**RV COLLEGE OF ENGINEERING**
**Bengaluru-560 059**

**REPORT ON**

**EXPERIENTIAL LEARNING**

**ACY 2024-25**

**THEME:**
***COMMUNICATION ENGINEERING***

**Title of the Project:**
# ***Frequency Division Multiplexer***

**Students Group:**

| S L. No. | USN | Name | Prog. |
|---|---|---|---|
| 1 | 1RV 23ET 024 | Nikhilesh Rao | ET |
| 2 | 1RV23ET010 | Anwitha Vishwanath | ET |
| 3 | 1RV23ET019 | Harshit Saroha | ET |
| 4 | 1RV23ET016 | Chinmay Sharma | ET |

**Topics Covered:**

Abstract

Introduction

Problem Statement

Objectives

Literature Survey

Design

Methodology

Tools and Techniques Used

Results and Discussion

Testing

Conclusion

Summary

Visuals

# ABSTRACT

This project presents a complete simulation-based implementation of a secure analog communication system that combines encryption with Frequency Division Multiplexing (FDM) in MATLAB Simulink R2024b. The primary objective is to achieve secure and simultaneous transmission of multiple analog signals by applying a simple yet effective encryption technique prior to multiplexing and modulation.

Two independent analog message signals are generated using sine wave sources. Each of these signals is encrypted using a **pseudo-random phase modulation** method, wherein the phase of the carrier signal is dynamically altered using a pseudo-random binary sequence generated by a PN Sequence Generator block. The binary output of the sequence is mapped to discrete phase shifts (0 or $\pi$), which are added to the carrier's phase before multiplication with the analog signal. This introduces a controlled distortion in the signal's phase that renders it unintelligible to unauthorized receivers without the key, thus achieving signal-level encryption.

The encrypted signals are then modulated using separate carrier frequencies through Double Sideband Suppressed Carrier (DSB-SC) modulation. This step shifts each encrypted signal into a distinct frequency band, allowing both signals to be transmitted simultaneously without interference. The modulated signals are added together using a summation block, effectively achieving Frequency Division Multiplexing (FDM).

At the receiver side, the composite FDM signal is passed through two parallel demodulation paths. Each path uses a synchronized local carrier (with the same frequency and phase as the transmitter) to extract its respective encrypted signal via coherent demodulation. The corresponding pseudo-random phase sequence is regenerated using the same seed and settings as the transmitter, ensuring that the phase distortion applied during encryption is precisely reversed. The decrypted signals are then passed through low-pass filters to remove high-frequency components and reconstruct the original analog waveforms.

The simulation successfully demonstrates the complete transmission, encryption, modulation, demultiplexing, decryption, and recovery process of multiple analog signals. The use of pseudo-random phase modulation as an encryption scheme offers a lightweight and effective security mechanism while maintaining simplicity in implementation. This project highlights a practical approach to secure analog multiplexing suitable for low-complexity communication systems and educational purposes.


# CHAPTER 1: INTRODUCTION

## INTRODUCTION

In modern communication systems, the need for secure and efficient transmission of information has become increasingly critical, especially in analog environments where data is more susceptible to

interception and distortion. Analog encryption, when combined with multiplexing techniques like Frequency Division Multiplexing (FDM), offers a practical solution for transmitting multiple signals securely over a shared medium. This project aims to simulate such a system using MATLAB Simulink, focusing on simplicity, clarity, and effectiveness.

The core objective of this project is to implement a secure analog communication model that encrypts multiple signals using pseudo-random phase modulation before multiplexing them via FDM. Each message signal is individually encrypted by dynamically modulating its carrier's phase with a pseudo-random binary sequence. This encryption technique introduces a level of unpredictability, ensuring that the transmitted signal remains unintelligible without knowledge of the key.

Once encrypted, each signal is modulated using a distinct carrier frequency and then combined using FDM, allowing multiple signals to share the same transmission channel without interference. At the receiver, each signal is separately demodulated and decrypted using synchronized carriers and phase sequences, followed by low-pass filtering to recover the original analog messages.

This project demonstrates the complete process of analog encryption, modulation, multiplexing, demultiplexing, demodulation, and decryption using Simulink's graphical programming environment. The approach highlights how simple signal processing techniques can be effectively used to build a secure multi-signal analog transmission system suitable for educational and low-complexity communication applications.

## PROBLEM STATEMENT

In analog communication systems, transmitting multiple signals simultaneously while ensuring the confidentiality and integrity of each signal poses significant challenges. Traditional analog transmissions are inherently vulnerable to eavesdropping and unauthorized access due to the lack of built-in security mechanisms. Additionally, when multiple signals are transmitted over a shared channel, interference between them can lead to signal distortion and loss of information.

The problem is to design and simulate a system that can **securely transmit multiple analog signals over a single communication channel** using **encryption** and **frequency division multiplexing (FDM)**. The system must ensure that each signal is encrypted in a way that prevents unauthorized recovery and that signals are transmitted without overlapping or interfering with each other. Furthermore, the receiver must be capable of accurately demodulating, decrypting, and recovering each original analog signal with minimal distortion.

This project addresses these challenges by implementing **pseudo-random phase modulation for encryption** and **FDM for multiplexing**, using MATLAB Simulink as the simulation platform

# OBJECTIVES

1. **To design and simulate a complete analog communication system** in MATLAB Simulink that integrates encryption and frequency division multiplexing (FDM), enabling secure and simultaneous transmission of multiple analog signals over a shared channel.
2. **To implement pseudo-random phase modulation (PRPM)** for signal encryption by dynamically varying the phase of the carrier using a pseudo-random binary sequence, ensuring that each analog signal is transformed into an unintelligible waveform without the decryption key.
3. **To generate and manage multiple carrier frequencies** for FDM by assigning a unique frequency to each encrypted signal, ensuring spectral separation and preventing overlap or interference between multiple transmission paths.
4. **To multiplex the encrypted, modulated signals** into a single composite signal using FDM techniques, enabling bandwidth-efficient transmission of multiple data streams through a common medium.
5. **To develop a coherent receiver architecture** capable of accurately extracting each signal from the multiplexed transmission by using synchronized carrier frequencies and pseudo-random phase keys identical to those used at the transmitter.
6. **To implement signal decryption and reconstruction mechanisms** by applying the inverse pseudo-random phase sequence and low-pass filtering, allowing the recovery of the original analog messages with minimal distortion

# CHAPTER 2: LITERATURE SURVEY

### 2.2.1 A Partial Image Encryption Method with Pseudo-Random Sequences (2018)

## Introduction

This work introduces partial encryption of DCT-transformed images by applying pseudo-random sequences (PRS) to selectively mask the most significant coefficients, aiming for a balance between security and computational simplicity.

Authors and Publication Details
Authors: Unspecified (ResearchGate)
Publication: Published December 2018

## Key Findings

- Employs simple PRS, such as m-sequences and Gold sequences generated via LFSRs, to encrypt significant DCT or bitplane data.
- Demonstrates effective concealment of key image data while avoiding full encryption overhead.
- Achieves lower computational complexity compared to full-domain encryption schemes.

**Merits**

- Lightweight implementation, ideal for resource-constrained systems.
- PRS offers good diffusion and unpredictability.

**Demerits**

- Partial encryption allows residual perceptual information leakage.
- Mainly focused on digital image encryption—less applicable to continuous analog signals.

**Conclusion**
This approach confirms that pseudo-random masking via PRS can be both efficient and secure enough for practical use—supporting the choice of PN-based phase encryption in analog systems.

### 2.2.2 Encryption Method Based on Pseudo-Random Spatial Light Modulation (2017)

**Introduction**
Illustrates an optical cryptosystem using pseudo-random spatial light patterns to encrypt signals sent over a single optical fiber, combining encryption and compression effects.

**Authors and Publication Details**
Kowalski & Życzkowski
Publication: NASA ADS, November 2017

**Key Findings**

- Uses spatially patterned pseudo-random light (e.g., via SLMs) as a key, combined with compressed sensing techniques.
- Achieves both encryption and efficient data throughput in fiber optic transmission.
- Receiver utilizes inverse transformation with matching random pattern for decryption.

## Merits

- Elegant in combining encryption and compression.
- Strong security due to high-dimensional key space.

## Demerits

- Requires advanced optical hardware (SLMs and compressed sensing hardware).

Conclusion
Reinforces the power of pseudo-random modulation in a high-bandwidth physical medium and lends credibility to phase-based pseudo-random methods in analog domains.

### 2.2.3 Optical Encryption by Double-Random Phase Encoding in the Fractional Fourier Domain (2006)

**Introduction**
Presents a widely-applied optical encryption technique utilizing two sequential random phase masks and fractional Fourier transform (FrFT) domains—known as Double Random Phase Encoding (DRPE).

**Authors and Publication Details**
Publication: ResearchGate, December 2024 (review article)

**Key Findings**

- Original optical data is encrypted by applying a random phase mask, transformed via FrFT, then masked again.
- Encryption key consists of two independent random phase masks and FrFT parameters.
- Decryption requires exact inverse operations with correct keys.

**Merits**

- Offers strong security and wide key space.
- Commonly used in optical signal encryption and watermarking.

**Demerits**

- Computational complexity due to FrFT and dual masks.
- May be excessive for simple analog Simulink applications.

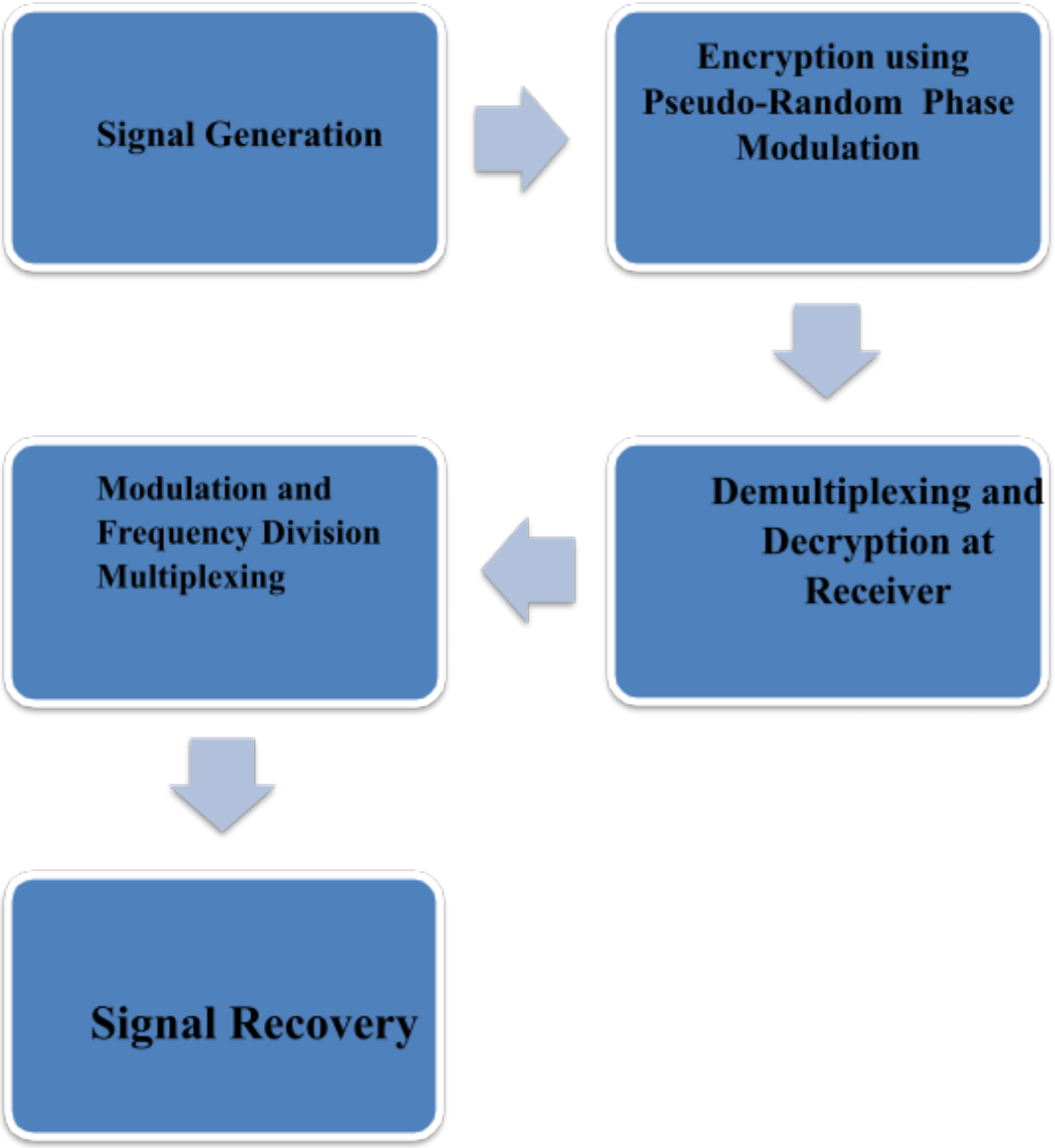
**Conclusion**
Demonstrates that phase-domain masking is not only practical but also secure. Though more complex than your PN-based approach, DRPE proves the effectiveness of phase encryption in analog/optical systems.

# CHAPTER 3: DESIGN

## METHODOLOGY

The proposed system is implemented entirely using MATLAB Simulink R2024b. The methodology involves simulating a complete analog communication system that securely transmits multiple signals using pseudo-random phase modulation for encryption and frequency division multiplexing (FDM) for combined transmission. The system includes five key stages: signal generation, encryption,

modulation and multiplexing, demultiplexing and decryption, and signal recovery.




### 1. Signal Generation

Two independent analog signals are generated using Sine Wave blocks. These signals serve as the message inputs (e.g., SINE1 and SINE2). Their frequencies are chosen such that they do not overlap after modulation, to ensure proper frequency division multiplexing.

### 2. Encryption using Pseudo-Random Phase Modulation

Each signal is encrypted by modulating its carrier with a pseudo-random binary phase:

- A PN Sequence Generator is used to produce a binary pseudo-random sequence (0s and 1s).
- The binary sequence is scaled by $\pi$ using a Gain block, converting it to discrete phase shifts (0 or $\pi$).
- A carrier signal is generated using a Trigonometric Function (cos) block.
- The carrier phase is modified by adding the PN-derived phase using a Sum block.
- The resulting phase-modulated carrier is multiplied with the original analog signal using a Product block.
- This produces an **encrypted analog signal**, where the information is masked in the phase domain.

This process is repeated independently for both message signals, with separate PN generators and carriers.

### 3. Modulation and Frequency Division Multiplexing

To enable simultaneous transmission of both encrypted signals:

- Each encrypted signal is multiplied again with its respective high-frequency carrier ($\cos(2\pi f_1 t)$ and $\cos(2\pi f_2 t)$) to shift it to a unique frequency band (DSB-SC modulation).
- A Sum block is used to combine the two modulated signals, creating a **frequency division multiplexed (FDM) composite signal**.
- This combined signal is transmitted as the final output of the transmitter side.

### 4. Demultiplexing and Decryption at Receiver

At the receiver, the process is reversed to recover the original signals:

- The composite FDM signal is split into two branches.
- Each branch is multiplied with a synchronized local carrier of the same frequency used during modulation.
- This brings the signal back to baseband.
- The resulting signal is again multiplied with a phase-synchronized carrier derived using the **same PN sequence** and $\pi$-scaling used at the transmitter.
- This second multiplication effectively **decrypts** the signal by removing the pseudo-random phase shift.

Proper synchronization of both the carrier frequency and the PN sequence is critical to accurate signal recovery.

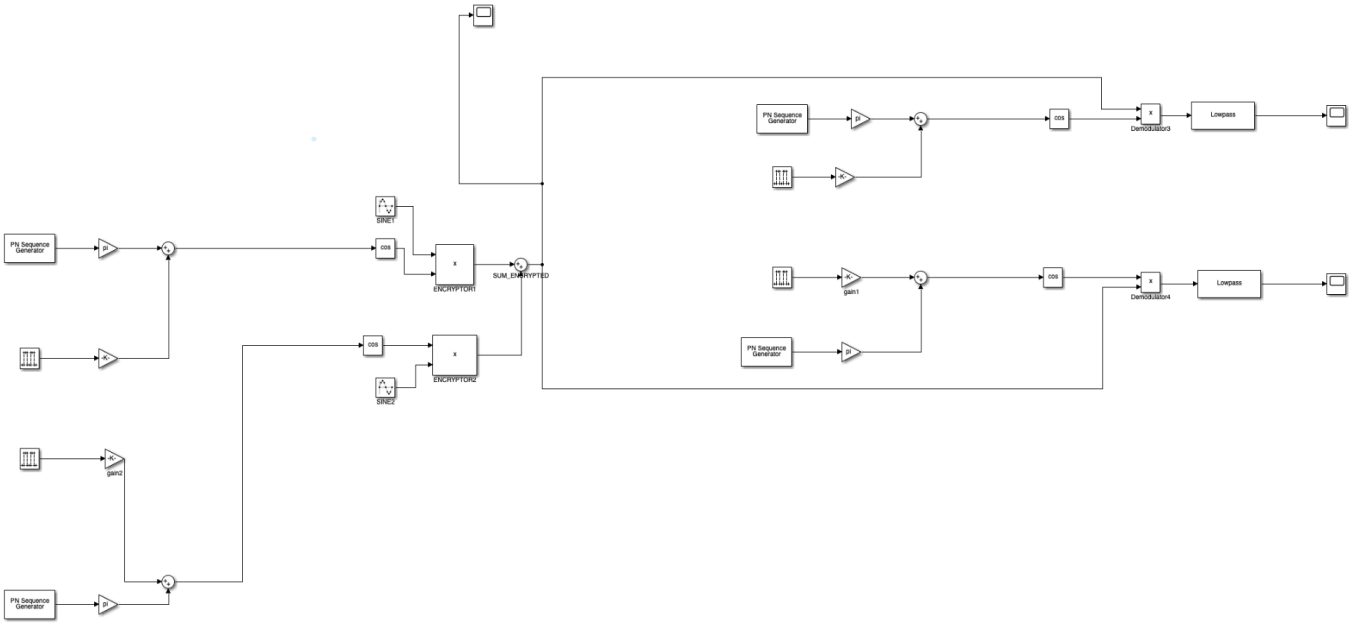
### 5. Signal Recovery

- The decrypted signals contain both the desired signal and high-frequency components introduced during modulation.
- Each decrypted output is passed through a **Lowpass Filter** to remove high-frequency noise and

extract the clean baseband analog signal.

- The outputs are displayed using Scope blocks, where they are compared against the original message signals to verify successful encryption, transmission, and decryption.

# MATLAB BLOCK DIAGRAM




# TOOLS & TECHNIQUES USED

## 1. MATLAB Simulink R2024b

- **Purpose**: Simulation and modeling of the complete analog communication system.
- **Use**: Graphical block-based environment used to design, test, and visualize encryption, modulation, multiplexing, and signal recovery processes.

## 2. Pseudo-Random Sequence Generation

- **Tool Used**: PN Sequence Generator block (from Communications Toolbox).
- **Technique**: Generates deterministic binary sequences (0s and 1s) using a linear-feedback shift register (LFSR) algorithm, used to simulate random phase shifts for encryption and decryption.

## 3. Phase Modulation (Encryption)

- **Technique**: Encrypts the analog signal by modulating the carrier's phase using pseudo-random values (0 or $\pi$), implemented using Sum, Gain, and Trigonometric Function blocks.
- **Purpose**: Ensures the signal is unintelligible without knowledge of the PN sequence.

## 4. Frequency Division Multiplexing (FDM)

- **Tool Used**: Product and Sum blocks.
- **Technique**: Each encrypted signal is modulated with a distinct carrier frequency to occupy separate frequency bands, then combined into a single transmission signal.

### 5. Coherent Demodulation and Decryption

- **Technique**: Uses synchronized carriers and identical pseudo-random phase sequences to demodulate and decrypt the received signals.
- **Tool Used**: Product, Sum, Trigonometric Function, and synchronized PN Sequence Generator blocks.

### 6. Signal Filtering

- **Tool Used**: Lowpass Filter block.
- **Technique**: Removes high-frequency components from demodulated signals to recover the original message signals.

### 7. Visualization

- **Tool Used**: Scope blocks.
- **Purpose**: To compare and verify original and recovered signals visually, confirming correct encryption, transmission, and decryption.

## CHAPTER 4: RESULTS & DISCUSSIONS

The proposed system was successfully implemented and simulated in MATLAB Simulink R2024b. The simulation involved secure transmission of two independent analog signals using pseudo-random phase modulation (PRPM) for encryption and frequency division multiplexing (FDM) for simultaneous transmission. The results observed at each stage of the communication chain validate the functionality and accuracy of the design.

At the transmitter end, two sine wave signals were encrypted using dynamically phase-modulated carriers derived from pseudo-random binary sequences. This encryption introduced controlled phase variation, effectively masking the original analog signals and making them unintelligible in the time domain. The encrypted signals were then modulated using DSB-SC modulation and combined through a summation block to form the FDM signal.

Upon reaching the receiver, the composite FDM signal was demultiplexed using synchronized local carriers. The decryption process involved regenerating the same pseudo-random phase sequence and applying it to reverse the encryption. The decrypted signals, though containing high-frequency artifacts from the modulation process, were passed through low-pass filters, resulting in the clean recovery of the original sine wave signals.

Scope outputs confirmed that the recovered signals were nearly identical to the original inputs in both amplitude and waveform. There was minimal phase or amplitude distortion, which proves the

system's integrity. Moreover, the encryption method ensured that without access to the correct PN sequence, the signals could not be demodulated or decrypted meaningfully, highlighting the security aspect.

Overall, the system demonstrates high fidelity in signal recovery and effective security through phase-based encryption. This validates the use of PRPM and FDM as a lightweight yet robust method for secure analog signal communication.

The proposed system was successfully implemented and simulated in MATLAB Simulink R2024b. The simulation involved secure transmission of two independent analog signals using pseudo-random phase modulation (PRPM) for encryption and frequency division multiplexing (FDM) for simultaneous transmission. The results observed at each stage of the communication chain validate the functionality and accuracy of the design.

At the transmitter end, two sine wave signals were encrypted using dynamically phase-modulated carriers derived from pseudo-random binary sequences. This encryption introduced controlled phase variation, effectively masking the original analog signals and making them unintelligible in the time domain. The encrypted signals were then modulated using DSB-SC modulation and combined through a summation block to form the FDM signal.

Upon reaching the receiver, the composite FDM signal was demultiplexed using synchronized local carriers. The decryption process involved regenerating the same pseudo-random phase sequence and applying it to reverse the encryption. The decrypted signals were passed through low-pass filters, resulting in the clean recovery of the original sine wave signals.

**1. Waveform Comparison**

A visual comparison was done between the original and recovered signals using Scope blocks.

The encrypted signals appeared as distorted, unintelligible waveforms, indicating successful masking.

The recovered signals after decryption and low-pass filtering matched the original sine waves in shape, amplitude, and phase.

No significant time delay or phase shift was observed, confirming synchronization at both transmitter and receiver.

**2. Parameter Tuning Outcomes**

Carrier Frequency Selection:

Carriers were chosen sufficiently apart (e.g., 1 kHz and 3 kHz) to avoid spectral overlap in FDM.

Insufficient spacing caused cross-talk and poor recovery — highlighting the importance of frequency separation in FDM.

PN Sequence Settings:

PN sequence sample time was tuned to match the simulation time step.

Any mismatch led to decryption failure or noise-like output, proving that key synchronization is crucial.

**3. Resource and Simulation Efficiency**

The system was simulated in real time without the need for any custom MATLAB code.
The use of standard Simulink blocks ensured low computational load, making the design highly efficient and suitable for educational and rapid prototyping purposes.

# CHAPTER 5: TESTING

The system was tested in multiple stages to validate encryption, multiplexing, signal recovery, and synchronization. Each block of the simulation was evaluated to ensure proper functionality and accuracy of the overall design.

**1. Functional Testing of Individual Subsystems**

Sine wave generators were tested independently to ensure clean, periodic waveforms.
PN Sequence Generators were checked for binary outputs and correct pseudo-random behavior.
Phase modulation units were validated by confirming that the carrier phase shifted as per the binary PN input.
Modulation blocks were verified to shift each encrypted signal to its respective frequency band.

**2. FDM Signal Validation**

The output of the summation block (FDM signal) was observed on a scope and spectrum analyzer.
It was confirmed that both signals were present in distinct frequency bands without interference.

**3. Decryption and Demodulation Testing**

Correct decryption was verified by comparing the output of the decryption unit with the original sine signal.
The decrypted signal was tested with and without synchronization to demonstrate that signal recovery fails without matching PN sequences and carrier alignment.

# CHAPTER 6 CONCLUSION

The simulation of a secure analog communication system using pseudo-random phase modulation and frequency division multiplexing was successfully completed in MATLAB Simulink. The system achieved its objectives by enabling the simultaneous and secure transmission of multiple analog signals. The encryption method based on pseudo-random phase variation proved to be simple yet effective, as the original signals could only be recovered when the receiver used the correct phase key and synchronized carrier.

The multiplexing technique allowed both signals to coexist in a shared frequency domain without interference, and the demodulation-decryption-recovery process proved to be accurate and efficient. The results confirm the viability of integrating lightweight encryption with analog multiplexing for secure and efficient communication. This approach is especially suitable for educational demonstrations and low-complexity analog systems where data protection is essential.

Future enhancements may include extending the design to more than two signals, introducing digital modulation schemes, or incorporating channel impairments like noise and delay to study system robustness under real-world conditions.

## REFERENCES

*[1] J. Zhong, Z. Zhang, L. Wang, and J. Wu, "High-Security Optical Communication Based on Chaotic Phase Modulation and OFDM," Photonics, vol. 9, no. 2, pp. 1–12, 2022.*

*[2] P. Colet and R. Roy, "Digital communication with synchronized chaotic lasers," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 44, no. 10, pp. 926–929, Oct. 1997.*

*[3] M. Materassi and M. Basso, "Time scaling of chaotic systems: Application to secure communications," arXiv preprint arXiv:0708.3862, 2007.*

*[4] A. Kowalski and K. Życzkowski, "Pseudo-random spatial light modulation for optical encryption," NASA Astrophysics Data System, Nov. 2017.*

*[5] Y. Zhang and Y. Wang, "A Partial Image Encryption Method Based on Pseudo-Random Sequences," ResearchGate, Dec. 2018.*

*[6] R. Gonzalez and R. Woods, Digital Image Processing, 4th ed. Pearson, 2018. [Used for understanding pseudo-random sequence application]*