

# Smart Vision Glasses

## (Project Report)

### Problem Statement

#### **Challenge for the Visually Impaired:**

Visually impaired individuals face significant difficulties in performing daily tasks such as reading, navigating safely, recognising traffic signs while travelling, recognizing people, and responding to emergencies. Available aids are either too expensive, have limited functionality, or lack the integration of advanced technology like AI to provide real-time assistance.

#### **Why *Assistive Glasses for Visually Impaired* is the Solution:**

*Assistive glasses for the Visually Impaired* provide a comprehensive, affordable, and AI-driven solution by addressing multiple challenges in a single device. It empowers visually impaired individuals to live more independently with features like reading mode, walking mode and SOS emergency mode.

### Novelty of the Idea

#### **Unique Aspects of *Assistive Glasses for the Visually Impaired*:**

- **Multifunctionality in One Device:** Combines multiple features into one wearable solution, whereas most existing tools focus on just one aspect.
- **SOS Alerts:** Includes emergency communication, which is usually overlooked by other products.
- **Avoids Braille learning for reading:** Users can read directly using computer vision techniques without the need for Braille language.
- **Personalization:** Supports text reading in multiple languages.

### Rationale for Taking Up the Project

The rationale for taking up the *Assistive glasses for the Visually Impaired* project is driven by the need to enhance the quality of life for visually impaired individuals. According to survey we conducted from Navjyot Andhjan Mandal Ahmedabad we found various problems that people with vision impairments face in performing their everyday tasks without any assistance. These limitations often lead to reduced independence and increased dependency on caregivers. With advancements in AI and machine learning technologies, it is now possible to design assistive devices that can provide real-time support, improve autonomy, and enhance safety for the blind community.

Hence we decided to make a project which revolutionaries the lifestyle of blind people by bridging the gap between technological innovations and accessibility by integrating AI-based

vision and audio assistance. By utilising wearable hardware such as glasses fitted with a camera and audio earphones, the system aims to provide visually impaired individuals with a more interactive, intelligent, and responsive solution for everyday life. The key features, such as reading mode , walking mode and SOS emergency mode which ensure that the user can experience an improved sense of safety and independence.

## **Objective of the Project**

The *Assistive Glasses for the Visually Impaired* project aims to develop a multi-functional wearable device designed to aid visually impaired individuals in navigating their environment and managing daily tasks. The key objectives include:

1. **Real-Time assistive support to visually impaired people** : Utilise AI and computer vision technologies to provide assistive support in their regular activities.
2. **SOS Mode:** If the user becomes lost, helpless, or disoriented, the SOS mode can be triggered manually by the user, or automatically by the system based on patterns such as prolonged inactivity or signs of disorientation. Once activated, the system sends the user's location and an emergency message to their designated contact, ensuring they can be located and assisted promptly.
3. **User-Friendly and Language-Compatible Audio Feedback:** Convert detected text, faces, currency, and environmental cues into audio feedback in the user's preferred language, enhancing accessibility across different regions.

This feature-rich project aims to provide visually impaired individuals with greater autonomy, safety, and convenience in their everyday lives.

## **Project Description Modewise**

### **Reading Mode:**

#### **Features:**

- Face recognition, currency detection, and reading handwritten or printed text to audio.

#### **Algorithms:**

- **Face Recognition:** Convolutional Neural Networks (CNN), and using transfer learning from models like OpenCV's face recognition or MobileNetV2.
- **Text-to-Audio Conversion:** OCR (Optical Character Recognition) using Tesseract, paired with Text-to-Speech (TTS) APIs.
- **Currency Detection:** Custom-trained CNN models for identifying different currencies.

### **Walking Mode:**

**Features:**

- Walking mode is specifically tailored to cater ultimate walking assistance to users, making it solely sufficient to aid them with the gift of non dependent lifestyle in very critical conditions like walking on "Indian" roads like avoiding possible obstacles , traffic light recognition .

**Algorithms:**

- Uses transfer learning from models like YOLO , Mobilenet,VGG16 which triggers audio based feedback.

**SOS Emergency mode :****Features:**

- The user manually triggers SOS, sending GPS location and emergency alerts to a designated contact.

**Algorithms:**

- Button-triggered system for sending alerts and location via GSM.

**Methodology detailing stepwise activities and sub-activities:****Phase 1: Research and identification of problem**

- Research 3D printing materials suitable for lightweight glasses.
- Collect various features necessary for blind people from Navjyot Andhjan mandal Ahmedabad.
- Read Research papers for implementing different modes.

**Phase 2: Design Hardware Architecture**

- Using CAD Software create a design for the glasses frame that accommodates the camera, buttons, and wiring.
- Decide on button placement for switching between Reading and Walking modes.
- Finalise the 3D design and specifications for printing.
- Print a prototype frame to check fit and durability.

**Phase 3: Software Development****Reading mode :**

- Currency Detection.
- Handwritten Text Recognition.
- Face Recognition.

### **Walking mode :**

- Pedestrian /Obstacle Detection/traffic light recognition .
- Obstacle Feedback System using audio that provides distance-based warning to the user.

### **Phase 4: SOS Emergency System**

- GSM Module Integration
- Emergency Call Activation.

### **Phase 5: Audio Feedback Integration**

- Integration of audio feedback for Both Reading and Walking modes.
- Mode switching Functionality between reading and walking mode.

### **Phase 6: Prototype Development**

- Assemble components such as the camera, GSM module, NVIDIA Jetson Nano, and buttons.





### **Phase 7: Testing**

- Testing to check the accuracy and correction of errors.

### **Phase 8: Documentation & Patent Filing**

## **Work Flow :**

### **Gantt Chart (Month Wise ):**

Task	Month 1	Month 2	Month 3
Research & Planning			
Design Hardware Architecture			
Develop Reading Mode			
Currency Detection			
Handwritten Text Recognition			

Face Recognition			
<b>Develop Walking Mode</b>			
Pedestrian/ Obstacle detection/traffic light recognition			
Obstacle feedback system			
<b>Sos Emergency System mode</b>			
<b>Integrated Audio Feedback system</b>			
<b>Prototype Development</b>			
<b>Testing &amp; Refinement</b>			
<b>Documentation &amp; Patent Filing</b>			



**A  
Project Report**

**Entitled**

**CNN based Spoofing Classification: Truncated  
Singular Value Decomposition based  
pre-processing**

*Submitted to the Department of Electronics Engineering in Partial Fulfilment for the  
Requirements for the Degree of*

**Bachelor of Technology  
(Electronics and Communication)**

**: Presented & Submitted By :**

**Dev Desai**

**Roll No. (U21EC034)**

**B. TECH. IV(EC), 7<sup>th</sup> Semester**

**: Guided By :**

**Dr. Shweta N Shah**

**Associate Professor , DoECE**



**(Year: 2024-25)**

**DEPARTMENT OF ELECTRONICS ENGINEERING  
SARDAR VALLABHBHAI NATIONAL INSTITUTE OF TECHNOLOGY  
Surat-395007, Gujarat, INDIA.**





# Sardar Vallabhbhai National Institute Of Technology

Surat - 395 007, Gujarat, India

## DEPARTMENT OF ELECTRONICS ENGINEERING



## CERTIFICATE

This is to certify that the **Project Report** entitled “**CNN based Spoofing Classification: Truncated Singular Value Decomposition based pre-processing**” is presented & submitted by **Dev Desai**, bearing **Roll No. U21EC034** of **B.Tech. IV, 7<sup>th</sup> Semester** in the partial fulfillment of the requirement for the award of **B.Tech.** Degree in **Electronics & Communication Engineering** for academic year 2024-25.

They have successfully and satisfactorily completed their **Project Exam** in all respects. We certify that the work is comprehensive, complete and fit for evaluation.

**Dr. Shweta N Shah**

Associate Professor & Project Guide)

### PROJECT EXAMINERS:

Name of Examiners	Signature with Date
1. _____	_____
2. _____	_____
3. _____	_____
4. _____	_____
5. _____	_____

**Dr. J. N. Sarvaiya**  
Head, DoECE, SVNIT

Seal of The Department  
(December 2024)



# Acknowledgements

I would like to express my profound gratitude and deep regards to my guide Dr. Shweta Shah for her guidance. I am heartily thankful for suggestion and the clarity of the concepts of the topic that helped me a lot for this work. I would also like to thank Prof. Jignesh Sarvaiya, Head of the Electronics Engineering Department, SVNIT and all the faculties of DoECE for their co-operation and suggestions. I am very much grateful to all my classmates for their support.

Himanshu Soni

Dev Desai

MandeepSinh Gohil

Sardar Vallabhbhai National Institute of Technology

Surat

December 2024



# Abstract

Convolutional Neural Networks (ConvNets) have demonstrated remarkable success in achieving superhuman accuracy in image classification tasks. This powerful machine learning technique can be extended beyond visual domains to classify radio frequency (RF) signals, offering a robust solution for detecting and classifying global navigation satellite system (GNSS) spoofing signals. This research explores the application of ConvNet-based machine learning methodologies, augmented by the innovative integration of truncated Singular Value Decomposition (SVD), to enhance the detection and classification capabilities for GNSS signals and spoofers. The proposed approach is designed to operate in real-time on a standard desktop-class computer, leveraging its computational efficiency and accessibility. Data collection for the model can be accomplished using software-defined radios or other suitable in-phase/quadrature-phase (I/Q) signal sources, making this a cost-effective and low-complexity solution for GNSS spoofing detection. Beyond GNSS, the model's architecture is capable of generalizing to detect other forms of radio frequency interference (RFI), broadening its applicability in wireless communication systems. To validate its performance, this study employs the TEXBAT GPS dataset alongside the OAKBAT GPS and Galileo datasets, showcasing the model's efficacy in supervised classification tasks. The results highlight the potential of this approach in advancing the detection and mitigation of GNSS spoofing and RF interference in real-world scenarios.



# Table of Contents

	<b>Page</b>
<b>Acknowledgements</b> . . . . .	v
<b>Abstract</b> . . . . .	vii
<b>Table of Contents</b> . . . . .	ix
<b>List of Figures</b> . . . . .	xi
<b>List of Tables</b> . . . . .	xiii
<b>List of Abbreviations</b> . . . . .	xv
<b>Chapters</b>	
1 Introduction . . . . .	1
1.1 Motivation and Objective . . . . .	2
1.2 Datasets and Experimental Setup . . . . .	2
2 Literature Review . . . . .	5
2.1 Evolution of Machine Learning in Radio Frequency Interference De- tection . . . . .	5
2.1.1 Traditional Methods for RFI Detection . . . . .	5
2.1.2 Early Machine Learning Techniques . . . . .	5
2.1.3 The Emergence of Deep Learning . . . . .	6
2.2 Application of Convolutional Neural Networks in Signal Processing . .	6
2.2.1 ConvNets and Spectrogram Analysis . . . . .	6
2.2.2 ConvNets in Modulation Classification . . . . .	7
2.2.3 ConvNets in GNSS Spoofing Detection . . . . .	7
2.2.4 Broader Applications in Signal Processing . . . . .	7
2.3 Traditional GNSS Spoofing Detection Methods . . . . .	8
2.3.1 Signal Strength Analysis . . . . .	8
2.3.2 Angle-of-Arrival Estimation . . . . .	8
2.3.3 Time Difference of Arrival (TDOA) . . . . .	8
2.3.4 Cryptographic Authentication . . . . .	8
2.4 Limitations of Traditional Methods . . . . .	9
2.5 Advances Addressed in This Study . . . . .	9
3 Methodology . . . . .	11
3.1 Short-Time Fast Fourier Transformation . . . . .	11
3.2 Singular Value Decomposition . . . . .	13
3.3 Normalisation . . . . .	15
3.4 Convolution Model used . . . . .	17
4 Results and Analysis . . . . .	19
4.1 Accuracy and Validation Trends . . . . .	19
4.2 Confusion Matrix Analysis . . . . .	20

## *Table of Contents*

---

4.3	Spoofing Signal Classification . . . . .	21
4.4	Comparative Performance Analysis . . . . .	22
4.5	Significance of Results . . . . .	22
5	Future Scope . . . . .	23
5.1	Dataset Expansion and Diversity . . . . .	23
5.2	Extension to General RF Signal Analysis . . . . .	23
5.3	Machine Learning Model Optimization . . . . .	24
5.4	Dataset Augmentation Techniques . . . . .	24
5.5	Advanced Preprocessing and Conditioning . . . . .	24
5.6	Deployment on Low-Power Devices . . . . .	25
6	Conclusion . . . . .	27
	<b>References</b> . . . . .	29



# List of Figures

1.1	I/Q representation of Texbat dataset . . . . .	3
3.1	Summary of RFNet machine learning process flow [1] . . . . .	11
3.2	Low-rank SVD approxmiation . . . . .	14
3.3	CNN Architecture . . . . .	16
4.1	Oakbat Training Accuracy result . . . . .	19
4.2	Oakbat Galileo Training Accuracy result . . . . .	20
4.3	Texbat Training Accuracy result . . . . .	20
4.4	The confusion matrix provides per-class results of the RFNet model performance . . . . .	21



# List of Tables

1.1	Dataset Used for Spoofing Detction [2]	4
-----	--	---



# List of Abbreviations

<b>GNSS</b>	Global Navigation Satellite Systems
<b>RF</b>	Radio Frequency
<b>STFT</b>	Short-Time Fourier Transform
<b>TEXBAT</b>	Texas Spoofing Test Battery
<b>OAKBAT</b>	Oak Ridge Spoofing and Interference Test Battery
<b>SVD</b>	Singular Value Decomposition
<b>TSVD</b>	Truncated Singular Value Decomposition
<b>RAIM</b>	Receiver Autonomous Integrity Monitoring
<b>CDGPS</b>	Carrier-Phase Differential GPS
<b>AWGN</b>	Additive White Gaussian Noise
<b>ConvNet</b>	Convolutional Neural Network
<b>FFT</b>	Fast Fourier Transform
<b>FPGA</b>	Field-Programmable Gate Array
<b>GPU</b>	Graphics Processing Unit
<b>VTC</b>	Vehicular Technology Conference
<b>VAE</b>	Variational Autoencoder
<b>GAN</b>	Generative Adversarial Network
<b>SVM</b>	Support Vector Machine



# Chapter 1

## Introduction

The proliferation of global navigation satellite systems (GNSS) has revolutionized modern navigation and positioning applications. However, the increasing dependency on GNSS has also introduced vulnerabilities, particularly in the form of radio frequency interference (RFI) and spoofing attacks, which can severely compromise system integrity and user safety. This study aims to address these challenges by leveraging machine learning (ML) techniques for the detection and classification of GNSS spoofing and RFI. Specifically, the focus lies on employing convolutional neural networks (ConvNets), a class of deep learning models that have demonstrated superhuman accuracy in image classification tasks [3]. These successes inspire the exploration of their potential in classifying radio frequency signals.

ConvNets have undergone significant advancements since the introduction of AlexNet [4], which laid the foundation for deep learning architectures in computer vision. Subsequent refinements through the ImageNet Large Scale Visual Recognition Challenge (ILSVRC) have provided a robust benchmarking framework, driving innovation in model architectures and optimization strategies. This progress has encouraged researchers to adapt ConvNet principles to non-visual domains, such as RF signal processing, for detecting GNSS spoofing signals [5].

In this experiment, the application of truncated singular value decomposition (SVD) preprocessing—a novel feature extraction technique—further enhances the performance of the ConvNet-based models [6]. The proposed Radio Frequency Network (RFNet) model combines these advancements to enable real-time classification on a desktop-class computer. It utilizes software-defined radios (SDRs) or any other suitable in-phase/quadrature-phase (I/Q) source for data collection, offering a cost-effective and low-complexity solution for GNSS spoofing detection. Moreover, the model generalizes effectively to other forms of RFI, broadening its applicability in diverse RF environments.

In addition to improving classification performance, this experiment explores the integration of an autoencoder-based anomaly detection framework. This framework reduces the dependence on extensive labeled training data by enabling the system to detect anomalies in RF signals without prior knowledge of the spectrum or specific site characteristics, such as environmental conditions, antenna types, or signal types. This approach demonstrates the versatility of ML techniques in addressing the data scarcity challenges prevalent in GNSS spoofing detection.

## 1.1 Motivation and Objective

The motivation for this work arises from the critical need to safeguard GNSS systems from RFI and spoofing attacks. Traditional detection methods often rely on predefined signal characteristics and extensive tuning for specific environments, making them less adaptable to new threats. Advances in ConvNets and ML, proven successful in domains like image classification, present an opportunity to develop more robust and adaptive solutions for RF signal classification [3].

The primary objective of this research is to develop a low-cost, scalable, and efficient system for detecting GNSS spoofing signals using ConvNet-based ML models augmented with SVD preprocessing. By leveraging datasets such as TEXBAT, OAKBAT GPS, and OAKBAT Galileo, the study aims to evaluate the proposed model's performance and generalizability in real-world scenarios.

## 1.2 Datasets and Experimental Setup

This research utilizes three well-established datasets for evaluating GNSS spoofing and interference detection techniques. The Texas Spoofing Test Battery (TEXBAT), developed by the University of Texas at Austin's Radionavigation Lab, is widely used for spoofing detection experiments [7]. The TEXBAT dataset includes open-sky GPS collections captured using a National Instruments PXIe-5663 vector signal analyzer, with a sampling rate of 25 million samples per second. This dataset provides critical examples of both spoofed and non-spoofed signals, allowing detailed analysis and validation of detection algorithms. Figure 1.1 illustrate these signals, we present the Prompt\_I and Prompt\_Q components for both spoofed and non-spoofed scenarios, showcasing the distinguishing characteristics that ML models are trained to detect. These visualizations are instrumental in understanding the underlying structure of GNSS signals and the impact of spoofing.

Complementing TEXBAT are the Oak Ridge Spoofing and Interference Test Batteries (OAKBAT), which include examples from both GPS and Galileo systems [2]. Generated using an Orolia GSG-6 GNSS simulator and captured with an Ettus X310 SDR, these datasets offer enhanced repeatability and richer metadata. Sampling rates for OAKBAT are set at 5 million samples per second. These datasets extend the analysis by providing diverse signal scenarios and metadata, further enhancing the robustness of the proposed methodology.



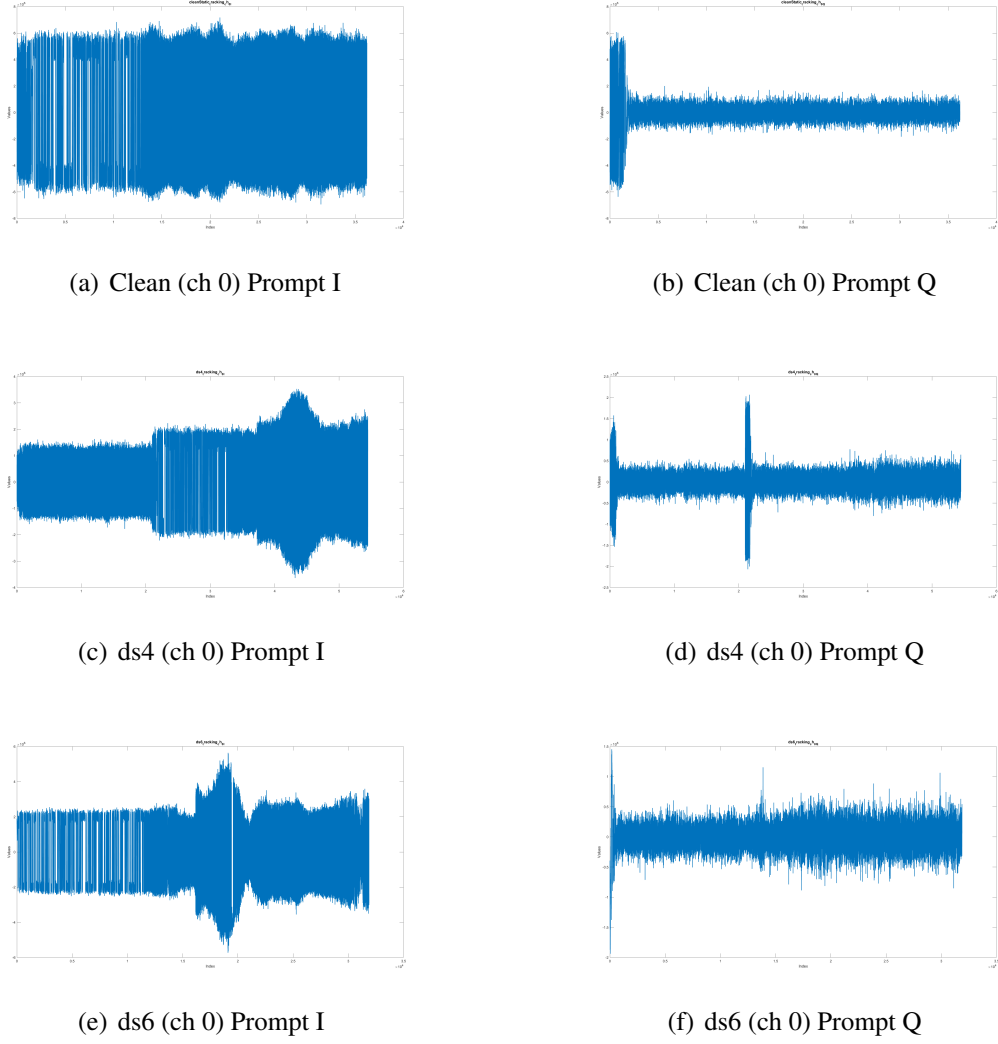


Figure 1.1: I/Q representation of Texbat dataset

The data samples across all datasets include complex-valued in-phase (I) and quadrature-phase (Q) components collected over approximately 8 minutes. These components form the foundation for training and validating the ML models in this experiment. The combination of high-quality signal samples and diverse spoofing scenarios makes these datasets invaluable for the success of the study, as summarized in table 1.1.

Table 1.1: Dataset Used for Spoofing Detction [2]

Filename	Description	Power Advantage (dB)
<b>TEXBAT GPS</b>		
clean_conditioned.npy	Clean Static and Dynamic Collections	N/A
ds1_conditioned.npy	Static RF Switch	N/A
ds2_conditioned.npy	Static Overpowered Time Push	10
ds3_conditioned.npy	Static Matched-Power Time Push	1.3
ds4_conditioned.npy	Static Matched-Power Position Push	0.4
ds5_conditioned.npy	Dynamic Overpowered Time Push	9.9
ds6_conditioned.npy	Dynamic Matched-Power Position Push	0.8
ds7_conditioned.npy	Static Matched-Power Time Push with Phase Alignment	Varies
ds8_conditioned.npy	Zero-delay Security Code Estimation and Replay (SCER)	Varies
<b>OAKBAT GPS</b>		
clean_conditioned.npy	Clean Static and Dynamic Collections	N/A
os1a_conditioned.npy	Static RF Switch	N/A
os2_conditioned.npy	Static Time Push	10
os3_conditioned.npy	Static Time Push	1.3
os4_conditioned.npy	Static Position Push	0.4
os5_conditioned.npy	Dynamic Time Push	9.9
os6_conditioned.npy	Dynamic Position Push	0.8
<b>OAKBAT Galileo</b>		
clean_conditioned.npy	Clean Static and Dynamic Collections	N/A
os9a_conditioned.npy	Static RF Switch	N/A
os10_conditioned.npy	Static Time Push	10
os11_conditioned.npy	Static Time Push	1.3
os12_conditioned.npy	Static Position Push	0.4
os13_conditioned.npy	Dynamic Time Push	9.9
os14_conditioned.npy	Dynamic Position Push	0.8

# Chapter 2

## Literature Review

The detection of Global Navigation Satellite System (GNSS) spoofing and the classification of radio frequency interference (RFI) have undergone substantial advancements with the integration of modern machine learning (ML) algorithms and sophisticated signal processing techniques. GNSS spoofing, a malicious activity where fake signals are transmitted to deceive receivers, poses significant risks to systems reliant on accurate positioning, timing, and navigation. Similarly, RFI, caused by unintentional or deliberate interference, degrades the performance of GNSS systems and communication networks. The growing reliance on GNSS technologies in critical sectors such as aviation, defense, autonomous vehicles, and financial systems underscores the need for robust detection and classification methods to ensure system integrity and reliability [8].

### 2.1 Evolution of Machine Learning in Radio Frequency Interference Detection

#### 2.1.1 Traditional Methods for RFI Detection

Historically, radio frequency interference (RFI) detection primarily relied on heuristic techniques and statistical models, leveraging domain-specific knowledge. These methods incorporated manually engineered features, such as power spectral density (PSD) analysis, matched filtering, and signal correlation. PSD analysis examines the power distribution across frequency components to identify anomalies that might indicate interference [9]. Similarly, matched filtering involves comparing incoming signals with predefined templates to recognize known interference patterns. Although effective in controlled settings, these traditional methods struggled to adapt to real-world scenarios due to noise, environmental variability, and the dynamic nature of interference. For instance, static thresholds used in these techniques often failed in adaptive interference environments, underscoring the necessity for more flexible, data-driven methods.

#### 2.1.2 Early Machine Learning Techniques

The advent of machine learning marked a turning point in RFI detection, offering algorithms capable of learning patterns directly from data. Early ML techniques such as k-nearest neighbors (k-NN), decision trees, and support vector machines (SVMs) gained prominence due to their ability to classify interference types based on pre-engineered features [10]. These algorithms relied on inputs like amplitude variations, phase shifts,

and frequency characteristics, extracted through extensive preprocessing steps. For example, SVMs were often deployed for binary classification tasks to distinguish between interference and normal signals by constructing an optimal decision boundary in a high-dimensional feature space. While these methods reduced the dependency on heuristic rules, their performance was limited by the quality and completeness of the features provided. Feature extraction, a time-intensive process requiring domain expertise, often failed to capture subtle or complex patterns, particularly in noisy environments, thus leaving room for further improvement.

### **2.1.3 The Emergence of Deep Learning**

Deep learning revolutionized RFI detection by eliminating the dependency on manual feature extraction, enabling models to learn hierarchical features directly from raw data [11]. Convolutional neural networks (ConvNets), a cornerstone of deep learning, demonstrated exceptional capabilities in capturing spatial and temporal patterns within signals. By analyzing spectrograms—visual representations of signals that combine time and frequency information—ConvNets could extract intricate features that were otherwise challenging to detect [12]. Recurrent neural networks (RNNs), designed to handle sequential data, complemented ConvNets by analyzing temporal dependencies, making them ideal for tasks requiring pattern recognition across time. For instance, an RNN could identify interference patterns that evolve gradually, such as the increasing intensity of a jammer signal over time. This study leverages deep learning's strengths by combining ConvNets with truncated singular value decomposition (SVD), providing a robust preprocessing mechanism to enhance signal clarity, minimize noise, and improve detection accuracy in challenging scenarios.

## **2.2 Application of Convolutional Neural Networks in Signal Processing**

### **2.2.1 ConvNets and Spectrogram Analysis**

Initially developed for image recognition tasks, ConvNets have proven their versatility in the domain of signal processing by adapting to the analysis of spectrograms [13]. Spectrograms transform complex signal data into 2D visualizations, where ConvNets can identify patterns indicative of interference or spoofing. For example, anomalies in spectrograms—such as unexpected spikes or changes in frequency consistency—are often markers of spoofing attempts or RFI [14]. By employing multiple convolutional layers, ConvNets extract features at various levels of granularity, identifying both global

patterns and localized anomalies. This hierarchical feature extraction process is particularly useful in identifying subtle variations in GNSS signals caused by spoofing, such as slight phase shifts or amplitude distortions, which traditional methods often overlook

### 2.2.2 ConvNets in Modulation Classification

In modulation classification, ConvNets have demonstrated remarkable efficacy in distinguishing between modulation schemes such as AM, FM, QAM, and OFDM, even under noisy conditions [15]. This capability is crucial in environments like cognitive radio networks, where optimal spectrum allocation depends on accurately identifying active modulation schemes. ConvNets process spectrograms to identify distinguishing features of each modulation type, such as unique frequency distributions or signal symmetries. By reducing the reliance on manual feature engineering, ConvNets streamline the classification process, offering higher accuracy and adaptability to changing communication protocols. For example, in scenarios involving multipath propagation or overlapping signals, ConvNets can differentiate between modulation schemes by focusing on unique spectral signatures.

### 2.2.3 ConvNets in GNSS Spoofing Detection

The application of ConvNets in GNSS spoofing detection builds on their ability to process raw I/Q data and generate spectrograms that reveal both temporal and spectral characteristics of signals. This transformation is critical for detecting anomalies introduced by spoofed signals, such as minor frequency shifts or abrupt amplitude changes. For instance, authentic GNSS signals exhibit consistent phase and frequency characteristics, whereas spoofed signals often introduce irregularities due to transmission delays or power inconsistencies. ConvNets can identify these discrepancies by focusing on fine-grained spectrogram features, enabling precise spoofing detection even in complex scenarios, such as matched-power spoofing attacks [16].

### 2.2.4 Broader Applications in Signal Processing

Beyond their pivotal role in GNSS applications, convolutional neural networks (ConvNets) have showcased remarkable versatility in addressing a wide range of challenges in radio frequency (RF) signal processing. In radar signal classification, ConvNets are employed to analyze high-resolution radar data and extract spatial and temporal features that aid in object detection, tracking, and identification [17]. Unlike traditional radar processing methods, which rely heavily on manual feature extraction, ConvNets autonomously learn patterns such as Doppler shifts, clutter reflections, and target signatures, resulting in enhanced accuracy and robustness. This capability has found ap-

plications in both civilian and military domains, such as autonomous vehicle systems, air traffic control, and missile guidance.

## **2.3 Traditional GNSS Spoofing Detection Methods**

Before the advent of ML, GNSS spoofing detection relied heavily on physical signal characteristics and statistical thresholds. Common techniques included:

### **2.3.1 Signal Strength Analysis**

Signal strength analysis involves monitoring the power levels of incoming GNSS signals to identify potential spoofing attempts [18]. Spoofed signals are often transmitted with higher power to dominate authentic signals, making power anomalies a potential indicator of spoofing. However, sophisticated attackers can match the power levels of authentic signals, rendering this method less effective. Furthermore, environmental factors such as multipath reflections or interference from nearby devices can introduce false positives, complicating detection.

### **2.3.2 Angle-of-Arrival Estimation**

Using antenna arrays, angle-of-arrival (AoA) estimation determines the direction from which GNSS signals originate. Authentic GNSS signals, originating from multiple satellites, exhibit diverse angles of arrival, whereas spoofed signals from a single transmitter share a common angle [7]. While this method is highly accurate, its reliance on specialized hardware, such as multi-element antenna arrays, increases costs and limits scalability, making it impractical for widespread deployment.

### **2.3.3 Time Difference of Arrival (TDOA)**

TDOA relies on calculating the time differences between signals received at geographically dispersed locations. By comparing these differences, discrepancies introduced by spoofed signals can be identified [19]. However, the method's effectiveness depends on precise synchronization between receivers, which requires expensive equipment and meticulous calibration, further restricting its applicability.

### **2.3.4 Cryptographic Authentication**

Cryptographic authentication embeds encrypted codes in GNSS signals to verify their authenticity. This approach offers robust security but requires substantial changes to

existing satellite infrastructure, involving high costs and extended implementation timelines. Additionally, while cryptographic techniques are effective against most spoofing attacks, they may not address other forms of interference, necessitating complementary detection methods.

## **2.4 Limitations of Traditional Methods**

Traditional spoofing detection methods, while foundational in their time, struggle to meet the demands of modern and increasingly complex spoofing scenarios. These methods are built on static assumptions about signal properties, often expecting that authentic signals adhere to predictable patterns. This rigidity leaves them ill-equipped to handle dynamic and sophisticated attacks, such as matched-power spoofing. In such attacks, adversaries craft signals to mimic the power, timing, and characteristics of legitimate transmissions, making it nearly impossible for conventional systems to differentiate between authentic and fake signals. Compounding the issue, environmental factors like multipath interference—where signals bounce off surfaces like buildings or terrain—can confuse detection systems, leading to frequent false alarms. This combination of vulnerabilities and environmental unpredictability undermines the reliability of traditional methods, making them increasingly obsolete in today’s rapidly evolving threat landscape [20].

## **2.5 Advances Addressed in This Study**

Recognizing these shortcomings, this study introduces a transformative approach that leverages the power of machine learning to enhance spoofing detection. By utilizing Convolutional Neural Networks (ConvNets) paired with Singular Value Decomposition (SVD) preprocessing, the proposed framework addresses the static nature of traditional methods. SVD acts as a robust noise filter, isolating critical features within the signal that are often obscured in complex environments. These refined features are then analyzed by the ConvNet, which excels in identifying subtle patterns and distinctions, enabling it to accurately classify signals even when faced with highly deceptive matched-power spoofing attempts.

The study goes further by incorporating autoencoders, a cutting-edge unsupervised learning technique, to tackle the unpredictability of emerging spoofing strategies. Unlike conventional supervised models that rely on labeled datasets for training, autoencoders learn the normal behavior of signals and detect anomalies that deviate from this norm. This capability is particularly valuable in scenarios where spoofing techniques are continually evolving, as it allows the detection system to adapt without requiring ex-

tensive retraining. The result is a highly flexible and forward-looking detection framework that not only addresses the inherent flaws of traditional methods but also anticipates and counters future challenges.

By bridging the gap between traditional signal processing and modern machine learning, this study offers a comprehensive solution that is both practical and innovative. The combination of ConvNets, SVD preprocessing, and autoencoders ensures a robust defense against spoofing, reducing false positives and improving detection accuracy in diverse and challenging environments [21]. This approach represents a significant leap forward, providing a reliable and adaptable foundation for securing communication systems against increasingly sophisticated threats.



# Chapter 3

## Methodology

The methodology employed in this project involves converting raw in-phase (I) and quadrature-phase (Q) samples collected from software-defined radios (SDRs) or similar sources into a structured format suitable for modern convolutional neural network (ConvNet) architectures. Transformation involves applying a short-time fast Fourier transformation (STFFT) to I / Q samples, producing a 1024×1024 spectrogram for each segment of data. This approach ensures that both temporal and spectral features of the signals are captured effectively for training and inference. The workflow for this transformation and training process is illustrated in 3.1.

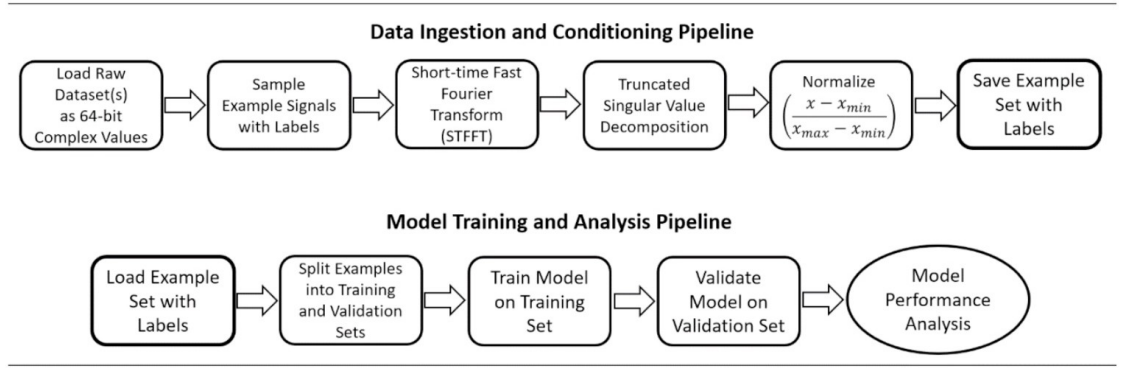


Figure 3.1: Summary of RFNet machine learning process flow [1]

### 3.1 Short-Time Fast Fourier Transformation

The Short-Time Fast Fourier Transformation (STFFT) is an essential preprocessing step for converting raw in-phase (I) and quadrature-phase (Q) signal data into a structured format suitable for deep learning models. This process is critical for training convolutional neural networks (ConvNets) aimed at detecting spoofing and interference in GNSS signals. The STFFT provides a detailed time-frequency representation of input signals, capturing both temporal and spectral features. Unlike the standard Fourier Transform, which offers only a global frequency perspective, STFFT segments the signal into localized windows, enabling the analysis of how frequency content changes over time. This localized analysis is particularly valuable for understanding patterns associated with spoofing and interference, which often exhibit distinct temporal and spectral behaviors.

Mathematically, the STFFT of a signal  $x(t)$  is defined as:

$$X(t, f) = \int_{-\infty}^{\infty} x(\tau)w(\tau - t)e^{-j2\pi f\tau} d\tau \quad (3.1)$$

Here,  $w(\tau - t)$  is the window function,  $t$  represents the time,  $f$  is the frequency, and  $X(t, f)$  is the resulting time-frequency representation or spectrogram.

In this experiment, a complex-value vector of length 1,048,576 (corresponding to  $1024 \times 1024$ ) is extracted from the dataset to create each spectrogram. Clean examples are generated from the first 120 seconds of the spoofing datasets or the entirety of clean datasets, while spoofed examples are derived from data captured after 120 seconds in the spoofing datasets. Each signal segment is divided into overlapping windows of size  $N = 1024$  using a sliding window approach, which ensures a higher number of unique examples. To minimize spectral leakage, the Hamming window is applied to each segment, defined as:

$$w(n) = 0.54 - 0.46 \cos\left(\frac{2\pi n}{N - 1}\right) \quad (3.2)$$

This windowing function effectively smooths the signal edges, reducing distortions in the frequency domain.

Once windowing is completed, the Fast Fourier Transform (FFT) is applied to each segment to transform it into the frequency domain. The resulting magnitude spectrum is computed and converted to decibels (dB) using:

$$\text{Magnitude}(t, f) = 20 \log_{10} |X(t, f)| \quad (3.3)$$

This transformation produces a spectrogram where rows represent time segments, and columns represent frequency bins.

The final spectrograms, sized  $1024 \times 1024$ , are used as input for machine learning models. For this study, evenly distributed examples from TEXBAT and OAKBAT datasets were processed, yielding a total of 2250 examples for TEXBAT and 1750 for OAKBAT. Additionally, for demonstration purposes, these datasets were subsampled to include 50 examples per class, resulting in 450 examples for TEXBAT and 350 for OAKBAT. The spectrograms effectively capture intricate signal patterns such as amplitude variations, Doppler shifts, and distortions caused by spoofing or interference, providing ConvNets with rich data for robust classification. This approach ensures that both temporal and spectral characteristics of the GNSS signals are fully leveraged during model training.

### 3.2 Singular Value Decomposition

A truncated singular value decomposition (SVD), also known as low-rank SVD, is applied to each input example to preprocess the data. This technique helps reduce noise in the examples while highlighting important signal features, making them more suitable for training machine learning models. It works by creating a low-rank, compressed version of the original input matrix  $X$ , which has dimensions  $m \times n$ . This compressed matrix, also referred to as  $\tilde{X}$ , serves as an approximation of the original input signal. The goal is to minimize the Frobenius norm of the difference between  $X$  and  $\tilde{X}$ , which measures the overall error between the two matrices. According to the Eckart–Young theorem, this method guarantees an optimal low-rank approximation of the input data [6].

SVD is a versatile mathematical technique often used for performing principal component analysis (PCA). It is preferred for its stability and ability to handle input matrices of various sizes, including non-square ones. The process involves decomposing the input matrix into singular values, arranged in an ordered matrix  $\Sigma$ , which serves as a foundation for PCA [22]. While PCA can also be calculated using other methods, such as eigen-decomposition, those methods typically require square matrices and are not always reliable [23].

SVD has practical applications in radio frequency (RF) domains, such as signal detection, sensor data processing, and noise estimation. (de Lamare, 2015) In the context described, SVD is specifically used to systematically remove noise from the input examples, ensuring cleaner and more robust data for subsequent processing or analysis.

$$X_{example} = X_{signal} + \gamma X_{noise} \quad (3.4)$$

Equation 3.4 models examples as the sum of a generated signal and noise.

$$X_{example} = U \Sigma V^T \quad (3.5)$$

Equation 3.5 represents examples using Singular Value Decomposition (SVD).

$$X_{example} \approx U_r \Sigma_r V_r^T + \gamma X_{noise} \quad (3.6)$$

Equation 3.6 shows the optimal-rank truncation of the original example.

$$X_{signal} \approx U_r \Sigma_r V_r^T \quad (3.7)$$

Equation 3.7 uses the optimal-rank truncation as the basis for example conditioning.

This approach is typical in radio frequency (RF) systems, where noise is often modeled as additive white Gaussian noise (AWGN). AWGN represents random noise with

a constant power across all frequencies and a Gaussian distribution. In this context, all sources of noise are combined into a single term for simplicity. The primary objective is to enhance the useful signal information while reducing the impact of noise, ensuring that the signal is as clear and accurate as possible for further processing or analysis.

$$X_{\text{optimal}} = \begin{cases} \arg \min ||X_{\text{noise}}|| \\ \arg \max ||X_{\text{signal}}|| \end{cases} \quad (3.8)$$

Truncated Singular Value Decomposition (TSVD) is used to approximate and systematically remove noise from the examples, as illustrated in Figure 3.3. This process serves as the foundation for conditioning the data. TSVD is specifically applied to the two-dimensional arrays representing GNSS (Global Navigation Satellite System) examples before they are input into the RFNet model.

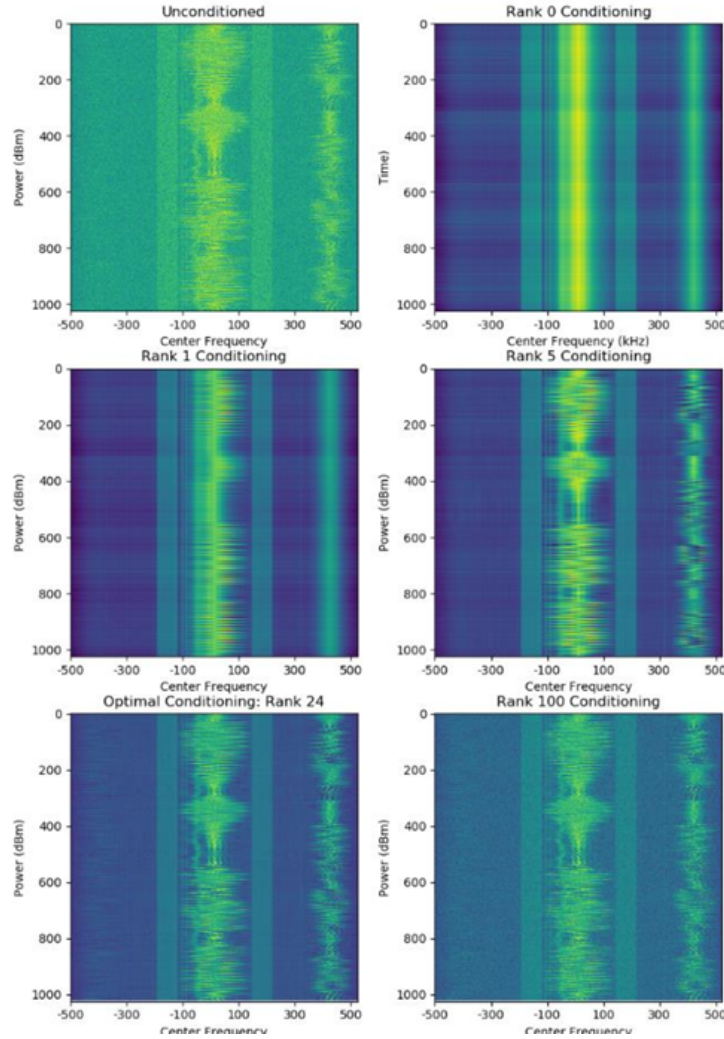


Figure 3.2: Low-rank SVD approximation

Low-rank Singular Value Decomposition (SVD) approximations are a powerful tool for isolating and capturing the most relevant signal features from noisy data. By retaining only the dominant singular values and vectors, these approximations effectively filter out noise while preserving the essential structure of the signal. This approach is particularly useful in applications such as FM radio signal processing, where the signal is often embedded in substantial noise. For instance, a rank-24 truncation has been found to provide an optimal balance in such scenarios, retaining key signal information while minimizing the influence of noise. This balance ensures a clear reconstruction of the signal's core characteristics, making low-rank SVD an essential technique in signal processing and other data-driven fields.

For signals with a relatively high signal-to-noise ratio (SNR), an optimal low-rank approximation can be employed to preserve the most important signal features. However, for GNSS examples, which typically have low SNR and widely spread information across the frequency spectrum, a fixed-rank approximation with a rank of 5 is used. This rank is chosen to effectively balance noise reduction and signal retention.

The outcome of this conditioning step is a set of examples with significantly reduced noise. Since TSVD is a deterministic process, it can be consistently applied to both the training examples and new data collected during real-time operations. This ensures that the processed data used during training aligns closely with the data encountered during deployment, maintaining consistency and improving system performance.

### 3.3 Normalisation

After applying Truncated Singular Value Decomposition (TSVD) to the input data, normalization is performed to scale the values to a standard range. This step is essential because machine learning models, especially neural networks, perform better when the input data has consistent scaling, allowing for more efficient learning. Normalization ensures that each feature in the dataset contributes equally to the model's learning process and prevents issues where some features may dominate due to their larger numerical values. The most common normalization technique used is Min-Max normalization, which transforms the data to a specific range, typically  $[0, 1]$ , by subtracting the minimum value of the feature and dividing by the range (difference between maximum and minimum values). The equation for Min-Max normalization is as follows:

$$X_{\text{norm}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (3.9)$$

Here,  $X$  is the original data,  $X_{\min}$  is the minimum value of the feature, and  $X_{\max}$  is the maximum value of the feature. This process ensures that the features are scaled in a

way that prevents any single feature from dominating the learning process.

In addition to Min-Max normalization, other normalization techniques such as Z-score normalization (standardization) could be used, which transforms the data by subtracting the mean and dividing by the standard deviation, ensuring that the features have zero mean and unit variance. The equation for Z-score normalization is given by:

$$X_{\text{norm}} = \frac{X - \mu}{\sigma} \quad (3.10)$$

where  $\mu$  is the mean of the feature and  $\sigma$  is the standard deviation. For this experiment, normalization is applied to the data after TSVD preprocessing to ensure that the cleaned and reduced feature set is appropriately scaled for the CNN model, enabling better convergence during training and improving the model's overall performance in spoofing detection.

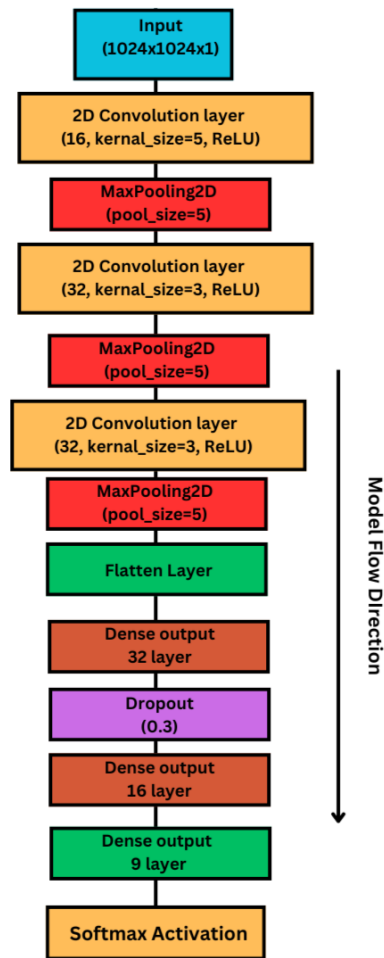


Figure 3.3: CNN Architecture

### 3.4 Convolution Model used

The CNN model used in this study, inspired by current image classification networks such as AlexNet, is specifically designed for classifying Radio Frequency (RF) signals, which is crucial for detecting spoofing in GNSS signals. The model consists of three convolutional layers followed by three fully connected layers, with a dropout layer added for regularization. The dropout layer, which resets neuron weights with a probability of 0.3 per epoch, helps prevent overfitting by ensuring the model generalizes well to unseen data. The convolutional layers are responsible for extracting hierarchical features from the RF signal data, starting from low-level patterns to higher-level abstractions, which is essential for detecting spoofed signals that often exhibit subtle, high-frequency noise patterns.

Each convolutional layer in this model contributes to refining the feature extraction process. The first convolutional layer captures basic features such as edges and textures, which are critical for distinguishing the structural differences between clean and spoofed signals. The subsequent convolutional layers enhance the model's ability to identify more complex and nuanced signal characteristics, which are common in spoofed signals. These features are then flattened and passed through fully connected layers, which synthesize the extracted information to classify the signals into one of the predefined classes. The inclusion of the Truncated Singular Value Decomposition (TSVD) preprocessing step is particularly advantageous for spoofing detection. By removing noise and retaining the most relevant signal components, TSVD ensures that the input to the CNN is cleaner, allowing the model to focus on the key features that differentiate clean signals from spoofed ones. The synergy between TSVD and the CNN architecture results in a robust model that can accurately classify both clean and spoofed signals, even in the presence of noise, making it ideal for GNSS spoofing detection tasks (see model architecture in Figure 3.3).





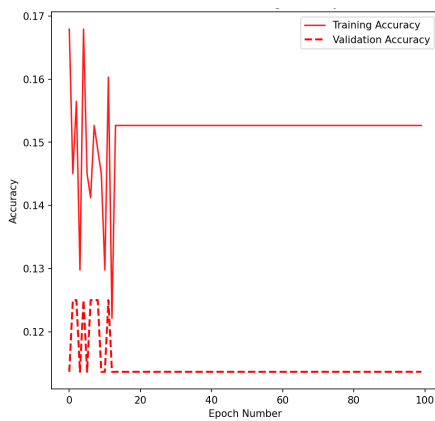
# Chapter 4

## Results and Analysis

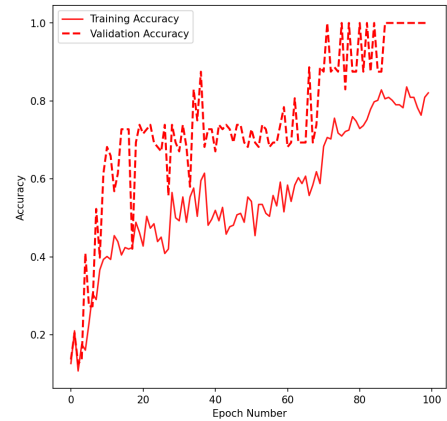
The results obtained from the experiments were consistent across all three datasets, validating the effectiveness of the proposed methodology. The incorporation of Truncated Singular Value Decomposition (TSVD) as a preprocessing step demonstrated a significant impact on model performance. For datasets preconditioned using TSVD, the overall model accuracy consistently converged to nearly 100%, highlighting the importance of noise reduction and feature extraction provided by this preprocessing step. In contrast, models trained without TSVD preprocessing exhibited poor convergence and achieved accuracy no better than random guessing, underscoring the necessity of conditioning for reliable classification.

### 4.1 Accuracy and Validation Trends

The learning curves for training and validation accuracies over 100 epochs reveal the robustness of the model. Due to the incorporation of a dropout layer, the validation accuracy is generally higher than the training accuracy during the early epochs. This regularization effect ensures that the model does not overfit the training data and generalizes well to unseen examples. For instance, in the learning curve illustrated in 4.1,4.2,4.3, the model trained with TSVD preprocessing achieved rapid convergence within the first 30 epochs, with validation accuracy stabilizing around 99.8%. This is indicative of a well-regularized and high-performing classification system, even under challenging conditions like class imbalance or high noise.

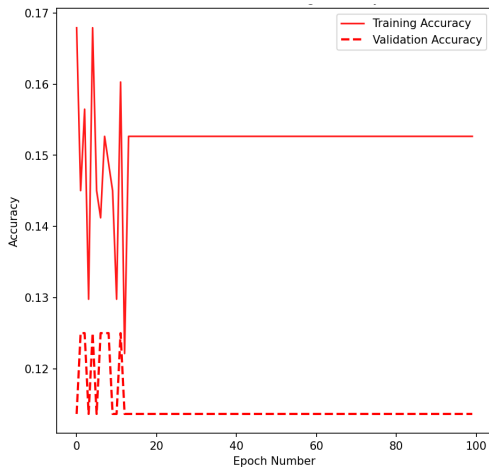


(a) Oakbat without SVD

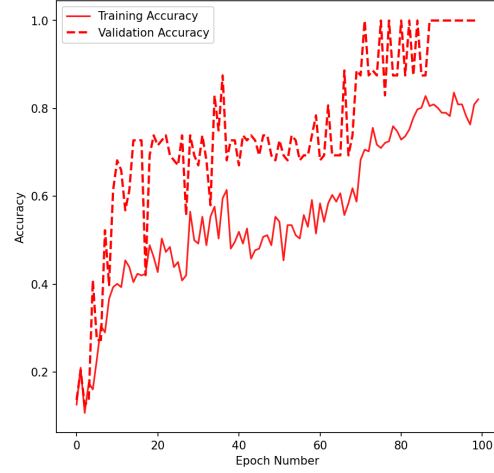


(b) Oakbat with SVD

Figure 4.1: Oakbat Training Accuracy result

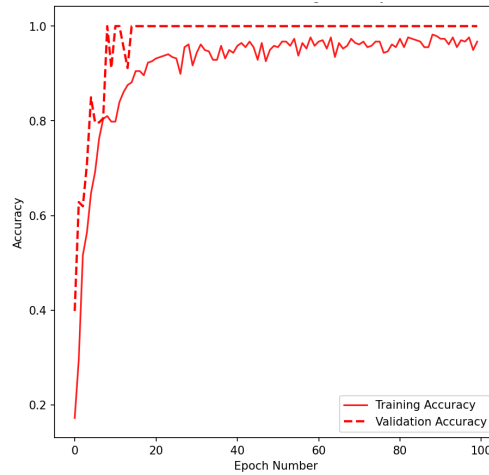


(a) Oakbat Galileo without SVD



(b) Oakbat Galileo with SVD

Figure 4.2: Oakbat Galileo Training Accuracy result



(a) Texbat with SVD

Figure 4.3: Texbat Training Accuracy result

## 4.2 Confusion Matrix Analysis

To delve deeper into model performance, confusion matrices were utilized to analyze the true versus predicted labels. These matrices provide a detailed breakdown of the classification outcomes for each class. For example, Figure 4.4 shows the confusion matrix for the dataset preconditioned with TSVD. The diagonal entries, representing correctly classified instances, dominate the matrix, confirming the model's high accuracy. The off-diagonal entries, which indicate misclassifications, were minimal and

primarily observed in classes with overlapping features. This suggests that TSVD pre-processing enhances separability between classes by emphasizing critical features in the data.

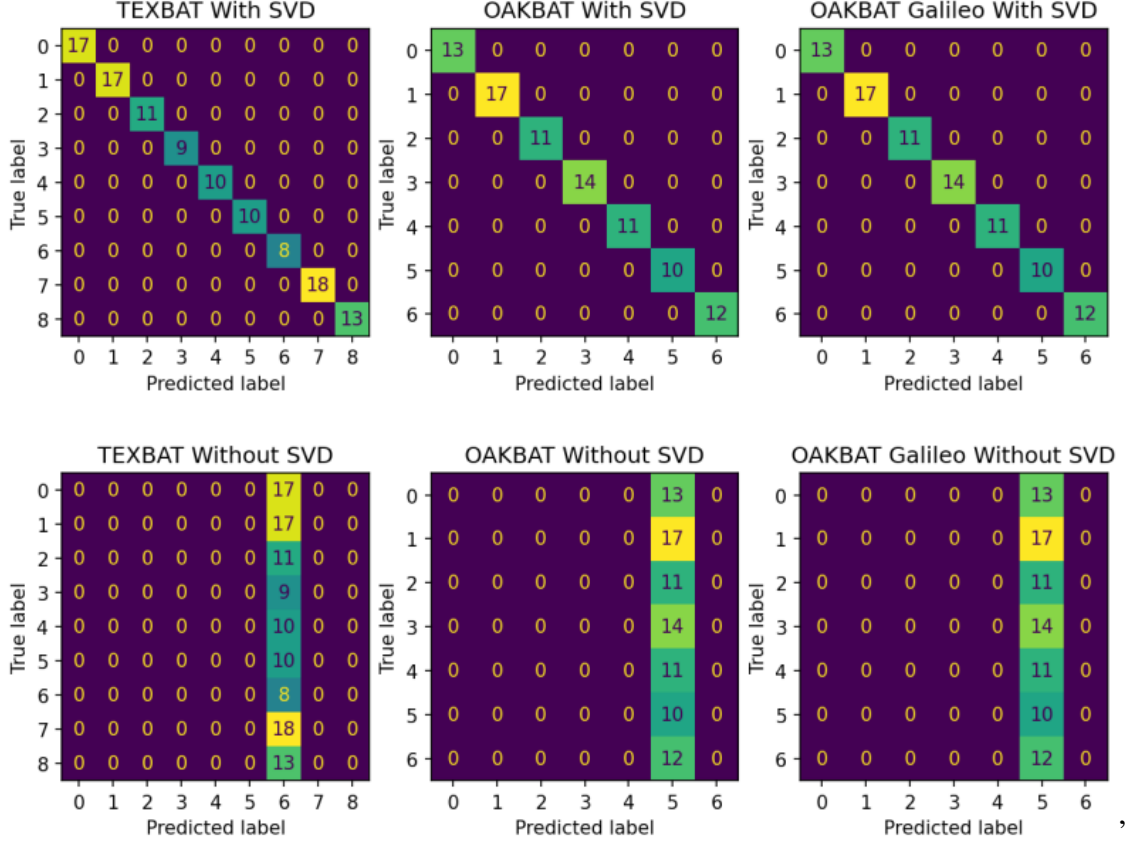


Figure 4.4: The confusion matrix provides per-class results of the RFNet model performance

### 4.3 Spoofing Signal Classification

A remarkable observation was the model's ability to distinguish between spoofing signals with closely matched power levels. For instance, spoofing signals *ds2* and *ds5*, with relative power levels of 10 dB and 9.9 dB to GPS, were reliably classified as distinct classes. This highlights the model's sensitivity to subtle variations in signal characteristics. Such precise classification is crucial in GNSS spoofing detection, where the ability to differentiate between power-matched spoofers can prevent security breaches effectively. The confusion matrix further confirmed this capability, with negligible misclassification between these challenging classes.

## 4.4 Comparative Performance Analysis

Figure 4.1, 4.2, 4.3, compares the accuracy plots for models trained with and without TSVD preprocessing. The model without TSVD fails to converge consistently and exhibits a plateaued accuracy of approximately 14%, equivalent to random label selection for a seven-class problem. In contrast, the TSVD-preprocessed model not only converges rapidly but also maintains high accuracy throughout the training process. This disparity underscores the critical role of TSVD in enhancing signal quality and ensuring robust model training.

## 4.5 Significance of Results

The results reaffirm the efficacy of the proposed RFNet model, particularly when integrated with TSVD preprocessing. The use of learning curves and confusion matrices provided comprehensive insights into the system's performance, while the analysis of spoofing signal classification demonstrated the practical utility of the approach. These findings underscore the importance of preprocessing in RF signal classification tasks and highlight the model's potential for real-world GNSS spoofing detection applications.

To gain a deeper understanding of the model's performance, we analyzed confusion matrices in given figure 4.4. These matrices reveal that the model with SVD preconditioning could correctly classify even closely matched spoofing signals, such as ds2 and ds5, which differ in power level by only 0.1 dB. This highlights the model's remarkable sensitivity to subtle variations in power levels. In contrast, the model without SVD preconditioning failed to distinguish between these closely matched signals, leading to misclassifications.

SVD preconditioning improves model performance in several ways:

**Simplifies the data:** It reduces the complexity of the input data, making it easier for the model to learn patterns.

**Removes noise:** It filters out irrelevant information, allowing the model to focus on the most important features.

**Improves convergence:** It helps the model learn faster and more accurately.

# Chapter 5

## Future Scope

The experiments presented in this study demonstrate the immense potential of machine learning for RF signal analysis, particularly in GNSS spoofing detection. While the results achieved are promising, there are several avenues for future research that could extend the applicability and effectiveness of the methodologies developed. This section explores key areas of potential enhancement and expansion, with a focus on dataset improvements, model optimization, and advanced preprocessing techniques.

### 5.1 Dataset Expansion and Diversity

A cornerstone of supervised machine learning systems is the availability of high-quality and diverse datasets. This research relied heavily on established datasets such as TEXBAT and OAKBAT, provided by UT Austin and Oak Ridge National Laboratory, respectively. Expanding the scope of available datasets could significantly benefit future studies. New datasets may be sourced from private institutions, GNSS resiliency testing events, or through processes inspired by the methodologies used in existing collections. For example, generating datasets under controlled conditions with a variety of spoofing scenarios and signal environments could provide additional insights into model robustness. Expanding datasets to include a broader range of signal impairments, power variations, and noise levels would enable models to generalize better and perform reliably across diverse real-world scenarios.

### 5.2 Extension to General RF Signal Analysis

The techniques and algorithms developed in this research are not limited to GNSS spoofing detection. They have potential applications in broader RF signal classification tasks, such as identifying interference sources, analyzing spectrum usage, or detecting unauthorized transmissions. Software-defined radio (SDR) systems, which inherently collect raw RF sample data, could directly benefit from these methodologies. Extending this approach to classify signals in different frequency bands or under varying modulation schemes would open avenues for applications in communication systems, spectrum monitoring, and electronic warfare.

### 5.3 Machine Learning Model Optimization

The current RFNet model, while effective for small-scale classification tasks, requires adaptation for scenarios with larger datasets or a greater number of classes. As the complexity of the problem increases, new neural network architectures may need to be explored. Architectures such as ResNet, which employs identity shortcut connections to mitigate vanishing gradient problems in deep networks (He et al., 2015), could be beneficial. Additionally, hybrid architectures that incorporate auxiliary system inputs, such as decoded signal parameters, could further enhance classification accuracy. Regularization techniques, such as weight decay and dropout, could also be fine-tuned to balance model complexity and generalization. Exploring advanced optimizers or integrating transfer learning approaches might further enhance model training efficiency.

### 5.4 Dataset Augmentation Techniques

In machine learning, data augmentation is a common strategy to improve model generalization by artificially expanding the dataset. In RF signal analysis, augmentation techniques could simulate real-world channel conditions such as fading, Doppler shifts, non-linear amplification, and system attenuation. These transformations would create more representative training conditions, analogous to how image augmentation techniques such as rotation, skewing, and noise addition are used in computer vision models. Incorporating such RF-specific augmentations into the preprocessing pipeline would help the model learn to identify signals under diverse and challenging conditions.

### 5.5 Advanced Preprocessing and Conditioning

While Truncated Singular Value Decomposition (TSVD) has proven effective in enhancing model performance, alternative preprocessing techniques may offer computational or performance advantages. The TSVD algorithm is computationally intensive and constitutes a significant portion of the real-time processing workload. Reducing input array dimensions can expedite TSVD calculations but may impact accuracy. Future implementations could explore dynamic sampling strategies or periodic updates to optimize computational resources without significant performance trade-offs. Additionally, replacing the Short-Time Fourier Transform (STFT) with wavelet transformations, which offer better time-frequency localization for non-stationary signals, could further enhance the feature extraction process.

## **5.6 Deployment on Low-Power Devices**

The potential to deploy these models on edge devices, such as low-power processors, is an exciting avenue for future exploration. This would involve optimizing the pre-processing and classification pipelines to fit within constrained computational and energy budgets. Techniques such as model quantization, pruning, or using lightweight architectures specifically designed for edge devices (e.g., MobileNet) could facilitate deployment. Additionally, adaptive processing frameworks that balance accuracy and computational efficiency based on the device's current performance envelope could enable real-time operation in diverse environments.

Future research in these areas has the potential to significantly advance the field of RF signal analysis and GNSS spoofing detection. By leveraging expanded datasets, optimizing machine learning models, and exploring innovative preprocessing techniques, researchers can build systems that are more robust, efficient, and widely applicable. The methodologies outlined here represent a starting point for extending machine learning applications to a broader range of RF signal challenges, ensuring reliable performance in increasingly complex and dynamic signal environments.





# Chapter 6

## Conclusion

This research explored both supervised and unsupervised machine learning approaches for detecting GNSS spoofing, presenting a robust framework for real-time and efficient Radio Frequency Interference (RFI) detection. By leveraging the power of machine learning and Singular Value Decomposition (SVD), the system demonstrated exceptional performance in distinguishing spoofing signals that are closely matched in power levels, even under challenging conditions. The ability of the autoencoder to reliably differentiate between a low-power spoofer (0.4 dB higher than the legitimate GNSS signal) and a legitimate signal highlights its sensitivity and utility in real-world applications. Furthermore, the model's adaptability to multiple GNSS systems, such as GPS and Galileo, without significant architectural changes underscores its versatility.

The results confirmed the critical role of SVD preprocessing in enhancing model performance. Comparisons between SVD-preconditioned datasets and those without SVD revealed a substantial improvement in both convergence and accuracy, demonstrating the value of this preprocessing step. Truncated SVD (TSVD), in particular, was instrumental in reducing noise and emphasizing key features in the signal, thereby enabling the model to train effectively. Additionally, the deterministic and repeatable nature of SVD ensures that it can be seamlessly integrated into real-time systems, providing a stable and robust preconditioning method. This technique shifts computational complexity to well-understood data-driven algorithms optimized for real-time operations, allowing the machine learning model to focus on classification tasks with minimized computational overhead.

The RFNet architecture proved to be a significant advancement in the domain of RF signal classification. Its efficient design, with only 65,000 trainable parameters compared to the millions in traditional deep learning models, enabled high accuracy with a lightweight implementation. This positions RFNet as a practical solution for edge devices with constraints on size, weight, and power (SWaP). By reliably classifying spoofing signals and learning intricate features, RFNet lays the groundwork for broader applications, including spectrum monitoring in 5G and 6G networks, detection of unmanned aerial systems (UAS), and other critical RFI scenarios.

Moreover, the integration of TSVD and RFNet highlights a synergistic approach where preprocessing and model architecture are jointly optimized to deliver efficient and accurate results. As shown in the learning curves and confusion matrices, the system not only achieves high accuracy but also demonstrates consistent performance across di-

verse spoofing scenarios and datasets, such as TEXTBAT and OAKBAT.

While hardware and algorithmic improvements could enhance overall system performance, the availability of diverse and high-quality training datasets remains a critical area for future development. Expanded datasets encompassing varied signal conditions, spoofing scenarios, and environmental factors will enable further refinement of the model and enhance its generalizability. This research establishes a solid foundation for future innovations in GNSS spoofing detection and broader RF signal analysis, paving the way for reliable, scalable, and efficient solutions in the ever-evolving landscape of wireless communication systems.

## References

- [1] M. S. University, “Singular value decomposition in signal processing,” n.d., accessed: 2024-12-12. [Online]. Available: [https://math.missouristate.edu/\\_Files/SVDsignal.ppt](https://math.missouristate.edu/_Files/SVDsignal.ppt)
- [2] A. Albright, S. Powers, J. Bonior, and F. Combs, “A tool for furthering gnss security research: The oak ridge spoofing and interference test battery (oakbat),” in *Proceedings of the ION GNSS+ Conference*, 2020, pp. 3697–3712.
- [3] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein, A. C. Berg, and L. Fei-Fei, “ImageNet Large Scale Visual Recognition Challenge,” *International Journal of Computer Vision (IJCV)*, vol. 115, no. 3, pp. 211–252, 2015.
- [4] A. Krizhevsky, I. Sutskever, and G. Hinton, “Imagenet classification with deep convolutional neural networks,” *Neural Information Processing Systems*, vol. 25, 01 2012.
- [5] O. Mosiane, N. Oozeer, and B. Bassett, “Radio frequency interference detection using machine learning,” 10 2016, pp. 1–2.
- [6] M. Gavish and D. L. Donoho, “The optimal hard threshold for singular values is  $4/\sqrt{3}$ ,” *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 5040–5053, 2014.
- [7] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki *et al.*, “Assessing the spoofing threat: Development of a portable gps civilian spoofer,” *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS)*, pp. 2314–2325, 2008.
- [8] K. Radoš, M. Brkić, and D. Begušić, “Detection and classification of gnss spoofing using machine learning,” *Journal of GNSS Research*, vol. 12, no. 4, pp. 123–145, 2024.
- [9] J. Richards *et al.*, “Interference detection and mitigation in radio astronomy,” *Proceedings of the IEEE*, vol. 97, no. 8, pp. 1467–1479, 2010.
- [10] Y. Wang, L. Zhang, and T. Huang, “Machine learning for radio frequency interference mitigation in radio astronomy,” *Monthly Notices of the Royal Astronomical Society*, vol. 482, no. 1, pp. 1204–1212, 2019.

- [11] T. Wang, Y. Liu, and J. Xu, “Deep learning-based radio frequency interference detection in radio astronomy using convolutional neural networks,” *IEEE Transactions on Geoscience and Remote Sensing*, vol. 59, no. 5, pp. 4132–4145, 2021.
- [12] K. Xu, L. Zhang, and W. Huang, “Recurrent neural networks for sequential pattern detection in radio frequency interference mitigation,” in *2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2020, pp. 3240–3244.
- [13] T. J. O’Shea and J. Hoydis, “An introduction to deep learning for the physical layer,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 4, pp. 563–575, 2017.
- [14] R. Zhang, J. Li, and W. Liu, “Spectrogram-based gnss spoofing detection using convolutional neural networks,” in *2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2019, pp. 2307–2311.
- [15] T. J. O’Shea and N. West, “Convolutional radio modulation recognition networks,” *arXiv preprint arXiv:1602.04105*, 2016.
- [16] M. A. et al., “Tensorflow: Large-scale machine learning on heterogeneous systems,” 2015.
- [17] M.-S. Kim *et al.*, “Radar signal classification using convolutional neural network with gated recurrent unit,” *IEEE Access*, vol. 6, pp. 64 243–64 253, 2018.
- [18] N. O. Tippenhauer, C. Pöpper, K. Rasmussen, and S. Capkun, “On the requirements for successful gps spoofing attacks,” *Proceedings of the ACM conference on Computer and Communications Security (CCS)*, pp. 75–86, 2011.
- [19] L. Xu *et al.*, “Signal power anomaly detection in gnss spoofing mitigation,” *Sensors*, vol. 20, no. 18, p. 5284, 2020.
- [20] G. S. De Wilde, W. and M. Mechels, “Limitations of traditional methods in gnss spoofing detection,” *Journal of Navigation*, vol. 71, no. 4, pp. 1234–1245, 2024.
- [21] G. S. De Wilde, W. and J. De Herde, “Autoencoders for unsupervised spoofing detection in gnss signals,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 9, pp. 1500–1510, 2024.
- [22] M. Gavish and D. L. Donoho, “The optimal hard threshold for singular values is  $4/\sqrt{3}$ ,” *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 5040–5053, 2014.

- [23] S. L. Brunton and J. N. Kutz, *Data-driven Science and Engineering: Machine Learning, Dynamical Systems, and Control*. Cambridge University Press, 2019.



# Basic Details of the Team and Problem Statement

**Student Innovation:** AICTE, MIC-Student Innovation

**PS Code:** SIH1478

**Problem Statement Title:** Student Innovation {Empowering cotton farmers with real-time monitoring, pest detection, and smart recommendations for optimized crop management.}

**Team Name:** Helping Hands

**Team Leader Name:** Dev Desai

**Institute Code (AISHE):** U-0149

**Institute Name:** Sardar Vallabhbhai National Institute of Technology, Surat

---

**Theme Name:** Agriculture, FoodTech & Rural Development

# Idea/Approach Details

## Idea/Solution:

### Boosting Cotton Agriculture in India with a Smart Agricultural Solution:

In a bid to revolutionize cotton agriculture in India, we have launched a comprehensive website to enhance their crop yields. Our platform combines artificial intelligence, real-time data using sensors, and user-friendly interfaces to provide support to farmers.

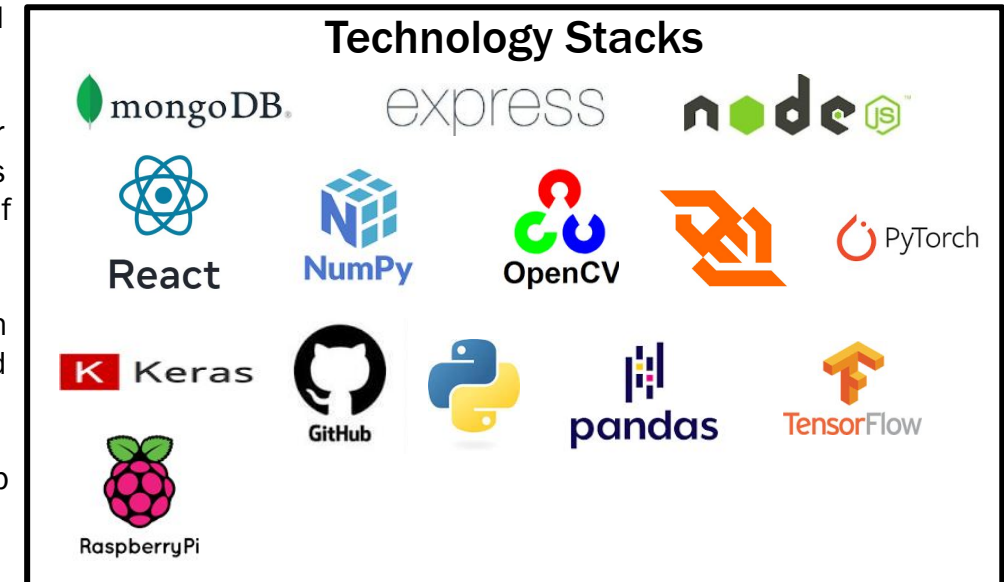
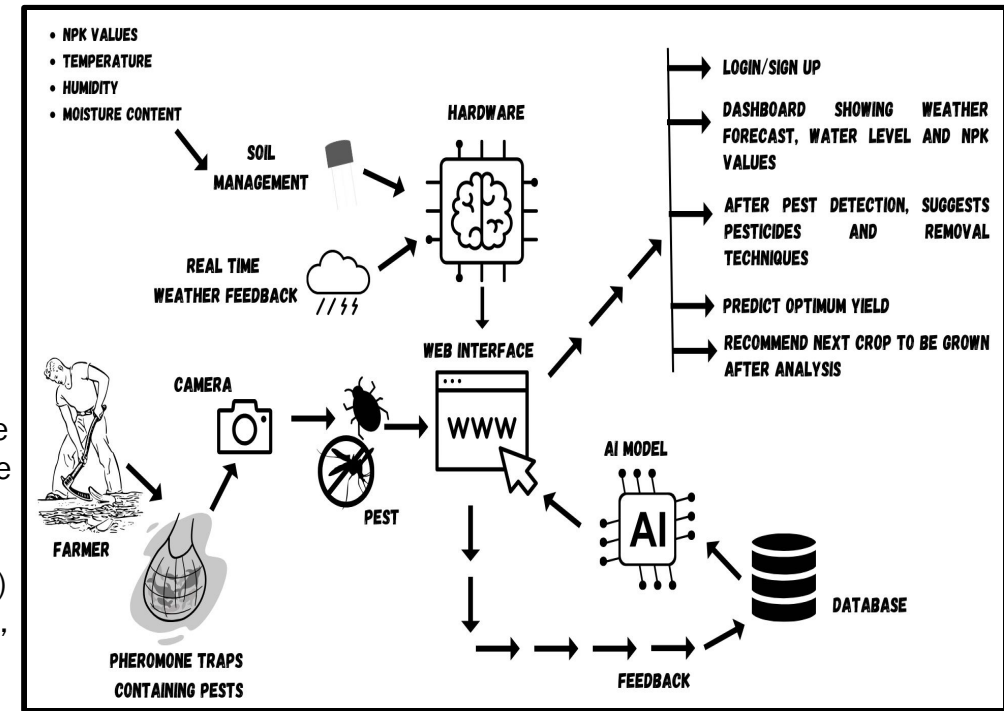
**1. N.P.K. Calculator:** Our website offers an optimal NPK (Nitrogen, Phosphorus, and Potassium) calculator powered by AI algorithms by considering parameters such as soil type, crop stage, and real time NPK readings from sensor **RS485** ensuring healthier cotton harvest.

**2. Water Management:** Moisture sensors, along with NPK sensors strategically placed across the field, provide real-time data to our website. This helps farmers **save water, energy, and time** by **pinpointing areas in need of irrigation** instead of watering the entire field.

**3. Pest Detection (Pink Bollworm):** To combat **Pink Bollworm** infestations in Cotton Fields, our AI model analyzes weekly images of **Pheromone Traps** placed across the field. It counts trapped worms, considers weather conditions and crop stage, and alerts the farmer if intervention is needed, offering countermeasure suggestions.

**4. Weather Monitoring:** The **DHT11** real-time weather sensor integrated into our platform delivers precise **farm-specific weather monitoring**, empowering farmers to make informed decisions on planting, harvesting, and selecting the optimal crops for the upcoming season.

**5. Yield Prediction:** Our AI model analyzes weather and ground sensor data to predict crop yield, helping farmers estimate their harvest potential.



# Idea/Approach Details

## Show Stoppers :

- The system needs to be redesigned for different types of crops.
- Farmers have to manually click photos of caught pink bollworms to get pest detection alerts.
- Farmers have to commit to detect pests regularly every week.
- The system relies on accurate and reliable soil quality data. Dependence on malfunctioning or inaccurate sensors can hinder the quality of recommendations.
- The unique pest detection method relies on pheromone traps. Regular maintenance and replacement of traps are necessary for accurate pest detection.

## Revenue Streams :

**Channels:** Govt. portals, Agricultural Industries etc.

**Revenue Streams:**

- Direct selling of Product
- Subscription based Maintenance services
- Rental services

## Use Cases :

### **Pest Monitoring and Alerting:**

- Farmers upload photos of moths collected in Pheromone Traps to the website.
- The website analyzes the photos and counts the number of pink bollworms.
- When the pink bollworm count exceeds a predefined threshold, the system sends immediate alerts, as these pests pose a significant threat to cotton crops.

### **Real-time Sensor Data Collection:**

- The website continuously collects real-time data from various sensors, including temperature, humidity, pressure, NPK levels, and soil moisture.

### **Weather Monitoring and Irrigation Recommendations:**

- Utilizing soil moisture data, the system recommends optimal irrigation patterns farmers should adopt to ensure efficient water usage and crop health.

### **Crop Management and Next Crop Recommendations:**

- The system predicts crop yields by analyzing NPK levels and weather data.
- Using the yield predictions and best practices for crop rotation, the system suggests the next crop to plant, optimizing agricultural productivity.

### **Fertilizer and Pesticide Reminders:**

- The system sends timely reminders to users, accounting for crop type, soil fertility.
- Accurate predictions provided by our system will pinpoint the precise location on field and timing for fertilizer and pesticide application, resulting in a significant reduction in the quantity of pesticides and fertilizers required, thus promoting more sustainable and eco-friendly agricultural practices.

### **User Interaction and Recommendations:**

- Users access the system through a secure login on the web interface with role-based access control.
- The dashboard provides real-time data, weather conditions, NPK levels, and soil moisture, allowing farmers to make informed decisions.
- Users receive recommendations covering pest control, irrigation practices, crop selection, and fertilizer/pesticide application, enhancing crop management and overall farm cost-effectiveness.