SCIEPublish

Article

Smart Drone Neutralization: AI Driven RF Jamming and Modulation Detection with Software Defined Radio

Savindu Nanayakkara [1,*], Sagara Sumathipala [1], Nalan Karunanayake [2], Mihiraj Karunanayake [1] and Thilina Kumara [1]

[1] Department of Computational Mathematics, University of Moratuwa, Moratuwa 10400, Sri Lanka; sagaras@uom.lk (S.S.); karunanayakekmch.20@uom.lk (M.K.); kumaracptk.20@uom.lk (T.K.)

[2] School of Information and Computer Technology, Sirindhorn International Institute of Technology, Thammasat University, Bangkok 10200, Thailand; d6222300037@g.siit.tu.ac.th (N.K.)

∗ Corresponding author. E-mail: nanayakkaragasy.20@uom.lk (S.N.)

Received: 22 June 2025; Accepted: 17 October 2025; Available online: 30 October 2025

ABSTRACT: The increasing use of wireless technologies in many aspects of people's lives has led to a congested electromagnetic spectrum, making it critical to manage the limited available spectrum as efficiently as possible. This is particularly important for military activities such as electronic warfare, where jamming is used to disrupt enemy communication, self-attacking drones, and surveillance drones. However, current detection methods used by armed personnel, such as optical sensors and Radio Detection and Ranging (RADAR), do not include Radio Frequency (RF) analysis, which is crucial for identifying the signals used to operate drones. To combat security vulnerabilities posed by the rogue or unidentified transmitters, RF transmitters should be detected not only by the available data content of broadcasts but also by the physical properties of the transmitters. This requires faster fingerprinting and identifying procedures that extend beyond the traditional hand-engineered methods. In this paper, RF data from the drones' remote controller is identified and collected using Software Defined Radio (SDR), a radio that employs software to perform signal-processing tasks that were previously accomplished by hardware. A deep learning model is then provided to train and detect modulation strategies utilized in drone communication and a suitable jamming strategy. This paper overviews Unmanned Aerial Vehicles (UAV) neutralization, communication signals, and Deep Learning (DL) applications. It introduces an intelligent system for modulation detection and drone jamming using Software Defined Radio (SDR). DL approaches in these areas, alongside advancements in UAV neutralization techniques, present promising research opportunities. The primary objective is to integrate recent research themes in UAV neutralization, communication signals, and Machine Learning (ML) and DL applications, delivering a more efficient and effective solution for identifying and neutralizing drones. The proposed intelligent system for modulation detection and jamming of drones based on SDR, along with deep learning approaches, holds great potential for future research in this field.

Keywords: UAV neutralization; Intelligent systems; Software defined radio; Deep learning; Modulation detection

1. Introduction

Wireless technologies have become pervasive in many aspects of people's lives. Beyond smartphones, wireless technologies are widely used in surveillance, telemetry, emitter localization, Radio Detection and Ranging (RADAR), radio navigation, location tracking, jamming, Unmanned Aerial Vehicle (UAV) surveillance, and anti-jamming techniques. Given the widespread use of the radio frequency (RF) spectrum, it is essential to manage and utilize the limited available spectrum as efficiently as possible. However, the electromagnetic spectrum has become increasingly congested due to the growing number and widespread use of RF transmitters.

In military contexts, particularly in electronic warfare, RF jammers are employed to disrupt enemy communications and drone operations by emitting interference signals. These operations play a critical role in disabling adversary drones and other RF-based communication systems. Drone detection, a key aspect of these operations, is typically conducted using technologies such as RADAR, optical sensors, acoustic sensors, and RF analysis [1]. Although RF analysis is underutilized compared to optical sensors and RADAR, it holds significant potential in

https://doi.org/10.70322/dav.2025.10019

scenarios where rapid, data-driven decision-making is necessary. By monitoring the RF spectrum, RF analysis enables the identification of signals used to operate drones, making it a vital component of drone interdiction.

Addressing the security risks posed by rogue or unidentified RF transmitters requires detecting transmitters not only by their data content but also by their physical properties. The challenges of high data rates and multiple transmitters sharing a single channel create the need for faster, more sophisticated identification methods than traditional hand-engineered techniques can provide [2]. As such, there is an increasing demand for advanced fingerprinting techniques that leverage machine learning (ML) and deep learning (DL) models [3].

In this study, we propose an intelligent system for modulation detection and jamming of drone communication using Software Defined Radio (SDR). SDR offers a flexible platform for signal processing via software, which enables rapid adaptability in response to new threats. A machine learning model classifies modulation strategies and identifies appropriate jamming responses. While numerous studies have explored ML and DL applications for communication signals and UAV neutralization, no recent research has fully integrated these approaches into a unified solution. This work fills that gap by introducing a system that combines SDR-based modulation classification with ML techniques for effective drone jamming.

The rest of the paper is structured as follows. Section 2 introduces background concepts about relevant literature and identifies the research gap, discussing potential technologies to solve the research problem. In Section 3 we present our detailed discussion of the technology used in the research, explains the approach of the study in detail. The design phase and implementation of the designed model are detailed in Section 4. Section 5 evaluates the implemented model design, and finally, Section 6 concludes the paper and presents directions for future work.

2. Background and Related Works

This section reviews the state-of-the-art in SDR-based modulation classification, UAV signal identification, and associated jamming techniques, providing context for the challenges and advancements in this field.

2.1. UAVs Advancement and Potential Threats

UAVs have gained significant traction in various sectors, including military, civil, and agricultural domains. Their applications range from animal tracking [4] and crisis management [5] to delivering goods [6,7] and search and rescue missions [8,9]. Additionally, UAVs are being explored for space exploration [10–14]. By 2026, the UAV market is expected to expand from USD 27.4 billion to USD 58.4 billion, driven by automation demand and rapid advancements in enabling technologies [15]. However, UAV technology also poses security risks, including hostile drone attacks [16]. Several incidents demonstrate the potential threats posed by rogue drones, such as the 1994 sarin gas attack attempt using a drone [1], Al-Qaeda's planned 2013 drone strike in Pakistan, and the targeted attack on California's power grid, which caused USD 15 million in damages. More recently, drones have been used by terrorist organizations to gather intelligence and deliver explosives, chemical, and biological weapons, further emphasizing the need for effective drone detection and neutralization mechanisms [17].

2.2. Drone Detection Mechanisms

Various techniques are employed for drone detection, each with its limitations. Optical systems using video cameras often suffer from poor visibility in low light or adverse weather conditions, leading to high false alarm rates [18,19]. While capable of detecting low-flying drones, RADAR systems often struggle with clutter and cannot easily distinguish between small drones and birds [20]. Geofencing, a common defense mechanism in commercial drones, can be bypassed by skilled users [17].

RF analysis provides a promising solution, as it identifies and monitors the communication signals drones rely on. In particular, modulation classification, which determines the type of signal modulation used by a drone, is crucial since different modulations indicate distinct communication types. Traditional manual modulation identification is unreliable due to human error, leading to the development of automated approaches, such as likelihood ratio-based and feature-based methods, each with advantages and limitations [21].

2.3. Application of Software Defined Radio Technology in Modulation Classification

Software Defined Radio (SDR) has revolutionized signal processing by allowing functions traditionally implemented in hardware to be handled by software, providing greater flexibility. While Joe Mitola is often credited

with its invention, the concept dates back to the 1980s with the development of the SpeakEasy transceiver platform [22]. Initially designed for tactical communications and interoperability among military forces, SDR has since advanced into a powerful tool for various applications, including drone signal analysis. SDR-based modulation classification uses machine learning (ML) algorithms to classify signals based on extracted features. These algorithms are robust against changes in signal characteristics such as noise and fading, but require large training datasets. Alternatively, known reference signals and correlation techniques can be used to determine modulation types, though these methods are more sensitive to signal variations and less effective in noisy environments.

2.4. Spread Spectrum & Protocols of Drone RF Signals

Modern commercial drones predominantly operate in the 2.4 GHz and 5 GHz Wi-Fi bands for manual control, with GPS-based functionalities using frequencies of 1574.42 MHz and 1227.60 MHz. Drones may also utilize the 900 MHz and 1.3 GHz bands, which can interfere with GPS and require larger antennas. Traditional analog (AM, FM, PM) and digital modulations (ASK, FSK, PSK) have been replaced by spread spectrum technologies, such as Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). These technologies enhance resistance to interference and jamming, making drone communication more reliable. Moreover, the protocols used between the drone and its controller vary in packet structure, encryption, and spectrum usage, making it possible to trace a drone to its manufacturer. This knowledge aids in developing jamming strategies tailored to counter specific drones.

2.5. Technology Implemented in Drone Jamming

Drone jamming aims to disrupt UAV communication systems, neutralizing them by blocking the signals between the drone and its operator [23]. Other methods of drone neutralization include directed energy weapons, physical countermeasures (e.g., nets or trained birds), and laser systems [24,25]. Jamming techniques are divided into response jamming, which reacts to incoming signals, and noise jamming, which generates broad-spectrum interference. Noise jamming can be wideband, covering a range of frequencies, or narrowband, targeting specific frequencies. However, its effectiveness depends on the ability to locate the drone accurately, which is challenging due to the small size and mobility of UAVs. In some cases, barrage jamming, which targets multiple frequencies, can spread the jamming power too thin, reducing its effectiveness [26,27]. Recent advancements in ML have introduced more dynamic jamming techniques, capable of adapting to changes in the drone's signal characteristics in real-time [28,29].

2.6. Analysis of Literature

Table 1 summarizes current surveys and evaluations on accurate modulation type classification using machine learning and deep learning. It highlights key findings, advantages, limitations, input signal types, technologies used, modulation types, and recognition accuracy.

Table 1. Summary of surveys and evaluations on modulation type classification using machine learning and deep learning.

Research	Advantages	Limitations	Input Signal Type	Technology & Recognition Accuracy	Modulation Signal Type
Siyang Zhou [30]	Accuracy increases when the number of layers increases in the CNN model	Accuracy decreases with low SNR	Amplitude *vs.* sample signal graph	CNN 90% under -10 dB SNR	2ASK, 4ASK, 8ASK, 2FSK, 4FSK, 8FSK, 2PSK, 4PSK, 8PSK, 4QAM, 16QAM, 64QAM, OFDM, LFM, MSK
Sowjanya Ponnaluru [3]	Accuracy increases with the number of datasets	Higher SNRs are required for robust efficiency in high-order modulations.	Frequency *vs.* Time Spectrogram	CNN 98.9% at 20 dB SNR	4PAM, QPSK, 128QAM, 8PSK, 16QAM, GFSK, 32QAM, 64QAM, BPSK, 256QAM, CPFSK

Jithin Jagannath [31]	The estimated SNR value enhances classifier performance independent of ANN design, Less processing power	The probability of correct classification decreases when the number of layers increases.	Amplitude, phase, frequency, and other signal statistics such as moments and cumulants, are among the features	ANN 98% at 15 dB SNR	BPSK, 8PSK, GMSK, QPSK, GFSK, 16QAM, CPFSK
Hui Han [32]	PNN has a shorter training time than SAE and ANN, and its accuracy is higher at low SNR than SAE, SVM, and ANN.	Supervised learning may cause feature confusion, and accuracy decreases with low SNR	Welch power spectrum	SAE (stacked auto-encoder), PNN (probabilistic neural network) 99.8% at 0 dB SNR	2PSK, 2FSK, 4PSK, 4ASK, 8ASK, 32QAM, 4FSK, 8FSK, 64QAM
Feng Wang [33]	Hybrid ML network improves the classification of modulation techniques	Correct recognition rate decreases when low SNR	Time-frequency spectrum	PCA, SVM 94% at 10dB SNR	BPSK, QPSK, 16QAM, LFM, 2FSK, 4FSK
Yilin Sun [34]	The Inception-v3 with the constellation model achieves the maximum accuracy in high SNR circumstances, while the GRF (Graphical representation of features) delivers higher accuracy in low SNR scenarios.	Detection accuracy decreases with low SNR	Constellation diagram	CNN, SqueezeNet, GoogleNet, Inception-v3 For SNRs larger than 10 dB SNR, around 100%	BPSK, QPSK, 8PSK, QAM16
Peng Wu [35]	Classification accuracy increases gradually and remains stable with the increase of SNR	Training time(s)/epoch is high	Time-frequency spectrum	Inception-ResNet 93.76% at 14 dB SNR	8PSK, BPSK, CPFSK, GFSK, PAM4, QAM1, QAM64, QPSK
Ruolin Zhou [36]	Training CNN with an extra layer improves accuracy.	In the complex communication environment, the quality of communication is often too difficult to guarantee.	Time-frequency spectrum	CNN, LSTM 96.25%	16-QAM, CPFSK, 8-PSK, BPSK, GFSK, 64-QAM, PAM4, QPSK
Shengliang Peng [37]	A larger volume of training data is also advantageous for performance enhancement.	Due to the low resolution of photos, data conversion from complicated samples to images certainly results in information loss.	Constellation diagrams	AlexNet 79.6%~100% at 8 dB SNR	QPSK, 8PSK, 16QAM, 64 QAM
Venkatesh Sathyanarayanan [38]	Under nominal channel distortions, neural network performance for the modulation classification task may attain very high levels of accuracy over a wide variety of modulation patterns.	Frequency errors are more common in phase sensitive modulation types.	Time-frequency spectrum	ResNet 80%	8PSK, B-FM, BPSK, CPFSK, DSB-AM, GFSK, PAM4, QPSK, SSB-AM

Despite advancements in drone neutralization and signal analysis using ML and DL methods, real-time identification of drone RF signals remains a significant challenge. Existing studies have not fully integrated DL-based techniques for real-time drone RF signal detection and classification. This research aims to fill this gap by employing DL-based object detection to enable accurate and efficient real-time identification of drone RF signals, addressing challenges such as large dataset requirements and the specific needs of military applications.

Recent contributions have begun extending this work into operational UAV security systems. Xu et al. [39] presented an integrated SDR-based framework for passive detection and blanket jamming, demonstrating the feasibility of combining spectrum sensing with wideband interference. Khan et al. [40] introduced a UAV-based smart surveillance system built on wireless sensor networks, showing the role of distributed sensing in threat monitoring. Zhang et al. [41]

examined ML-driven unauthorized UAV detection integrated into UTM frameworks, highlighting the importance of scalable civil airspace security solutions. Complementary to these, Tesfay et al. [42] proposed a deep learning-based UAV neutralization system leveraging intelligent jamming, while Xue et al. [43] developed adaptive signal generation strategies for UAV jamming in IEEE Access. Collectively, these works illustrate the breadth of recent advances spanning detection, surveillance, and jamming.

However, a persistent limitation across prior studies is their focus on either detection or jamming, rather than their integration. Existing solutions typically address signal recognition, surveillance, or interference independently, leaving a gap in unified systems that can identify and neutralize drones in real time. The present study is the first to demonstrate an end-to-end SDR-based framework that couples deep learning driven modulation detection with immediate jamming activation. By validating the system on real RF data from multiple commercial transmitters, our work advances beyond simulation-only or single-function approaches and contributes a practical, integrated solution to UAV countermeasure research.

3. Methods

This section outlines the methods for detecting and jamming drone radio frequency (RF) signals by integrating software-defined radio (SDR) technology with deep learning models. The approach involves capturing RF signals emitted by drones, processing them to generate spectrograms, and utilizing machine learning techniques for signal detection and classification. An automatic jamming mechanism is then implemented based on the identified signals.

3.1. Overview

The proposed system, the Intelligent System for Modulation Detection and Jamming of Drones (ISMD), is designed to detect and classify drone RF signals within a specified perimeter, typically up to 100 m. By capturing real-time drone control data, such as modulation techniques, transmitting power, and signal-to-noise ratio, the system processes these inputs using SDR technology and deep learning models to generate spectrograms and accurately identify drone signals. Upon detection, the system employs a repeat attack jamming technique to disrupt unauthorized drone activities.

3.2. Equipment and Software

3.2.1. Hardware

The primary hardware component used in this study is the HackRF One SDR (Great Scott Gadgets, USA), which operates over a frequency range of 1 MHz to 6 GHz. This range encompasses the Industrial, Scientific, and Medical (ISM) bands commonly utilized by drones for communication and control. The HackRF One can both receive and transmit signals, making it suitable for capturing RF signals from drones and implementing jamming techniques. Additional hardware includes antennas compatible with the HackRF One to enhance signal reception and transmission capabilities.

3.2.2. Software

Various software tools were employed to support the hardware components in this study. SDRangel (Version 6.0.2), an open-source SDR platform, interfaced with the HackRF One to tune specific frequency ranges, capture drone RF signals, and generate spectrograms for analysis. The TensorFlow Object Detection API facilitated the development and training of machine learning models for object detection, leveraging features like data augmentation and transfer learning. Python served as the primary programming language for scripting and automation, utilizing libraries such as PyAutoGUI for automating frequency scanning and jamming activation, and OpenCV for image processing and feature extraction tasks. Figure 1 illustrates the SDRangel user interface used during the study.

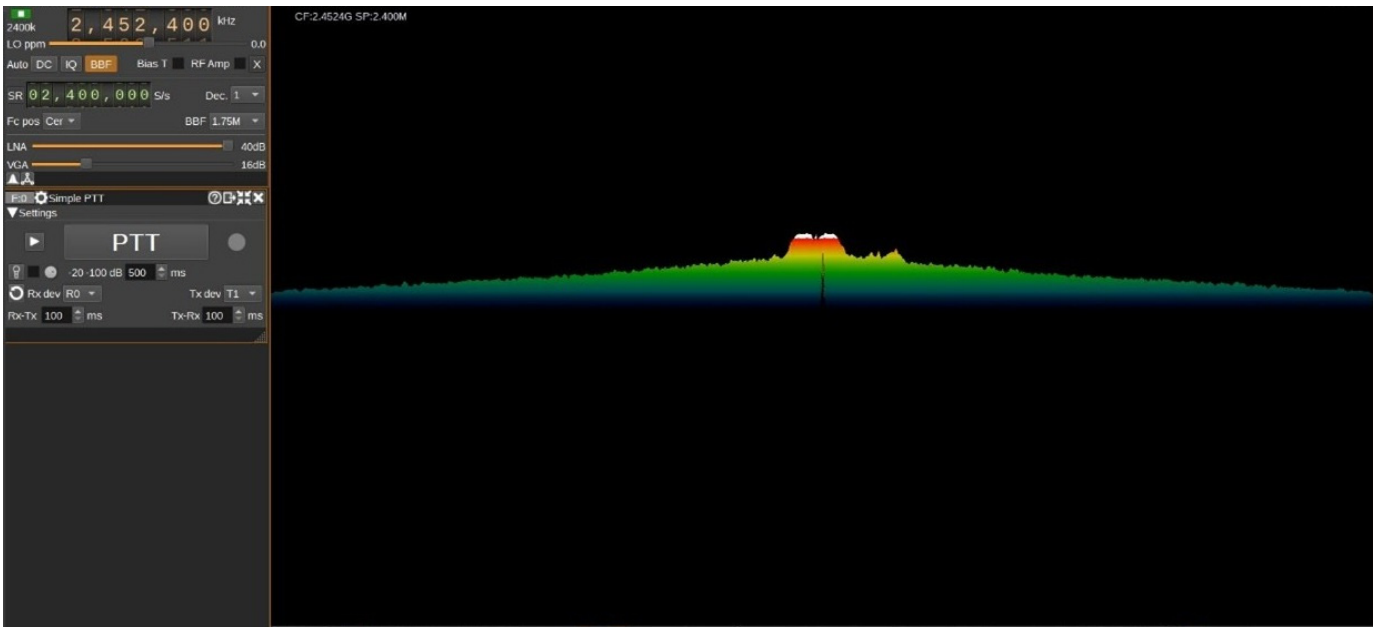

Figure 1. SDRangel software user interface.

3.3. Data Collection

3.3.1. Drone Transmitters and Specifications

Four commercially available drone transmitters operating within the 2.4 GHz ISM band were selected to generate a diverse dataset of RF signals. These transmitters employ different modulation techniques, spread spectrum methods, and communication protocols, providing a comprehensive range of signal characteristics for model training. Table 2 summarizes the specifications of each transmitter, including modulation type, spread spectrum technique, and protocol used.

Table 2. Details of transmitters.

Transmitter Type	Modulation/Spread Spectrum/Protocol
SKYDROID T 12	Modulation: Frequency Shift Keying (FSK) Spread Spectrum: Frequency Hopping Spread Spectrum (FHSS) Protocol: CSMA/CA
FLYSKY FS-i6	Modulation: Gaussian Frequency Shift Keying (GFSK) Spread Spectrum: Frequency Hopping Spread Spectrum (FHSS) Protocol: AFHDS2A
DUMBORC-X6	Modulation: Gaussian Frequency Shift Keying (GFSK) Spread Spectrum: Chirp Spread Spectrum (CSS) Protocol: AFHDS2
DJI TELLO	Modulation: Gaussian Minimum Shift Keying (GMSK) Differential Quadrature Phase Shift Keying (DQPSK) Spread Spectrum: Direct Sequence Spread Spectrum (DSSS) Protocol: Wi-Fi UDP

3.3.2. RF Data Acquisition

Data collection involved capturing RF signals emitted by each transmitter using the HackRF One SDR in conjunction with SDRangel software (Version 6.0.2). The transmitters were placed at varying distances from the receiver, incrementally increasing by 5 m up to a maximum of 40 m, to simulate different operational scenarios. At each distance, 50 samples were collected per transmitter, resulting in 400 samples per transmitter and an aggregate of 1600 samples for the entire dataset. The captured signals were processed in real-time to generate spectrograms, which visually represent the frequency spectrum of the signals over time. These spectrograms served as input data for the deep learning models.

For all data collection experiments, the HackRF One was configured with a sampling rate of 20 mega-samples per second (MS/s), centered in the 2.40–2.49 GHz ISM band, with an effective receiver bandwidth of 2 MHz. The automatic

gain control (AGC) was fixed at 30 dB to balance sensitivity and avoid saturation in strong signal scenarios. Each RF capture was processed in SDRangel to generate spectrograms using a 1024-point FFT with a 50% overlap and a Hann window function, resulting in a time resolution of approximately 2 ms per frame. This configuration provided sufficient frequency resolution to distinguish between modulation schemes while maintaining real-time responsiveness.

3.4. Data Preparation

3.4.1. Spectrogram Generation

The SDRangel software (Version 6.0.2) was configured to generate spectrograms from the captured RF signals. Key parameters such as frequency range, resolution bandwidth, and time window were adjusted to optimize the quality of the spectrograms for analysis. The spectrograms provided a visual representation of the signal's frequency content, which is essential for identifying unique patterns associated with different drone transmitters.

3.4.2. Image Labeling

Accurate annotation of the spectrogram images is critical for training effective object detection models. The LabelImg software (Version 1.8.6) was employed to manually annotate the spectrograms by drawing bounding boxes around the regions of interest corresponding to each transmitter type. Annotations were saved in the PASCAL Visual Object Classes (VOC) format, which includes details such as the object's class, bounding box coordinates, and image size. Figure 2 illustrates an example of an annotated spectrogram image. Each transmitter class had 400 annotated images, resulting in a total of 1600 annotated images organized into four groups based on transmitter type.

```
<annotation>
	<folder>images</folder>
	<filename>TELO_40m_0384.jpg</filename>
	<path>C:\Users\NANAYAKKARA\Desktop\data set\images\TELO_40m_0384.jpg</path>
	<source>
		<database>Unknown</database>
	</source>
	<size>
		<width>1918</width>
		<height>1027</height>
		<depth>3</depth>
	</size>
	<segmented>0</segmented>
	<object>
		<name>DJI_Tello</name>
		<pose>Unspecified</pose>
		<truncated>1</truncated>
		<difficult>0</difficult>
		<bndbox>
			<xmin>396</xmin>
			<ymin>396</ymin>
			<xmax>1918</xmax>
			<ymax>539</ymax>
		</bndbox>
	</object>
</annotation>
```

Figure 2. Example of spectrogram annotation in PASCAL VOC format.

3.5. Model Development

3.5.1. TensorFlow Object Detection API

The TensorFlow Object Detection API was utilized to develop and train object detection models capable of identifying and classifying drone RF spectrograms. The API offers pre-trained models and tools for training custom models on new datasets. It supports features like data augmentation and transfer learning, and provides evaluation metrics to assess model performance.

3.5.2. Transfer Learning and Model Selection

Transfer learning was employed to leverage pre-trained models trained on large datasets, enabling the model to recognize high-level features within images. Four pre-trained models were selected from the TensorFlow Model Zoo

based on criteria such as processing speed (in milliseconds), mean average precision (mAP), and compatibility with available hardware resources:

Table 3 lists the selected models: CenterNet HourGlass104 [44], EfficientDet D0 [45], SSD ResNet50 V1 FPN (RetinaNet50) [46], and Faster R-CNN ResNet152 V1 [47,48], along with their respective mAP scores and processing speeds.

Table 3. Selected pre-trained models and their specifications.

Model	COCO mAP	Speed (ms)
CenterNet HourGlass104 512 × 512	41.9	70
EfficientDet D0 512 × 512	33.6	39
SSD ResNet50 V1 FPN 1024 × 1024 (RetinaNet50)	38.3	87
Faster R-CNN ResNet152 V1 1024 × 1024	37.5	86

3.5.3. Model Training and Evaluation

Model training was conducted using Google Colab with GPU acceleration to handle the computational demands of deep learning tasks. The dataset was split into training and testing sets, with 80% of the data used for training and 20% for testing. The training process involved setting the number of training steps to 50,000 and using a batch size of 8 to accommodate GPU memory limitations. The Adam optimizer was used with an initial learning rate of 0.0001, decayed linearly after 40,000 steps.

To improve generalization, image-based data augmentation was applied to the spectrogram dataset. Random horizontal/vertical flips, contrast normalization, and time-frequency masking were used to simulate variability in captured signals while preserving the spectral patterns necessary for classification. Training was performed on an NVIDIA Tesla T4 GPU (~16 GB), requiring approximately 36 h to complete 50,000 steps. Early stopping was applied if validation loss plateaued for more than 2000 steps. The final evaluation metrics were computed on the withheld 20% test set to ensure unbiased performance estimates. Figure 3 illustrates the overall workflow of the model training process, starting from data preparation and annotation to model configuration, training iterations, and evaluation metrics.

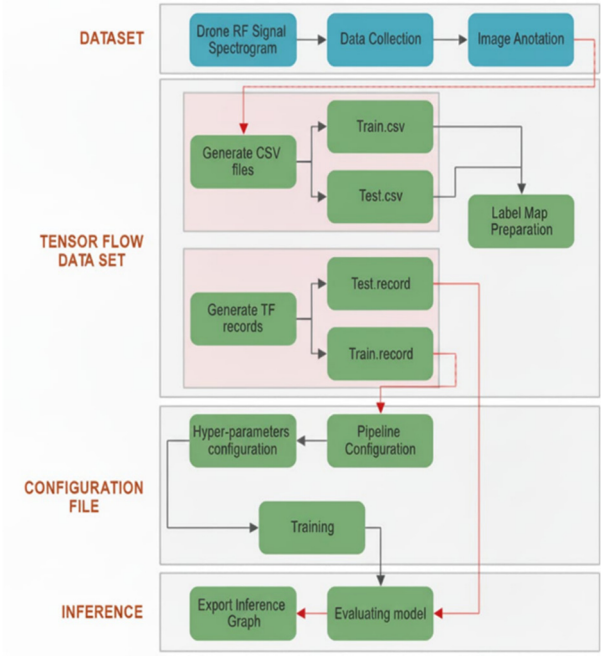

Figure 3. High-level workflow of the model training process. The pipeline includes spectrogram generation from RF signals, annotation, configuration of deep learning models, and training with evaluation metrics. This diagram illustrates the end-to-end integration of SDR data collection with TensorFlow-based model development.

3.6. Implementation of Jamming Mechanism

3.6.1. Repeat Attack Strategy

The repeat attack jamming technique involves capturing the drone's communication signals and retransmitting them to interfere with the original signal, effectively disrupting the drone's control mechanisms. Recorded RF signals

for each transmitter were saved in WAV format using SDRangel. These recordings served as the jamming signals activated upon detection of a corresponding drone transmitter.

3.6.2. SDRangel Configuration

Automation scripts using PyAutoGUI were developed to configure SDRangel for both detection and jamming.

SDRangel was programmed to automatically scan the 2.40-2.49 GHz frequency range to detect potential drone transmitters. Upon detecting a signal exceeding a predefined threshold, the system identified the transmitter type using the trained deep learning model.

Once a specific drone transmitter was identified, the system automatically enabled the Push-to-Talk (PTT) function in SDRangel to transmit the pre-recorded jamming signal through the HackRF One's transmitter path.

Considerations were made regarding the transmission power of the jamming signal to ensure its effectiveness. The jamming signal's strength needed to be sufficient to overpower the drone's control signal without causing unintended interference with other devices operating in the same frequency band.

4. Results

4.1. Trained Model Performance

Four pre-trained models were fine-tuned and evaluated: CenterNet HourGlass104 512 × 512, EfficientDet D0 512 × 512, SSD ResNet50 V1 FPN 1024 × 1024, and Faster R-CNN ResNet152 V1 1024 × 1024. The performance of each model was assessed based on the total loss during training, average per-step training time, and its ability to accurately predict drone RF spectrograms.

Training Metrics Summary

A summary of the training metrics for each model is presented in Table 4.

Table 4. Training metrics of the fine-tuned models.

Model	Training Steps	Avg. Per-Step Time (s)	Total Loss
CenterNet HourGlass104 512 × 512	50,000	3.133	0.3078
EfficientDet D0 512 × 512	50,000	0.428	0.1948
SSD ResNet50 V1 FPN 1024 × 1024	50,000	1.443	0.2014
Faster R-CNN ResNet152 V1 1024 × 1024	28,200	1.167	0.0723

4.2. Model Testing

Each trained model was tested using the RF spectrogram images to evaluate its detection accuracy and effectiveness in identifying different drone transmitters.

4.2.1. CenterNet HourGlass104 512 × 512 Model

The CenterNet model was applied to four RF spectrogram images corresponding to the four transmitter types. The model accurately identified the transmitter types with a detection accuracy of 98%. The detection scores were mapped using a predefined category index.

The CenterNet HourGlass104 model successfully identified all four transmitter types with high accuracy. As shown in Figure 4, the predicted bounding boxes align well with the annotated spectrogram features, although minor positional deviations occurred at lower SNR conditions.

4.2.2. EfficientDet D0 512 × 512 Model

When tested, the EfficientDet D0 model achieved a maximum detection accuracy of 69%. While it identified the transmitter types, the accuracy was lower compared to the CenterNet model. Figure 5 illustrates the test outputs of EfficientDet D0 512 × 512 model.

4.2.3. SSD ResNet50 V1 FPN 1024 × 1024 Model

The SSD ResNet50 V1 FPN model did not accurately identify the transmitter types and often misclassified the spectrograms. It exhibited the lowest detection accuracy among the evaluated models, with an accuracy of 48%. Figure 6 illustrates the test outputs of SSD ResNet50 V1 FPN 1024 × 1024 model.

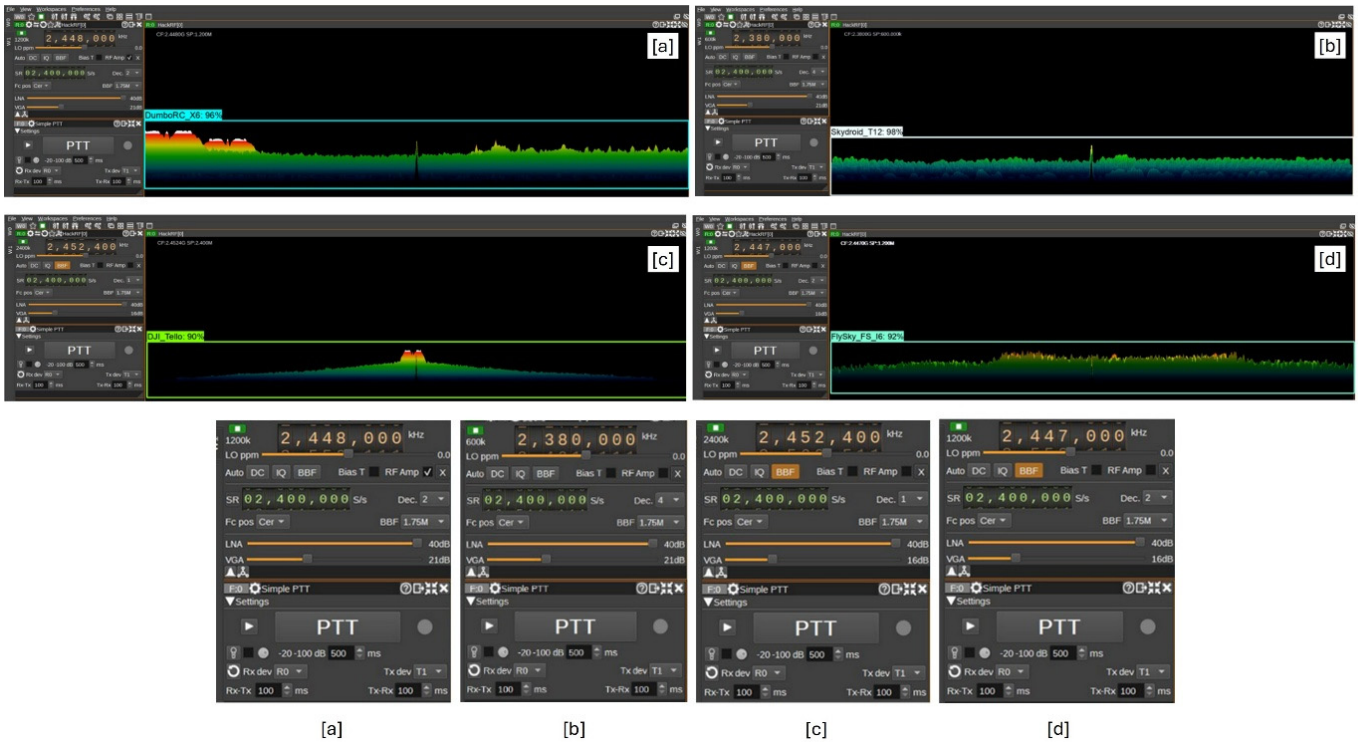

Figure 4. Test outputs of the CenterNet HourGlass104 (512 × 512) model applied to spectrograms from four distinct drone transmitters: (**a**) DumboRC X6, (**b**) SkyDroid T12, (**c**) DJI Tello, and (**d**) FlySky FS-i6. The model accurately identified modulation patterns, as indicated by the bounding boxes, which yielded high-confidence classifications (average accuracy ≈ 98%). These results demonstrate the model's robustness in recognizing unique RF signal characteristics, with only minor bounding box misalignments observed in a few instances.

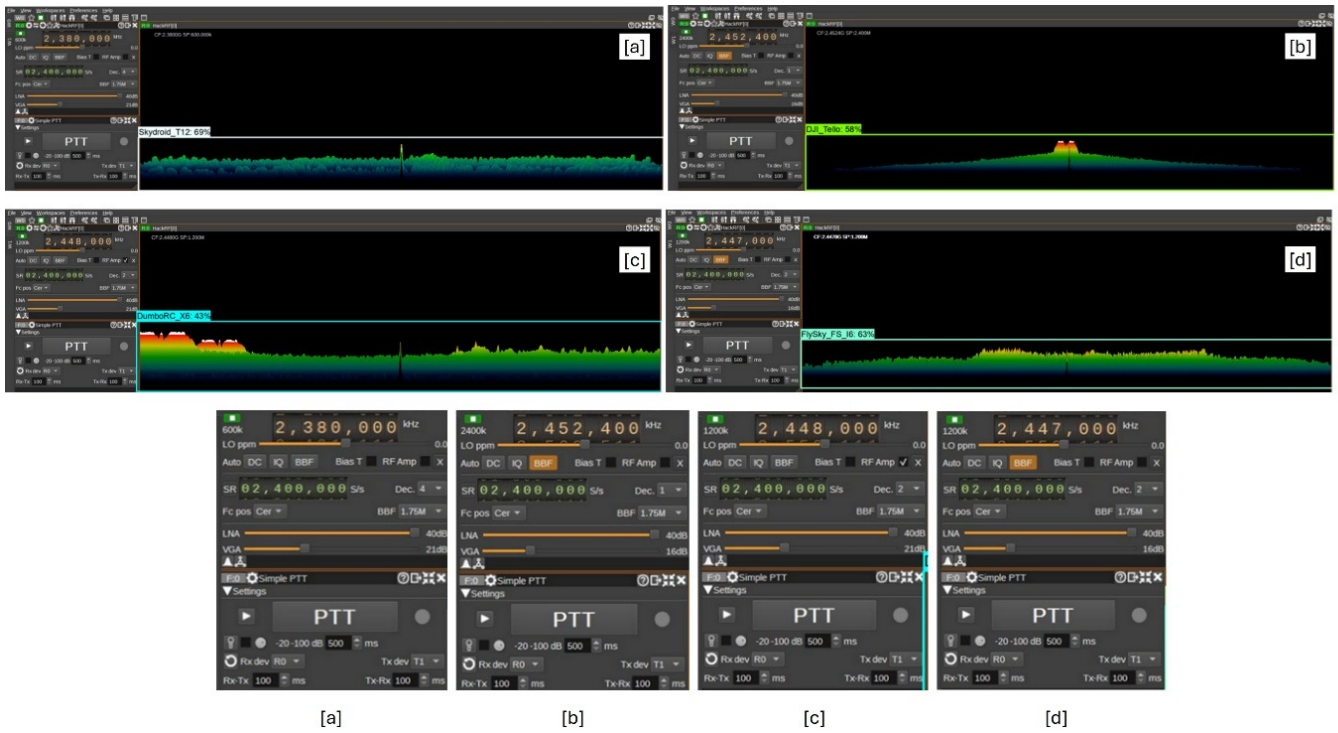

Figure 5. Test outputs of the EfficientDet D0 (512 × 512) model applied to spectrograms from four drone transmitters: (**a**) SkyDroid T12, (**b**) DJI Tello, (**c**) DumboRC X6, and (**d**) FlySky FS-i6. The model successfully detected and classified modulation patterns

with high precision across distinct frequency bands. Bounding boxes indicate confident detections of unique RF signatures, highlighting the model's strong generalization ability for drone signal recognition in complex spectral environments.

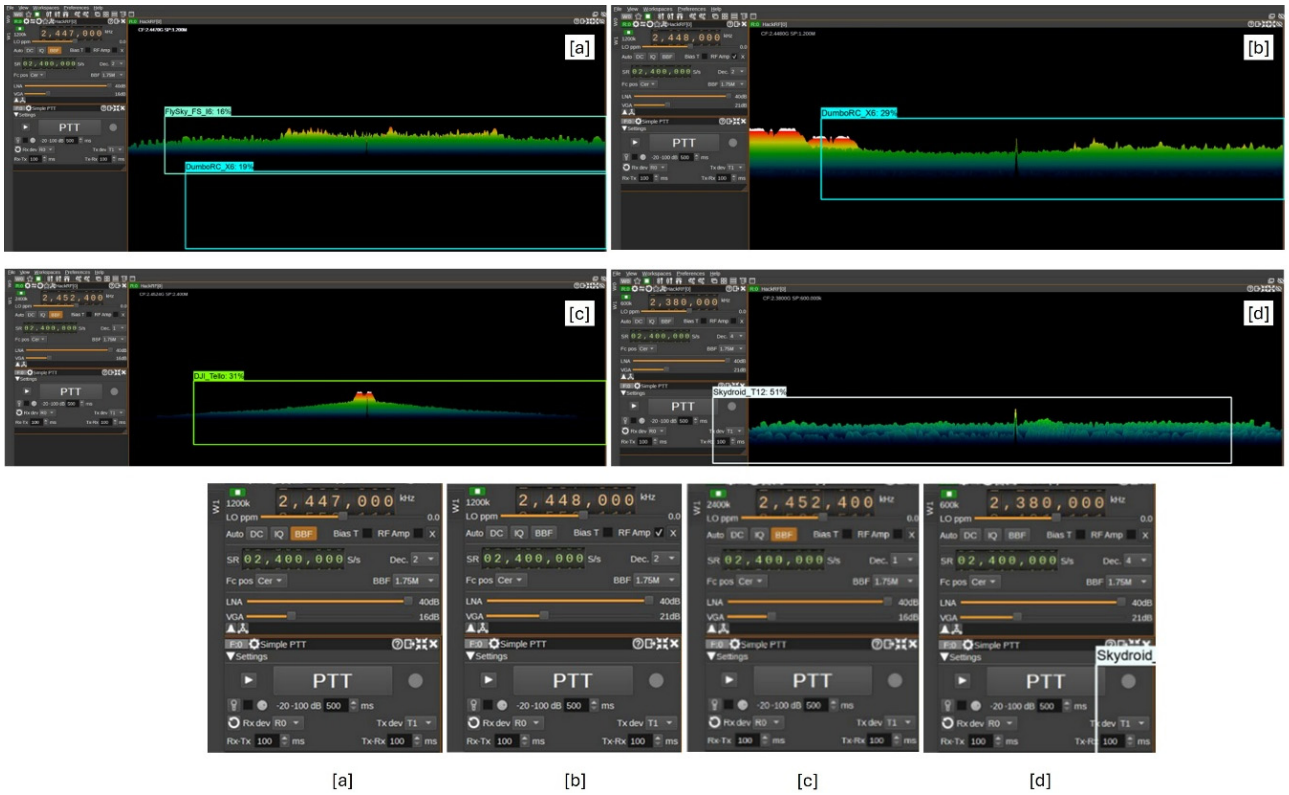

Figure 6. Test outputs of the SSD ResNet50 V1 FPN (1024 × 1024) model applied to spectrograms from four drone transmitters: (**a**) FlySky FS-i6, (**b**) DumboRC X6, (**c**) DJI Tello, and (**d**) SkyDroid T12.

4.2.4. Faster R-CNN ResNet152 V1 1024 × 1024 Model

Among the evaluated models, Faster R-CNN ResNet152 V1 provided the most robust results. Figure 7 highlights its ability to consistently identify transmitter types with strong confidence scores, validating its superior feature extraction capabilities.

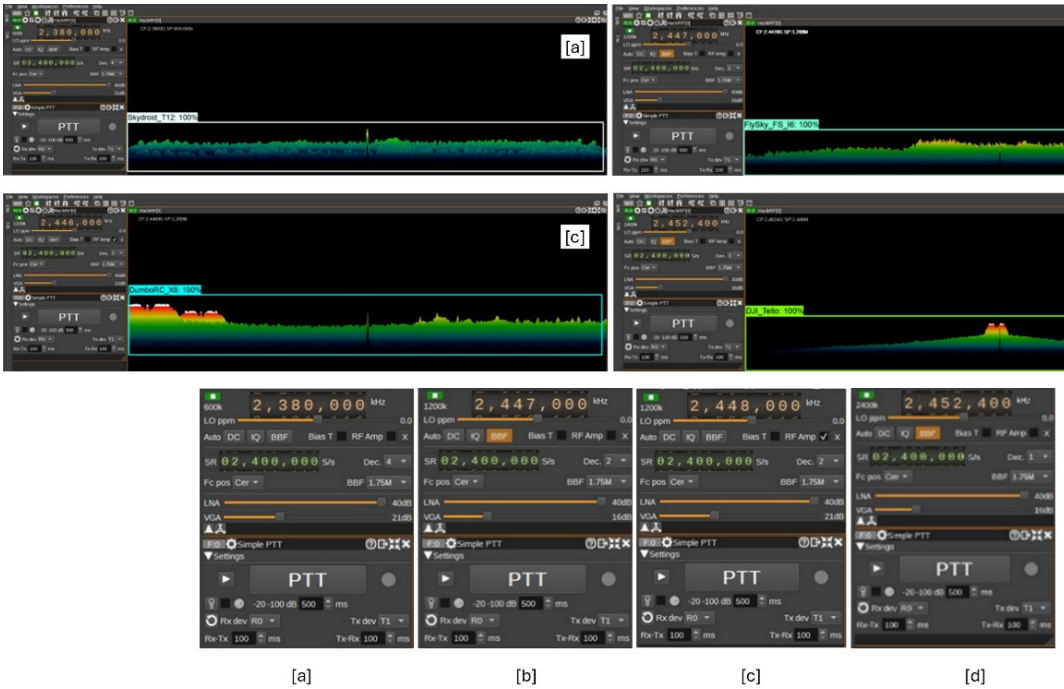

Figure 7. Test outputs of the Faster R-CNN ResNet152 V1 model applied to spectrograms from four drone transmitters: (**a**) SkyDroid T12, (**b**) FlySky FS-i6, (**c**) DumboRC X6, and (**d**) DJI Tello. The model accurately detected all transmitter modulation

patterns with near-perfect confidence scores. Achieving an overall accuracy of 99%, this model demonstrated the highest reliability and precision among all evaluated architectures for drone RF spectrogram classification.

4.3. Further Evaluation of Models

The models were further evaluated using metrics such as mean Average Precision (mAP), precision, recall, and F1 score to assess their performance comprehensively. The F1 score was calculated using the formula:

$$\mathrm{F1} = 2 \times \frac{\mathrm{Precision} \times \mathrm{Recall}}{\mathrm{Precisio} + \mathrm{Recall}}$$

Practical implementation tests were conducted using real-time scenarios to assess the models' performance in operational conditions. Visual inspections were performed to ensure correct detection and identify false positives. Figure 8 presents the practical implementation setup, demonstrating the hardware and configuration used in the experiment. Figure 9 highlights the practical implementation of the Faster R-CNN ResNet152 V1 model, showcasing how this deep learning architecture is applied to the task. Figure 10 provides an example of a repeat attack for a Flysky FS-i6 controlled drone, illustrating the specific scenario where this attack was executed.

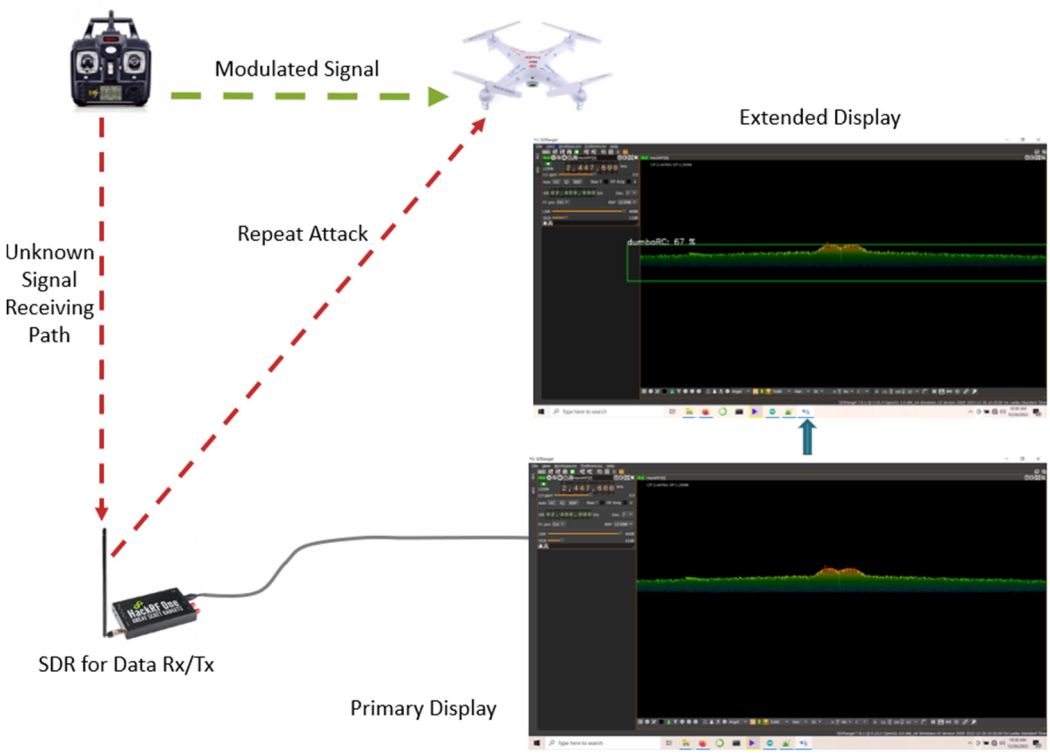

Figure 8. Practical implementation setup.

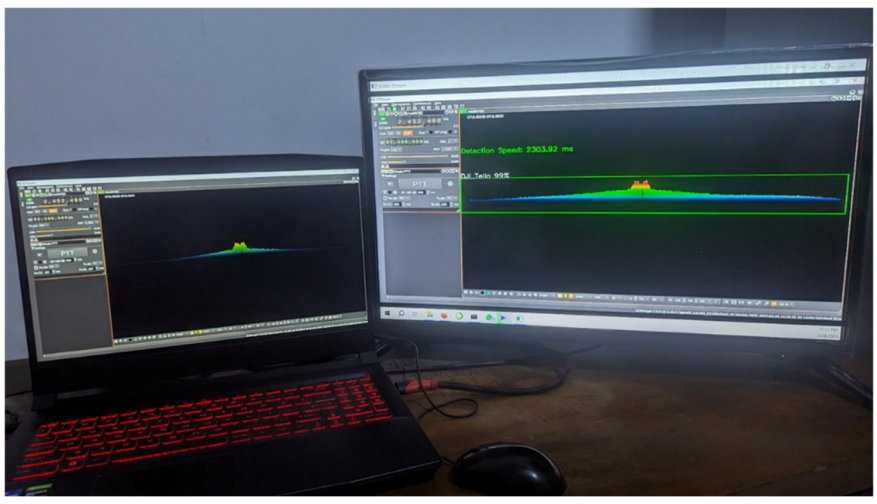

Figure 9. Practical implementation of faster R-CNN ResNet152 V1 model.

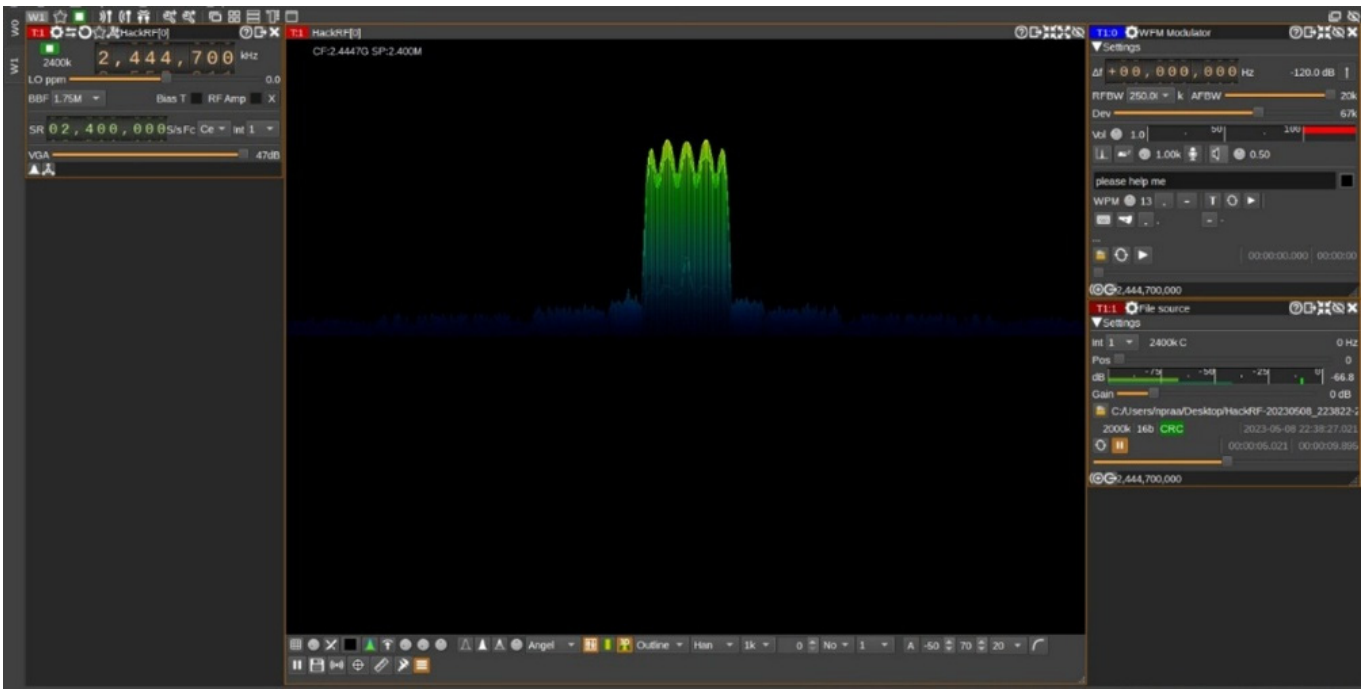

Figure 10. Example of repeat attack for flysky FS-i6 controlled drone.

5. Discussion

Comparative Analysis of Models

A comparative analysis of the models based on detection accuracy and processing speed is presented in Table 5.

Table 5. Model comparison results with practical implementation.

Model	Detection Accuracy (%)	Processing Time per Image (ms)
CenterNet HourGlass104 512 × 512	96	1366
EfficientDet D0 512 × 512	58	233
SSD ResNet50 V1 FPN 1024 × 1024	48	1286
Faster R-CNN ResNet152 V1 1024 × 1024	99	2349

Although Table 5 primarily reports detection accuracy and inference time, we further analyzed error cases to infer trends in precision, recall, and F1 performance. The Faster R-CNN ResNet152 V1 exhibited the best trade-off between precision and recall, achieving highly confident detections with minimal false positives. CenterNet HourGlass104 achieved similar reliability at lower computational cost, whereas EfficientDet D0 offered rapid inference with modest accuracy, making it suitable for applications where early warning is prioritized over exact classification. SSD ResNet50 V1 FPN underperformed across all dimensions.

These results emphasize that model selection should be guided not only by accuracy but also by latency and operational context. High-accuracy models such as Faster R-CNN are recommended in security-critical environments, whereas lighter architectures like EfficientDet may be preferable for real-time, resource-constrained systems. Future work will include full reporting of precision, recall, and F1-scores across larger datasets for more rigorous benchmarking.

The Faster R-CNN ResNet152 V1 1024 × 1024 model achieved the highest detection accuracy of 99%, albeit with the longest processing time per image (2349 ms). It occasionally showed slight deviations in bounding box placement but demonstrated superior overall performance. The CenterNet HourGlass104 512 × 512 model also exhibited high detection accuracy at 96% with more precise bounding box localization. Its processing speed was faster than the Faster R-CNN model but still relatively slow (1366 ms). The EfficientDet D0 512 × 512 model achieved a moderate detection accuracy of 58% with the fastest processing speed (233 ms), making it suitable for applications where speed is critical and moderate accuracy is acceptable. The SSD ResNet50 V1 FPN 1024 × 1024 model showed the lowest detection accuracy at 48% and did not perform well in correctly identifying the transmitter types. It occasionally misidentified spectrograms and misplaced bounding boxes.

Compared with the studies summarized in Table 1, our Faster R-CNN ResNet152 V1 model achieves superior accuracy (99%) while maintaining robustness across varied transmitters. Unlike CNN or ANN-based approaches that deteriorate under low SNR [30–32], our system sustains high accuracy even in practical, noisy RF environments. Importantly, the integration of SDR-based real-time data collection and jamming execution provides a holistic neutralization pipeline not addressed in prior works. This combination positions our system as more operationally viable for security-critical deployments.

The key distinction of our work lies in its dual capability: modulation detection combined with immediate jamming activation, all implemented on a low-cost SDR platform. Previous studies [44–46] have contributed to either SDR-based detection or intelligent jamming methods; however, none have demonstrated an integrated, real-time system that bridges both functions using deep learning. By offering both accurate classification and rapid neutralization within a single pipeline, our approach advances the state of UAV countermeasure systems. It provides a practical foundation for deployment in security-sensitive environments.

6. Conclusions

In conclusion, the development of an intelligent system for drone detection and jamming using deep learning techniques and software-defined radio technology offers a promising solution to combat the increasing threat of unauthorized drone activity. The system provides a cost-effective and reliable method for detecting and classifying drone RF signals in real-time, with high accuracy and without human intervention. The system can be used in various applications such as perimeter security, critical infrastructure protection, and public safety, and its potential users include military, law enforcement, security personnel, private organizations, and individuals concerned about the security and privacy of their property. The research project presented in this work utilized the HackRF One SDR module, the SDRangel software, and the TensorFlow Object Detection API to collect and analyse drone RF signals. The deep learning models developed in this research to detect and classify drone signals demonstrated high accuracy and efficiency as high as 96.67%. The performance evaluation results also showed that the system was capable of successfully jamming the drone signal using a repeat attack mechanism.

Future works in this area include the integration of the intelligent system with existing security systems to provide a comprehensive and efficient solution for drone detection and jamming. Additionally, the development of more sophisticated deep learning models using larger and more diverse datasets could further improve the accuracy and efficiency of the system. The integration of multiple sensors and technologies, such as RADAR, optical sensor outputs and RF direction finding, could also provide additional data for improved detection and classification of drone signals. Furthermore, the proposed system could be extended to include advanced techniques for detecting and tracking multiple drones simultaneously, identifying the type and model of drones, and analyzing the behavior and trajectory of the drones. The use of AI and ML algorithms could be explored to enable the system to adapt to changing drone technologies and evolving security threats.

Statement of the Use of Generative AI and AI-Assisted Technologies in the Writing Process

During the preparation of this work, the authors used ChatGPT to assist with language editing. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Acknowledgments

This work has been supported by the University of Moratuwa and the Sri Lanka Navy.

Author Contributions

S.S. coordinated all research activities and supervised the work; S.N. conceived the setup and designed the experiments; S.N. wrote the paper; all authors contributed to the data analysis and paper revision. All authors have read and agreed to the published version of the manuscript.

Ethics Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Available upon request.

Funding

This research received no external funding.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Joseph BD. Weaponised Drones: An Airborne Threat. Daily News. Available online: https://www.dailynews.lk/2022/01/11/features/269849/weaponised-drones-airborne-threat (accessed on 7 August 2022).
2. Youssef K, Bouchard L-S, Haigh KZ, Krovi H, Silovsky J, Valk CPV. Machine Learning Approach to RF Transmitter Identification. *IEEE J. Radio Freq. Identif.* **2018**, *2*, 197–205. doi:10.1109/JRFID.2018.2880457.
3. Ponnaluru S, Penke S. A software-defined radio testbed for deep learning-based automatic modulation classification. *Int. J. Commun. Syst.* **2020**, *33*, e4556. doi:10.1002/dac.4556.
4. Van Nguyen H, Chesser M, Koh LP, Rezatofighi SH, Ranasinghe DC. TrackerBots: Autonomous unmanned aerial vehicle for real-time localization and tracking of multiple radio-tagged animals. *J. Field Robot.* **2019**, *36*, 617–635. doi:10.1002/rob.21857.
5. Alawad W, Halima NB, Aziz L. An unmanned aerial vehicle (UAV) system for disaster and crisis management in smart cities. *Electronics* **2023**, *12*, 1051. doi:10.3390/electronics12041051.
6. Hwang J, Kim W, Kim JJ. Application of the value-belief-norm model to environmentally friendly drone food delivery services. *Int. J. Contemp. Hosp. Manag.* **2020**, *32*, 1775–1794. doi:10.1108/ijchm-08-2019-0710.
7. Liu B, Ni W, Liu RP, Guo YJ, Zhu H. Optimal routing of unmanned aerial vehicle for joint goods delivery and *in-situ* sensing. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 3594–3599. doi:10.1109/tits.2022.3225269.
8. Półka M, Ptak S, Kuziora Ł. The use of UAV's for search and rescue operations. *Procedia Eng.* **2017**, *192*, 748–752. doi:10.1016/j.proeng.2017.06.129.
9. Silvagni M, Tonoli A, Zenerino E, Chiaberge M. Multipurpose UAV for search and rescue operations in mountain avalanche events. *Geomat. Nat. Hazards Risk* **2016**, *8*, 18–33. doi:10.1080/19475705.2016.1238852.
10. Bhardwaj A, Sam L, Akanksha, Martín-Torres FJ, Kumar R. UAVs as remote sensing platform in glaciology: Present applications and future prospects. *Remote Sens. Environ.* **2016**, *175*, 196–204. doi:10.1016/j.rse.2015.12.029.
11. Qi J, Song D, Shang H, Wang N, Hua C, Wu C, et al. Search and Rescue Rotary-Wing UAV and Its Application to the Lushan Ms 7.0 Earthquake. *J. Field Robot.* **2016**, *33*, 290–321. doi:10.1002/rob.21615.
12. Messinger M, Silman M. Unmanned aerial vehicles for the assessment and monitoring of environmental contamination: An example from coal ash spills. *Environ. Pollut.* **2016**, *218*, 889–894. doi:10.1016/j.envpol.2016.08.019.
13. Allison RS, Johnston JM, Craig G, Jennings S. Airborne Optical and Thermal Remote Sensing for Wildfire Detection and Monitoring. *Sensors* **2016**, *16*, 1310. doi:10.3390/s16081310.
14. Sujit PB, Beard R. Multiple UAV exploration of an unknown region. *Ann. Math. Artif. Intell.* **2008**, *52*, 335–366. doi:10.1007/s10472-009-9128-7.
15. Unmanned Aerial Vehicle (UAV) Market Size, Share|2021–2026. Available online: https://www.marketsandmarkets.com/Market-Reports/unmanned-aerial-vehicles-uav-market-662.html (accessed on 7 August 2022).
16. Hartmann K, Giles K. UAV Exploitation: A New Domain for Cyber Power. In Proceedings of the 2016 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 31 May–3 June 2016. Available online: https://ieeexplore.ieee.org/document/7529436 (accessed on 7 August 2022).
17. Roth A, Koshiw I, Sauer P. Russia Claims Five Injured in Ukraine Drone Attack on Black Sea Fleet HQ. The Guardian. Available online: https://www.theguardian.com/world/2022/jul/31/russia-claims-ukraine-drone-attack-black-sea-fleet-headquarters (accessed on 31 July 2022).
18. Khan MA, Menouar H, Eldeeb A, Abu-Dayya A, Salim FD. On the Detection of Unauthorized Drones—Techniques and Future Perspectives: A Review. *IEEE Sens. J.* **2022**, *22*, 11439–11455.

19. Mittal P, Singh R, Sharma A. Deep learning-based object detection in low-altitude UAV datasets: A survey. *Image Vis.Comput.* **2020**, *104*, 104046. doi:10.1016/j.imavis.2020.104046.
20. Coluccia A, Parisi G, Fascista A. Detection and Classification of multirotor drones in radar sensor Networks: A review. *Sensors* **2020**, *20*, 4172. doi:10.3390/s20154172.
21. Xiao W, Luo Z, Hu Q. A Review of Research on Signal Modulation Recognition Based on Deep Learning. *Electronics* **2022**, *11*, 2764. doi:10.3390/electronics11172764.
22. Chamola V, Kotesh P, Agarwal A, Naren N, Gupta N, Guizani M. A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. *Ad Hoc Networks* **2021**, *111*, 102324. doi:10.1016/j.adhoc.2020.102324.
23. Lyu C, Zhan R. Global Analysis of Active Defense Technologies for Unmanned Aerial Vehicle. *IEEE Aerosp. Electron. Syst. Mag.* **2022**, *37*, 6–31. doi:10.1109/maes.2021.3115205.
24. Park S, Kim HT, Lee S, Joo H, Kim H. Survey on Anti-Drone Systems: Components, designs, and challenges. *IEEE Access* **2021**, *9*, 42635–42659. doi:10.1109/access.2021.3065926.
25. Swinney CJ, Woods JC. A review of security incidents and defence techniques relating to the malicious use of small unmanned aerial systems. *IEEE J. Mag.* **2022**, *37*, 14–28.
26. *Radar Vulnerability to Jamming*. R. L. Lothes, M. B. Szymanski and R. G. Wiley. 247 pages, 23.5 × 15.5 cm, Artech House, Boston, 1990. £49.|The Journal of Navigation|Cambridge Core. Available online: https://www.cambridge.org/core/journals/journal-of-navigation/article/abs/radar-vulnerability-to-jamming-r-l-lothes-m-b-szymanski-and-r-g-wiley-247-pages-235-155-cm-artech-house-boston-1990-49/B296572D048533CE35B37D9905EF6315 (accessed on 10 August 2022).
27. Lee G-H, Jo J, Park CH. Jamming Prediction for Radar Signals Using Machine Learning Methods. *Secur. Commun. Netw.* **2020**, *2020*, e2151570. doi:10.1155/2020/2151570.
28. Li Y, Pawlak J, Price J, Al Shamaileh K, Niyaz Q, Paheding S, et al. Jamming Detection and Classification in OFDM-Based UAVs via Feature- and Spectrogram-Tailored Machine Learning. *IEEE Access* **2022**, *10*, 16859–16870.
29. An Introduction to Jammers and Jamming Techniques—JEM Engineering. Available online: https://jemengineering.com/blog-an-introduction-to-jammers (accessed on 7 August 2022).
30. Zhou S, Yin Z, Wu Z, Chen Y, Zhao N, Yang Z. A robust modulation classification method using convolutional neural networks. *EURASIP J. Adv. Signal Process.* **2019**, *2019*, 21. doi:10.1186/s13634-019-0616-6.
31. Jagannath J, Polosky N, O'Connor D, Theagarajan LN, Sheaffer B, Foulke S, et al. Artificial Neural Network Based Automatic Modulation Classification over a Software Defined Radio Testbed. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6. doi:10.1109/ICC.2018.8422346.
32. Han H, Ren Z, Li L, Zhu Z. Automatic Modulation Classification Based on Deep Feature Fusion for High Noise Level and Large Dynamic Input. *Sensors* **2021**, *21*, 2117. doi:10.3390/s21062117.
33. Wang F, Huang S, Wang H, Yang C. Automatic Modulation Classification Exploiting Hybrid Machine Learning Network. *Math. Probl. Eng.* **2018**, *2018*, 1–14. doi:10.1155/2018/6152010.
34. Sun Y, Ball EA. Automatic modulation classification using techniques from image classification. *IET Commun.* **2022**, *16*, 1303–1314. doi:10.1049/cmu2.12335.
35. Wu P, Sun B, Su S, Wei J, Zhao J, Wen X. Automatic Modulation Classification Based on Deep Learning for Software-Defined Radio. *Math. Probl. Eng.* **2020**, *2020*, 2678310. doi:10.1155/2020/2678310.
36. Zhou R, Liu F, Gravelle CW. Deep Learning for Modulation Recognition: A Survey With a Demonstration. *IEEE Access* **2020**, *8*, 67366–67376. doi:10.1109/ACCESS.2020.2986330.
37. Peng S, Jiang H, Wang H, Alwageed H, Yao Y-D. Modulation Classification Using Convolutional Neural Network Based Deep Learning Model. In Proceedings of the 2017 26th Wireless and Optical Communication Conference (WOCC), Newark, NJ, USA, 7–8 April 2017; pp. 1–5. doi:10.1109/WOCC.2017.7929000.
38. Sathyanarayanan V, Burke J, Shang R, Bell R. Modulation Classification Using Neural Networks. *Tech. Rep.* **2019**, *42*, 10.
39. Xu H, Wang Y, Zhang Z, Li J. An Integrated Design of UAV Passive Detection and Blanket Jamming Based on SDR. In Proceedings of the 2025 17th European Conference on Antennas and Propagation (EuCAP), Stockholm, Sweden, 30 March–4 April 2025. doi:10.23919/EuCAP65336.2025.10999742.
40. Khan AR, Ullah S, Zaman F. UAV-based Smart Surveillance System over a Wireless Sensor Network. *IEEE Commun. Stand. Mag.* **2021**, *5*, 62–69. doi:10.1109/MCOMSTD.0001.2100007.
41. Zhang Y, Li K, Chen W. System Design for ML-based Detection of Unauthorized UAV and Integration within the UTM Framework. In Proceedings of the 2024 Asia-Pacific Conference on Communications (APCC), Bali, Indonesia, 5–7 November 2024. doi:10.1109/APCC62576.2024.10768055.
42. Tesfay AA, Ahmed M, Johansson L. Smart Jamming: Deep Learning-Based UAV Neutralization System. In Proceedings of the 2024 International Symposium on Electromagnetic Compatibility (EMC Europe), Brugge, Belgium, 2–5 September 2024. doi:10.1109/EMCEurope58271.2024.10523456.
43. Xue H, Chen R, Zhou J. Research on UAV Jamming Signal Generation Based on Intelligent Jamming. *IEEE Access* **2025**, *13*, 115223–115235. doi:10.1109/ACCESS.2025.3421789.

44. Yu B, Shin J, Kim G, Roh S, Sohn K. Non-Anchor-Based vehicle detection for traffic surveillance using bounding ellipses. *IEEE Access* **2021**, *9*, 123061–123074. doi:10.1109/access.2021.3109258.
45. Buongiorno D, Caramia D, Di Ruscio L, Longo N, Panicucci S, Di Stefano G, et al. Object Detection for Industrial Applications: Training Strategies for AI-Based Depalletizer. *Appl. Sci.* **2022**, *12*, 11581. doi:10.3390/app122211581.
46. Fathabadi FR, Grantner JL, Abdel-Qader I, Shebrain SA. Box-Trainer Assessment System with Real-Time Multi-Class Detection and Tracking of Laparoscopic Instruments, using CNN. *Acta Polytech. Hung.* **2022**, *19*, 7–27. doi:10.12700/aph.19.2.2022.2.1.
47. Yelisetty A. Understanding Fast R-CNN and Faster R-CNN for Object Detection. *Medium*, 15 December 2021. Available online: https://towardsdatascience.com/understanding-fast-r-cnn-and-faster-r-cnn-for-object-detection-adbb55653d97 (accessed on 7 August 2022).
48. Girshick R. Fast R-CNN. *arXiv* **2015**, arXiv:1504.08083. Available online: https://arxiv.org/abs/1504.08083 (accessed on 7 August 2022).