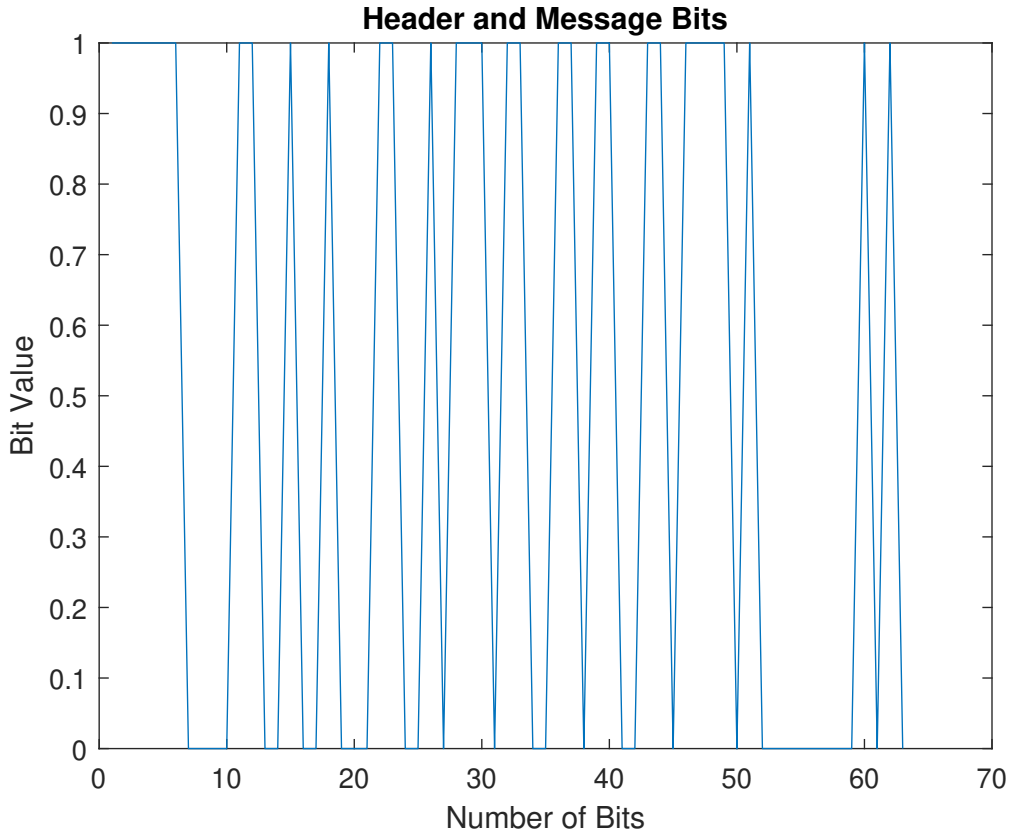

Figure 3.3: Transmitted header with one message

Variable Symbol Duration Modulation

This function operates on input signals with random symbol lengths and predetermined angle inputs. Given a vector of symbol lengths, denoted as $L = [L_1, L_2, \ldots, L_N]$, the incoming signal at index L_N is replicated a number of times corresponding to its value. Each replication value L_N indexes a vector of angle lengths for modulation, where M is the total number of values in the vector. These values, $\theta = [\theta_1, \theta_2, \ldots, \theta_M]$, represent the angles to be modulated as in Eq. 2.3. The modulation process can be represented as:

$$y = [L_1 \cdot e^{i\theta}, L_1 \cdot e^{i\theta}, \ldots, L_N \cdot e^{i\theta}] \tag{3.4}$$

The output signal y is generated by repeating each element of the input signal x according

to the symbol lengths specified externally, and then modulating each repetition with the corresponding phase angle from the vector θ.

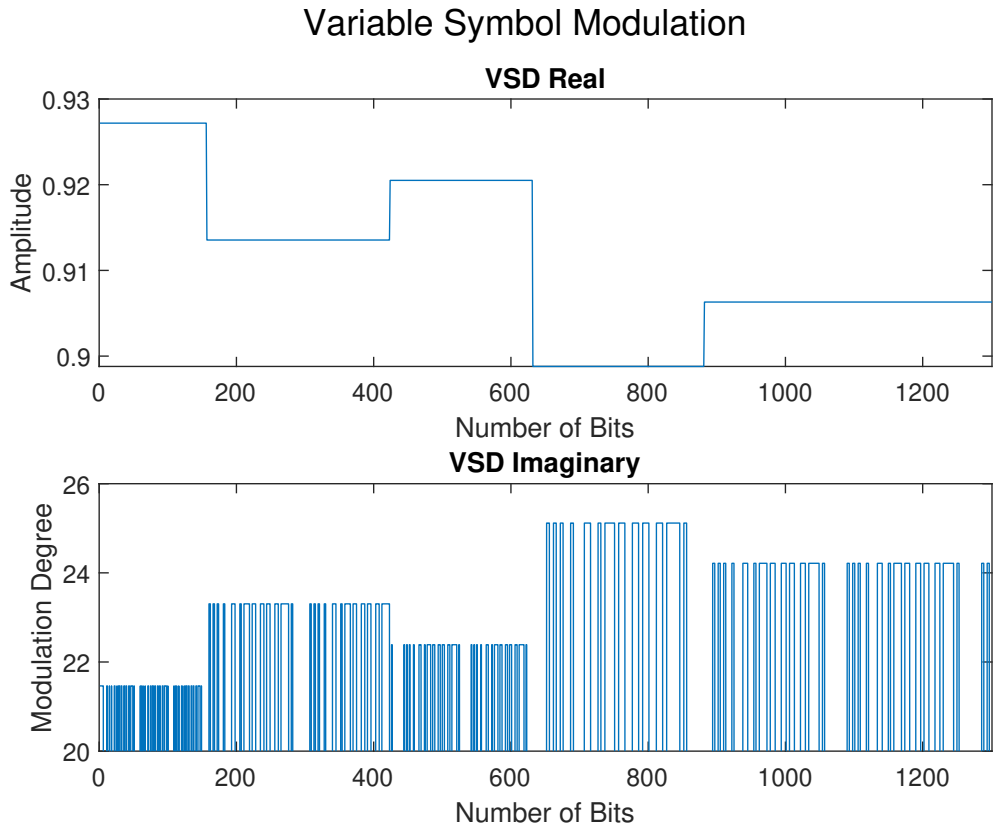

Figure 3.4: Variable symbol duration and corresponding phase

Linear Frequency Modulation

The LFM subsystem processes the VSD-modulated signal to generate a signal modulated by RF steganography. This output signal incorporates both VSD and LFM modulation techniques, with the goal of minimizing cyclostationary aspects. To preserve the integrity of frequency ramping, which is governed by the chirp rate k as described in Eq. 2.1, the signal undergoes upsampling by a factor of 20.

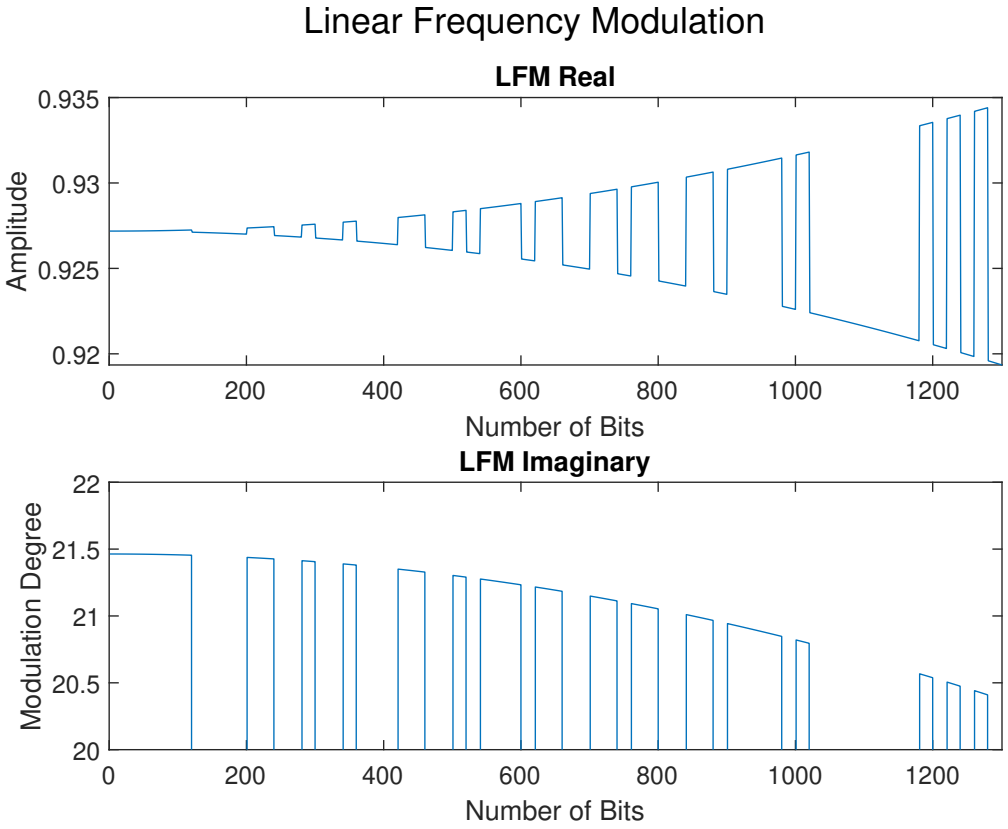

Figure 3.5: Linear frequency modulated signal

Square Root Cosine Filter

The square root cosine filter is applied to the RF steganography signal to reduce intersymbol interference due to the finite bandwidth of the system. The filter response used for signal transmission can be seen in Fig. 3.6 below.

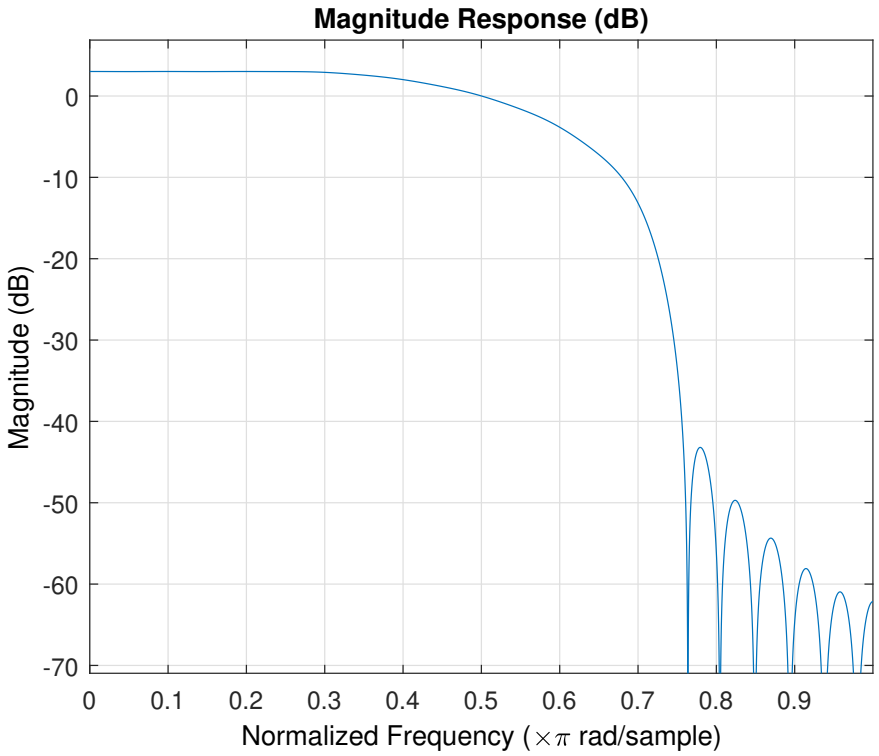

Figure 3.6: Raised cosine transmit filter response

USRP Transmission

The MATLAB SDRu Transmitter s-function is embedded code that communicates between the Simulink model and USRP device through the NI Configuration Utility, and writes to the Universal Hardware Driver (UHD) of the board of interest. The major subsection components are outlined in Fig. 3.7 below.

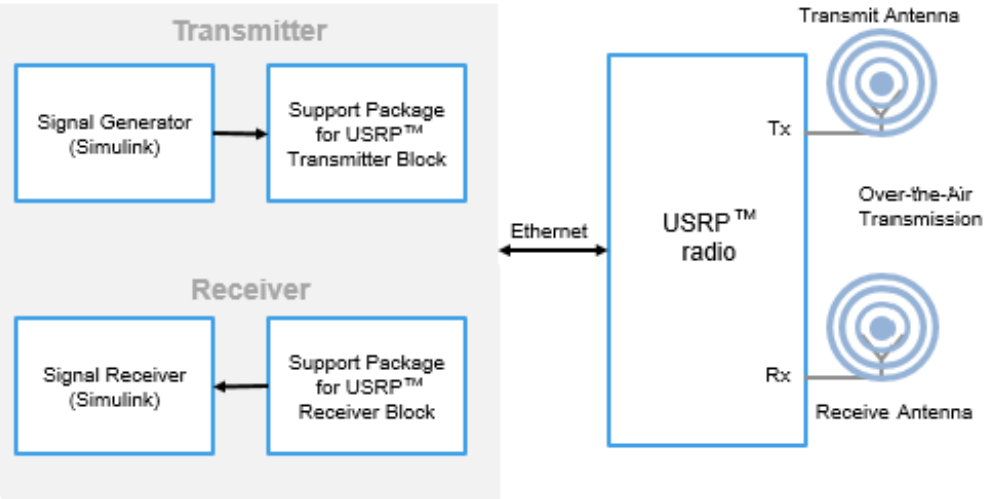

Figure 3.7: MATLAB SDRu transmit and receive functions [3]

3.1.2 Receiver Architecture

The receiver is a more complex design, containing eleven major system blocks within the Simulink model. As with the transmitter, each subsystem corresponds to a mathematical action. The actions will be expanded upon in the following sections including USRP reception, overflow consideration, automatic gain control, square root cosine filter, LFM demodulation, course frequency compensation, VSD demodulation, carrier synchronization, preamble detection, frame synchronization, and data decoding.

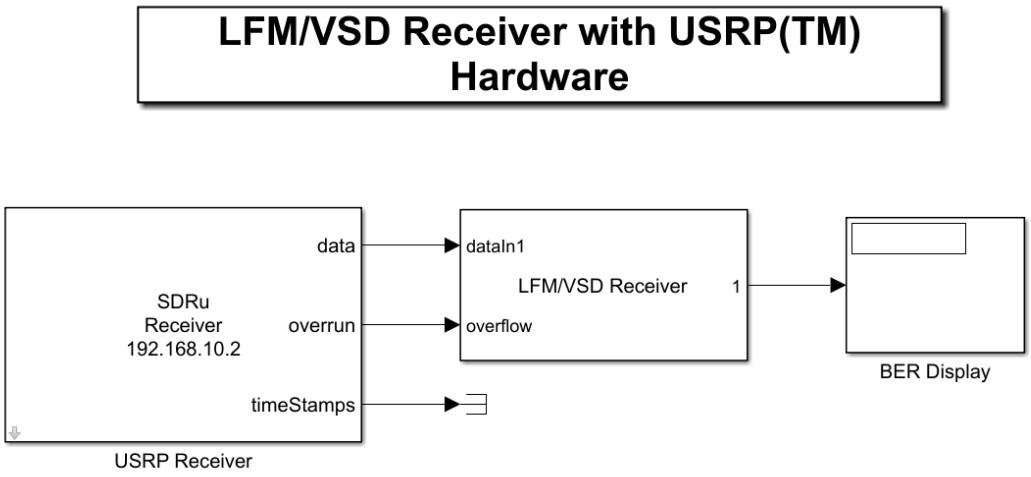

Figure 3.8: Simulink high level receiver architecture

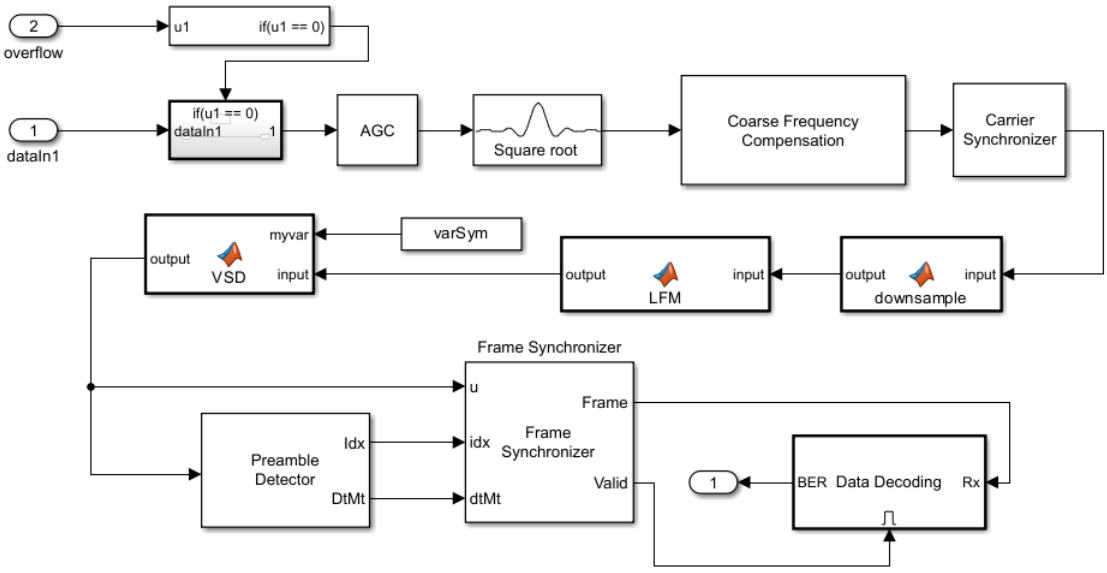

Figure 3.9: Simulink low level receiver architecture

USRP Reception

As with the transmitter, the MATLAB SDRu Receiver s-function communicates between the Simulink model and USRP device through the NI Configuration Utility and writes from the Universal Hardware Driver (UHD) of the board of interest. The major subsection components are outlined in Fig. 3.7.

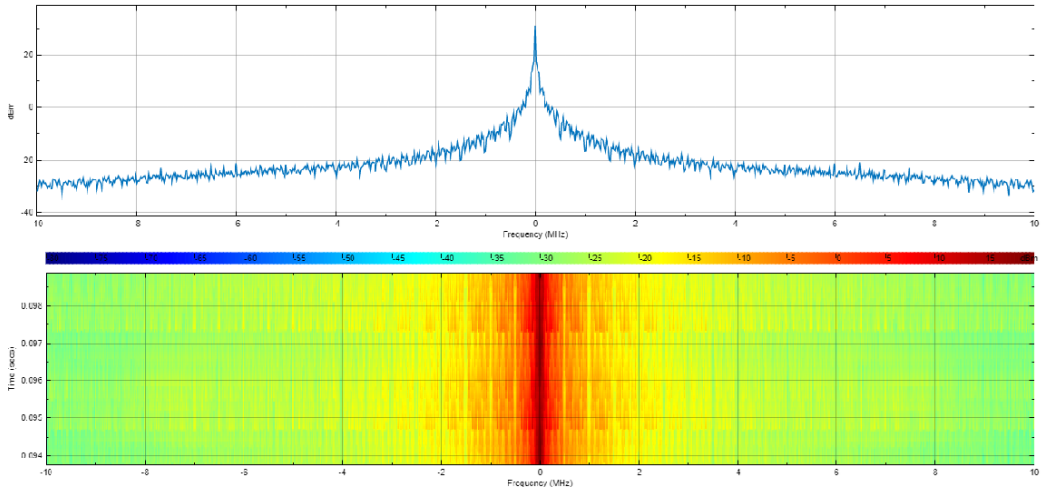

Figure 3.10: Received signal spectrum

Overflow

The overflow architecture manages scenarios in which the data output from the model surpasses the processing capacity of the USRP. If the model generates data at a rate higher than what the USRP can handle, it may result in buffer overflow issues, potentially leading to data loss or unexpected hardware behavior. The overflow architecture ensures that the rate at which data is consumed by the model aligns with the capabilities of the device.

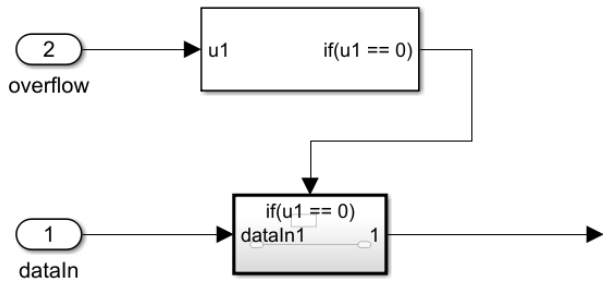

Figure 3.11: Simulink overflow architecture

This architecture implements a feedback loop, implementing flow control to manipulate the data from the model based on feedback from the USRP overflow output.

Automatic Gain Control

Automatic Gain Control (AGC) is a critical mechanism used in amplifiers to maintain a stable output level despite fluctuations in input signal strength. Mathematically, it adjusts the amplifier gain by multiplying the input signal $x(t)$ with a gain control function $G(t)$ to produce the output signal $y(t)$. This function dynamically adapts the gain based on input signal characteristics, boosting weaker signals and reducing amplification for stronger ones. In adaptive gain control, $G(t)$ is expressed as a function f of both output and input signal levels, incorporating feedback loops. The objective is to achieve an output power of 2 Watts while maintaining a maximum power gain of 60 dBm, considering hardware limitations [4].

Square Root Cosine Filter

The square root cosine filter is used to filter the RF steganography signal and downsamples it using a square root raised cosine finite impulse response (FIR) filter. The square root cosine filter also downsamples the filtered signal with an interpolation factor of 2 and a decimation factor of 1. In this case, the downsampled signal $y_d(t)$ is obtained as $y_d(t) = y(2t)$. The filter response for the receiver can be visualized in Fig. 3.6, depicting how the filter alters the amplitude and phase characteristics of the signal.

Course Frequency Compensation and Carrier Synchronization

The Course Frequency Compensation subsystem addresses frequency offsets in the received signal by precisely adjusting the input signal's frequency to synchronize it with the desired frequency reference. This adjustment process can be mathematically represented as

$$y_c(t) = y(t) \cdot e^{-j2\pi\Delta f t} \tag{3.5}$$

where $\Delta f = f_{\text{received}}(t) - f_{\text{desired}}$ represents the frequency offset between the received signal

and the desired frequency reference. In this equation, j denotes the imaginary unit, and $e^{-j2\pi\Delta ft}$ signifies the phase adjustment needed to align the frequencies.

As a pragmatic solution for limitations in software, 8PSK was selected as the most suitable frequency map. Although 8PSK modulation may not directly address the required frequency compensation, it provides a frequency map that can be utilized to align the received signal with the desired frequency reference. This alignment effectively minimizes the adverse effects of frequency drift or inaccuracies inherent in both transmitter and receiver components, thereby enhancing the overall system performance and reliability. Considerations for the phase offsets will be made further in the signal processing chain.

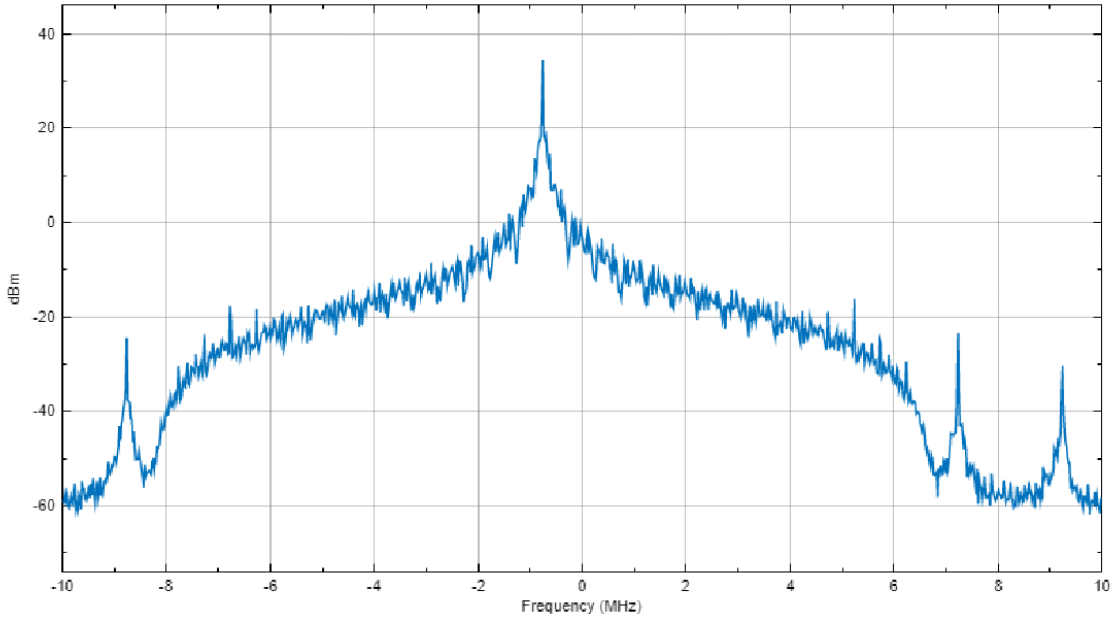

Figure 3.12: Signal after frequency adjustments

The Carrier Synchronization subsystem adjusts the phase and frequency of the received signal to facilitate accurate demodulation in subsequent stages. It achieves this by estimating the phase and frequency offset between the received signal and the local oscillator reference. Mathematically, the synchronization process involves adjusting the phase of the received signal to align it with the phase of the local oscillator reference. This ad-

justment can be represented as

$$y_s(t) = y(t) \cdot e^{-j(\phi_{\text{received}}(t) - \phi_{\text{local}}(t))} \tag{3.6}$$

where j denotes the imaginary unit, $y(t)$ is the received signal, $y_s(t)$ is the synchronized signal, $\phi_{\text{received}}(t)$ represents the phase of the received signal, and $\phi_{\text{local}}(t)$ represents the phase of the local oscillator reference. By ensuring synchronization of the carrier, this subsystem ensures proper alignment of the received signal with the demodulation process, further enhancing the accuracy of information recovery from the transmitted signal.

LFM Demodulation

After downsampling the signal to account for transmitted interpolation, the Linear Frequency Modulation (LFM) components of the signal are demodulated. With a frequency ramp k used in the transmitter, the demodulation follows the standard form:

$$y = e^{j2\pi \cdot 0.5 \cdot k \cdot t^2} \tag{3.7}$$

Where y represents the demodulated signal, j denotes the imaginary unit, and t represents time. This demodulation process transforms the signal to eliminate linear frequency components, effectively extracting the modulated information.

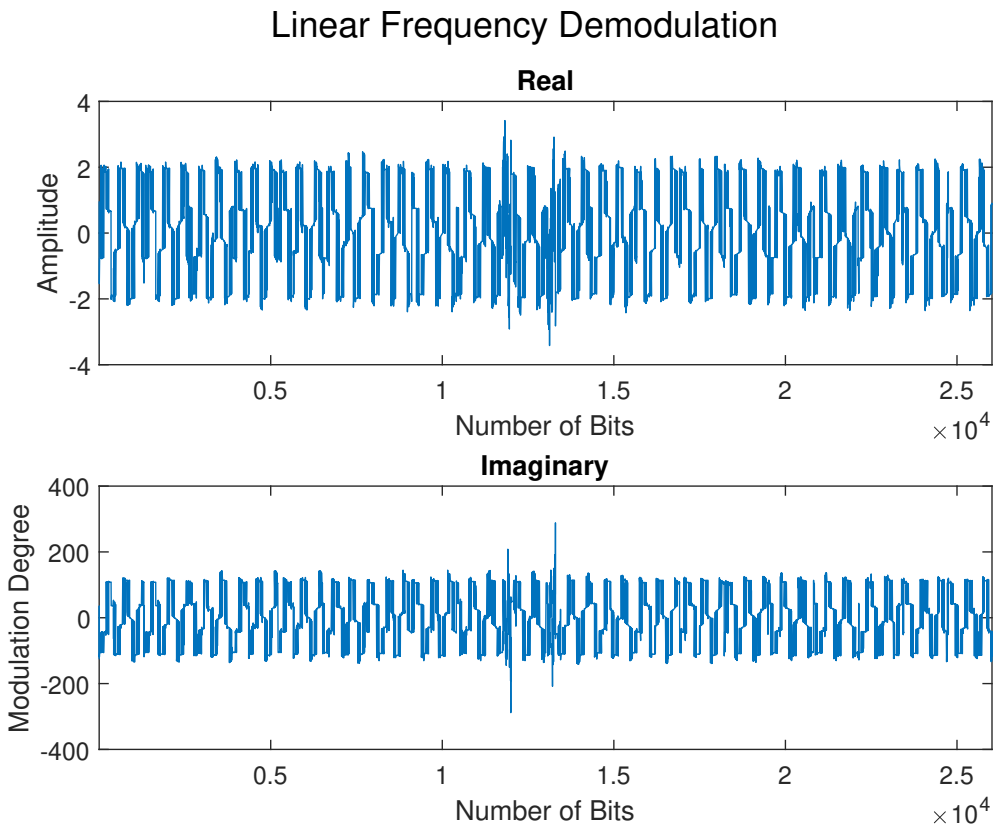

Figure 3.13: Signal after linear frequency demodulation

VSD Demodulation

The VSD demodulation subsystem requires prior knowledge of the modulation scheme of the transmitter. The receiver synchronizes with the intended signal length and downsamples the received signal accordingly. The downsampled signal, coupled with the predetermined random VSD sequence utilized by the transmitter, is used also in the demodulation process. Upon formatting the signal to match the intended frame size, as known by the receiver, the values within the VSD sequence dictate each variable symbol segment and restore the original symbol length. The demodulation involves extracting the VSD components by analyzing the sign of the imaginary phase portion of each segment. This process can be represented as:

$$y(t) = \text{sign}(L_i \cdot \text{Im}[\phi_i(t)]) \tag{3.8}$$

where $Li = [L_1, L_2, \ldots, L_N]$ is the incoming signal duration and $\phi_i = [\phi_1, \phi_2, \ldots, \phi_N]$ is the corresponding angle at the at the i-th value.

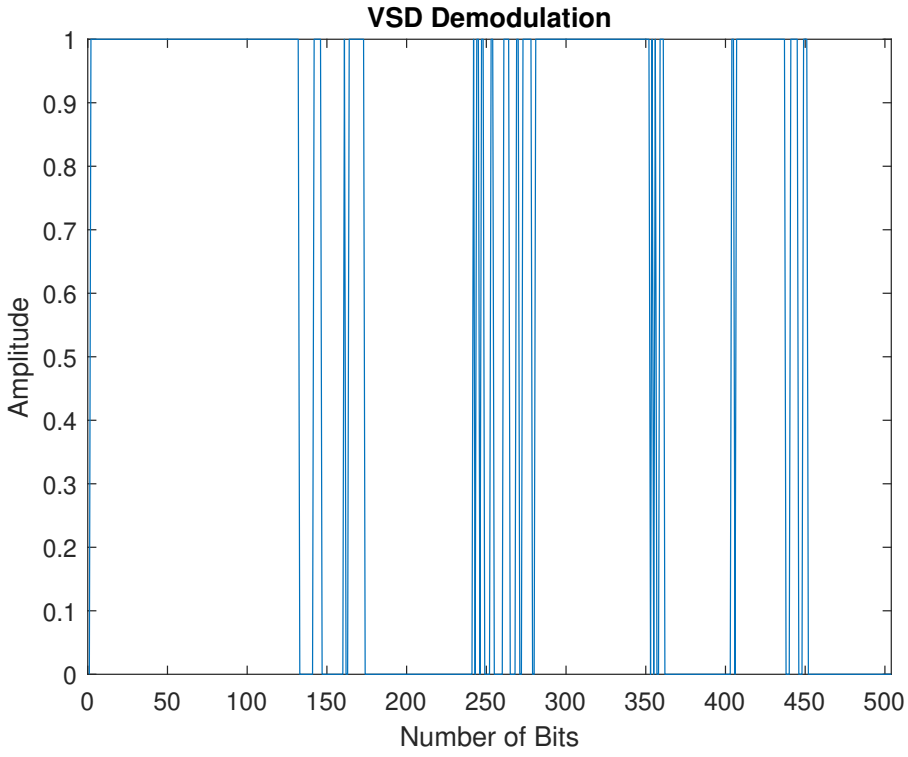

Figure 3.14: A signal frame after variable symbol demodulation

By leveraging prior knowledge of the transmitter's modulation scheme, the receiver synchronizes with the intended signal length and efficiently downsamples the received signal. Through careful formatting to match the intended frame size, dictated by the values within the VSD sequence, the subsystem effectively restores the original symbol length with consideration of the 8PSK signal mapping angle difference.

Preamble Detection

The preamble detection subsystem identifies the initiation point of a data frame or packet within the received signal. This packet contains the transmitted header sequence modulated with the corresponding angle modulated at the beginning of the packet. Given the reliance on the modulation scheme for VSD, prior knowledge of this scheme is important in this context as well.

The preamble detection subsystem compares the received signal with the modulated Barker sequence header, actively seeking a correlation between the received signal and the anticipated preamble pattern. Upon detecting a match, the block signifies the start of a new data frame, establishing synchronization and frame alignment.

The mathematical representation of the preamble detection process involves cross-correlating the received signal $y(t)$ with the preamble, modulated Barker pattern $P(t)$ to identify a potential match

$$x(t) = \int_{-\infty}^{\infty} y(t) \cdot P^*(t)\, dt \tag{3.9}$$

Where $P^*(t)$ denotes the complex conjugate of the preamble pattern.

Frame Synchronization

The following subsystem aligns received data frames or packets to a known reference point within the data packet, ensuring that the receiver correctly identifies the boundaries of each frame for accurate decoding of transmitted information. Mathematically, this alignment process involves detecting the presence of a frame by examining the received signal for specific characteristics or patterns that indicate the start of a new frame. Once a frame is detected, the block aligns it with a predefined reference point or marker within the frame. Let $t_{\text{reference}}$ denote the time corresponding to the predefined reference point or marker within the frame. The alignment operation can be mathematically represented as a time shift of

the received signal to align it with the reference point

$$y_{\text{aligned}}(t) = y(t - t_{\text{shift}}) \tag{3.10}$$

where t_{shift} represents the time shift required to align the frame with the predefined reference point. This mathematical representation captures the essence of the alignment process, where the received signal is shifted in time to align the frame with a known reference point, ensuring subsequent processing steps operate on the correct portion of the received data.

Data Decoding

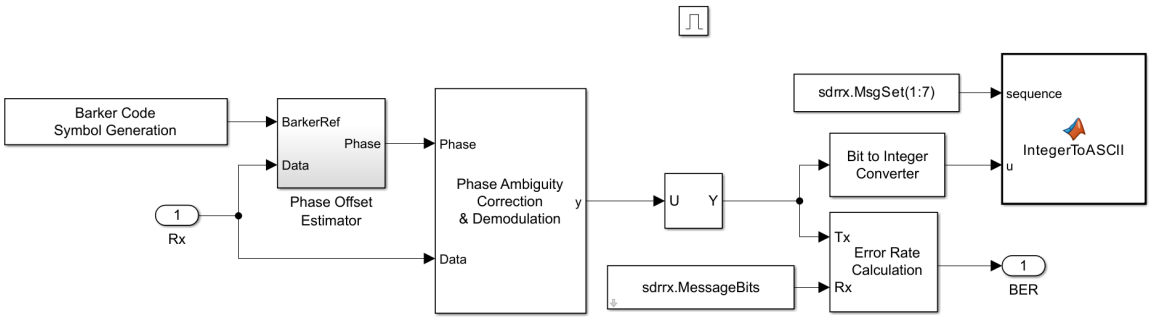

Figure 3.15: Data decoding architecture

The data decoding block processes the data received from the frame synchronization block and compares it to the unipolar Barker code from the message transmission. This comparison involves cross-correlating the received data $y(t)$ with the Barker code sequence $B(t)$ to identify and estimate any remaining phase offset after post-processing. Mathematically, this can be represented as:

$$x(t) = \int_{-\infty}^{\infty} y(t) \cdot B^*(t)\, dt \tag{3.11}$$

where $B^*(t)$ denotes the complex conjugate of the Barker code sequence.

The Phase Ambiguity Correction & Demodulation step applies a corresponding complex phase shift to the incoming data according to the variable symbol index and demodulates it using a Rotated Binary Phase Shift Keying (RBPSK) modulation scheme. Mathematically, this can be represented as:

$$y_{\text{corrected}}(t) = y(t) \cdot e^{i\phi(t)}$$

Where $y_{\text{corrected}}(t)$ represents the corrected data, and $\phi_i(t)$ represents the complex phase shift applied based on the variable symbol index i.

After decoding, the bits undergo two simultaneous processes. First, they are converted into ASCII format to enable visual message output. Second, they are cross-checked with the original message bits to compute the BER for the system.

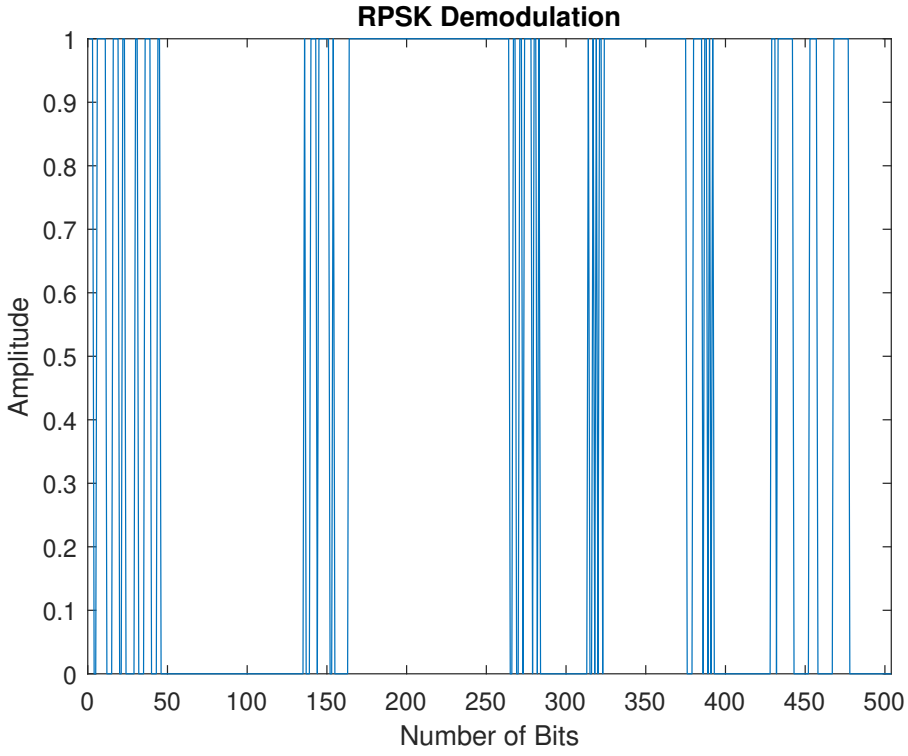

Figure 3.16: Signal of a frame after angle decoding and frame synchronization

3.2 Results

The effectiveness of RF steganography in real-world applications was demonstrated through successful signal reception. In the experiments, 3-5 messages per frame were recovered at 22-26°, confirming its ability to conceal and transmit information. Despite using identical equipment and architecture as the RF steganography transmitter, both radar and BPSK communications receivers failed to recover the signal. This highlights the unique nature of the RF steganography signal, lacking the cyclic properties of the BPSK receiver, thereby rendering the transmitted message undetectable to unintended recipients. Despite limitations in the hardware, the successful demonstration of RF steganography in real-life scenarios validates its potential for use in covert applications.

In analyzing the performance of RF steganography tests over varying angles and distances, a clear correlation between the angle and distance of transmission was observed. Across the range of distances tested, from 0.5 to 1 yard, the recovery of messages was notably highest. This suggests that proximity plays a significant role in the successful transmission and recovery of messages within the tested RF environment. The number of recovered messages showed consistent trends, indicating that shorter distances and specific angles yielded more reliable results, highlighting the importance of distance and angle optimization in the USRPs using RF steganography. Overall, with 28 packets transmitted, these findings underscore the importance of considering both distance and angle factors in optimizing RF steganography performance.

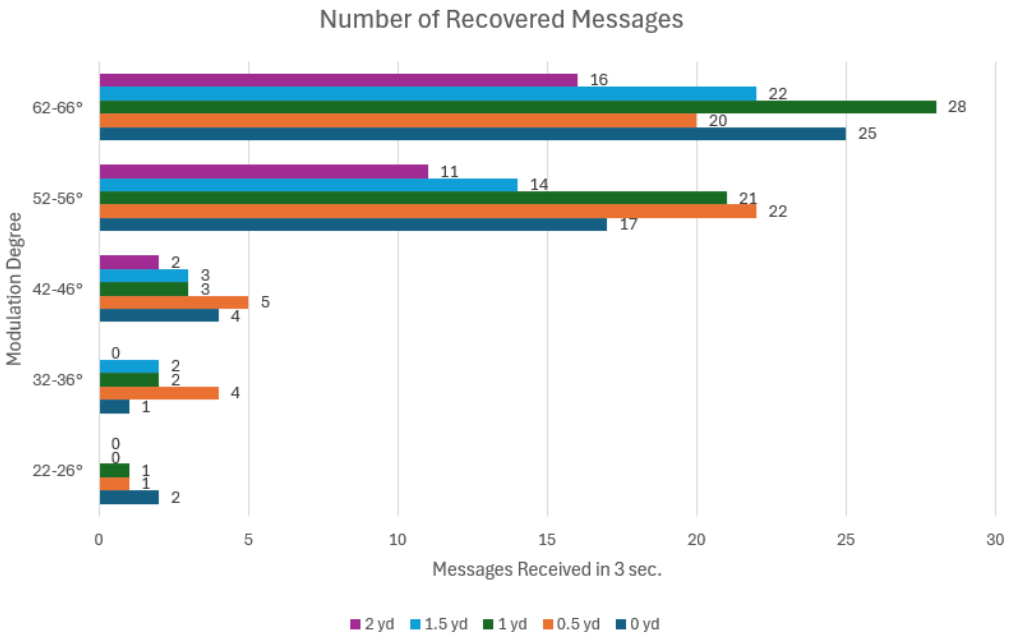

Figure 3.17: Recovered messages over varying distances

The analysis of cyclostationary features considers plots generated both with and without variable symbol duration. Notably, variable symbol duration emerged as a crucial factor in mitigating cyclostationary aspects.

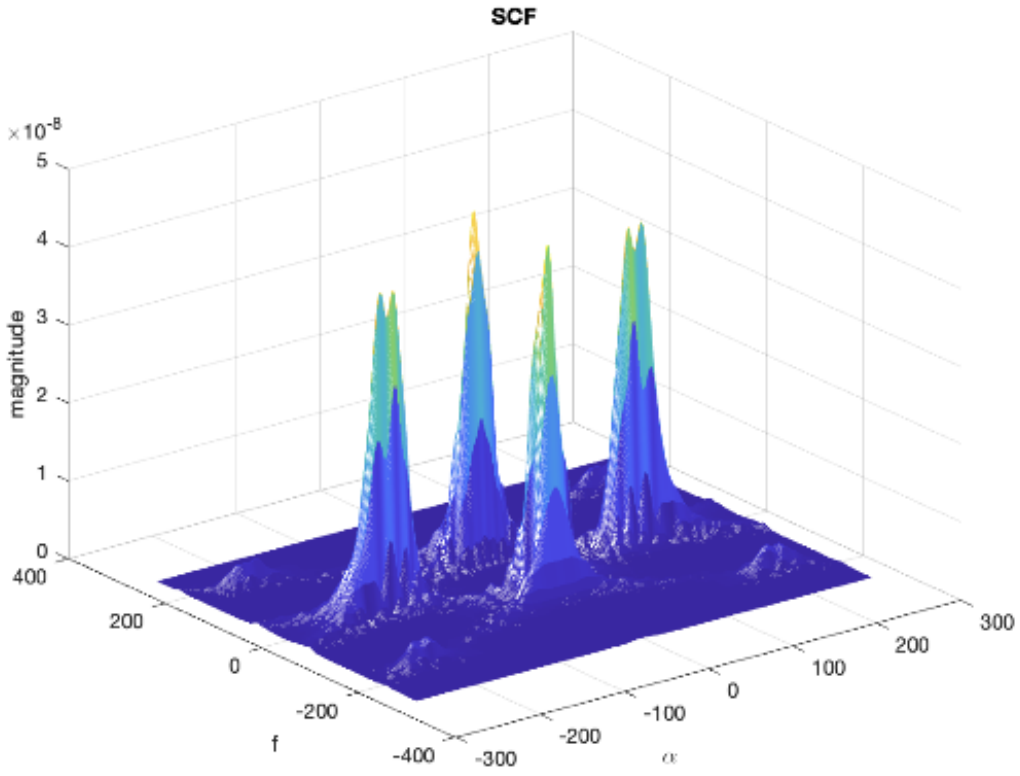

Figure 3.18: Spectral correlation of RBPSK

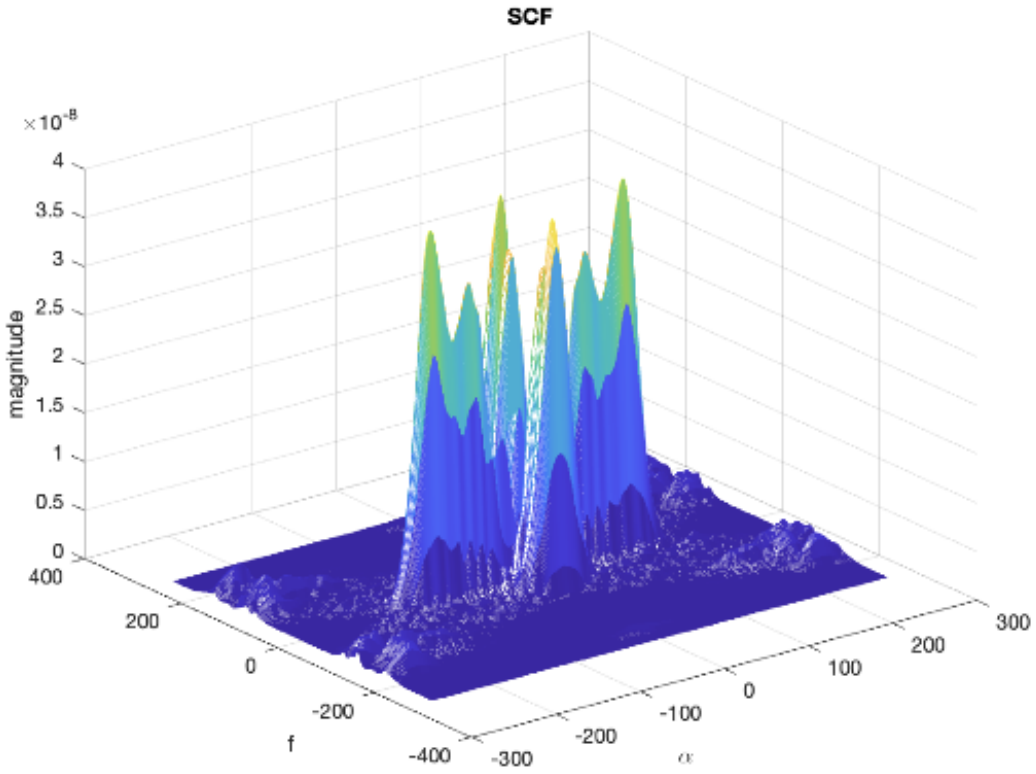

Figure 3.19: Spectral correlation of signal with variable symbols

The figures clearly demonstrate a significant reduction in the cyclic aspects of the signal with the addition of variable symbol duration. This highlights the importance of these features in concealing information and their impact on the effectiveness of RF steganography. Minimizing the cyclostationary features of a signal is crucial to counter advanced detection schemes, which is currently one of the most sophisticated known.

3.2.1 Limitations and Implications

In modeling RF steganography, several limitations stemmed primarily from hardware constraints and software capabilities. One notable restriction was the 60-degree phase offset required of the entire signal to accommodate the 8PSK mapping within the frequency compensation subsystem in the Simulink architecture. This limitation hindered the process while modulating with a non-standard mapping scheme, restricting the flexibility of the demodulation process. However, the frequency compensation and offset detection were crucial for the message recovery process in the receiver, especially in RF steganography at low transmission angles. This limitation had a trickle-down effect, requiring careful monitoring and consideration during demodulation and angle checking at various locations.

Another significant challenge arose during VSD demodulation, where issues such as demodulation shifts and a limited number of symbols per frame occurred. Despite indications in the literature [1, 2] of successful message recovery at angles between 15 to 16.5°, practical experiments failed to achieve such recovery even with radios positioned at their optimal locations of 0.5 to 1 yard, or connected through a wire, limiting over-the-air noise contributions. This failure can be contributed to insufficient transmission power and data packet size limitations of the hardware, resulting in the receiver's inability to recover all transmitted messages. Even with the transmission of ten messages, less than half were successfully recovered per frame, demonstrating the practical limitations faced in real-world scenarios.

The NI-2901 SDR, primarily designed for communication applications, introduced further limitations. This included requirements for upsampling and chirp rate limitations in LFM modulation, which resulted in transmission power issues. These issues likely contributed to the challenges faced by the radios in angle detection. Despite efforts to maximize the transmit and receive gains of the system, the recoverable signals did not precisely align with theoretical expectations. The hardware limited signal recovery in variable symbol duration, as variable symbol sizes below 50 identical, consecutive samples were not detected

in variable symbol modulation. This complication added to the modulation process's complexity and imposed constraints on signal recovery.

These limitations describe the complexity of modeling RF steganography on USRPs and highlight the importance of addressing practical constraints in experimental setups. Since the USRP is already transmitting at maximum power, 0.1 W, for these tests, achieving a higher-power signal or increased sampling capabilities to enhance message recovery requires a more robust transmitter. Access to more advanced equipment suitable for research or military purposes may provide insights into overcoming these challenges.

Conclusion

The modeling of RF steganography in NI-2901 SDRs encountered constraints primarily due to sampling limitations and architectural restrictions of the system. A notable challenge was the software's inflexibility in handling complex demodulation schemes, which hindered the system's demodulation adaptability. Additionally, hardware limitations constrained the reception of symbols per frame, preventing significant message recovery even in controlled experimental setups.

Practical experiments exposed disparities between theoretical predictions and real-world outcomes of implementing RF steganography, highlighting the importance of addressing limitations in transmission power and data packet size. Despite endeavors to optimize hardware capabilities, recoverable signals often diverged from theoretical expectations. Though the system's BER was less than ideal, both LFM and communications receivers of the same architecture failed to recover the signal, ensuring the ability of implementing RF steganography into SDRs with certain limitations.

The proposed cyclostationary post-processing of the algorithm validated the implementation of the architecture, revealing the absence of peaks in a BRPSK signal when variable symbol duration was introduced. This proves the necessity of variable symbol duration to circumvent advanced post-processing algorithms.

Further research may be conducted in potential solutions could involve revising the 8PSK mapping source code to better accommodate expected angles and identifying constraints in message recovery and variable symbol detection due to sampling limitations.

Another avenue of research may be addressing sampling and power constraints by adjusting power capabilities based on transmitted angles or designing messages to meet hardware requirements for full recovery. Tackling these challenges is crucial for advancing secure communication techniques, especially in scenarios where traditional encryption methods fall short.

Overall, the project contributes to enhancing secure communication by integrating RF steganography into joint radar/communication waveforms through software defined radios. The method's fusion of RBPSK modulation and variable symbol duration ensures secure transmission while preventing detection by hostile receivers or advanced post-processing algorithms. Implementation using SDRs demonstrates effectiveness in covert communication scenarios, despite encountered challenges. Future enhancements are imperative to improve the method's real-world applicability and address the limitations identified in this study.

Bibliography

[1] Z. Zhang, M. Nowak, M. Wicks, Y. Qu, and Z. Wu, "Rf steganography via lfm chirp radar signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, pp. 1221–1236, June 2018.

[2] Z. Zhang, M. Nowak, M. Wicks, and Z. Wu, "Bio-inspired rf steganography via linear chirp radar signals," *IEEE Communications Magazine*, vol. 54, pp. 82–86, June 2016.

[3] MathWorks, *SDRu Transmitter*, 2011.

[4] N. Instruments, *USRP-2901 Manual*.

[5] N. Instruments, "What is ni usrp hardware."

[6] W. Gardner, "Cyclostationarity in communications and signal processing," 1993.

[7] W. Gardner, W. Brown, and C.-K. Chen, "Spectral correlation of modulated signals: Part ii - digital modulation," *IEEE Transactions on Communications*, vol. 35, no. 6, pp. 595–601, 1987.

[8] W. A. Gardner and C. M. Spooner, "Signal interception: Performance advantages of cyclic feature detectors," *IEEE Transactions on Communications*, vol. 40, pp. 149–159, January 1992.

[9] Gardner, "Signal interception: Performance advantages of cyclic-feature detectors," *IEEE*, 2023.

[10] Jang, "Blind cyclostationary spectrum sensing in cognitive radios," *IEEE*, 2023.

[11] N. Levanon and E. Mozeson, *Radar Signals*. New York, NY, USA: Wiley, 2004.

[12] J. S. W. Melvin, *Principles of Modern Radar, Vol. 2*. SciTech Publishing, 2013.

[13] Q. Wang, G. Fu, P. Chen, Z. Wu, and Z. Wang, "Covert waveform for dual-function radar communication system," *Accepted for publication in IEEE Communication Letters*, 2024.

[14] C. Zhao, J. Yu, G. Luo, and Z. Wu, "Radio frequency fingerprinting identification of few-shot wireless signals based on deep metric learning," *Wireless Communications and Mobile Computing*, 2023.

[15] J. Ellinger, Z. Zhang, M. Wicks, and Z. Wu, "Dual-use multi-carrier waveform for radar detection and communication," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, pp. 1265–1278, June 2018.

[16] M. Nowak, Z. Zhang, M. Wicks, and Z. Wu, "Co-designed radar-communication using linear frequency modulation waveform," *IEEE Aerospace and Electronic Systems Magazine*, vol. 31, pp. 28–35, October 2016.

[17] N. Nowak, Z. Zhang, L. LoMonte, M. Wicks, and Z. Wu, "Mixed-modulated linear frequency modulated radar-communications," *IET Radar, Sonar Navigation*, pp. 1–20, August 2016.

[18] J. Ellinger, Z. Zhang, M. Wicks, and Z. Wu, "Multi-carrier radar waveforms for communications and detection," *IET Radar, Sonar Navigation*, pp. 1–9, September 2016.

[19] Napolitano, "Aircraft acoustic signal modeled as oscillatory almost-cyclostationary process," *IEEE Xplore*, 2020.

[20] J. X. B. S. A. Kanazawa, H. Tsuj, "Spatial and temporal processing of cyclostationary signals in array antennas based on linear prediction model," *IEEE Xplore*, 1998.

[21] O. Guschina, "A simulation study on the detection of a cyclostationary signal buried in a stationary noise for unknown power scenario," *IEEE Xplore*, 2023.

[22] R. Izzo and Napolitano, "Generalized almost-cyclostationary signals," *Signal Processing*, vol. 84, no. 5, pp. 1007–1020, 2004.

[23] M. Richards, *Fundamentals of Radar Signal Processing*. McGraw-Hill Professional, 2005.

[24] Y. Z. Z. Huang, W. Wang, "Design and implementation of cognitive radio hardware platform based on usrp," 2011.

[25] I. L. A. Mate, K. Lee, "Spectrum sensing based on time covariance matrix using gnu radio and usrp for cognitive radio," 2011.

[26] R. Schoolcraft, "Low probability of detection communications-lpd waveform design and detection techniques," in *MILCOM 91 - Conference record*, pp. 832–840 vol.2, 1991.

[27] H. Lu, L. Zhang, M. Jiang, and Z. Wu, "High-security chaotic cognitive radio system with subcarrier shifting," *IEEE Communications Letters*, vol. 19, no. 10, pp. 1726–1729, 2015.

[28] M. Kowatsch and J. Lafferl, "A spread-spectrum concept combining chirp modulation and pseudonoise coding," *IEEE Transactions on Communications*, vol. 31, no. 10, pp. 1133–1142, 1983.

[29] C. E. Cook, "Linear fm signal formats for beacon and communication systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-10, no. 4, pp. 471–478, 1974.

[30] M. Kowatsch, F. J. Seifert, and J. Lafferl, “Comments on transmission system using pseudonoise modulation of linear chirps,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. AES-17, no. 2, pp. 300–303, 1981.