ME-498P

Major Technical Project I

Drone Detection and Neutralization

Team Members:

Akash Kumar (B21272)

Ayush Kumar Singh (B21283)

Atharva Ayanar (B21282)

Ritik Rajput (B21220)

Supervisor

Dr. Amit Shukla

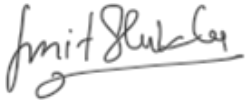
Faculty Advisor

Dr. Prateek Saxena

Indian Institute of Technology Mandi

Certificate

This is to certify that the work contained in the project report entitled “Drone Detection and Neutralization”, submitted by Group 8 to the Indian Institute of Technology Mandi, for the course ME-498P Major Technical Project I, is a record of bonafide research works carried out by him under our direct supervision and guidance.



30/11/2024

Mentor
Dr. Amit Shukla

Signature and Date

Acknowledgements

First and foremost, we would like to express our deepest gratitude to Dr. Amit Shukla for his invaluable guidance, knowledge, and feedback throughout this project. His insights have been crucial in shaping the research and ensuring its quality.

We also extend our sincere thanks to our faculty advisor, Dr. Prateek Saxena, for his continuous support and mentorship. His advice has been instrumental in refining the research process.

Finally, we would like to acknowledge IIT Mandi for providing us with the necessary resources and an environment conducive to innovation and learning. This project would not have been possible without the contributions of all involved.

Thank you all for your contributions to this project.

Abstract

This end-term report highlights the progress made this semester in developing a system for detecting unauthorized drones. The focus has been on creating a robust visual detection mechanism using the YOLOv9 algorithm. A custom dataset was generated by capturing air-to-air drone videos, which were processed into labeled images for model training. Optimizations such as advanced hyperparameter tuning and the use of adaptive optimizers were applied to enhance the accuracy of drone detection. Initial testing on diverse datasets demonstrated promising results. Future work will involve integrating detection with air-to-air neutralization to form a comprehensive counter-drone system.

Table of Contents

List of Figures

Abbreviations

UAVs - Unmanned Aerial Vehicles

YOLO - You Only Look Once(model)

VTOL - Vertical Takeoff and Landing

IMU - Inertial Measurement Unit

GPS - Global Positioning Systems

NATO - North Atlantic Treaty Organization

LOS - Line of Sight

RF: Radio Frequency

HPM: High-Power Microwave

GPU: Graphics Processing Unit

Chapter 1
Introduction

Problem Statement

“The increasing use of drones poses significant security risks, including unauthorized surveillance, smuggling, and threats to critical infrastructure. This project aims to develop a real-time system for detecting and neutralizing unauthorized drones, ensuring effective mitigation of these risks while minimizing collateral damage.”

1. Background of the problem

Unmanned Aerial Vehicles (UAVs) have revolutionized the aviation and technology landscape, with widespread applications in remote sensing, surveillance, and delivery services. These advancements have made UAVs indispensable tools in both civilian and military sectors. However, the increasing accessibility and advanced capabilities of UAVs have raised significant security concerns.

UAVs' ability to operate autonomously and remotely has led to their exploitation in various malicious activities, including unauthorized surveillance, smuggling, and attacks on critical civilian, industrial, and military infrastructure. These threats highlight the urgent need for effective countermeasures to detect and neutralize rogue drones in real-time.

In response to these growing concerns, this project focuses on developing a robust visual detection system using the YOLOv9 algorithm, specifically tailored to address the challenges posed by UAVs. This includes creating a custom dataset using air-to-air drone footage and optimizing detection accuracy through advanced training techniques. The future phases aim to integrate detection with air-to-air neutralization methods to provide a comprehensive solution for mitigating UAV-related threats, ensuring the safety of life and property.

2. Scope of the problem

The proliferation of UAVs has introduced several significant risks, which can be broadly categorized as follows:

1. **Unauthorized Access to Protected Areas**:
    - UAVs can be exploited for malicious activities, such as terrorism, smuggling, or espionage, by infiltrating restricted or sensitive zones, threatening national security and privacy.
2. **Accidents Due to Operator Inexperience**:

    - The growing adoption of UAVs by commercial entities and hobbyists increases the likelihood of accidents, particularly near sensitive locations, often caused by unskilled or careless operators.
3. **Airfield Interference**:
    - UAVs pose severe risks to aviation safety, especially near airports, where collisions with aircraft during take-offs and landings could lead to catastrophic incidents.
4. **Hybrid Warfare and Assassinations**:
    - UAVs have become tools in modern warfare, used for assassination attempts, surveillance, and hybrid attacks that integrate conventional tactics with cyber and psychological operations.

Addressing these risks necessitates the development of robust detection and neutralization systems to safeguard sensitive areas and ensure public safety.

3. Design philosophy used in this report

Modularity:

- The system is divided into two distinct phases: **detection** and **neutralization**.
- Each phase is independently developed and tested, allowing for seamless integration and easier incorporation of future enhancements or alternative approaches.

Scalability:

- The design ensures adaptability to various environments, from localized operations to larger areas.
- YOLOv9's real-time detection capabilities and drone-based neutralization methods make the system scalable for diverse scenarios.

Efficiency:

- Leveraging YOLOv9 ensures the system operates in real-time, crucial for detecting and neutralizing threats in dynamic and high-risk situations.

Redundancy:

- The integration of a secondary drone for neutralization introduces an additional layer of security, ensuring that threats can be addressed even if detection systems encounter challenges.

Reliability:

- The system is designed to minimize false positives while ensuring dependable performance.
- Accurate detection and effective neutralization reduce interruptions and ensure safety.

Future-Proofing:

- The system is designed to accommodate evolving technologies.
- Open architecture allows for refining detection algorithms and exploring emerging neutralization methods to maintain relevance as UAV technologies advance.

4. Problem statement

The increasing use of drones (UAVs) presents significant security risks. Therefore, there is a need to develop effective methods to **detect** and **neutralize** unauthorized drones in various environments.

Objective:

- To develop a **real-time system** capable of detecting unauthorized drones and neutralizing potential threats quickly and efficiently.

Importance:

- **Securing Critical Infrastructure**: Drones can be used to attack or disrupt vital infrastructure, including power plants, airports, and military facilities.
- **Preventing Unauthorized Surveillance**: Drones have been used for illegal surveillance, infringing on privacy and security.
- **Protecting Public Events and Restricted Zones**: Drones operating near public gatherings or restricted areas pose a significant safety risk and can interfere with sensitive operations.

Detection Issues:

- **Small Size & Low Altitudes**: Drones are often compact and can fly at low altitudes, making them challenging to detect with traditional detection systems such as radar or cameras.
- **Environmental Interference**: Weather conditions, lighting variations, and background noise can cause false positives, reducing detection accuracy.

Neutralization Challenges:

- **Collateral Damage**: Existing neutralization methods often risk causing damage to surrounding infrastructure or unintended objects.
- **Ineffectiveness at Long Ranges**: Many counter-drone technologies are limited in range and may not work efficiently when the drone is far away or operating at high altitudes.
- **Development of Safe and Reliable Methods**: There is still ongoing research to develop methods for safely neutralizing drones, such as using drones for interception, which need to be refined and optimized.

5. Beneficiaries (Intended market)

Government Agencies (Defense, Law Enforcement):

- These agencies require advanced anti-UAV technologies to protect **national security** and enforce **no-fly zones**.
- They are particularly concerned with mitigating threats from **espionage**, **terrorism**, and **illegal surveillance**.
- **Defense agencies** often use UAVs for reconnaissance, making it crucial to have robust detection systems to counter potential misuse for harmful purposes.

Critical Infrastructure Operators:

- Entities such as **airports**, **nuclear power plants**, and other **sensitive infrastructures** need reliable UAV detection systems to ensure **operational safety**.
- These systems are essential for preventing **unauthorized access** and mitigating risks of **sabotage** or **espionage** that could disrupt critical operations.

Corporations Requiring High-Level Security:

- **Industrial plants**, **oil refineries**, and high-profile **corporate events** are vulnerable to unauthorized UAVs that could be used for surveillance or sabotage.
- These corporate clients require solutions to safeguard **intellectual property**, **personnel**, and **assets** from drone-based threats, ensuring business continuity and security.

Private Property Owners with High-Security Needs:

- High-net-worth individuals and private entities, such as owners of large estates or those hosting private events, need advanced UAV countermeasures to safeguard **privacy** and ensure **personal safety**.
- UAV detection and neutralization technologies are critical in preventing breaches of privacy and protecting against potential drone-based intrusions.

6. Organization of this report

This report is structured to provide a comprehensive overview of the work completed so far and the planned future steps. The following sections detail the flow of the report:

1. **Introduction**:
    - This section introduces the **motivation** behind the project, emphasizing the growing **security risks** posed by drones. It also defines the **primary objective** of the project: to develop a system capable of detecting and neutralizing unauthorized drones.
2. **Literature Review**:
    - This section provides an in-depth overview of the **existing technologies**, algorithms, and methodologies relevant to drone detection and neutralization. It also explores the

state-of-the-art approaches in the field and justifies the selection of the **YOLOv9** algorithm as the primary approach for this project.

3. **Methodology**:
    - The methodology section explains the steps taken in the initial phase of the project, including the **YOLOv9-based detection system** and preliminary considerations for **neutralization strategies**, such as using a secondary drone for interception. This section outlines the approach adopted to address the detection challenges and the rationale behind it.
4. **Results and Discussion**:
    - This section discusses the **progress made in detection**, including initial test results, the challenges encountered during model training, and the effectiveness of the YOLOv9 model. It also presents the expected next steps for improving the detection system. As this is a midterm report, the section highlights the goals for the next phases of the project, focusing on enhancing both detection and neutralization capabilities.
5. **Conclusion and Future Work**:
    - The final section summarizes the key findings from the current phase of the project and provides an outlook for future work. This includes refining the **detection system**, integrating the **neutralization system**, and ensuring the technology is ready for real-time deployment to address UAV-related security threats.

Chapter 2
Literature Review

1. Classification of UAV

The UAV industry is vast and diverse, with no universally accepted classification system. In this section, we classify UAVs based on several key parameters—such as weight, altitude, range, wings, rotors, and application—to give readers a clearer understanding of how UAVs are categorized. This overview provides a useful framework for understanding the different types of UAVs and their capabilities, which will be referenced throughout the paper. Our classification adheres to the guidelines set by the Indian government, offering a structured approach that aligns with local regulations, though standards may vary across regions.

a. Based on Weight

• Nano: UAVs with weight less than 250 gm

• Micro: UAVs with weight greater than 250 gm and less than 2 kg

• Small: UAVs with weight greater than 2 kg and less than 25 kg

• Medium: UAVs with weight greater than 25 kg and less than 150 kg

• Large: UAVs with weight greater than 150 kg

b. Based on Altitude and Range

• Hand-held: UAVs that can fly at altitudes of less than 600 m and have a range of less than 2 km.

• Close: UAVs with an altitude of less than 1500 m and range less than 10 km.

• NATO: UAVs with an altitude of less than 3000 m and range less than 50 km.

• Tactical: UAVs with an altitude of less than 5500 m and range less than 160 km.

• MALE (Medium Altitude Long Endurance): UAVs with an altitude of less than 9100 m and range less than 200 km.

• HALE (High Altitude Long Endurance): UAVs with altitude more than 9100 m and indefinite range.

• Hypersonic: UAVs with altitude around 15200 m and range greater than 200 km.

c. Based on Wings and Rotors

• Fixed Wing: UAVs that resemble an airplane design with fixed wings.

• Single Rotor: UAVs that resemble a helicopter design with one main rotor and another small one at the tail.

• Multi-rotor: UAVs that have more than one rotor. The most commonly found are tricopters, quadcopters, hexacopters and octa-copters.

• Fixed-Wing Hybrid VTOL: Hybrid UAVs with longer flight time. They have the stability of fixed-wing UAVs as well as the ability to hover, take off and land vertically.

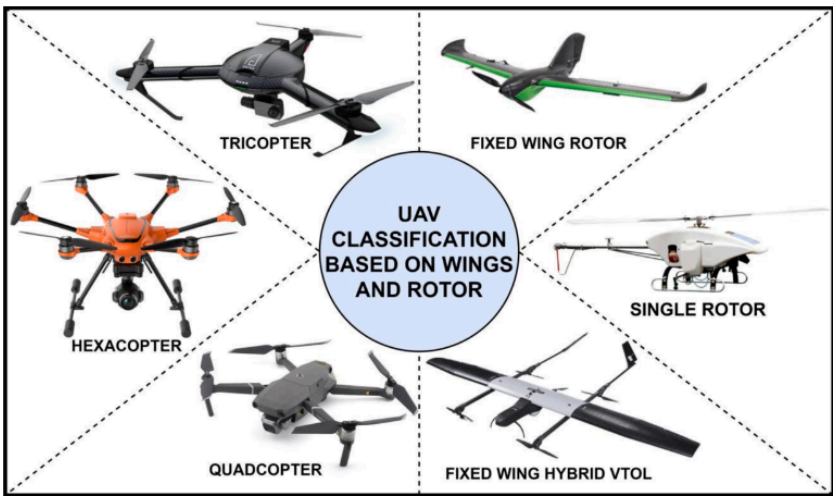


Fig. 1 Classification of UAV based on wings and rotors. [2]

d. Based on Application

• Personal: Used for applications such as videography and entertainment.

• Commercial: Used for applications such as infrastructure monitoring, product delivery, and aerial imaging.

• Government and Law enforcement: Used for applications such as fire fighting and patrolling.

• Military: Used for application such as surveillance and combat

attacks.

2. Sensors used in drones

a. IMU (Inertial Measurement Unit)

i. Function: Combines accelerometers, gyroscopes, and magnetometers to provide data on orientation, velocity, and position.
ii. Purpose: Ensures stable flight by measuring the drone's acceleration and angular velocity.
iii. Application: Stabilization, navigation, and flight control.

b. GPS (Global Positioning System)

i. Function: Uses satellite signals to provide real-time geolocation and time information.
ii. Purpose: Allows drones to know their precise position, enabling autonomous navigation and waypoint-based flight.
iii. Application: Mapping, surveying, delivery systems.

c. LiDAR (Light Detection and Ranging)

i. Function: Measures distances by illuminating the target with laser light and analyzing the reflected signals.
ii. Purpose: Generates high-resolution 3D maps of the environment.
iii. Application: Obstacle detection, terrain mapping, and autonomous navigation.

d. Ultrasonic Sensors

i. Function: Emits ultrasonic waves and measures the time it takes for the echoes to return.
ii. Purpose: Detects nearby obstacles and helps in maintaining altitude.
iii. Application: Low-altitude flying, collision avoidance, and precise landing.

e. Optical Sensors (Cameras)

i. Function: Captures visual data in various spectrums (visible, infrared).
ii. Purpose: Provides real-time video, enables object detection, and helps in visual navigation.
iii. Application: Surveillance, photography, inspection, and optical flow navigation.

f. Infrared Sensors

i. Function: Detects thermal radiation emitted by objects.
ii. Purpose: Allows drones to operate in low visibility conditions (e.g., nighttime).
iii. Application: Search and rescue, wildlife monitoring, and thermal inspections.

g. Barometric Pressure Sensors

i. Function: Measures air pressure to estimate altitude.
ii. Purpose: Helps drones maintain a stable and consistent flight altitude.
iii. Application: Altitude control and flight stabilization.

h. Magnetometer

i. Function: Measures magnetic fields to determine the drone's heading.
ii. Purpose: Acts as a digital compass, providing directional information for accurate navigation.

iii. Application: Autonomous flight and precise maneuvering.

i. Proximity Sensors

i. Function: Detects the presence of objects in the immediate surroundings using infrared or laser technology.
ii. Purpose: Helps prevent collisions and assists in landing.
iii. Application: Obstacle avoidance and close-range navigation.

3. Methods of Detection

Feature	Sensing devices	Advantages	Disadvantages	Detection range
Heat	Infrared camera	• Less affected by weather • Long range	• Low accuracy	1—15 km
RF signal	RF receiver	• Obstacle-free • Detect the drone operator	• Unable to detect • Autonomous flight	3-50 km
Physical object	Radar	• Less affected by weather • Long range	• High expense • Regulations on RF license • Vulnerable to obstacles	1—20 km
Visibility	Optical camera	• Low expense • Miniaturized • Identification	• Highly affected by the weather • Vulnerable to obstacles	0.5-3 km
Acoustic signal	Acoustic receiver	• Compatible with RF based sensors • Miniaturized	• Extremely low detection range • Low accuracy • High signal detection complexity	< 0.2 km

Fig.2 Methods of detection

a. Optical Detection

i. Principle: Utilizes cameras and sensors to capture UAVs in visible, infrared, and ultraviolet spectrums.
ii. Benefits: Identifies UAVs by their visual signatures; integrates with existing camera systems.
iii. Limitations: Challenged by poor weather conditions and difficulty in determining distance and speed.
iv. Use Cases: Critical infrastructure, military facilities.

b. Acoustic Detection

i. Principle: Detects drones by listening for their rotor noise using acoustic locators.
ii. Benefits: Detects drones even outside optical range, including non-communicating ones.
iii. Limitations: Impacted by wind, short range, and less accuracy.
iv. Use Cases: Smaller buildings, critical infrastructure.

c. Radio Frequency (RF) Detection

i. Principle: Detects RF signals emitted by drones for communication.

ii. Benefits: Locates both the drone and its operator.
iii. Limitations: Ineffective against non-communicating drones and fragmented spaces.
iv. Use Cases: Airports, military facilities, power plants.

d. Radar Detection

i. Principle: Emits high-energy radio waves and analyzes reflections from drones.
ii. Benefits: Long-range detection, effective for non-communicating drones.
iii. Limitations: Struggles with small, slow, or low-flying drones; prone to false alarms.
iv. Use Cases: Open spaces, unpopulated areas.

e. Infrared Detection

i. Principle: Detects thermal radiation from drone engines and batteries.
ii. Benefits: Works in all weather conditions, low cost, compact size.
iii. Limitations: Low resolution, risk of false positives (e.g., birds).
iv. Use Cases: Indoor spaces, limited outdoor areas.

f. Machine Learning-Enhanced Detection

i. Radar-Based Systems: ML (e.g., CNNs, LSTMs) improves accuracy by analyzing Doppler signatures.
ii. Acoustic Systems: Algorithms like CNNs and random forests classify drones based on unique sounds.
iii. Imaging Systems: ML models (e.g., YOLOv5) enhance drone detection from visual data.
iv. RF-Based Systems: Deep learning (e.g., CNNs) improves classification of RF signals with up to 99.8% accuracy

4. Methods of Neutralization

a. Electronic Countermeasures (ECM)

i. Jamming: Jamming involves disrupting the communication between the UAV and its controller. This can disable the drone's ability to receive commands, rendering it ineffective.
ii. Frequency Hopping Spread Spectrum (FHSS): FHSS involves rapidly switching between frequencies, making it difficult to detect or jam the UAVs communication signal.
iii. Direct Sequence Spread Spectrum (DSSS): DSSS spreads the signal over a wider bandwidth, making it less susceptible to interference and providing robust resistance against jamming attempts.
iv. Pulse Jamming: This technique uses powerful pulses of RF energy to overwhelm a drone’s receiver, effectively neutralizing communication by drowning out legitimate signals.
v. Noise Jamming: Involves emitting broadband noise that interferes with the drone’s signal, preventing it from receiving or sending data properly.

vi. Spoofing: Spoofing deceives the drone's navigation and control systems.
vii. GPS Spoofing: Sends false GPS signals to the drone, tricking it into changing its route or landing in a different location.
viii. Control Signal Spoofing: Intercepts and manipulates the drone's control signals, allowing the attacker to steer the drone off course or disrupt its mission.

b. Kinetic Countermeasures

i. Net Guns: These are physical tools designed to capture drones by entangling them in nets.
ii. Harpoon Nets: Shoot projectiles with attached nets to ensnare and immobilize the drone mid-flight.
iii. Drag Nets: Large nets deployed across a flight path to trap drones as they fly through.
iv. Bird Strike Emulators: These mimic bird strikes to physically disrupt the drone's operation.
v. Projectile Launchers: Fire small projectiles at the drone to simulate the damage a bird strike would cause.
vi. Acoustic Devices: Emit high-frequency sounds that destabilize the drone's sensors, leading to flight disturbances.
vii. Laser Weapons: These offer direct and non-contact ways to neutralize drones.
viii. High-Energy Lasers (HELs): Focus concentrated beams of energy onto the drone to either damage its structure or fry its electronics.
ix. Laser Jamming: Involves using lasers to interfere with the drone's sensors, disrupting navigation or communication systems.

c. Environmental Countermeasures

i. Radio Frequency Interference (RFI) Zones: These create hostile environments for drone communication systems by interfering with RF signals.
ii. RF Emitters: Deploy devices that emit strong radio frequency signals, blocking or degrading the UAVs ability to communicate with its operator.
iii. RF Absorbing Materials: Use materials that absorb RF energy to create dead zones, making it difficult for UAVs to operate within these areas.
iv. Bird Deterrents:
v. Acoustic Devices: Use distress calls or predator sounds to deter drones from entering restricted areas.
vi. Visual Deterrents: Flashing lights or inflatable decoys that mimic predators can also frighten UAVs away.
vii. Falconry: Employs trained birds of prey to physically intercept and neutralize drones.

d. Regulatory Measures

i. Drone Registration and Licensing:

ii. Identification: Requires all drones to be registered with a unique identifier, ensuring accountability for drone usage.

iii. Operator Certification: Ensures that drone operators are certified, having received proper training to operate UAVs responsibly and safely.

iv. No-Fly Zones:Designated Areas: Government-enforced no-fly zones over sensitive areas, such as airports, military bases, and prisons, where UAV operations are strictly prohibited.

v. Temporary Restrictions: Special events or emergency situations may impose temporary restrictions on drone usage to ensure public safety.

vi. Drone Traffic Management Systems:

vii. Remote Identification: Requires drones to transmit identification and location information to prevent unauthorized use and aid in traffic management.

viii. Traffic Control: Systems that help manage drone traffic, ensuring safe integration with manned aircraft and reducing the risk of collisions.

5. Some Interesting Papers

a. Literature Review on "Adaptive Drone Identification and Neutralization Scheme for Real-Time Military Tactical Operations"

This research paper presents an adaptive, scenario-based approach to drone detection and neutralization, specifically designed for military applications. With the increasing use of unmanned aerial vehicles (UAVs) in various sectors, both for legal and illegal purposes, the paper addresses the growing concerns over unauthorized drones invading restricted areas. The proposed method utilizes an enhanced version of the YOLOv5 deep learning model to detect drones in real-time and identify attached objects such as weapons, making it suitable for real-time military operations.

i. Overview of the Problem

The authors highlight the need for proactive drone detection and neutralization systems due to the increased accessibility of UAVs. These drones pose serious threats to national security by facilitating unauthorized surveillance, smuggling, and even terrorism. Traditional drone detection systems, such as radar and video-based methods, have limitations in detecting smaller drones or distinguishing drones carrying dangerous payloads. The study focuses on overcoming these challenges by proposing a system that not only detects drones but also identifies the objects attached to them.

ii. Approach and Methodology

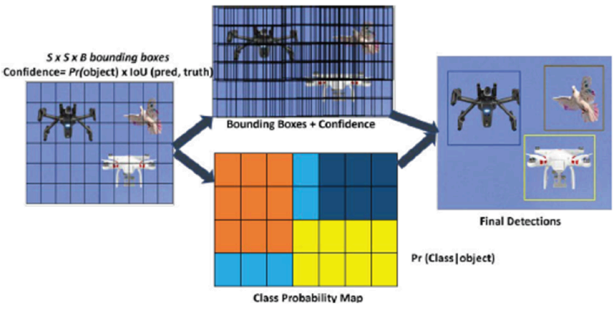


Fig 3. Feature extraction of drones

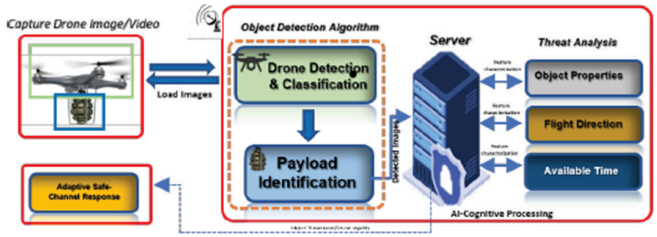


Fig 4. Architecture of proposed identification scheme

The core of the proposed system is an enhanced YOLOv5 deep learning model, specifically adapted for real-time military surveillance. The model is trained on a dataset containing six different drone models and eight types of attached objects, such as explosives and weapons. By employing a convolutional neural network (CNN), the model can efficiently detect and classify drones, even in varying environmental conditions like cloudy or evening settings.

The system's architecture is divided into four components: detection, classification, object identification, and neutralization. Once a drone is detected, the system identifies its payload and determines the level of threat posed by the UAV. This allows the system to recommend the best neutralization strategy, such as signal jamming or physical interception, depending on the drone's speed, size, and payload.

iii. Results and Performance

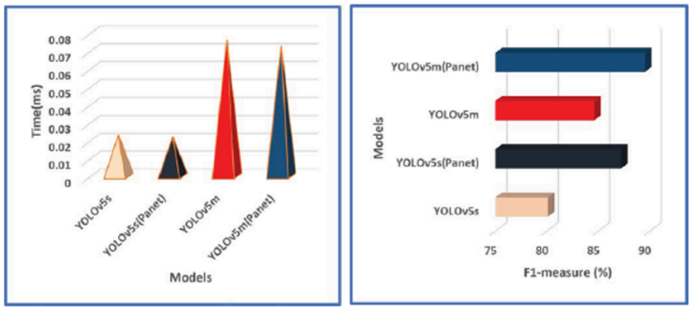


Fig 5. F1-measure and time graph of models

Models Adaptive Drone Detection						
Models	**Our Model**		**YOLOv5s**		**YOLOV5m**	
Metric	**mAP**	**R(%)**	**mAP**	**R(%)**	**mAP**	**R(%)**
Anafi_evening	99.1	99.2	97.1	97.9	98.9	98.7
DJIFPV_evening	99.7	99.6	98.2	98.3	99.3	99.2
ETF-E410S_evening	99.9	100	99.5	100	99.8	100
MAVIC-Air_evening	93.5	93.4	81.3	85.0	89.5	89.1
MAVIC-Zoom_evening	99.9	100	99.5	100	99.8	99.7
Anafi_cloudy	99.9	100	99.6	100	99.9	100
DJIFPV_cloudy	100	100	99.6	100	99.9	100
MAVIC-Air_cloudy	99.9	100	99.6	100	99.9	100

Fig 6. Scenario based drone detection

The performance of the proposed system is evaluated based on accuracy, sensitivity, and timeliness. In comparison to other models, the enhanced YOLOv5 achieves a superior detection precision of 100%, with a sensitivity of 99.9% and an F1-score of 87.2% for weapon identification. The high detection speed (0.021 seconds) makes the model suitable for real-time applications. The results indicate that the model performs exceptionally well in detecting and identifying drones across various scenarios and environmental conditions.

iv. System Design and Experimental Setup

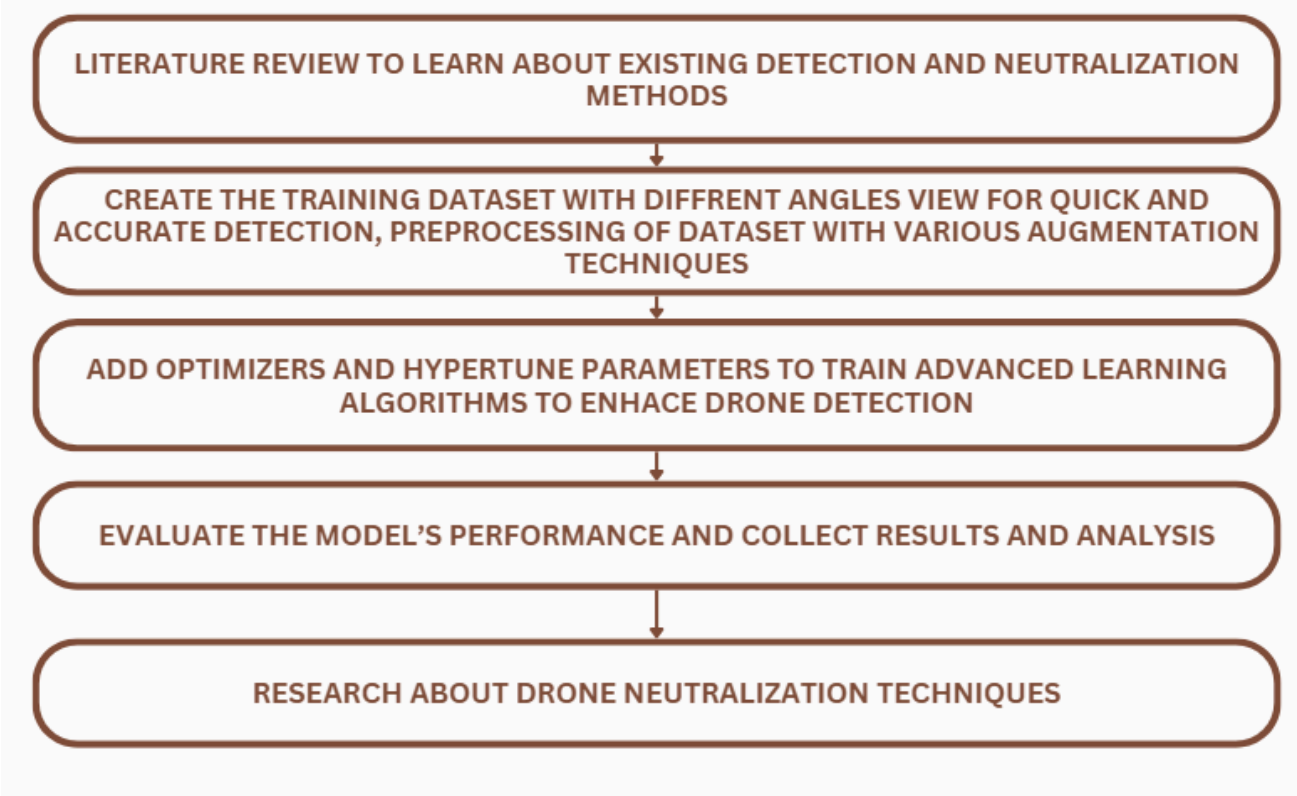
The model is implemented using a Python environment, with a hardware configuration that includes an Intel i5 processor and Tesla K80 GPU. The training dataset is split into 70% for training, 20% for testing, and 10% for validation. The system undergoes rigorous testing to ensure that it can detect drones under different conditions, such as cloudy weather or low-light environments. The use of transfer learning also allows the model to adapt to new tasks with minimal resource usage.

v. Conclusion

This paper presents a highly adaptive and accurate drone detection and neutralization system that leverages deep learning techniques for real-time military surveillance. The system’s ability to detect and classify drones, combined with its capability to identify dangerous payloads, makes it a valuable tool in military operations. However, challenges remain in improving the system's accuracy for smaller objects and real-world implementation.

Chapter 3

Plan of Action



1. Completed Work

This semester, we focused on developing a **drone detection system** using **YOLOv9** for real-time visual detection. Key milestones include:

1. **Dataset Creation**:
    - Captured air-to-air footage using two drones and processed it into labeled images, including both manual labeling and semi-automated labeling using pre-trained models.
2. **Data Splitting**:
    - The dataset was divided into **70% training**, **20% testing**, and **10% validation** to optimize model performance and prevent overfitting.
3. **Model Training**:

    - The YOLOv9 model was trained using advanced optimizers (Adam, Adagrad, SGD), resulting in improved detection accuracy for various drone types and environments.
4. **Performance Evaluation**:
    - The model was tested using precision-recall curves and confusion matrices, achieving promising results in detecting drones with minimal false positives.

For neutralization, initial research into **RF jamming** was conducted, with plans to integrate a jamming system on a secondary drone for real-time neutralization in the upcoming phases.

Key Insight:

The integration of traditional detection techniques, such as **Radar** and **RF Detection**, with **AI-based methods** like **YOLOv9** offers a highly effective approach to overcoming the challenges of detecting unauthorized drones. This hybrid model enhances **real-time detection** by leveraging YOLO's advanced capabilities in identifying drones under varying conditions (e.g., size, speed, environmental factors). Additionally, incorporating a **diverse dataset** with various drone models enables the system to handle real-world scenarios and significantly reduce false positives. The combination of deep learning for detection and traditional countermeasures for neutralization (e.g., RF jamming) presents a promising solution for securing airspace from drone-based threats.

2. Work Ahead

The next phase will focus on enhancing the **detection system** by further optimizing the YOLOv9 model. This includes expanding the dataset with additional drone types and scenarios to improve accuracy and robustness. Fine-tuning the model will address edge cases like small drones, low-light environments, and high-speed movements, ensuring reliable performance in real-world conditions.

The **neutralization phase** will involve developing and integrating an **RF jamming system** on a neutralizing drone. Directional jamming will be implemented to disrupt the target drone's communication without affecting the neutralizing drone's systems. This step will form the foundation for effective air-to-air neutralization strategies.

Finally, the project will focus on **system integration**, combining detection and neutralization into a unified framework. Real-world testing will validate the system's performance in diverse environments, paving the way for additional enhancements such as adaptive threat identification and alternate neutralization techniques like GPS spoofing or physical interception.

Chapter 4

Progress

YOLOv9 comparison with YOLOv8

YOLOv8 architecture

1. **Backbone:** YOLOv8 utilizes a modified version of the CSPDarknet53 architecture as its backbone. This network is known for its efficient balance between accuracy and computational cost. It employs crossstage partial connections to improve information flow between different layers.
2. **Neck:** Uses a simple Path Aggregation Network (PANet) for feature fusion, focusing on efficiency.
3. **Head:** Consists of multiple convolutional layers followed by fully connected layers. These layers analyze the features extracted by the backbone and make predictions for object detection.

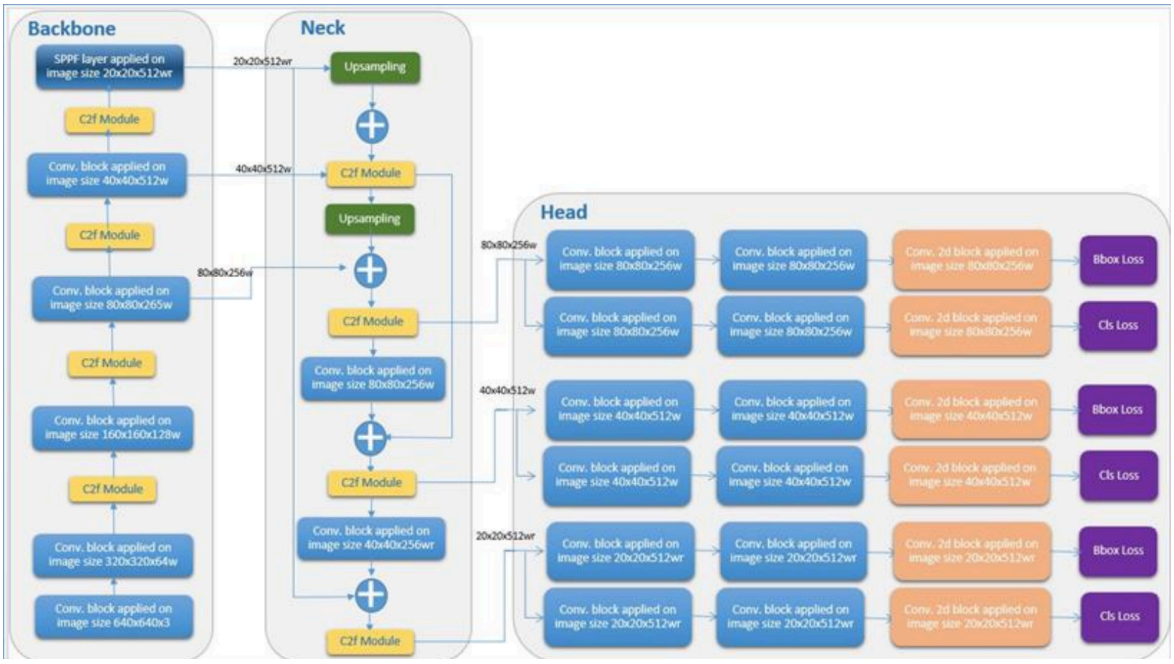


Fig 7 - YOLOv8 architecture

1. YOLOv9 architecture

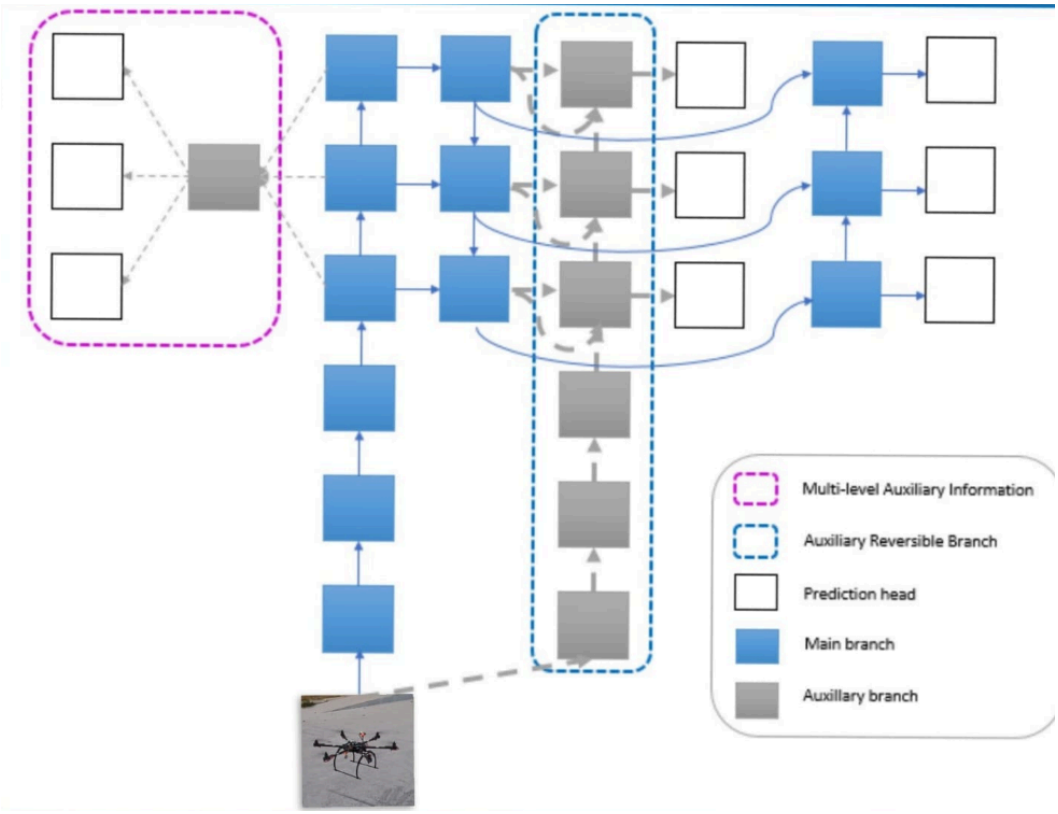


Fig 8 . Programmable Gradient Information (PGI) architecture in YOLOv9

Programmable Gradient Information (PGI): This technique addresses potential information loss during training, ensuring accurate model updates. PGI works by preserving information that retains all data required to calculate the model's objective function, leading to reliable gradient information for updating network weights and balancing efficiency and accuracy.

PGI acts as a training tool, enhancing gradient backpropagation through the network while minimizing inference cost. It achieves this by:

1. **Main branch:** YOLOv9 ensures that no extra inference cost is added because the other components of PGI are not necessary for the inference step.
2. **Removable auxiliary branch:** During training, an additional branch processes information to generate reliable gradients. However, this branch is removed at inference time to maintain model compactness and speed.
3. **Multi-level auxiliary information:** This uses an integration network to combine gradients from various network regions, providing the main branch with comprehensive information for accurate predictions.

2. Generalized Efficient Layer Aggregation Network (GELAN):

This architecture optimizes lightweight models by maximizing parameter efficiency and combining the strengths of existing approaches. GELAN, shown in Fig. 3, surpasses existing methods in its ability to leverage parameters effectively utilizing conventional convolution operations. It integrates the efficient gradient path planning of CSPNet with the fast inference capabilities of ELAN, achieving a balance between model size, speed, and accuracy. YOLOv9 comes in four versions (v9-S, v9-M, v9-C, and v9- E) with varying parameter counts, offering flexibility based on computational resources.

Table YOLOv9 versions

Module	**Parameters**	**FLOPs(G)**	**Test size**
YOLOv9-S	7.2	26.7	640
YOLOv9-M	20.1	76.8	640
YOLOv9-C	25.5	102.8	640
YOLOv9-E	58.1	192.5	640

3. Comparison between YOLOv8 and YOLOv9

YOLOv9 employs a wider range of modules compared to YOLOv8. This suggests that YOLOv9 might have a more complex architecture. YOLOv9 replaces C2f module with the RepNCSELAN4 module and SPPF module with the SPPLAN module. The C2f module's architecture incorporates two parallel gradient flow branches to enhance the robustness of gradient information flow. The architecture of the RepNCSELAN4 module is an enhanced version of CSP-ELAN designed to improve the feature extraction process. The input from the initial convolutional layer is divided into two routes, each processed through a sequence of RepNCSP and convolutional layers before being combined again. The dual-path technique improves gradient flow and feature reuse, boosting the model's learning efficiency and inference speed by maintaining depth without the usual computational cost of increased complexity.

The Spatial Pyramid Pooling Fusion (SPPF) module in YOLOv8 can extract contextual information from photos at different scales, which greatly improves the model's ability to generalize. SPPLAN integrates Spatial Pyramid Pooling (SPP) into the ELAN structure to enhance layer aggregation. The process begins with a convolutional layer that modifies the channel dimensions, and then proceeds with a sequence of spatial pooling operations to gather multi-scale contextual information. The combined outputs are then processed by an additional convolutional layer to enhance the network's ability to extract detailed data from different spatial levels. YOLOv9 introduces new modules: Adown, CBLinear and CBFuse. Both YOLOv8 and YOLOv9 utilize the Upsample module.

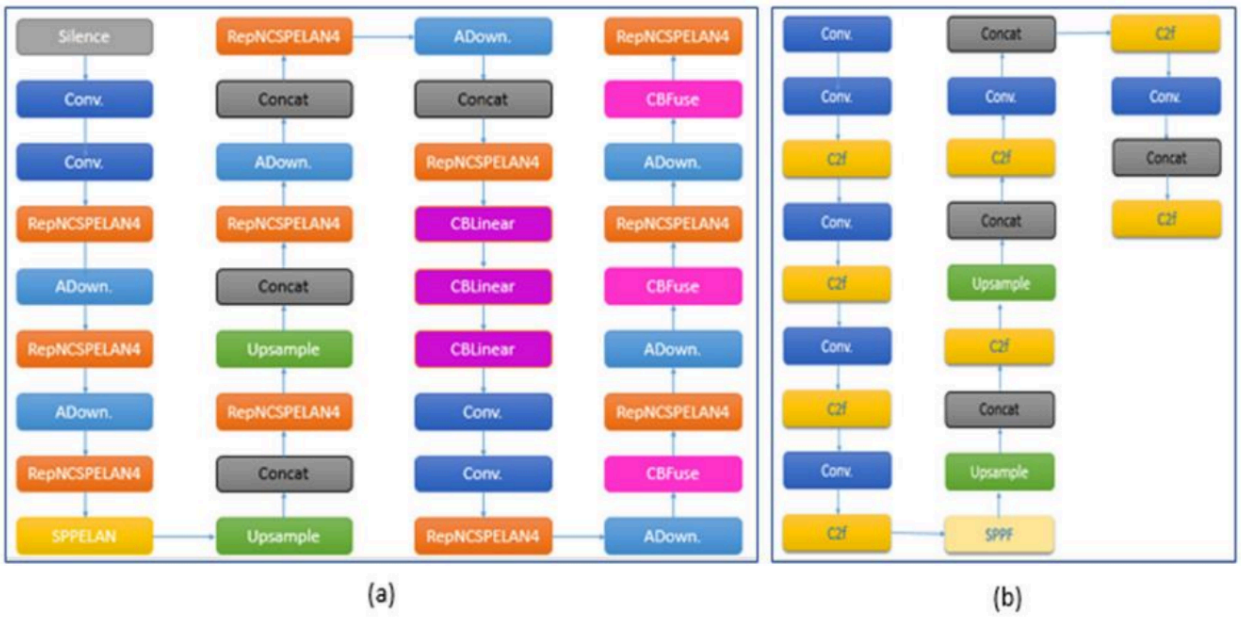


Fig 9- Modules in (a) YOLOv9 (b) YOLOv8

4. Data Collection and Preprocessing

Dataset:

The dataset consists of drone-captured videos recorded from various angles, views, lighting conditions, backgrounds, and times of the day. These videos were then converted into images to ensure optimal accuracy and robustness in detection and neutralization outcomes.

Visual Example:

Fig 10 - Captured Drone

Fig 11. Capturing Drones

Preprocessing:

1.1 Renaming and Organizing: Images were systematically renamed and labeled appropriately for further purposes.

1.2 Data Splitting:
The dataset was divided into training, validation, and test sets with the following distribution:

- Training set: 756 images
- Validation set: 352 images
- Test set: 248 images

1.3 Contrast Enhancement: Applied contrast enhancement techniques to improve the clarity of drone images, making object features more distinguishable.

1.4 Cropping and Resizing: Cropped the drone regions in the images and resized them to a uniform dimension to maintain consistency across the dataset.

1.5 Noise Removal: Utilized Gaussian and median filters to minimize noise in the images, enhancing the visibility of drone-specific features.

1.6 Normalization: Normalized pixel values to a range of 0 to 1 to support faster model convergence during training.

2. Data Augmentation: To increase the diversity of the training data and prevent overfitting, data augmentation techniques were applied. This included random rotations, width and height shifts, shear transformations, zooming, and horizontal flipping. These techniques help the model generalize better by introducing variations that the model might encounter in real-world data.

2.1 Rotation: Rotated images by random angles to simulate different viewing angles.

2.2 Flipping: Applied horizontal and vertical flips to create mirror images.

2.3 Zooming: Random zoom-in and zoom-out transformations to mimic different levels of magnification.

2.4 Translation: Shifted images horizontally and vertically to vary the position of the drone within the frame.

2.5 Shearing: Applied shearing transformations to introduce slanting distortions, mimicking variations in image acquisition.

Examples of Augmentation Used in our Model

Fig 12 - Original Image with drone at center

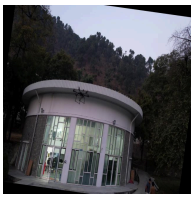
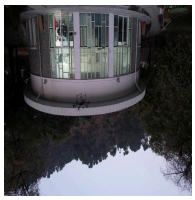
					
Exposure	20° rotation	Blur	Grayscale	Noise	Vertical Flip

Fig -13 Augmented Image

3. Training and Validation

3.1 Data Generators:

Data generators were designed for the training and validation datasets. The drone images were resized to 6400 x 640 pixels and processed in batches. The training data generator applied augmentation techniques such as rotations, flips, and zooming to enhance data diversity, while the validation data generator only normalized the images to ensure consistency during evaluation.

3.2 Model Training:

The model was trained using the training generator and evaluated using the validation generator. Training was conducted for 450 epochs with steps per epoch set to 200 and validation steps set to 90. This iterative process helped the model generalize to unseen data by learning from the training set while ensuring it did not overfit using the validation set.

5. Neutralization

Methods of neutralization:

1. Radio Frequency (RF) Drone Jamming:

    - Disables drones by disrupting communication or GPS signals through jamming or spoofing.
    - Non-destructive and widely used for protecting sensitive areas, though it may face challenges like encrypted communication and frequency-hopping.

2. Laser Systems:

    - Uses high-energy lasers to disable or destroy drones by targeting critical components.
    - Effective for precise neutralization, but performance is affected by weather conditions and requires a direct line of sight.

3. Killer Drones with Catching Nets:

    - Deploys nets to physically entangle and neutralize rogue drones.
    - Non-destructive and ideal for urban or sensitive environments, commonly used in law enforcement and event security.

4. GPS Spoofing:

    - Misleads the drone's navigation system by transmitting false GPS signals, causing it to lose control or veer off course.
    - Effective for GPS-reliant drones but requires advanced equipment.

5. High-Power Microwave (HPM) Systems:

    - Emits electromagnetic bursts to disable drones' electronics and communication links.
    - Useful for neutralizing multiple drones simultaneously, with minimal collateral damage.

1. The Idea: Drone integration with RF jamming device

Concept:

Mounting an RF jamming device onto a neutralizing drone allows real-time air-to-air interception of rogue drones. The neutralizing drone tracks and approaches the target, using its onboard jammer to disrupt communication and navigation, forcing the rogue drone to lose control or crash. This method is highly effective for protecting sensitive areas, offering mobility, precision, and minimal collateral damage, though it requires adherence to RF jamming regulations.

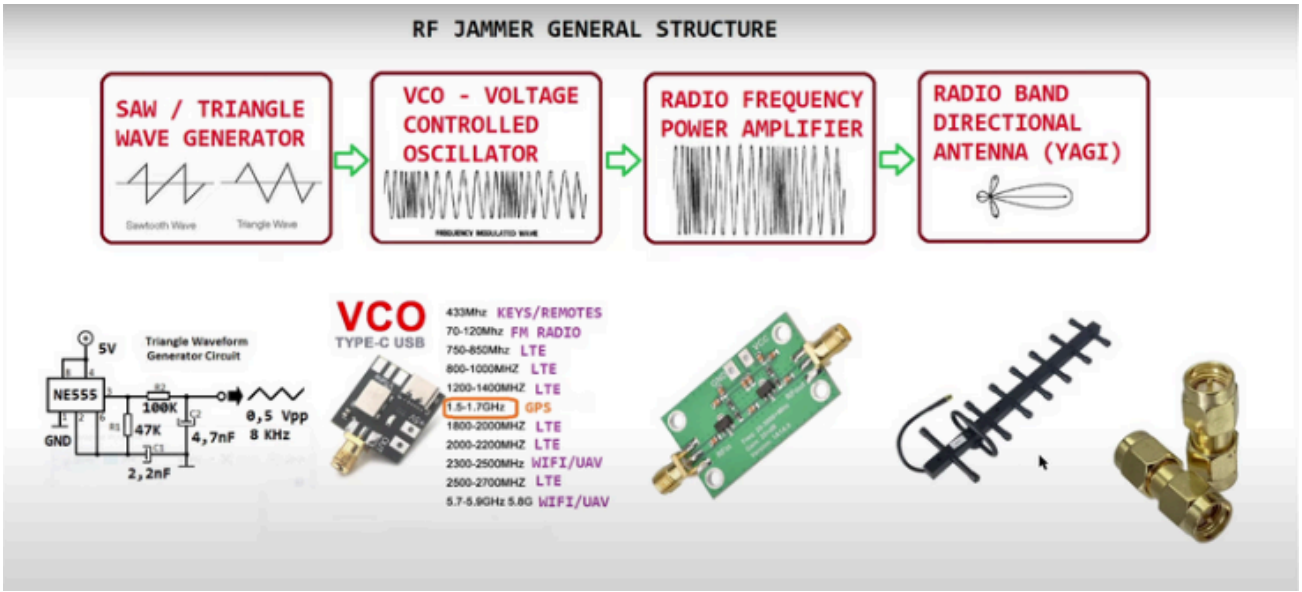


Fig-14 RF Jammer SETUP

Key Features:

1. Directional Jamming: The jamming device employs focused, directional beams aimed exclusively at the target drone. This precision minimizes the risk of interfering with the neutralizing drone's own systems or other nearby communication devices, ensuring operational integrity and reducing collateral impact.

2. Frequency Isolation: The neutralizing drone operates on a dedicated, unaffected communication frequency (e.g., 5.8 GHz), while the jammer targets commonly used drone frequencies (e.g., 2.4 GHz or GPS signals at 1.575 GHz). This separation

ensures uninterrupted control of the neutralizing drone while effectively disrupting the rogue drone's signals.

3. On-Demand Activation: The jammer is activated only when the neutralizing drone is in close proximity to the target, conserving power and avoiding unnecessary interference. Smart activation systems ensure the jammer operates efficiently, targeting rogue drones only during critical moments.

4. Adaptive Signal Targeting: The system dynamically identifies and targets the specific frequencies or protocols used by the rogue drone, adapting to various models and communication methods, including encrypted or frequency-hopping systems.

5. High Mobility and Agility: The neutralizing drone is equipped with advanced sensors and AI-based tracking systems to quickly intercept fast-moving targets and maintain close-range positioning for effective jamming.

6. Failsafe Mechanisms: If the jamming process encounters resistance or the rogue drone exhibits hardened electronics, the neutralizing drone can deploy secondary methods such as nets or directed energy systems for complete neutralization.

7. Low Collateral Impact Design: By combining directional jamming and on-demand activation, the system minimizes disruptions to nearby devices and ensures safe operation in urban or densely populated environments.

Advantages:

1. Reusability: The system can be used multiple times, and disabled drones can be inspected for analysis.
2. Real-Time Neutralization: Effectively disables rogue drones quickly in dynamic scenarios.
3. Minimal Collateral Damage: Focused jamming minimizes interference with other devices.
4. Non-Destructive: Neutralizes drones without causing physical damage, allowing for recovery.
5. Cost-Effective: Reusable components reduce long-term operational costs.

Chapter 5
Results and discussion

We looked into a few of the models and the yolov9 model.After training the YOLOv9 model, we evaluated its performance using standard metrics such as precision, recall, and confidence. The following sections provide a detailed analysis of the model's performance, illustrated with relevant curves and a confusion matrix.

1. Confusion Matrix

The **confusion matrix** is a table that provides a more detailed breakdown of the model's performance by comparing actual and predicted classifications. It contains:

- **True Positives (TP)**: Correctly predicted objects.
- **True Negatives (TN)**: Correctly identified non-objects.
- **False Positives (FP)**: Incorrectly predicted objects (false alarms).
- **False Negatives (FN)**: Missed detections.

The confusion matrix for the YOLOv8 model reveals its strength in correctly identifying objects (high true positive rate) with minimal false positives and false negatives.

This confusion matrix evaluates a binary classification model distinguishing between "drone" and "background."

- **True Positives (224)**: Correctly identified "drone" instances.
- **False Positives (12)**: Background misclassified as "drone."
- **False Negatives (14)**: Drones misclassified as "background."
- **True Negatives**: Correctly identified "background."

Key Observations:

- **High True Positives (224)** indicate strong performance in detecting drones.
- Misclassifications (12 FP, 14 FN) suggest minor improvement areas for reducing false alarms and missed detections.

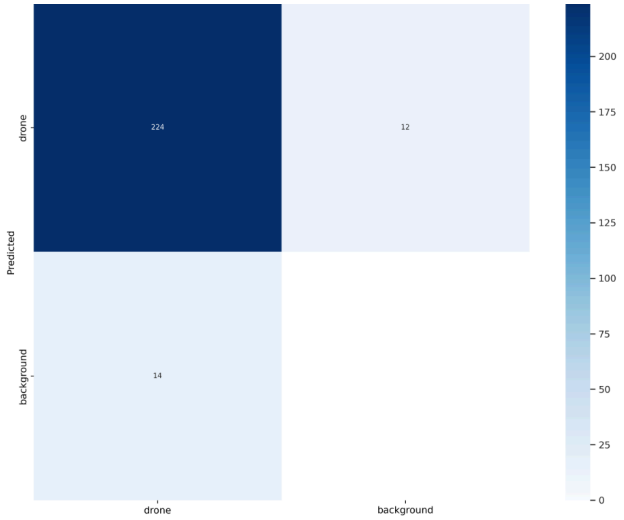


Fig 15. Confusion Matrix for the result

2. Precision-Recall Curve

The **precision-recall curve** visualizes the trade-off between precision (the proportion of true positive detections out of all positive detections) and recall (the proportion of true positive detections out of all actual positive instances). In our case:

- **High precision** indicates that the model successfully detects relevant objects with minimal false positives.
- **High recall** suggests that the model is able to detect most objects in the dataset, with fewer missed detections.

The curve demonstrates that as recall increases, precision drops slightly, indicating the model's strong performance in detecting objects.

The Precision-Recall Curve illustrates the model's excellent detection performance, achieving a mean Average Precision (mAP) of 0.962 for both the 'drone' class and all classes combined at an IoU threshold of 0.5, signifying its high reliability in minimizing false positives and negatives.

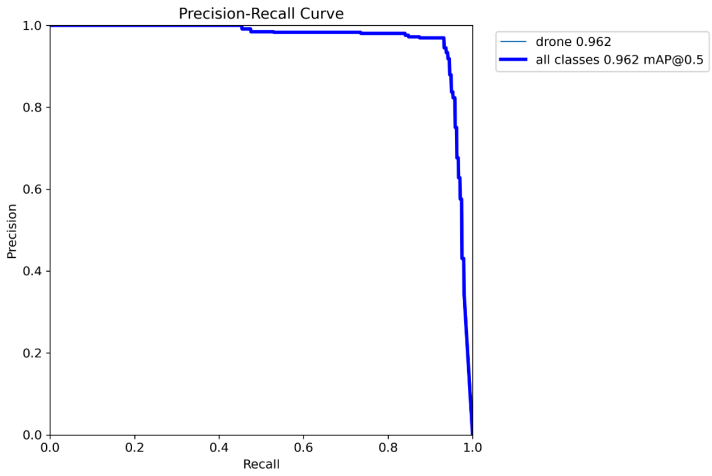


Fig 16. Precision v/s Recall Curve

3. Recall-Confidence Curve

The **recall-confidence curve** shows the model's recall performance at different confidence thresholds. This is important for understanding how varying the confidence level (the probability score the model assigns to a prediction) affects the recall rate.

- **Higher confidence thresholds** typically reduce false positives but may also lower recall as the model becomes more conservative in making predictions.

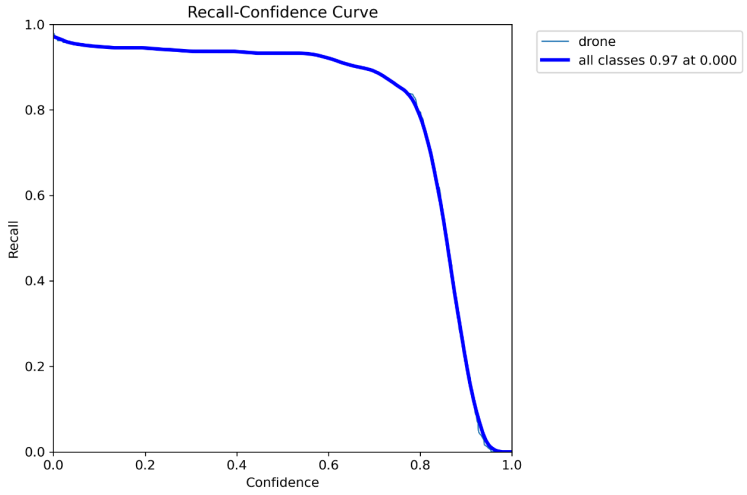


Fig 17 Recall v/s confidence curve

- **Lower thresholds** increase recall but may lead to more false positives.

This curve helps us set an optimal confidence threshold for specific applications of our model.

Observations:

- **Flat Start**:
    - The curve starts near a recall of 1, demonstrating that at low confidence thresholds, almost all true positives are detected.
- **Sharp Decline**:
    - As the confidence threshold increases (towards 1.0), recall sharply decreases, indicating that the model is filtering out predictions it considers uncertain. While this reduces false positives, it also excludes some true positives.

The Recall-Confidence Curve demonstrates the model's ability to detect nearly all true positives **(recall = 0.97**) at low confidence thresholds. However, as the confidence threshold increases, recall decreases sharply, reflecting the model's balance between sensitivity and prediction certainty. This analysis is critical for optimizing the threshold to suit specific use cases

4. Precision-Confidence Curve

The **precision-confidence curve** highlights how precision changes as the confidence threshold is adjusted. It provides insights into how confident the model is when making correct detections.

- **At higher confidence levels**, the m3. Precision-Confidence Curve
- The precision-confidence curve highlights how precision changes as the confidence threshold is adjusted. It provides insights into how confident the model is when making correct detections.
- At higher confidence levels, the model exhibits higher precision but may discard some correct detections.
- At lower confidence levels, more objects are detected but with a slight trade-off in precision.
- This curve assists in balancing precision and confidence to find the best threshold for real-world scenarios.odel exhibits higher precision but may discard some correct detections.
- **At lower confidence levels**, more objects are detected but with a slight trade-off in precision.

This curve assists in balancing precision and confidence to find the best threshold for real-world scenarios.

Key Observations from the Curve:

- **Overall Trend:** The curve generally rises from left to right, indicating that as the confidence threshold increases, the precision also increases. This is expected, as higher confidence predictions are more likely to be correct.

- **All Classes Precision:** The blue line represents the precision for all classes combined. It reaches a maximum precision of 1.00 at a confidence level of 0.891. This means that if the model is only considering predictions with a confidence level of 0.891 or higher, it will have

perfect precision.

- **Class-Specific Precision:** The light blue line represents the precision for the "drone" class specifically. It follows a similar trend to the overall precision but might have slight variations due to the specific characteristics of the "drone" class.

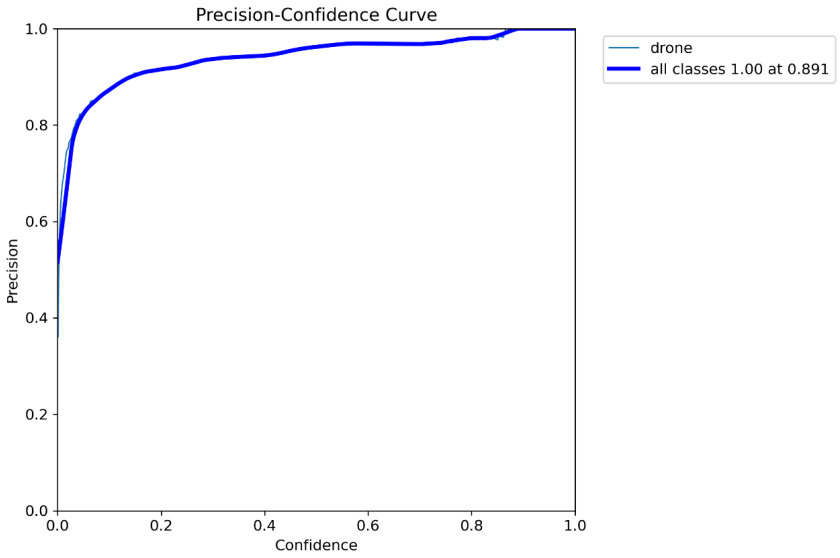


Fig 18. Precision v/s Confidence curve

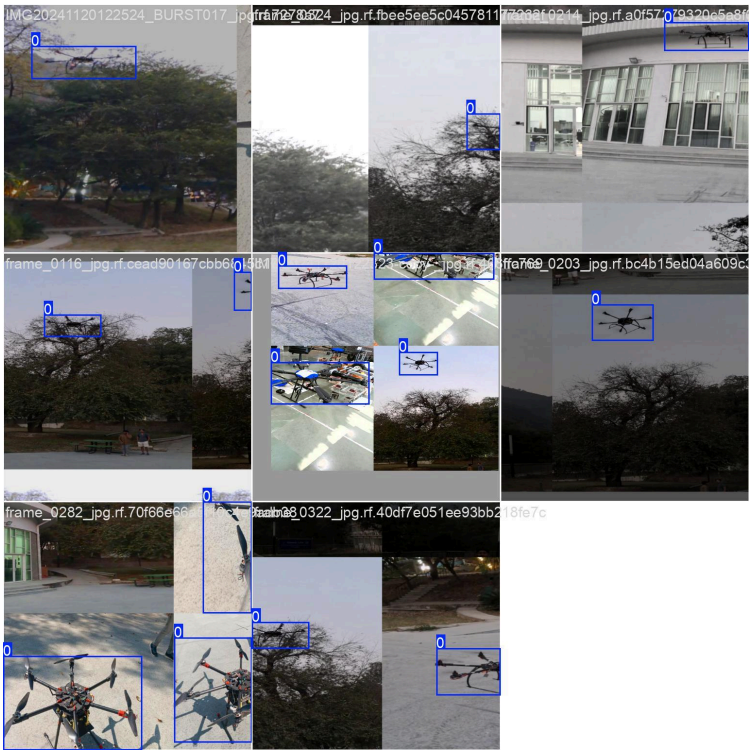


Fig 19. Training Dataset

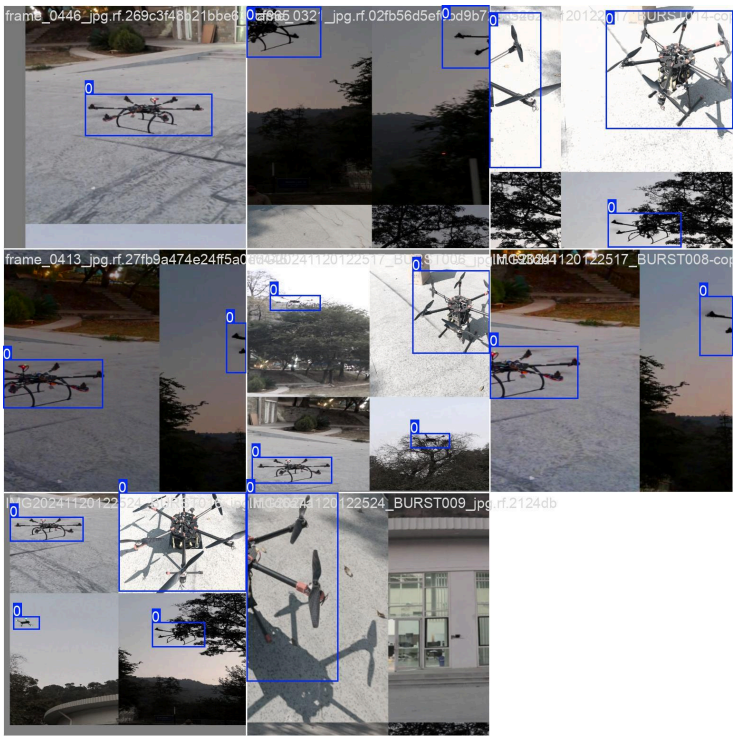


Fig 20. Testing Dataset

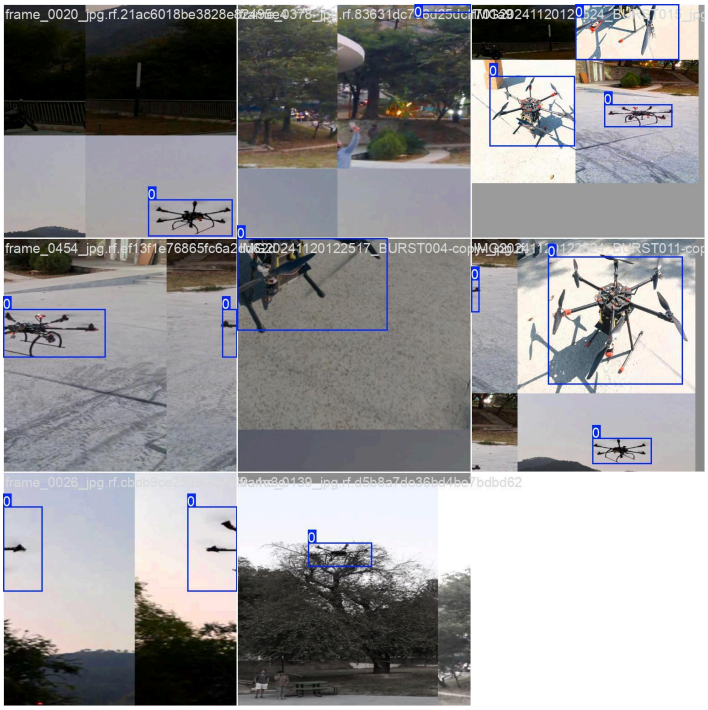


Fig 21. Valid Dataset

	from	n	params	module	arguments
0	-1	1	464	ultralytics.nn.modules.conv.Conv	[3, 16, 3, 2]
1	-1	1	4672	ultralytics.nn.modules.conv.Conv	[16, 32, 3, 2]
2	-1	1	6640	ultralytics.nn.modules.block.C3k2	[32, 64, 1, False, 0.25]
3	-1	1	36992	ultralytics.nn.modules.conv.Conv	[64, 64, 3, 2]
4	-1	1	26080	ultralytics.nn.modules.block.C3k2	[64, 128, 1, False, 0.25]
5	-1	1	147712	ultralytics.nn.modules.conv.Conv	[128, 128, 3, 2]
6	-1	1	87040	ultralytics.nn.modules.block.C3k2	[128, 128, 1, True]
7	-1	1	295424	ultralytics.nn.modules.conv.Conv	[128, 256, 3, 2]
8	-1	1	346112	ultralytics.nn.modules.block.C3k2	[256, 256, 1, True]
9	-1	1	164608	ultralytics.nn.modules.block.SPPF	[256, 256, 5]
10	-1	1	249728	ultralytics.nn.modules.block.C2PSA	[256, 256, 1]
11	-1	1	0	torch.nn.modules.upsampling.Upsample	[None, 2, 'nearest']
12	[-1, 6]	1	0	ultralytics.nn.modules.conv.Concat	[1]
13	-1	1	111296	ultralytics.nn.modules.block.C3k2	[384, 128, 1, False]
14	-1	1	0	torch.nn.modules.upsampling.Upsample	[None, 2, 'nearest']
15	[-1, 4]	1	0	ultralytics.nn.modules.conv.Concat	[1]
16	-1	1	32096	ultralytics.nn.modules.block.C3k2	[256, 64, 1, False]
17	-1	1	36992	ultralytics.nn.modules.conv.Conv	[64, 64, 3, 2]
18	[-1, 13]	1	0	ultralytics.nn.modules.conv.Concat	[1]
19	-1	1	86720	ultralytics.nn.modules.block.C3k2	[192, 128, 1, False]
20	-1	1	147712	ultralytics.nn.modules.conv.Conv	[128, 128, 3, 2]
21	[-1, 10]	1	0	ultralytics.nn.modules.conv.Concat	[1]
22	-1	1	378880	ultralytics.nn.modules.block.C3k2	[384, 256, 1, True]
23	[16, 19, 22]	1	430867	ultralytics.nn.modules.head.Detect	[1, [64, 128, 256]]

```
      Epoch    GPU_mem   box_loss   cls_loss   dfl_loss  Instances       Size
                 all        219        238      0.957      0.943      0.967      0.706

      Epoch    GPU_mem   box_loss   cls_loss   dfl_loss  Instances       Size
                 all        219        238      0.959      0.937      0.968      0.709

      Epoch    GPU_mem   box_loss   cls_loss   dfl_loss  Instances       Size
                 all        219        238      0.961       0.95       0.97      0.709

      Epoch    GPU_mem   box_loss   cls_loss   dfl_loss  Instances       Size
                 all        219        238      0.961      0.934      0.967        0.7

      Epoch    GPU_mem   box_loss   cls_loss   dfl_loss  Instances       Size
                 all        219        238      0.953      0.941      0.968      0.711

      Epoch    GPU_mem   box_loss   cls_loss   dfl_loss  Instances       Size
                 all        219        238      0.957      0.937      0.967      0.711

      Epoch    GPU_mem   box_loss   cls_loss   dfl_loss  Instances       Size
                 all        219        238      0.953      0.946      0.971      0.711

      Epoch    GPU_mem   box_loss   cls_loss   dfl_loss  Instances       Size
                 all        219        238      0.973       0.92      0.968      0.712
%[34m%[1mEarlyStopping: %[0mTraining stopped early as no improvement observed in last 10 epochs. Best results observed at epoch 47, best model saved as best
To update EarlyStopping(patience=10) pass a new patience value, i.e. `patience=300` or use `patience=0` to disable EarlyStopping.
```

```
%[1moptimizer:%[0m SGD(lr=0.0001795820470907558, momentum=0.8008394988275205) with parameter groups 81 weight(decay=0.0), 88 weight(decay=0.0001795583286792522),
87 bias(decay=0.0)
```

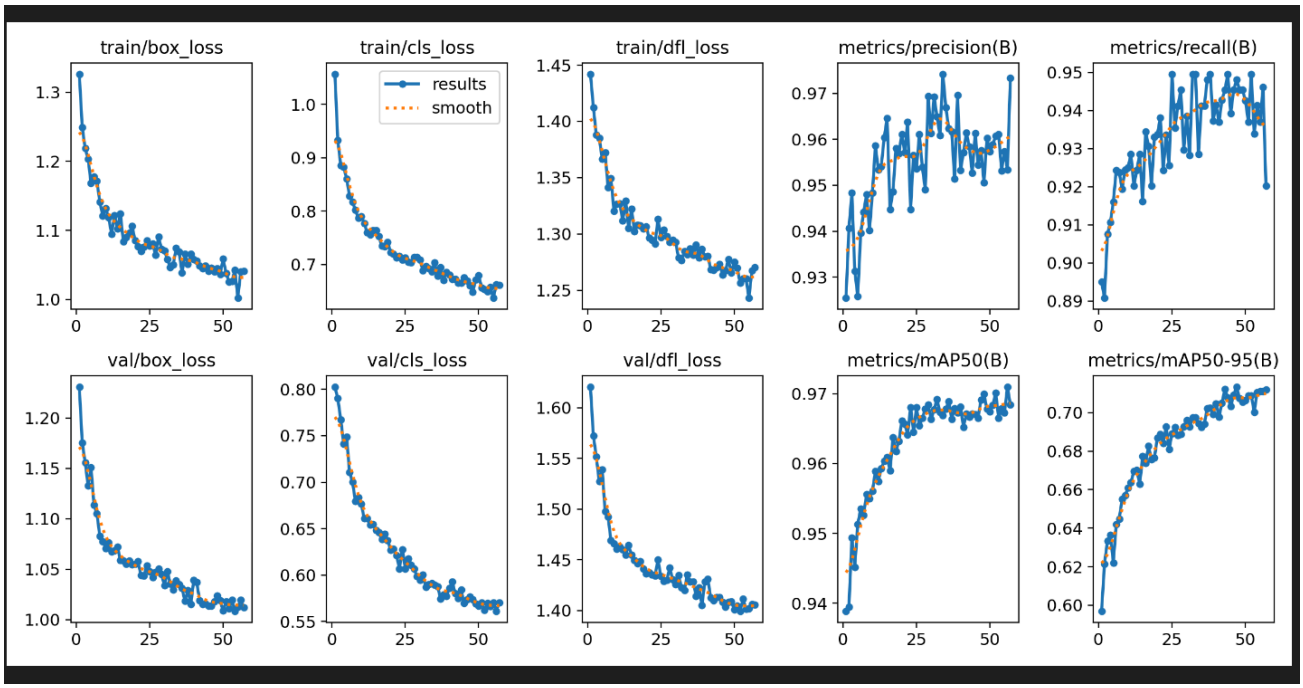


Fig 22. Results

5. Live Detection of Drone via our Model

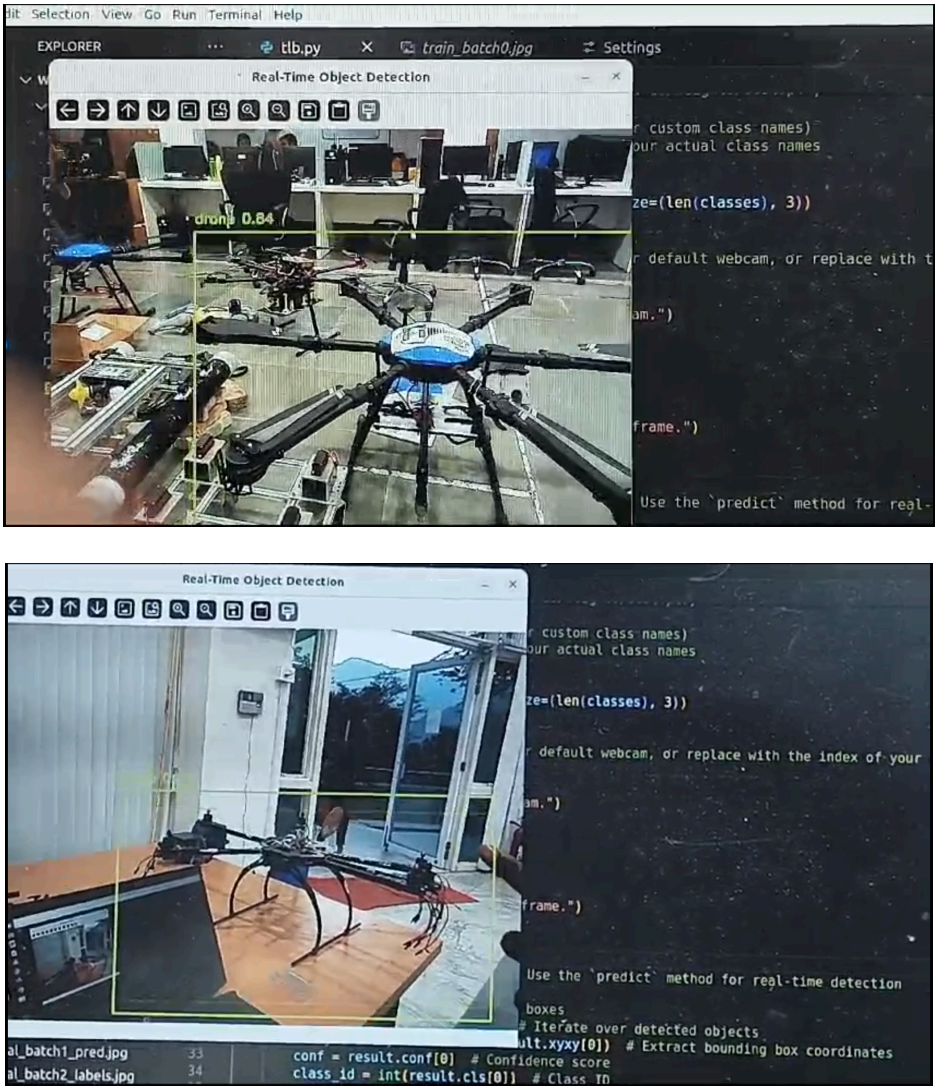


Fig 23. Live Detection

Our system successfully implements live drone detection using advanced deep learning model YOLOv9. The system processes real-time video streams, detects drones with high precision, and identifies under diverse conditions, including varying angles, lighting, and backgrounds. This capability ensures timely responses, enhancing the effectiveness of drone neutralization strategies in securing restricted zones.

Conclusion

The implementation of the YOLOv9-based drone detection system has demonstrated promising results in detecting various types of drones under diverse environmental conditions. The use of a custom dataset, featuring a wide range of drone models and scenarios, significantly enhanced the model's precision and minimized false positives. The split of the dataset into training, testing, and validation sets ensured effective generalization of the model, achieving reliable performance across unseen data.

Performance evaluations, including precision-recall curves and confusion matrices, indicated that the YOLOv9 model is highly capable of detecting drones in real-time,while training we got a precision of 93% and a recall of 97%, making it suitable for integration into a larger counter-drone system. While challenges such as small drone detection and environmental interference were encountered, optimization techniques like hyperparameter tuning and advanced optimizers helped mitigate these issues.

These findings form a solid foundation for the next phase of the project, which will focus on integrating the detection system with air-to-air neutralization techniques, ensuring a comprehensive and effective solution for addressing UAV-related threats.

References

[1] Barbora Kotkova, Airport defense systems against drones attacks

[2] Fidel Gonzalez, Rafael Caballero, Francisco J. Perez-Grau and Antidio Viguria, Vision-based UAV Detection for Air-to-Air Neutralization

[3] V. M. Nuzhdin, A. E. Ananenkov, D. V. Marin, Radar of Complex UAV Detection and Neutralization

[4] Vittorio ugo Castrillo, Angelo Manco , Domenico Pascarella and Gabriella Gigante, A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones

[5] Florin-Lucian Chiper, Alexandru Martian, Calin Vladeanu, Ion Marghescu, Razvan Craciunescu and Octavian Fratu, Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution

[6] Vinay Chamola, Pavan Kotesh, Aayush Agarwal, Naren, Navneet Gupta, Mohsen Guizani, A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques

[7] Vladimir Matić, Vladimir Kosjer, Aleksandar Lebl, Branislav Pavić, Jovan Radivojević, Methods for Drone Detection and Jamming

[8] Simeon Okechukwu Ajakwe, Vivian Ukamaka Ihekoronye, Rubina Akter, Dong-Seong Kim, Jae Min Lee, Adaptive Drone Identification and Neutralization Scheme for Real-Time Military Tactical Operations

[9] Younwoo Ki, Suhyun Chun, Jihoon Ryoo, Study on the Anti-Drone System: Today’s Capability and Limitation