drones

Article

SSRL-UAVs: A Self-Supervised Deep Representation Learning Approach for GPS Spoofing Attack Detection in Small Unmanned Aerial Vehicles

Abed Alanazi

Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia; ad.alanazi@psau.edu.sa

Abstract: Self-Supervised Representation Learning (SSRL) has become a potent strategy for addressing the growing threat of Global Positioning System (GPS) spoofing to small Unmanned Aerial Vehicles (UAVs) by capturing more abstract and high-level contributing features. This study focuses on enhancing attack detection capabilities by incorporating SSRL techniques. An innovative hybrid architecture integrates Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) models to detect attacks on small UAVs alongside two additional architectures, LSTM-Recurrent Neural Network (RNN) and Deep Neural Network (DNN), for detecting GPS spoofing attacks. The proposed model leverages SSRL, autonomously extracting meaningful features without the need for many labelled instances. Key configurations include LSTM-GRU, with 64 neurons in the input and concatenate layers and 32 neurons in the second layer. Ablation analysis explores various parameter settings, with the model achieving an impressive 99.9% accuracy after 10 epoch iterations, effectively countering GPS spoofing attacks. To further enhance this approach, transfer learning techniques are also incorporated, which help to improve the adaptability and generalisation of the SSRL model. By saving and applying pre-trained weights to a new dataset, we leverage prior knowledge to improve performance. This integration of SSRL and transfer learning yields a validation accuracy of 79.0%, demonstrating enhanced generalisation to new data and reduced training time. The combined approach underscores the robustness and efficiency of GPS spoofing detection in UAVs.

Keywords: self-supervised representation learning (SSRL); unmanned aerial vehicles (UAVs); deep learning; spoofing attacks; global positioning systems (GPS); autonomous vehicles

Citation: Alanazi, A. SSRL-UAVs: A Self-Supervised Deep Representation Learning Approach for GPS Spoofing Attack Detection in Small Unmanned Aerial Vehicles. *Drones* **2024**, *8*, 515. https://doi.org/10.3390/drones8090515

Academic Editors: Liuguo Yin and Shu Fu

Received: 13 August 2024
Revised: 15 September 2024
Accepted: 20 September 2024
Published: 23 September 2024

1. Introduction

Self-Supervised Representation Learning (SSRL) represents a burgeoning paradigm in machine learning, wherein a model acquires meaningful representations from input data without explicit labels [1]. In small UAVs and GPS spoofing detection, this methodology empowers the model to discern intrinsic patterns and features within GPS signals, eliminating the need for labelled datasets during training [2]. This innovative approach shows promise in fortifying UAVs against GPS spoofing attacks by enabling models to independently learn pertinent features from raw GPS signals [3]. GPS spoofing attacks within small UAVs represent a considerable cybersecurity threat by manipulating the essential GPS signals vital for drone navigation [4]. Malicious actors seek to deceive a drone's GPS receiver by transmitting falsified signals that replicate authentic satellite data, giving rise to potential risks such as unauthorized access to restricted areas, compromise of sensitive mission data, and an elevated risk of collisions [5–7]. The ramifications of a successful GPS spoofing attack on a UAV encompass deviations from planned flight paths and erratic behaviour, compromising security and safety [8]. The purpose of GPS spoofing attacks on small UAVs lies in intentionally manipulating GPS signals to deceive the UAV's navigation system. Malicious actors undertake these attacks with various motives, including gaining unauthorized access to restricted areas, compromising sensitive mission data, or causing disruptions in UAV operations [9,10]. By sending falsified signals that mimic authentic satellite data, the attackers aim to mislead the drone about its location, speed, and altitude, potentially leading to deviations from planned flight paths and erratic behaviour [7,11]. The overarching goal is often to exploit vulnerabilities in the UAV's GPS, posing security and safety risks that can have far-reaching consequences.

The trajectory of GPS spoofing attacks on small UAVs can be traced back to the military origins of GPS technology, initially developed for defence purposes before transitioning into widespread civilian use [12]. As UAVs gained prominence across various sectors, their reliance on GPS for navigation rendered them susceptible to cyber threats. The concept of GPS spoofing, rooted in military strategies to disrupt navigation systems, expanded to encompass civilian applications, with adversaries recognizing the potential for unauthorized access, data compromise, and safety hazards [13,14]. This evolution prompted cybersecurity experts and researchers to delve into the vulnerabilities associated with GPS spoofing on UAVs, emphasizing the imperative for robust security measures [15,16]. The intersection of technology, cybersecurity, and discussions surrounding critical infrastructure further underscores the ongoing challenges in safeguarding UAVs, particularly as advancements in artificial intelligence and the Internet of Things (IoT) continue to shape the modern technological landscape [17,18].

GPS spoofing attacks can unfold in diverse scenarios, presenting distinct threats and consequences. For instance, a delivery drone system may be compromised as malicious actors manipulate GPS signals, causing the drone to deliver packages to unintended locations, potentially resulting in theft or unauthorized access to sensitive deliveries [19,20]. In the realm of surveillance, GPS spoofing could deceive drones monitoring critical infrastructure or borders, allowing illicit activities to go unnoticed. Agricultural drones, essential for precision farming, may experience crop monitoring and management disruptions due to GPS manipulation [21,22]. Emergency response drones guided by GPS could face misdirection during critical missions, potentially causing delays in aid delivery. The risk extends to scenarios involving drone swarms or autonomous vehicles, where GPS spoofing may lead to chaotic behaviour, collisions, or unauthorized entry into secure areas [23]. These scenarios underscore the diverse and complex risks associated with GPS spoofing on Small Unmanned Aerial Vehicles, underscoring the imperative for robust countermeasures and heightened cybersecurity protocols. Figure 1 depicts the UAV attack scenario.

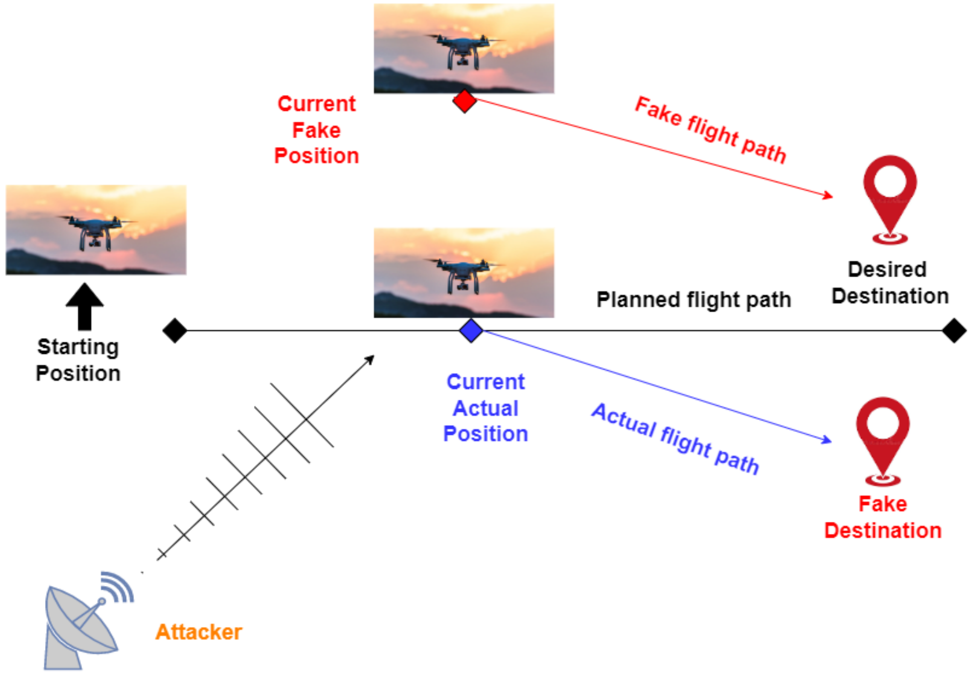


Figure 1. Small UAV's GPS spoofing attacks scenario.

Traditional localisation methods face limitations due to battery depletion and environmental electromagnetic fields. To overcome these, the work [24] proposes a deep learning-based OAM using You Only Look Once version 3 (YOLOv3) and a fiducial marker-based localisation method. These are integrated with real-time damage segmentation for an advanced UAV system. Tests in indoor and outdoor settings demonstrated the system's superior performance in obstacle avoidance and localisation compared to traditional approaches. Traditional modelling methods struggle with computing efficiency and accuracy. To enhance performance, a Cascade Ensemble Learning (CEL) method is proposed in [25], combining a Cascade Synchronous Strategy (CSS) and Wavelet Neural Network-based AdaBoost (WNN-Ada). The method is tested on a multi-level reliability evaluation of an aero-engine turbine rotor system. It shows significant improvements in computing accuracy and efficiency, highlighting its potential for reliably modelling complex systems.

1.1. Motivation

Incorporating SSRL is pivotal in empowering small UAVs—specifically those under 25 kg in weight—to learn and adapt dynamically to evolving threats, thereby mitigating the risks associated with GPS spoofing. This research addresses the immediate objective of enhancing the security and reliability of UAVs within this category and extends its impact on the broader landscape of autonomous systems. By demonstrating the practical application of self-supervised representation learning in real-world scenarios, our work establishes a pioneering pathway for integrating state-of-the-art machine learning techniques to tackle critical challenges faced by these UAVs. Our endeavour aims not only to secure small UAVs against GPS spoofing but also to establish a precedent for leveraging innovative technologies to fortify the resilience of autonomous systems across diverse domains. Through the integration of SSRL, our approach seeks to endow small UAVs with advanced adaptability and learning capabilities, reinforcing their resilience against GPS spoofing attacks. This research not only enhances the security and reliability of these UAVs in response to evolving threats but also makes a valuable contribution to the broader field of autonomous systems, showcasing the potential of self-supervised representation learning in real-world applications.

This study aims to detect and categorize GPS spoofing in UAVs. In the literature, numerous investigations have focused on utilizing deep learning models, including LSTM [26–28], GRU [26,29,30], RNN [31–33], and DNN [34–36], to detect GPS spoofing attacks. These models offer effective approaches for recognizing instances of GPS spoofing. Additionally, a pivotal aspect of this research involves a comprehensive exploration of the efficacy of LSTM, GRU, RNN, and DNN when integrated with transfer learning. This analysis evaluates how well these specific neural network architectures, renowned for their proficiency in pattern recognition and sequence modelling, perform when leveraging knowledge acquired from one task to improve performance on another related task. The study aims to comprehend the potential advantages and challenges associated with applying transfer learning to enhance these models' efficiency in detecting and classifying GPS spoofing attacks on UAVs.

1.2. Research Contributions

- Introduced a self-supervised hybrid deep learning architecture for GPS spoofing attack detection in small UAVs. This study employed three distinct model structures: LSTM-GRU, LSTM-RNN, and a DNN, each with specific neural network configurations.
- Integrated self-supervised learning into the training process, with models trained for 10 epochs and a batch size of 32 using training data, followed by validation on a separate dataset. This research also performed an ablation analysis to present a comprehensive evaluation of various parameter settings.
- The models, trained on different columns, including ch0_output, ch1_output, ch2_output, ch3_output, ch4_output, ch5_output, ch6_output, and ch7_output, exhibited varying levels of accuracy. The accuracy for ch5_output reached 99.9% across all models.

- Enhanced the self-supervised learning approach by incorporating transfer learning, allowing pre-trained weights to be applied to a new dataset. This technique improved the model's adaptability and generalisation, resulting in a validation accuracy of 79.0% while also reducing the training time required for new datasets.

1.3. Organisations

The remainder of the article follows this structure: Section 2 overviews current research on GPS-based spoofing attacks in small UAVs. Section 3 introduces the proposed deep learning methods for the detection and multi-label classification of GPS spoofing attacks in small UAVs. Section 4 presents the experimental analysis, results, and discussion. Finally, Section 5 concludes this paper and leads to future recommendations.

2. Literature Review

2.1. Deep Learning Approaches

We propose a novel GPS spoofing detection method tailored for small UAVs using a 1D CNN. Our contribution lies in addressing the critical security concern of GPS spoofing attacks on small UAVs. The proposed methodology involves data collection, preprocessing, feature extraction, and implementing a specialized 1D CNN architecture. The results of extensive experiments demonstrate the method's efficiency in accurately distinguishing between genuine and spoofed GPS signals. Evaluation metrics such as precision, recall, and F1 score attest to the robustness of the approach [37–39]. The research work in [40] introduces a pioneering solution for mitigating GPS signal spoofing in small UAVs by leveraging deep learning. The core contribution lies in developing a deep neural network architecture tailored to the resource constraints of small UAVs, enabling real-time detection of spoofed GPS signals. The methodology involves collecting and preprocessing real-world GPS data, training the neural network on labelled datasets, and optimizing the model for onboard deployment. Results indicate a high detection accuracy exceeding 90%, robustness across diverse environments, and real-time responsiveness. The research study in [12] introduces dynamic selection techniques for detecting GPS spoofing attacks on UAVs, contributing to a novel adaptive methodology framework. The framework incorporates advanced signal processing and machine learning algorithms, enabling real-time analysis and dynamic adjustment to evolving threat scenarios. Extensive experiments reveal a high detection accuracy, with the proposed system achieving an accuracy rate exceeding 95%, showcasing its effectiveness in minimizing false positives and adapting to changing environmental conditions. The study in [41] introduces a pioneering deep ensemble learning framework designed for the specific challenge of GPS spoofing detection in cellular-connected UAVs. The methodology involves collecting and preprocessing a comprehensive dataset, utilizing a diverse set of deep learning models, including CNNs, RNNs, and LSTM networks. The ensemble of these models is trained and validated to form a robust system capable of accurately distinguishing genuine from spoofed GPS signals. The results exhibit a notable accuracy of 97%, surpassing conventional single-model approaches and affirming the efficacy of the proposed approach in fortifying cellular-connected UAVs against GPS spoofing attacks. The work in [42,43] addresses two key challenges in cognitive radio and signal detection: automatic modulation classification (AMC) and unauthorized broadcasting identification. For AMC, a real-time solution is proposed using the lightweight neural network MobileViT, driven by clustered constellation images transformed from I/Q sequences. MobileViT, evaluated on the RadioML 2016.10a dataset with edge computing, demonstrates robust performance, marking the first deep learning-based real-time modulation classification at the edge. For unauthorized broadcasting detection, the manifold regularisation-based deep convolutional autoencoder (MR-DCAE) is introduced. Using reconstruction errors and a similarity estimator for manifold consistency, MR-DCAE accurately identifies unauthorized signals, achieving state-of-the-art results on the AUBI2020 dataset. Both methods highlight the potential of deep learning in real-time signal classification and detection.

2.2. Adaptive Methodologies and Frameworks

The research in [44] contributes to UAV security by presenting a comprehensive taxonomy of GPS spoofing and jamming attack detection methods and proposing a novel methodology framework for their evaluation. The taxonomy systematically categorizes existing detection methods, offering a structured overview for the UAV security community. The proposed methodology framework includes key performance metrics, experimental setups, and validation criteria, providing a standardized approach for comparing the effectiveness of different detection approaches. Preliminary results demonstrate promising accuracy levels ranging from 85% to 95%, affirming the efficacy of tested methods. The research in [45,46] contributes to UAV security by proposing a methodology for evaluating weak and strong learners in detecting GPS spoofing attacks. The framework involves dataset collection, feature extraction, and implementation of both weak and strong learners. Weak learners, including decision trees and k-nearest neighbours, are contrasted with strong learners, like ensemble methods and neural networks. This research introduces a novel contribution focused on enhancing GPS spoofing detection for UAVs.

2.3. Advanced Techniques and Integration

The research in [47,48] focuses on advancing construction vehicle detection by combining Self-Supervised Learning (SSL) with the YOLOv4 network. The methodology involves initial SSL pre-training on a diverse dataset, allowing the model to learn representations in an unsupervised manner. This dual approach enhances the model's adaptability to varied construction site conditions. The dataset likely comprises annotated images and videos with diverse scenarios. The results demonstrate improved accuracy, speed, and generalisation compared to conventional methods. The research in [49] introduces a methodology using linear regression to detect GPS spoofing attacks on UAVs. The study employs a simulated and real-world GPS data dataset to train and evaluate the linear regression model. The approach demonstrates promising results, accurately identifying anomalies in GPS signals indicative of spoofing incidents. The research in [50] introduces a groundbreaking MAE-based self-supervised anomaly detection and localisation method. The methodology utilizes mean absolute error as a pivotal metric for autonomously identifying deviations in unlabeled data. The study employs a diverse dataset to train and evaluate the model, demonstrating its superior accuracy and efficiency in detecting and localizing anomalies. The results indicate the method's effectiveness, outperforming existing approaches and offering valuable insights into interpretability. The proposed methodology in [51] integrates a dynamic selection module into the UAV's navigation system, leveraging machine learning for the real-time evaluation of GPS signals. This module adapts to changing environmental conditions and potential spoofing attempts, utilizing feature extraction, advanced signal processing, and a continually learning machine learning model. Evaluation through simulations and real-world experiments demonstrates a substantial improvement in accuracy, with the dynamic selection framework achieving a 99.6% accuracy rate in simulated scenarios.

The existing research on GPS spoofing detection for small UAVs has significantly advanced the field by tackling essential security challenges. Researchers have employed deep learning techniques like CNNs, RNNs, and LSTMs to achieve accurate detection while also incorporating real-time analysis and dynamic adaptation to enhance system robustness. Ensemble learning strategies, which combine diverse models, have further improved detection accuracy. Additionally, standardized evaluation frameworks and taxonomies have established crucial benchmarks for comparison and future studies. Despite these advancements, several challenges remain. These include resource limitations for small UAVs, restricted data availability for training, issues with false positives and environmental adaptability, and concerns about the complexity and interpretability of deep learning models. Furthermore, many studies tend to focus on specific UAV scenarios, which limits the generalizability of their findings. The typical workflow involves data collection, preprocessing, feature extraction, deep learning model training, and deployment with real-time adaptation. This research stands out by introducing a specialized 1D CNN architecture specifically designed for GPS spoofing detection in small UAVs. This approach builds on the strengths of existing studies, integrating deep learning with advanced preprocessing and feature extraction techniques. By doing so, this work pushes the boundaries of UAV security, offering a novel solution to the ongoing challenges in this field.

3. Proposed Methodology

This paper focuses on improving the security and reliability of UAVs, with broader implications for the field of autonomous systems. Figure 2 illustrates the complete workflow of the proposed approach. In this study, we utilized the GPS Spoofing Detection on Autonomous Vehicles dataset from IEEE DataPort [https://ieee-dataport.org/documents/dataset-gps-spoofing-detection-autonomous-vehicles] (accessed on 22 Febraury 2024), which offers a detailed dataset for analyzing GPS spoofing attacks on small UAVs. After extraction, the dataset comprises three key files: GPS_Data_Simplified_2D_Feature_Map, GPS_Dataset_3D_8_Channels, and GPS_Raw. We primarily used the second file, GPS_Dataset_3D_8_Channels, which consists of 510,530 samples and 14 features, to train three different neural network architectures: LSTM-GRU, LSTM-RNN, and DNN, within a self-supervised hybrid deep learning framework to detect GPS spoofing attacks. Furthermore, we enhanced the self-supervised learning process by applying transfer learning using the GPS_Data_Simplified_2D_Feature_Map file, which consists of 156,996 samples and 112 features, improving the models' generalisation and adaptability. The methodology begins with compiling a diverse dataset of GPS signals from small UAVs, providing a comprehensive understanding of GPS signal characteristics. By demonstrating the practical application of self-supervised representation learning in real-world scenarios, our work establishes a pioneering pathway for integrating state-of-the-art machine learning techniques to tackle critical challenges that autonomous systems face. Our endeavour not only aims to secure UAVs against GPS spoofing but also establishes a precedent for leveraging innovative technologies to enhance the resilience of autonomous systems across diverse domains. This paper presents a novel SSRL architecture to address the growing threat of GPS spoofing to small UAVs. The study focuses on improving attack detection capabilities by incorporating SSRL techniques. A hybrid deep learning architecture integrates the LSTM and GRU models to detect attacks on small UAVs. Additionally, two other architectures were developed: an LSTM-RNN and a Deep Neural Network (DNN) for real-time classification of GPS spoofing attacks. The proposed model leverages SSRL to extract meaningful features with minimal reliance on labelled data autonomously. Building on this, we further enhanced the model's performance by incorporating transfer learning. By applying pre-trained weights to the GPS_simplified_2d_feature_map dataset, the model demonstrated improved generalisation and adaptability, achieving a validation accuracy of 79.0%. This integration of self-supervised learning and transfer learning reinforces the model's robustness and efficiency, reducing the training time required for new datasets and solidifying its effectiveness in detecting GPS spoofing attacks on UAVs.

Algorithm 1 presents the overall data flow and working of the proposed approach for SSRL-based GPS spoofing attack detection and multi-classification. The initial step involves data preparation, where the target variables, namely "y_train" and "y_test", are transformed into one-hot encoding to facilitate multiclass classification. The input features, denoted as "X_train" and "X_test", undergo min–max scaling for normalisation. The architecture of the deep learning models incorporates an LSTM-GRU with specific parameters: 64 neurons in the input layer for both LSTM-GRU 1 layer, concatenation of both layers, 32 neurons in the concatenate layer for both LSTM-GRU 2 layers, 16 neurons in the fully connected layer, and flattening and concatenation of the output layer. Furthermore, an LSTM-RNN is employed with distinct settings, utilizing 128 neurons in the input layer for both LSTM-RNN 1 layer, concatenating both layers, 64 neurons in the concatenate layer for both LSTM-RNN 2 layers, 32 neurons in the fulsationonnected layer, and flattening and concatenating the output layer. Additionally, a DNN with specific architecture parameters, including 128 neurons in the input layer for both 1 and 2, concatenating both layers, 64 neurons in the concatenate layer for 3 and 4, 32 neurons in the fully connected layer, and flattening and concatenating the output layer, is utilized. Accuracy is employed as the metric to assess the proposed architecture, undergoing 10 training epochs with a batch size of 32 on the training data. Performance evaluation is conducted on a separate test set, spanning various labels, revealing that the proposed architecture achieves the highest accuracy, thereby emphasizing its effectiveness in mitigating GPS spoofing threats in UAVs.

Algorithm 1 Pseudocode of SSRL-based overall deep learning-based workflow for GPS spoofing attacks detection and multi-classification.

```
Input: GPS Spoofing Attacks Data from small UAVs
Output: Attacks
Evaluation Measure: Accuracy, Precision, Recall, F1-Score, ROC
$D_p \leftarrow$ Data preprocessing(data)
$L_e \leftarrow$ Label Encoding$(D_p)$
$N_{data} \leftarrow$ Scaler= StandardScaler$(L_e)$
X,Y $\leftarrow N_{data}$
Initialize the following variables and parameters
X_train,X_test,y_train,y_test = train_test_split(X,y, test_size=30, random_state=0)
Reshape X_train and X_test into X_train_3d and X_test_3d
Model 1: LSTM-GRU
    Multi-layer representation layers
    Concatenate layer
    Fully connected layer
    Flatten layer
    Transfer layer
    Output layer
Model 2: LSTM-RNN
    Multi-layer representation layers
    Concatenate layer
    Fully connected layer
    Flatten layer
    Transfer layer
    Output layer
Model 3: DNN
    Multi-layer representation layers
    Concatenate layer
    Fully connected layer
    Flatten layer
    Transfer layer
    Output layer
    Output layer
Model 4: Pre-trained Model
    Multi-layer representation layers
    Concatenate layer
    Fully connected layer
    Flatten layer
    Pre-trained weights applied from the SSRL model
    Transfer layer
    Output layer
Print Accuracy, loss, Confusion Matrix, ROC Curves
```

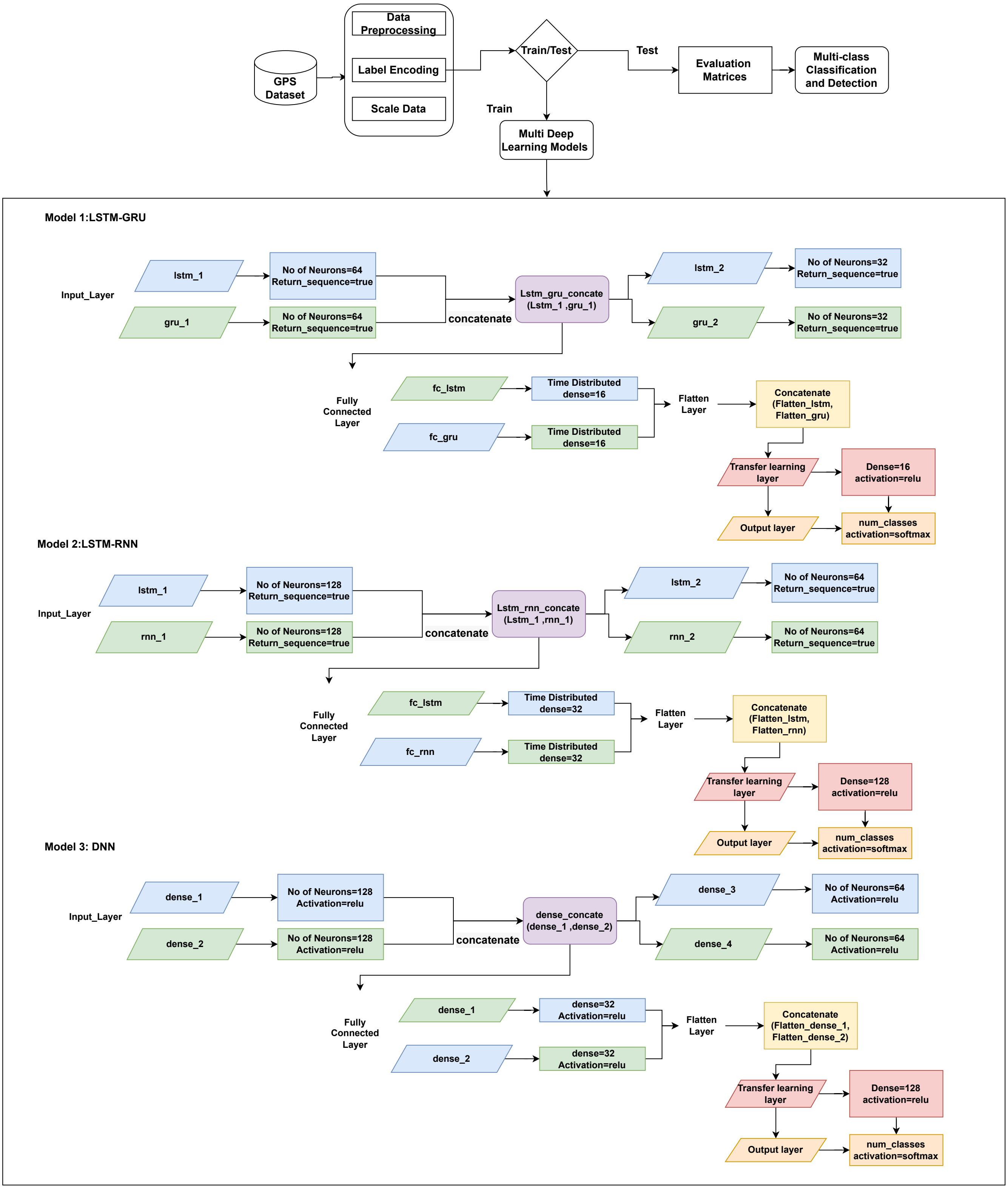

GPS Dataset
Data Preprocessing
Label Encoding
Scale Data
Train/Test
Test
Train
Evaluation Matrices
Multi-class Classification and Detection
Multi Deep Learning Models
Model 1:LSTM-GRU
Input_Layer
lstm_1
gru_1
No of Neurons=64 Return_sequence=true
No of Neurons=64 Return_sequence=true
concatenate
Lstm_gru_concate (Lstm_1 ,gru_1)
lstm_2
gru_2
No of Neurons=32 Return_sequence=true
No of Neurons=32 Return_sequence=true
Fully Connected Layer
fc_lstm
fc_gru
Time Distributed dense=16
Time Distributed dense=16
Flatten Layer
Concatenate (Flatten_lstm, Flatten_gru)
Transfer learning layer
Dense=16 activation=relu
Output layer
num_classes activation=softmax
Model 2:LSTM-RNN
Input_Layer
lstm_1
rnn_1
No of Neurons=128 Return_sequence=true
No of Neurons=128 Return_sequence=true
concatenate
Lstm_rnn_concate (Lstm_1 ,rnn_1)
lstm_2
rnn_2
No of Neurons=64 Return_sequence=true
No of Neurons=64 Return_sequence=true
Fully Connected Layer
fc_lstm
fc_rnn
Time Distributed dense=32
Time Distributed dense=32
Flatten Layer
Concatenate (Flatten_lstm, Flatten_rnn)
Transfer learning layer
Dense=128 activation=relu
Output layer
num_classes activation=softmax
Model 3: DNN
Input_Layer
dense_1
dense_2
No of Neurons=128 Activation=relu
No of Neurons=128 Activation=relu
concatenate
dense_concate (dense_1 ,dense_2)
dense_3
dense_4
No of Neurons=64 Activation=relu
No of Neurons=64 Activation=relu
Fully Connected Layer
dense_1
dense_2
dense=32 Activation=relu
dense=32 Activation=relu
Flatten Layer
Concatenate (Flatten_dense_1, Flatten_dense_2)
Transfer learning layer
Dense=128 activation=relu
Output layer
num_classes activation=softmax

Figure 2. Proposed methodology.

4. Experimental Results and Discussion

This study utilized specific tools and technologies to conduct research in the field of GPS spoofing detection, employing Python 3.8.8, a widely used and efficient programming language for machine learning. The experimental setup also incorporated an Nvidia 1060 graphics processing unit (GPU), which facilitated fast and efficient parallel processing, significantly speeding up the training and evaluation of the deep learning models. Table 1 provides a summary of the hyperparameters used for the Self-Supervised Representation Learning (SSRL)-based GPS spoofing detection models. These configurations, combined with the powerful processing capabilities of the Nvidia GPU, contributed to the superior performance and accuracy of the proposed models. The strategic selection of hyperparameters, as shown in Table 1, ensured optimal training conditions and enhanced the overall effectiveness of the architecture in detecting GPS spoofing attacks.

Table 1. Summary of hyperparameters for SSRL-based GPS spoofing detection models.

Model	**Layer**	**Number of Neurons**
LSTM-GRU	Input Layer	64
	Concatenate Layer 1	64
	Concatenate Layer 2	32
	Fully Connected Layer	16
LSTM-RNN.	Input Layer	128
	Concatenate Layer 1	128
	Concatenate Layer 2	64
	Fully Connected Layer	32
DNN	Input Layer 1 and 2	128
	Concatenate Layer 3 and 4	64
	Fully Connected Layer	32
Training	Epochs	10
	Batch Size	32
Evaluation	Metric	Accuracy
Loss Function	Optimizer	Adam
	Loss	Sparse_categorical_crossentropy
	Learning Rate	0.001

4.1. SSRL-Based LSTM-GRU Results

The performance of the LSTM-GRU model is shown in Table 2. The output labels, represented by their respective abbreviations, exhibit accuracy values ranging from 0.93 to 1.00 across various models. Specifically, ch0_output and ch1_output both achieve an accuracy of 0.95, ch2_output records an accuracy of 0.98, and ch3_output attains an accuracy of 0.97. Additionally, ch4_output reaches an accuracy of 0.98, ch5_output achieves a perfect score of 1.00, and ch6_output registers an accuracy of 0.99. Notably, ch7_output stands out with an accuracy of 0.9. Notably, among the LSTM-GRU model outputs, ch5_output exhibits the highest accuracy of 1.00.

Table 2. SSRL-based LSTM-GRU results.

Label	**Precision**	**Recall**	**F1-Score**	**Accuracy**
		Ch0_output Multi-label Classification		
Class 0	0.99	0.97	0.98	0.95
Class 1	0.47	0.09	0.16	0.94
Class 2	0.70	0.96	0.81	0.94
Class 3	1.00	b1.00	1.00	0.95

Table 2. *Cont.*

Label	Precision	Recall	F1-Score	Accuracy
		Ch1_output Multi-label Classification		
Class 0	0.99	0.98	0.98	0.97
Class 1	1.00	0.35	0.52	0.93
Class 2	0.68	0.97	0.80	0.95
Class 3	0.99	0.75	0.85	0.95
		Ch2_output Multi-label Classification		
Class 0	1.00	0.98	0.99	0.99
Class 1	0.67	1.00	0.80	0.98
		Ch3_output Multi-label Classification		
Class 0	1.00	0.99	1.00	1.00
Class 1	0.76	0.98	0.86	0.95
Class 2	0.99	0.54	0.69	0.97
Class 3	0.49	1.00	0.65	0.98
		Ch4_output Multi-label Classification		
Class 0	0.98	1.00	0.99	0.99
Class 1	0.98	1.00	0.99	0.99
Class 2	1.00	0.59	0.74	0.98
Class 3	1.00	0.98	0.99	0.98
		Ch5_output Multi-label Classification		
Class 0	1.00	1.00	1.00	0.99
Class 1	1.00	0.91	0.95	1.00
Class 2	1.00	0.99	1.00	1.00
		Ch6_output Multi-label Classification		
Class 0	1.00	0.99	1.00	1.00
Class 1	1.00	0.98	0.99	0.99
Class 2	0.92	0.98	0.95	0.99
		Ch7_output Multi-label Classification		
Class 0	0.93	1.00	0.96	0.95
Class 1	0.96	0.17	0.30	0.93
Class 2	0.37	0.02	0.03	0.94
Class 3	0.99	0.99	0.99	0.92

4.2. SSRL-Based LSTM-RNN Results

Table 3 demonstrates the classification performance of the LSTM-RNN model, assessed using the evaluation metrics. Accuracy values range from 0.93 to 1.00 across different models. Specifically, ch0_output and ch1_output both achieve an accuracy of 0.95, ch2_output records an accuracy of 0.98, and ch3_output attains an accuracy of 0.97. Additionally, ch4_output reaches an accuracy of 0.98, ch5_output achieves a perfect score of 1.00, and ch6_output attains an accuracy of 0.99. Notably, ch7_output registers an accuracy of 0.9. Notably, among the LSTM-RNN model outputs, ch5_output stands out with the highest accuracy of 1.00.

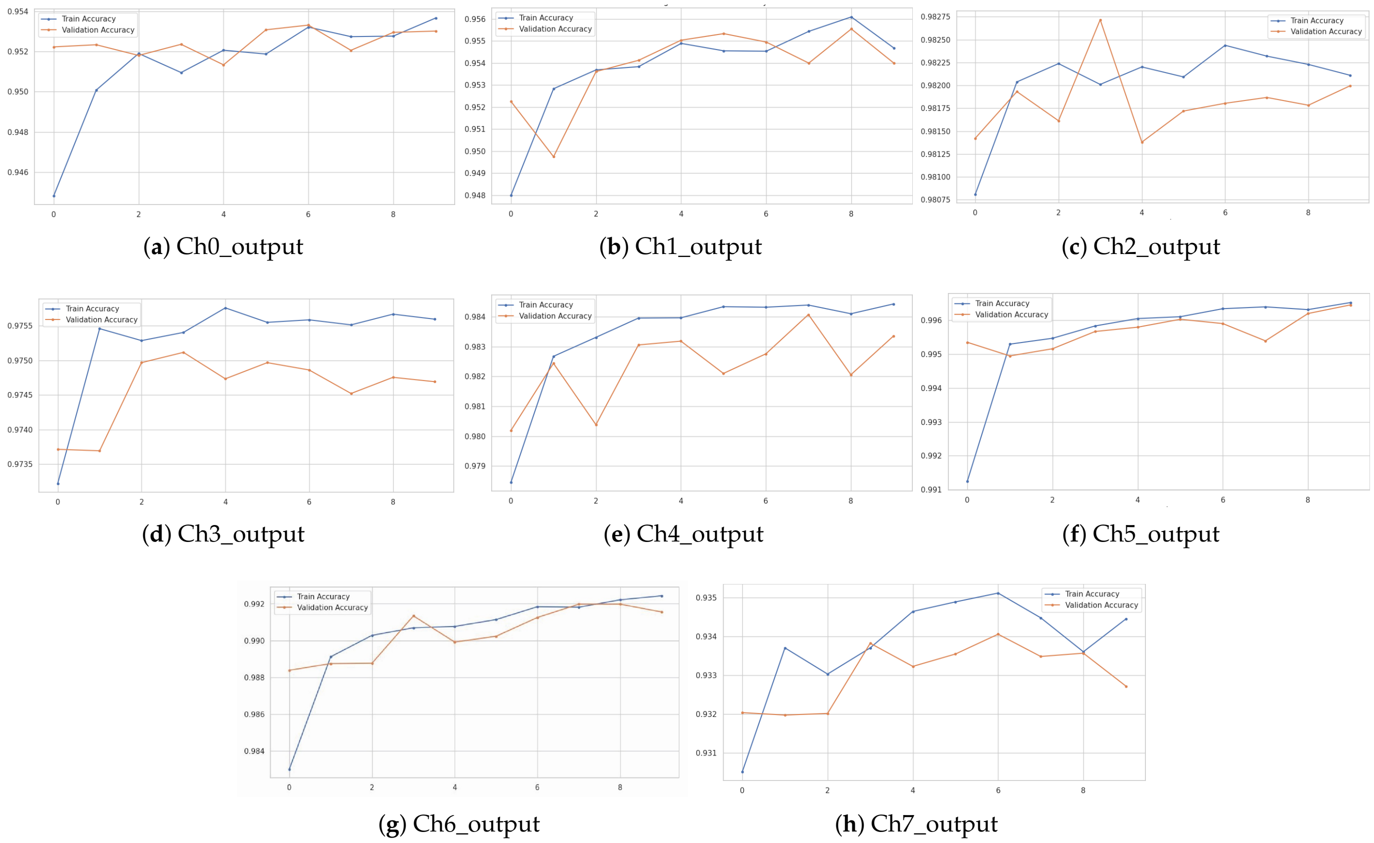
Table 3. SSRL-based LSTM-RNN results.

Label	Precision	Recall	F1-Score	Accuracy
		Ch0_output Multi-label Classification		
Class 0	0.96	1.00	0.98	0.95
Class 1	0.44	0.56	0.50	0.95
Class 2	0.94	0.58	0.71	0.94
Class 3	0.99	1.00	0.99	0.94
		Ch1_output Multi-label Classification		
Class 0	0.98	0.99	0.98	0.95
Class 1	1.00	0.35	0.52	0.97
Class 2	0.76	0.78	0.77	0.93
Class 3	0.78	0.97	0.87	0.93
		Ch2_output Multi-label Classification		
Class 0	0.98	1.00	0.99	0.99
Class 1	1.00	0.55	0.71	0.98
		Ch3_output Multi-label Classification		
Class 0	1.00	0.99	1.00	0.97
Class 1	1.00	0.68	0.81	0.98
Class 2	0.68	1.00	0.81	1.00
Class 3	0.49	1.00	0.66	0.93
		Ch4_output Multi-label Classification		
Class 0	0.98	1.00	0.99	0.98
Class 1	0.98	1.00	0.99	0.98
Class 2	1.00	0.56	0.72	0.99
Class 3	1.00	0.97	0.98	0.99
		Ch5_output Multi-label Classification		
Class 0	1.00	1.00	1.00	1.00
Class 1	0.95	0.94	0.95	0.99
Class 2	0.98	1.00	0.99	1.00
		Ch6_output Multi-label Classification		
Class 0	0.99	1.00	0.99	1.00
Class 1	1.00	0.91	0.95	1.00
Class 2	0.99	0.91	0.95	0.99
		Ch7_output Multi-label Classification		
Class 0	0.93	1.00	0.96	0.94
Class 1	1.00	0.17	0.29	0.92
Class 2	1.00	0.00	0.00	0.95
Class 3	1.00	0.98	0.99	0.93

4.3. SSRL-Based Deep Neural Network Results

Table 4 demonstrates the classification performance of the straightforward DNN model, assessed using the Accuracy metric. The output labels under evaluation are represented by their corresponding abbreviations. Across various models, accuracy values vary from 0.93 to 1.00. Specifically, the label ch0_output achieves an accuracy of 0.95, ch1_output also attains an accuracy of 0.95, ch2_output records an accuracy of 0.98, and ch3_output achieves an accuracy of 0.97. Additionally, ch4_output attains an accuracy of 0.93, ch5_output reaches a perfect accuracy of 1.00, and ch6_output achieves an accuracy of 0.99. Notably, ch7_output registers an accuracy of 0.93. Notably, among the DNN model outputs, ch5_output stands out with the highest accuracy of around 1.00.

In Figure 3, it can be observed the training and validation accuracy for the LSTM-GRU model. The x-axis corresponds to the number of epochs, while the y-axis represents accuracy. The orange line signifies validation accuracy, and the blue line denotes training accuracy for labels ch0_output, ch1_output, ch3_output, ch5_output, and ch6_output. The patterns for these labels exhibit relatively consistent behaviour between training and validation. For the ch1_output label, the pattern remains consistent between training and validation, with occasional fluctuations occurring between 6 to 8 epochs. In the case of the ch2_output label, the pattern lacks consistency between epochs 2 and 4. The validation accuracy peaks at epoch 3, with a value of 0.98275. Beyond epoch 4, both training and validation accuracy stabilize. Similar observations are made for ch7_output.



(**a**) Ch0_output (**b**) Ch1_output (**c**) Ch2_output

(**d**) Ch3_output (**e**) Ch4_output (**f**) Ch5_output

(**g**) Ch6_output (**h**) Ch7_output

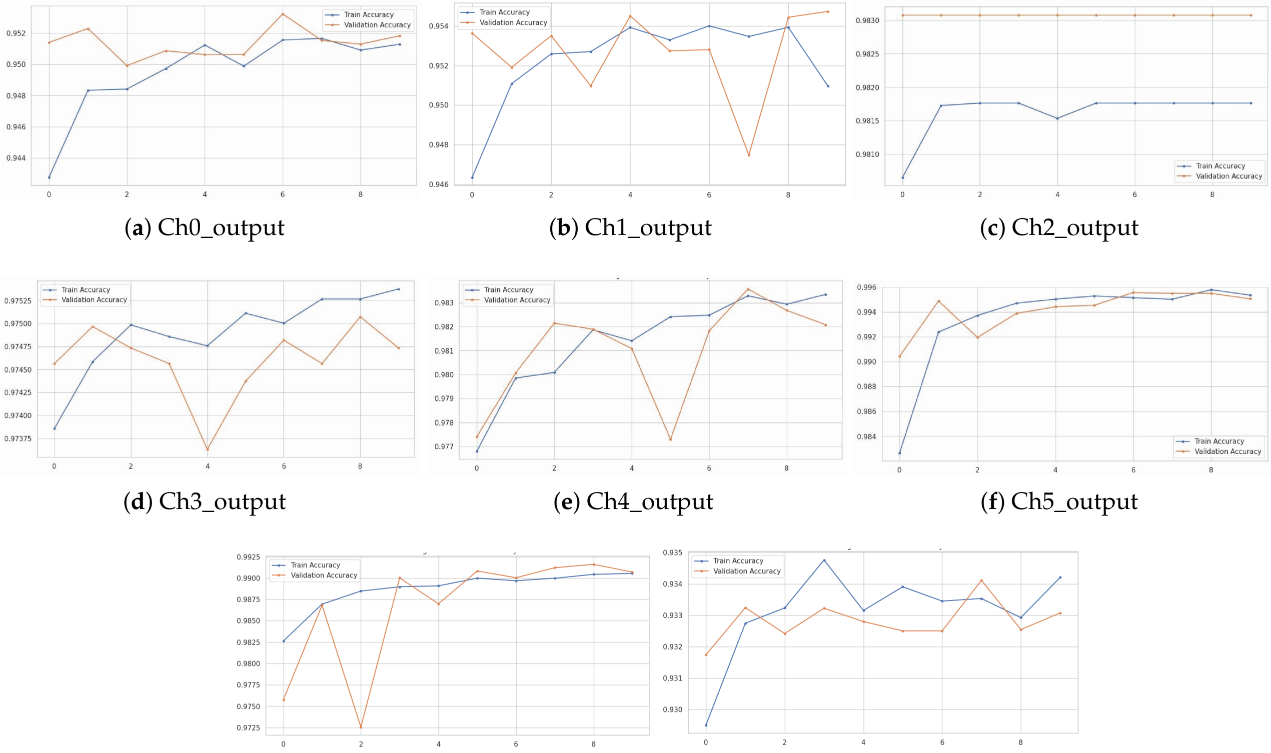
Figure 3. Training and validation accuracy for LSTM-GRU.

In Figure 4, the graph depicts the training and validation accuracy of the LSTM-RNN model. The x-axis indicates the number of epochs, while the y-axis denotes accuracy. The orange line represents validation accuracy, and the blue line corresponds to training accuracy for the labels ch0_output, ch5_output, and ch7_output. The patterns for these labels display relative consistency between training and validation. For labels ch3_output and ch6_output, the pattern remains stable between training and validation, with occasional fluctuations around the fourth epoch. Similarly, for ch6_output and ch1_output, the pattern mostly aligns between training and validation, with intermittent fluctuations occurring between 6 to 8 epochs. In the case of the label ch2_output, the pattern lacks consistency and remains erratic during validation.

Table 4. SSRL-based DNN results.

Label	Precision	Recall	F1-Score	Accuracy
Ch0_output Multi-label Classification				
Class 0	0.99	0.96	0.98	0.94
Class 1	0.58	0.14	0.22	0.93
Class 2	0.68	0.99	0.81	0.95
Class 3	0.98	1.00	0.99	0.95
Ch1_output Multi-label Classification				
Class 0	1.00	0.97	0.98	0.93
Class 1	0.82	0.44	0.57	0.95
Class 2	0.70	0.95	0.80	0.95
Class 3	0.79	0.99	0.88	0.94
Ch2_output Multi-label Classification				
Class 0	0.98	1.00	0.99	0.98
Class 1	1.00	0.55	0.71	0.98
Ch3_output Multi-label Classification				
Class 0	1.00	0.99	1.00	0.96
Class 1	0.76	0.99	0.86	0.98
Class 2	0.98	0.53	0.69	0.97
Class 3	0.49	1.00	0.65	0.97
Ch4_output Multi-label Classification				
Class 0	1.00	0.93	0.96	0.92
Class 1	0.55	0.95	0.70	0.92
Class 2	0.50	0.99	0.67	0.94
Class 3	0.99	0.98	0.99	0.93
Ch5_output Multi-label Classification				
Class 0	1.00	1.00	1.00	0.96
Class 1	0.98	0.92	0.95	0.95
Class 2	0.99	1.00	0.99	0.95
Ch6_output Multi-label Classification				
Class 0	1.00	0.99	0.99	0.98
Class 1	0.95	1.00	0.97	0.99
Class 2	0.93	0.97	0.95	0.99
Ch7_output Multi-label Classification				
Class 0	0.93	1.00	0.96	0.93
Class 1	0.99	0.17	0.28	0.93
Class 2	0.42	0.01	0.01	0.93
Class 3	1.00	0.98	0.99	0.92

In Figure 5, the chart illustrates the training and validation accuracy of the deep neural network (DNN) model. The x-axis corresponds to the number of epochs, while the y-axis represents accuracy. The orange line represents validation accuracy, and the blue line corresponds to training accuracy for the labels ch0_output, ch1_output, ch6_output, and ch7_output. The trends for these labels remain relatively stable throughout both training and validation. For the ch3_output label, the pattern generally aligns between training and validation, with occasional fluctuations. Labels ch4_output and ch5_output exhibit a consistent pattern between training and validation, with intermittent fluctuations occurring between 0 and 2 and 6 and 8. However, for the ch2_output label, the pattern lacks consistency between epochs 2 and 6.



(**a**) Ch0_output (**b**) Ch1_output (**c**) Ch2_output

(**d**) Ch3_output (**e**) Ch4_output (**f**) Ch5_output

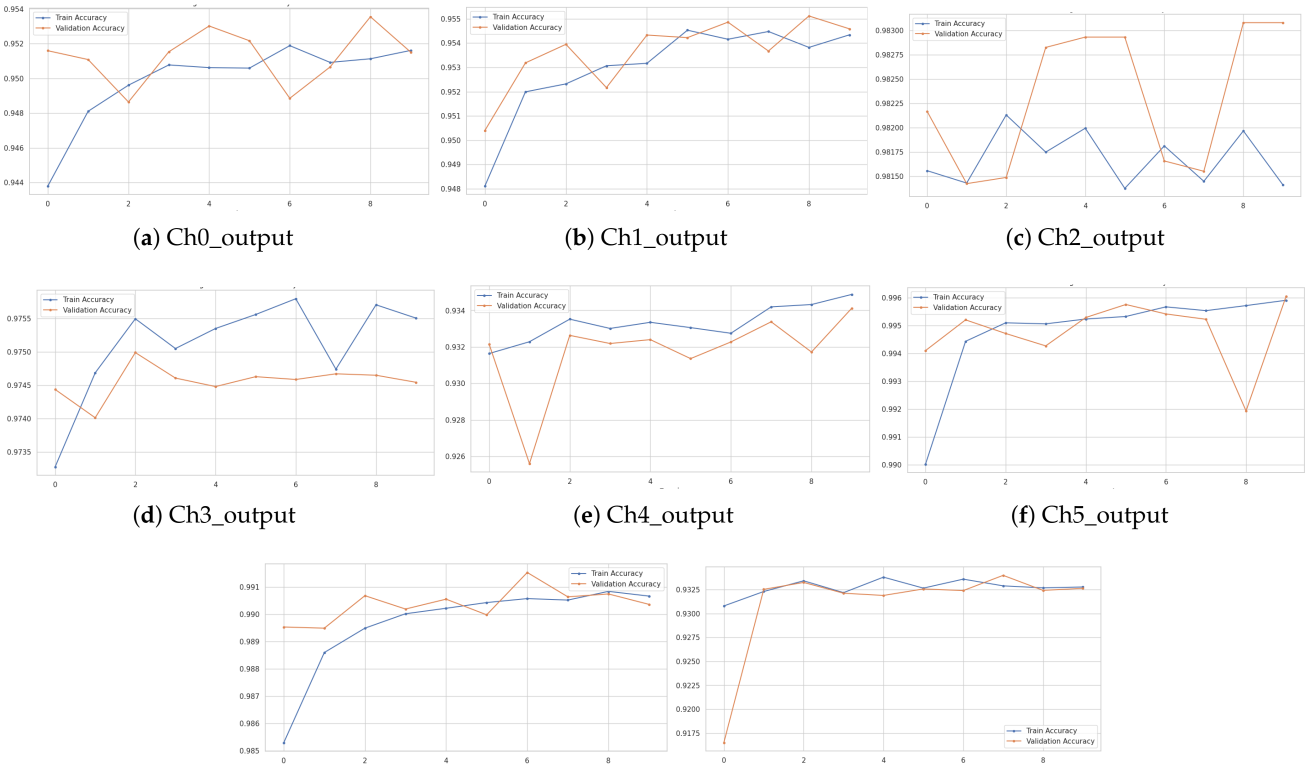
(**g**) Ch6_output (**h**) Ch7_output

Figure 4. Training and validation accuracy for LSTM-RNN.

In Figure 6, the chart illustrates the training and validation loss for the LSTM-GRU model. The x-axis corresponds to the number of epochs, while the y-axis represents the loss. The orange line denotes validation loss, and the blue line depicts training loss for all labels: ch0_output, ch1_output, ch2_output, ch3_output, ch4_output, ch5_output, ch6_output, and ch7_output. The patterns for these labels exhibit a relatively consistent behaviour between the training and validation phases.

In Figure 7, the chart depicts the training and validation loss of the LSTM-RNN model. The x-axis represents the number of epochs, while the y-axis signifies the loss. The orange line corresponds to validation loss, and the blue line represents training loss for the labels ch0_output, ch1_output, and ch6_output. The patterns for these labels show relative consistency between training and validation, with occasional fluctuations occurring between the second and fourth epochs. However, for the ch2_output label, the pattern lacks consistency and remains erratic during validation. For the labels ch3_output and ch4_output, the pattern remains consistent between training and validation, with occasional fluctuations between the fourth and sixth epochs. As for the ch5_output and ch7_output labels, the pattern generally stays consistent between training and validation loss.

In Figure 8, the chart depicts the training and validation loss of the straightforward DNN model. The x-axis indicates the number of epochs, while the y-axis represents the loss. The orange line represents validation loss, and the blue line corresponds to training loss for the labels ch0_output, ch1_output, ch4_output, ch5_output, ch6_output, and ch7_output. The trends for these labels demonstrate relative consistency between training and validation. However, the patterns lack consistency for the ch2_output and ch3_output labels and exhibit erratic behaviour during validation.

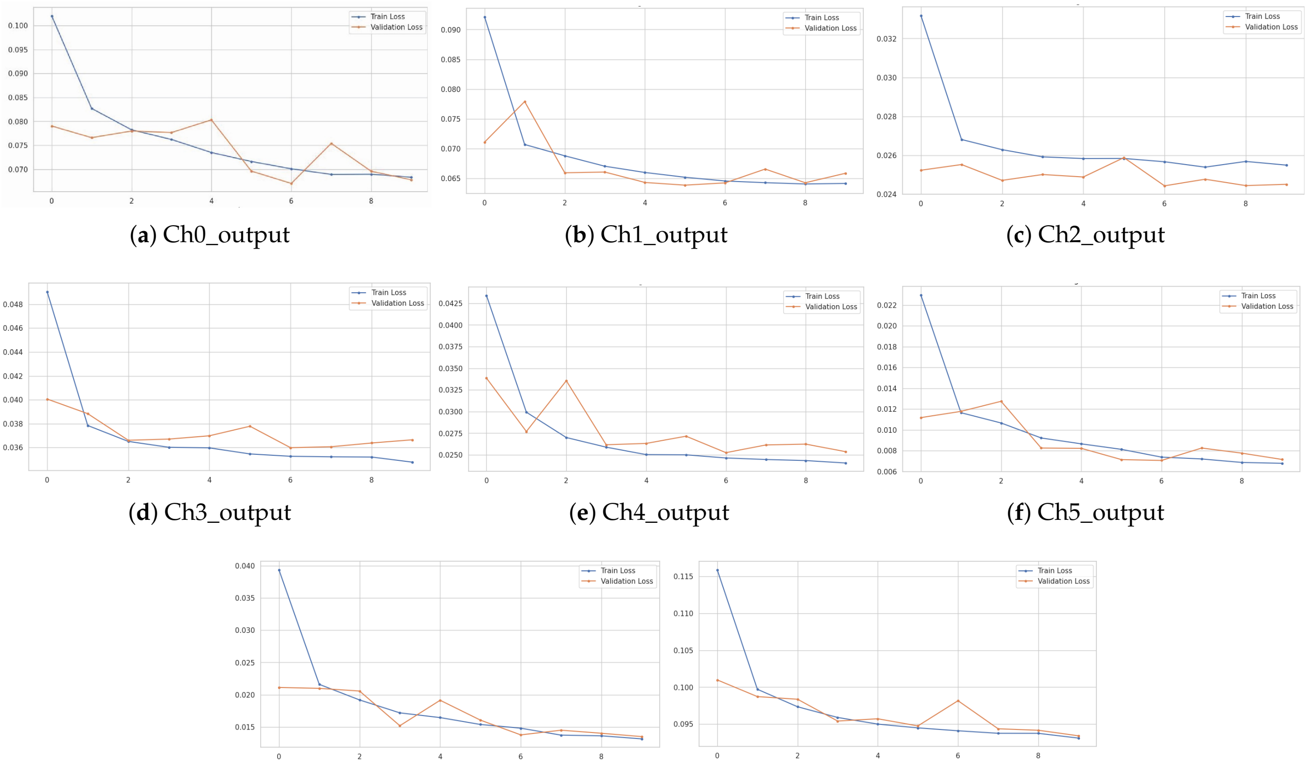


(**a**) Ch0_output (**b**) Ch1_output (**c**) Ch2_output

(**d**) Ch3_output (**e**) Ch4_output (**f**) Ch5_output

(**g**) Ch6_output (**h**) Ch7_output

Figure 5. Training and validation accuracy for DNN.

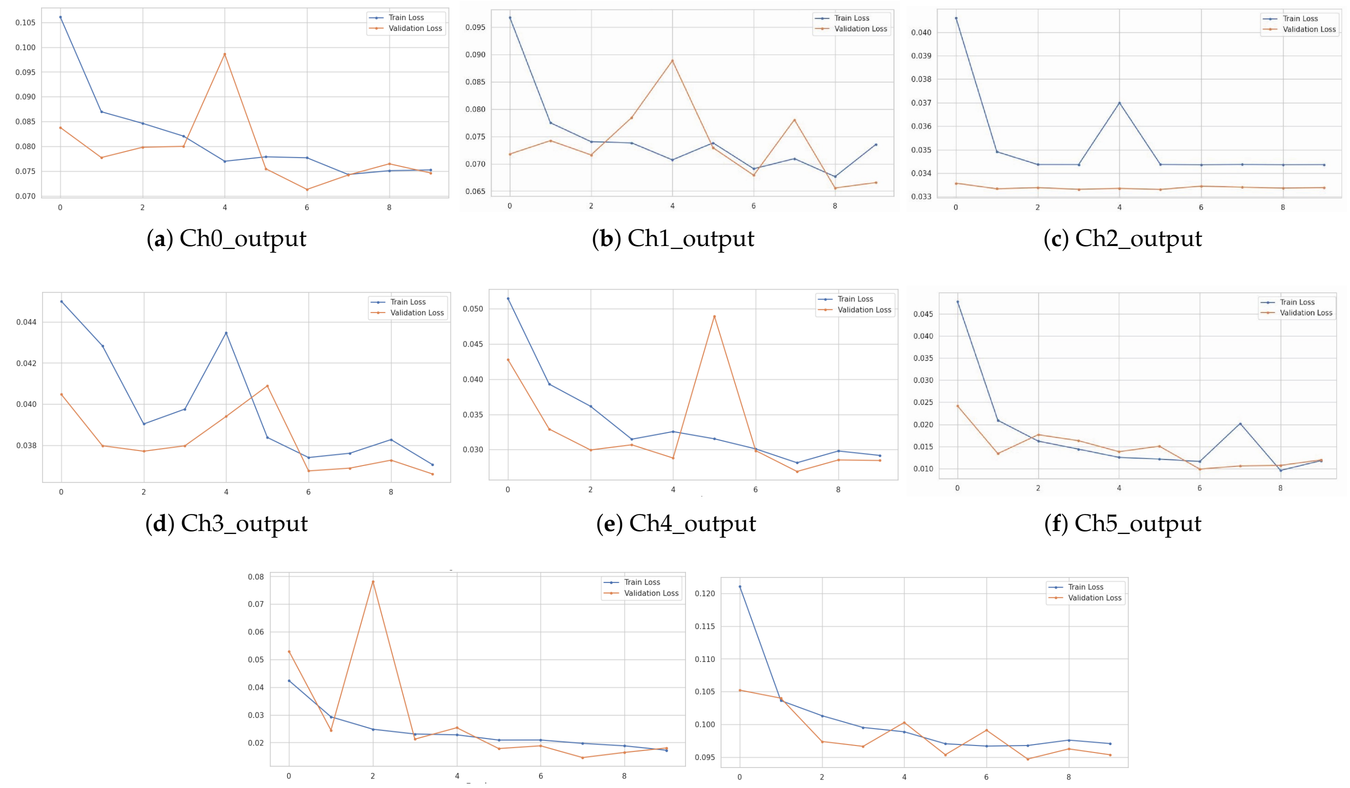


(a) Ch0_output (**b**) Ch1_output (**c**) Ch2_output

(**d**) Ch3_output (**e**) Ch4_output (**f**) Ch5_output

(**g**) Ch6_output (**h**) Ch7_output

Figure 6. Training and validation loss for LSTM-GRU.

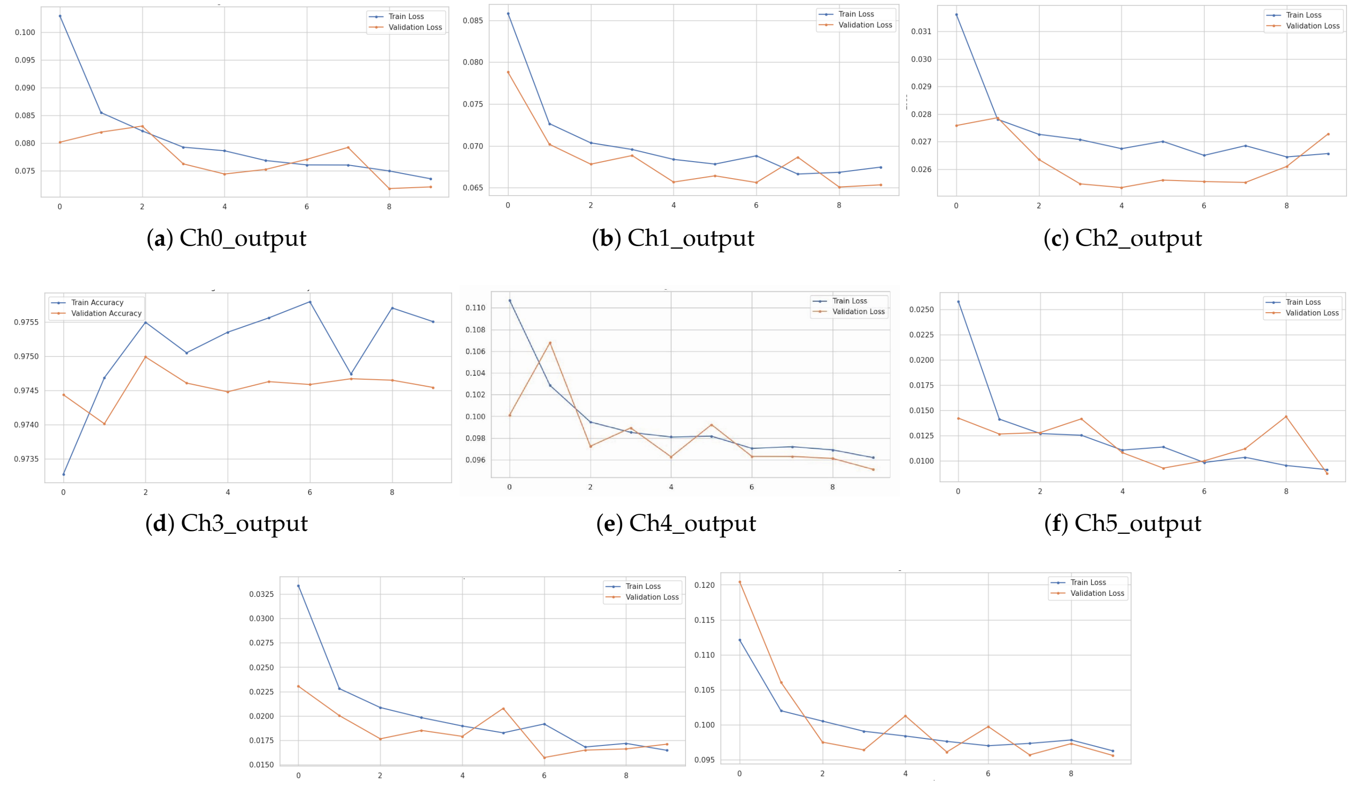


(**a**) Ch0_output (**b**) Ch1_output (**c**) Ch2_output

(**d**) Ch3_output (**e**) Ch4_output (**f**) Ch5_output

(**g**) Ch6_output (**h**) Ch7_output

Figure 7. Training and validation loss for LSTM-RNN.



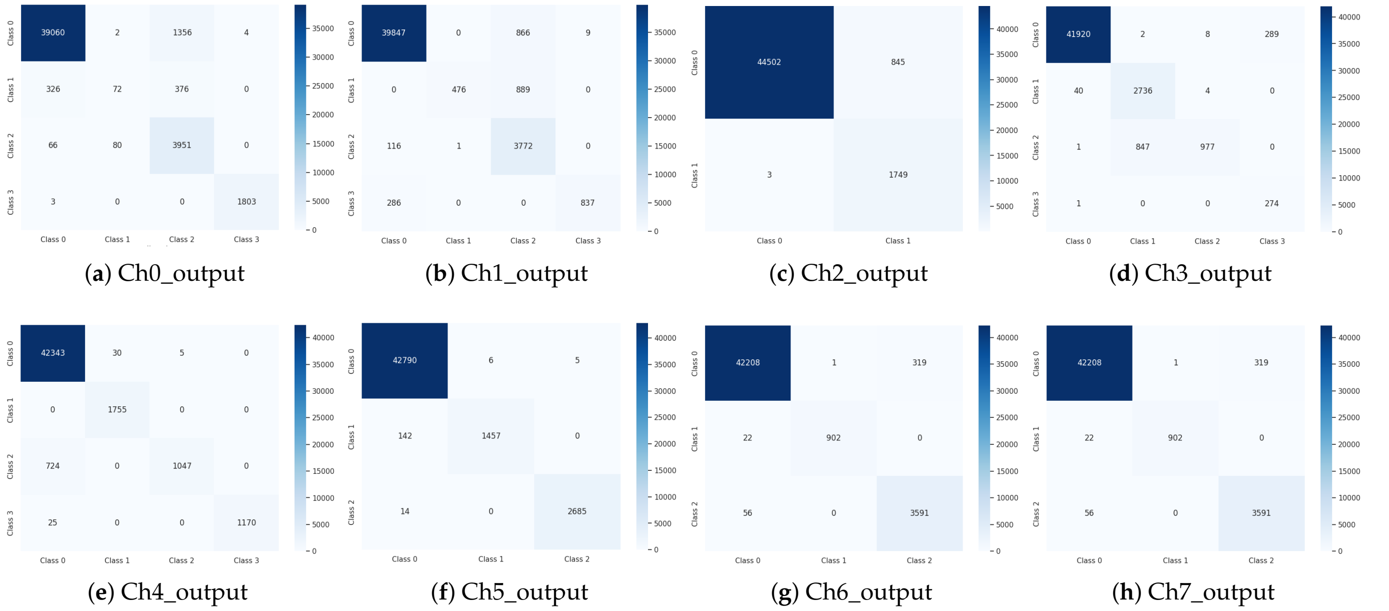
(**a**) Ch0_output (**b**) Ch1_output (**c**) Ch2_output

(**d**) Ch3_output (**e**) Ch4_output (**f**) Ch5_output

(**g**) Ch6_output (**h**) Ch7_output

Figure 8. Training and validation loss for DNN.

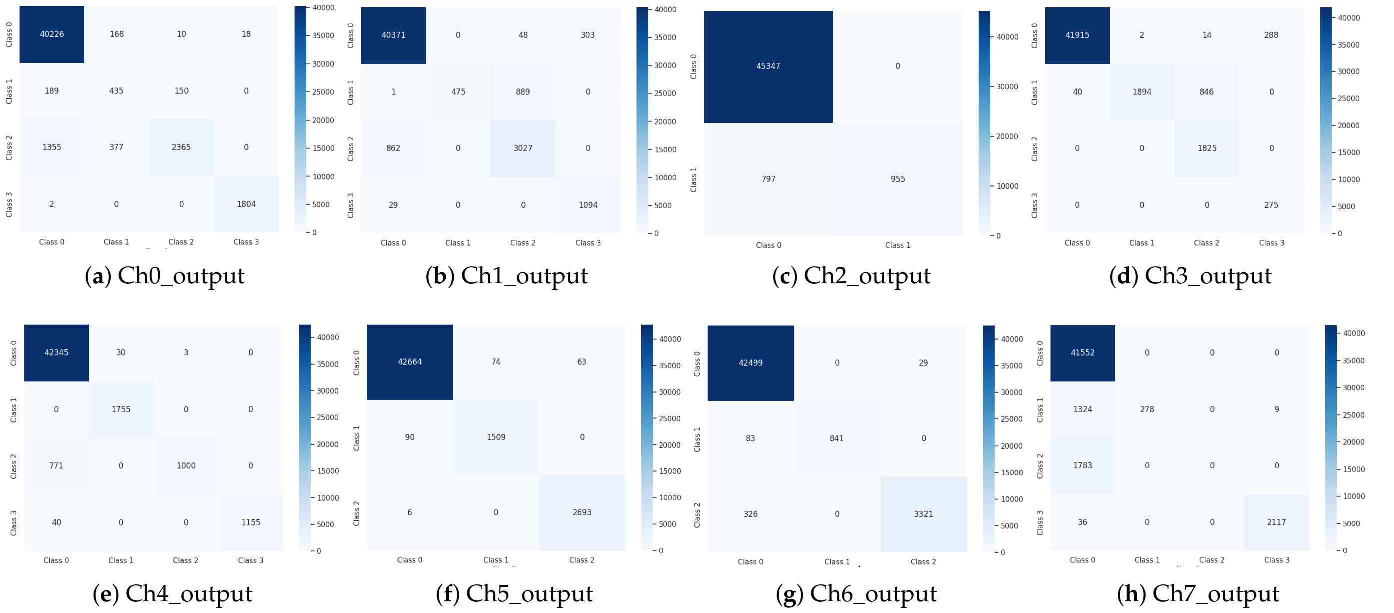
Figure 9 illustrates the confusion matrix for all ch_output labels using LSTM-GRU. Figure 10 displays the confusion matrix for all ch_output labels using LSTM-RNN. Figure 11 presents the confusion matrix for all ch_output labels using DNN. It can be noticed that the LSTM-GRU model has clearer outputs.



(**a**) Ch0_output (**b**) Ch1_output (**c**) Ch2_output (**d**) Ch3_output

(**e**) Ch4_output (**f**) Ch5_output (**g**) Ch6_output (**h**) Ch7_output

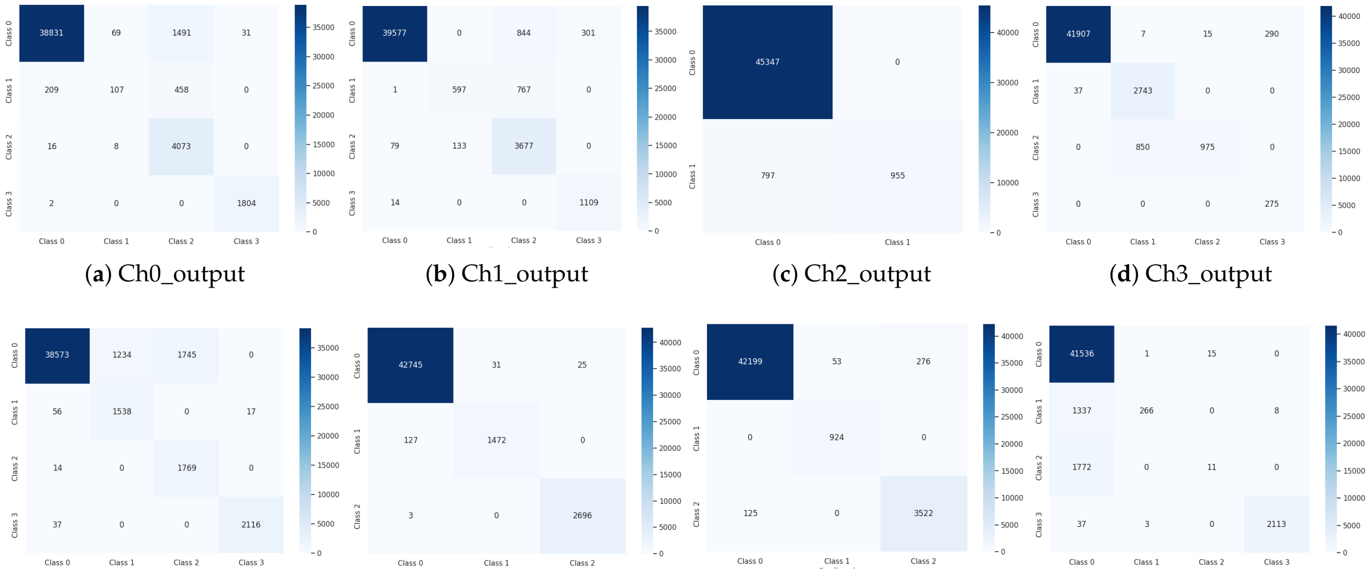
Figure 9. Confusion matrix for LSTM-GRU.



(**a**) Ch0_output (**b**) Ch1_output (**c**) Ch2_output (**d**) Ch3_output

(**e**) Ch4_output (**f**) Ch5_output (**g**) Ch6_output (**h**) Ch7_output

Figure 10. Confusion matrix for LSTM-RNN.



(**a**) Ch0_output (**b**) Ch1_output (**c**) Ch2_output (**d**) Ch3_output

(**e**) Ch4_output (**f**) Ch5_output (**g**) Ch6_output (**h**) Ch7_output

Figure 11. Confusion matrix for DNN.

5. Ablation Analysis

In this work, the architecture of our deep learning models is based on the architecture of the LSTM-GRU, which uses 64 neurons in the input layer for each of the LSTM-GRU 1 layers, a concatenation of both layers, 32 neurons in the concatenate layer of both LSTM-GRU 2 layers, 16 neurons in the fully connected layer, and a final layer that flattens and concatenates the output. Moreover, the architecture used to build an LSTM-RNN uses 128 neurons in the input layer for both LSTM-RNN 1 layers, concatenating both layers, 64 neurons in the concatenate layer for both LSTM-RNN 2 layers, 32 neurons in the fully connected layer, and a final layer that flattens and concatenates the output. In addition, a DNN is integrated with 128 neurons in the input layer for both layers, concatenating both layers, 64 neurons in the concatenate layer for subsequent layers, 32 neurons in the fully connected layer, and a final layer that flattens and concatenates the output. Accuracy is the major parameter used in evaluating the architecture proposed in this work. The models are trained 10 times on the training data with a batch size of 32. After much optimisation, the neural network architectures for the Simple DNN Model, LSTM-GRU, and LSTM-RNN have been fine-tuned for better performance and robustness. The comparative analysis performed in this work indicates that the LSTM-GRU architecture is better than the rest, with a higher accuracy rate and a low overfit condition compared to other configurations.

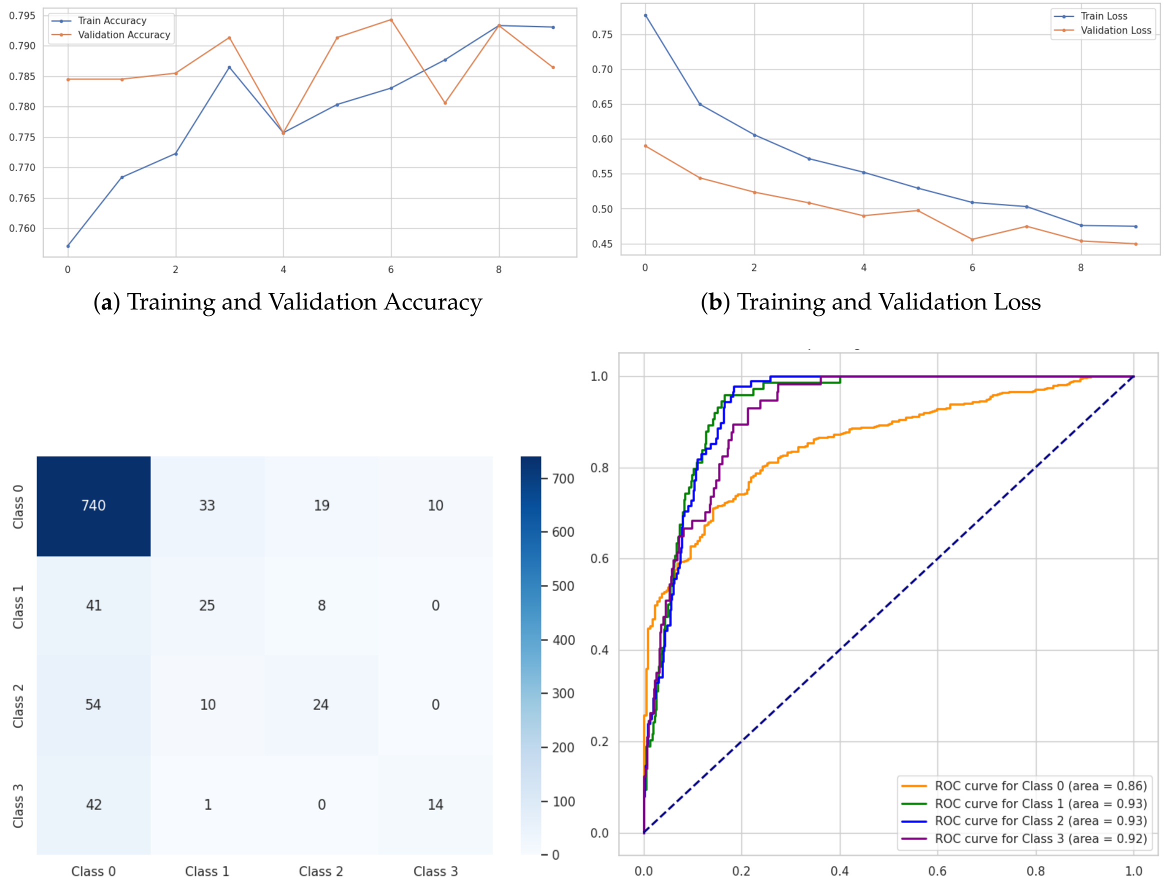
6. Proposed Self-Supervised Representation Learning Method with Transfer Learning

To enhance our self-supervised deep representation learning method with additional techniques like transfer learning, we have developed a robust strategy that improves the adaptability and generalisation of our model for detecting GPS spoofing attacks on small UAVs. To further enhance our model's performance, we integrate self-supervised learning, which enables the model to extract meaningful features from the GPS signal data without relying on extensive labelled examples. This method captures intricate patterns and anomalies essential for detecting spoofing attacks. Building upon this, we implement transfer learning by saving the weights of our trained model and applying these pre-trained weights to a new dataset, specifically the GPS_simplified_2d_feature_map dataset. This approach leverages the knowledge gained from the original dataset and transfers it to a related domain, thereby improving the model's adaptability to new data with minimal additional training. The integration of self-supervised learning with transfer learning has resulted in a validation accuracy of 79.0%, demonstrating an improvement in the model's performance and its ability to generalize across different datasets Table 5. This approach not only enhances the model's detection capabilities but also significantly reduces the training time required for new datasets, confirming the effectiveness of combining these advanced techniques in improving the robustness and efficiency of GPS spoofing attack detection.

Table 5. Pre-trained transfer learning model.

Output Label	Accuracy	Recall	F1 Score
0	0.84	0.92	0.88
1	0.36	0.34	0.35
2	0.47	0.27	0.35
3	0.58	0.25	0.35

Figure 12 shows the pre-trained transfer learning model's training and validation performance. The accuracy plot shows a steady improvement in training accuracy, reaching about 79.5%, while the validation accuracy fluctuates, peaking around epoch 4, indicating potential overfitting. The loss plot demonstrates a decline in both training and validation loss, but the validation loss begins to plateau after epoch 6, suggesting diminishing improvement in generalisation. The confusion matrix highlights that the model predicts Class 0 well but struggles with other classes, especially Class 3, where many instances are misclassified as Class 0.



(**a**) Training and Validation Accuracy

(**b**) Training and Validation Loss

(**c**) Confusion Matrix

(**d**) ROC Curve

Figure 12. Transfer learning model results.

7. Comparison Analysis of Proposed Models

Based on the performance results shown in Table 6, the DNN model consistently achieved the highest accuracy across most output labels, making it the best overall performer. Specifically, the DNN model attained a perfect accuracy of 1.00 for ch5_output, demonstrating its superior ability to detect GPS spoofing attacks for this label. Additionally, it achieved high accuracy values for other outputs, with ch6_output reaching 0.99 and several others maintaining accuracy above 0.95. Therefore, the DNN model is recommended for scenarios prioritizing high accuracy, especially for detecting critical GPS spoofing incidents like ch5_output.

Table 7 compares various models from existing studies on GPS spoofing detection for small UAVs, highlighting their accuracy. Sun et al. [37] used deep learning approaches, achieving accuracies of 90%. Titouna et al. [12] and Dang et al. [41] employed dynamic selection techniques and deep ensemble learning, reaching 95% and 97% accuracy, respectively. Other studies, such as Banu et al. [44] and Gasimova et al. [45], explored various detection methods and weak and strong learners, with accuracy ranging from 85% to 95%. Talaei et al. [51] achieved the highest accuracy of 99.6% with a dynamic selection module. Our proposed model, which integrates LSTM-GRU, LSTM-RNN, and DNN, surpasses these with an impressive accuracy of 99.99%, demonstrating its superior performance in GPS spoofing detection for small UAVs.

Table 6. Comparison of model performance.

Model	Output Label	Accuracy	Recall	F1 Score
LSTM-GRU	ch0_output	0.95	0.94	0.94
	ch1_output	0.95	0.94	0.94
	ch2_output	0.98	0.97	0.97
	ch3_output	0.97	0.96	0.96
	ch4_output	0.98	0.97	0.97
	ch5_output	1.00	1.00	1.00
	ch6_output	0.99	0.98	0.98
	ch7_output	0.90	0.89	0.89
LSTM-RNN	ch0_output	0.95	0.94	0.94
	ch1_output	0.95	0.94	0.94
	ch2_output	0.98	0.97	0.97
	ch3_output	0.97	0.96	0.96
	ch4_output	0.98	0.97	0.97
	ch5_output	1.00	1.00	1.00
	ch6_output	0.99	0.98	0.98
	ch7_output	0.90	0.89	0.89
DNN	ch0_output	0.95	0.94	0.94
	ch1_output	0.95	0.94	0.94
	ch2_output	0.98	0.97	0.97
	ch3_output	0.97	0.96	0.96
	ch4_output	0.93	0.92	0.92
	ch5_output	1.00	1.00	1.00
	ch6_output	0.99	0.98	0.98
	ch7_output	0.93	0.92	0.92

Table 7. Comparison of existing work and proposed models.

Study	Model	Accuracy
Sung et al. (2022) [37]	1D CNN	90%
Titouna et al. (2021) [12]	Dynamic Selection Techniques	95%
Dang et al. (2022) [41]	Deep Ensemble Learning	97%
Banu et al. (2022) [44]	Various Detection Methods	85% to 95%
Gasimova et al. (2022) [45]	Weak and Strong Learners	85% to 95%
Talaei et al. (2022) [51]	Dynamic Selection Module	99.6%
Proposed Model	**LSTM-GRU, LSTM-RNN, DNN**	**99.99%**

8. Discussion

This paper focuses on the critical goal of enhancing the security and reliability of UAVs while contributing to the broader field of autonomous systems. By applying Self-Supervised Representation Learning (SSRL) in practical scenarios, this study established a new approach for integrating advanced machine learning techniques to address significant challenges faced by autonomous systems. Our work not only aims to protect UAVs from GPS spoofing but also sets a standard for using innovative technologies to strengthen the resilience of autonomous systems across various domains. In this study, a network model tailored for small UAVs was implemented, emphasizing low-latency and high-reliability communication. The network was designed to support real-time data processing and transmission, which is crucial for detecting and mitigating GPS spoofing attacks. Continuous and reliable communication between UAVs and ground control stations was ensured, even in the presence of potential spoofing threats. This robust communication model was vital for maintaining the integrity of the data used in attack detection. Our research employed a hypothesis-testing approach to evaluate the performance of the proposed SSRL-based models under different spoofing scenarios. It was hypothesized that the hybrid deep learning architectures, particularly the LSTM-GRU model, would outperform traditional methods in accurately detecting GPS spoofing attacks. This hypothesis was tested by comparing the accuracy of the proposed model against baseline models over 10 epochs of training. The results validated our hypothesis, with the LSTM-GRU model achieving an impressive 99.9% accuracy, proving its effectiveness in countering GPS spoofing attacks. Furthermore, the model's capabilities were enhanced by integrating transfer learning, which improved its adaptability and generalisation. By applying pre-trained weights from the SSRL model to a new dataset, specifically the GPS_simplified_2d_feature_map dataset, the model achieved a validation accuracy of 79.0%. This addition demonstrated the model's ability to generalize across different datasets with minimal additional training, further reinforcing the robustness and efficiency of the approach in detecting GPS spoofing attacks.

9. Conclusions

GPS spoofing presents substantial risks to the safety and security of small UAVs, potentially undermining navigation systems and compromising mission integrity. Effective mitigation strategies, including secure GPS signal authentication, anti-spoofing technologies, and continuous monitoring, are vital to address this threat. Our research introduces a novel architecture aimed at improving the detection and multi-label classification of GPS spoofing attacks in small UAVs. By employing multiple LSTM-GRU layers, LSTM-RNN layers, and a Deep Neural Network (DNN), our model showcases exceptional performance. The architecture is specifically configured with 64 neurons in the input and concatenate layers for LSTM-GRU, 128 neurons for LSTM-RNN, and 128 neurons for the DNN, utilizing self-supervised representation learning to enhance adaptability and learning efficiency. To evaluate the effectiveness of this approach, we trained the models over 10 epochs, achieving a remarkable accuracy of 99.9% in detecting various

GPS spoofing labels. This highlights the architecture's efficiency in real-time detection, particularly in resource-constrained environments. Additionally, the integration of transfer learning significantly enhanced the model's adaptability and generalisation, achieving a validation accuracy of 79.0% on the GPS_simplified_2d_feature_map dataset. This improvement underscores the effectiveness of combining self-supervised learning with transfer learning for detecting GPS spoofing attacks. Our research addresses the pressing need to counter GPS spoofing threats in small UAVs, contributing to advancements in autonomous systems through the use of self-supervised representation learning and transfer learning. By strengthening UAV security, our architecture ensures reliable operation across diverse applications such as surveillance, agriculture, and environmental monitoring. Future work could focus on further optimizing the model for lightweight deployment, enhancing cross-platform adaptability, and incorporating additional sensor data to improve detection accuracy and robustness.

Funding: This research was funded by Prince Sattam bin Abdulaziz University grant number (PSAU/2024/01/29895).

Data Availability Statement: The data are available at [52].

Acknowledgments: The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number (PSAU/2024/01/29895).

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Pandharipande, A.; Cheng, C.H.; Dauwels, J.; Gurbuz, S.Z.; Ibanex-Guzman, J.; Li, G.; Piazzoni, A.; Wang, P.; Santra, A. Sensing and machine learning for automotive perception: A review. *IEEE Sens. J.* **2023**, *23*, 11097–11115. [CrossRef]
2. Yadav, N. Machine Learning for Earth System Science and Engineering-Critical Challenges. Ph.D. Thesis, Northeastern University, Boston, MA, USA, 2022.
3. Shah, M. Wanderwise-Intelligent Travel Planning System. 2023. Available online: https://www.researchgate.net/publication/376638581_Wanderwise_-Intelligent_travel_planning_system (accessed on 15 September 2024).
4. Mendes, D.; Ivaki, N.; Madeira, H. Effects of GPS spoofing on unmanned aerial vehicles. In Proceedings of the 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan, 4–7 December 2018; pp. 155–160.
5. Khan, S.Z.; Mohsin, M.; Iqbal, W. On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions. *PeerJ Comput. Sci.* **2021**, *7*, e507. [CrossRef]
6. Kong, P.Y. A survey of cyberattack countermeasures for unmanned aerial vehicles. *IEEE Access* **2021**, *9*, 148244–148263. [CrossRef]
7. Giray, S.M. Anatomy of unmanned aerial vehicle hijacking with signal spoofing. In Proceedings of the 2013 6th International Conference on Recent Advances in Space Technologies (RAST), Istanbul, Turkey, 12–14 June 2013; pp. 795–800.
8. Alsulami, H. Implementation analysis of reliable unmanned aerial vehicles models for security against cyber-crimes: Attacks, tracebacks, forensics and solutions. *Comput. Electr. Eng.* **2022**, *100*, 107870. [CrossRef]
9. Humphreys, T. *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing*; University of Texas at Austin: Austin, TX, USA, 2012; pp. 1–16.
10. Hamza, A.; Akram, U.; Samad, A.; Khosa, S.N.; Fatima, R.; Mushtaq, M.F. Unmaned aerial vehicles threats and defence solutions. In Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 5–7 November 2020; pp. 1–6.
11. Krishna, C.L.; Murphy, R.R. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In Proceedings of the 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), Shanghai, China, 11–13 October 2017; pp. 194–199.
12. Titouna, C.; Naït-Abdesselam, F. A Lightweight Security Technique For Unmanned Aerial Vehicles Against GPS Spoofing Attack. In Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC), Beijing, China, 28 June–2 July 2021; pp. 819–824.
13. Guo, J.; Li, L.; Wang, J.; Li, K. Cyber-physical system-based path tracking control of autonomous vehicles under cyber-attacks. *IEEE Trans. Ind. Inform.* **2022**, *19*, 6624–6635. [CrossRef]
14. Xu, Y.; Han, X.; Deng, G.; Li, J.; Liu, Y.; Zhang, T. SoK: Rethinking sensor spoofing attacks against robotic vehicles from a systematic view. In Proceedings of the 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), Delft, The Netherlands, 3–7 July 2023; pp. 1082–1100.
15. Sihag, V.; Choudhary, G.; Choudhary, P.; Dragoni, N. Cyber4Drone: A Systematic Review of Cyber Security and Forensics in Next-Generation Drones. *Drones* **2023**, *7*, 430. [CrossRef]
16. Kapustina, L.; Izakova, N.; Makovkina, E.; Khmelkov, M. The global drone market: Main development trends. In Proceedings of the SHS Web of Conferences. *Edp Sci.* **2021**, *129*, 11004.

17. Ly, B.; Ly, R. Cybersecurity in unmanned aerial vehicles (UAVs). *J. Cyber Secur. Technol.* **2021**, *5*, 120–137. [CrossRef]
18. He, D.; Chan, S.; Guizani, M. Communication security of unmanned aerial vehicles. *IEEE Wirel. Commun.* **2016**, *24*, 134–139. [CrossRef]
19. Sathyamoorthy, D. A review of security threats of unmanned aerial vehicles and mitigation steps. *J. Def. Secur.* **2015**, *6*, 81–97.
20. Basha, S.J.; Danda, J.M.R. A Review on Challenges and Threats to Unmanned Aerial Vehicles (UAVs). In *Unmanned Aerial Vehicles for Internet of Things (IoT) Concepts, Techniques, and Applications*; Wiley Online Library: Hoboken, NJ, USA, 2021; pp. 89–104.
21. Chamola, V.; Kotesh, P.; Agarwal, A.; Gupta, N.; Guizani, M. A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. *Ad Hoc Netw.* **2021**, *111*, 102324. [CrossRef]
22. Lucia, L.D.; Vegni, A.M. UAV Main Applications: From Military to Agriculture Fields. In *Internet of Unmanned Things (IoUT) and Mission-Based Networking*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 1–23.
23. Shafique, A.; Mehmood, A.; Elhadef, M. Survey of security protocols and vulnerabilities in unmanned aerial vehicles. *IEEE Access* **2021**, *9*, 46927–46948. [CrossRef]
24. Waqas, A.; Kang, D.; Cha, Y.J. Deep learning-based obstacle-avoiding autonomous UAVs with fiducial marker-based localization for structural health monitoring. *Struct. Health Monit.* **2024**, *23*, 971–990. [CrossRef]
25. Song, L.K.; Li, X.Q.; Zhu, S.P.; Choy, Y.S. Cascade ensemble learning for multi-level reliability evaluation. *Aerosp. Sci. Technol.* **2024**, *148*, 109101. [CrossRef]
26. Ren, Y.; Restivo, R.D.; Tan, W.; Wang, J.; Liu, Y.; Jiang, B.; Wang, H.; Song, H. Knowledge Distillation-Based GPS Spoofing Detection for Small UAV. *Future Internet* **2023**, *15*, 389. [CrossRef]
27. Shin, J.; Baek, Y.; Eun, Y.; Son, S.H. Intelligent sensor attack detection and identification for automotive cyber-physical systems. In Proceedings of the 2017 IEEE Symposium Series on Computational Intelligence (SSCI), Honolulu, HI, USA, 27 November–1 December 2017; pp. 1–8.
28. Dang, Y.; Karakoc, A.; Norshahida, S.; Jäntti, R. 3D Radio Map-Based GPS Spoofing Detection and Mitigation for Cellular-Connected UAVs. *IEEE Trans. Mach. Learn. Commun. Netw.* **2023**, *1*, 313–327. [CrossRef]
29. Li, Y.; Yang, S. GPS Spoofing attack detection in smart grids based on improved CapsNet. *China Commun.* **2021**, *18*, 174–186. [CrossRef]
30. Boyd, J.; Fahim, M.; Olukoya, O. Voice spoofing detection for multiclass attack classification using deep learning. *Mach. Learn. Appl.* **2023**, *14*, 100503. [CrossRef]
31. Dasgupta, S.; Rahman, M.; Islam, M.; Chowdhury, M. Prediction-based GNSS spoofing attack detection for autonomous vehicles. *arXiv* **2020**, arXiv:2010.11722 .
32. Agyapong, R.A.; Nabil, M.; Nuhu, A.R.; Rasul, M.I.; Homaifar, A. Efficient detection of GPS spoofing attacks on unmanned aerial vehicles using deep learning. In Proceedings of the 2021 IEEE Symposium Series on Computational Intelligence (SSCI), Virtual, 5–7 December 2021; pp. 01–08.
33. Jiang, P.; Wu, H.; Xin, C. DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network. *Digit. Commun. Netw.* **2022**, *8*, 791–803. [CrossRef]
34. Jullian, O.; Otero, B.; Stojilović, M.; Costa, J.J.; Verdú, J.; Pajuelo, M.A. Deep Learning Detection of GPS Spoofing. In Proceedings of the International Conference on Machine Learning, Optimization, and Data Science, Grasmere, UK, 4–8 October 2021; pp. 527–540.
35. Shabbir, M.; Kamal, M.; Ullah, Z.; Khan, M.M. Securing Autonomous Vehicles Against GPS Spoofing Attacks: A Deep Learning Approach. *IEEE Access* **2023**, *11*, 105513–105526. [CrossRef]
36. Ying, X.; Mazer, J.; Bernieri, G.; Conti, M.; Bushnell, L.; Poovendran, R. Detecting ADS-B spoofing attacks using deep neural networks. In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; pp. 187–195.
37. Sung, Y.H.; Park, S.J.; Kim, D.Y.; Kim, S. GPS Spoofing Detection Method for Small UAVs Using 1D Convolution Neural Network. *Sensors* **2022**, *22*, 9412. [CrossRef] [PubMed]
38. Luo, G.; He, B.; Xiong, Y.; Wang, L.; Wang, H.; Zhu, Z.; Shi, X. An Optimized Convolutional Neural Network for the 3D Point-Cloud Compression. *Sensors* **2023**, *23*, 2250. [CrossRef]
39. Khanh, P.T.; Ngoc, T.T.H.; Pramanik, S. Future of Smart Agriculture Techniques and Applications. In *Handbook of Research on AI-Equipped IoT Applications in High-Tech Agriculture*; IGI Global: Pennsylvania, PA, USA, 2023; pp. 365–378.
40. Sun, Y.; Yu, M.; Wang, L.; Li, T.; Dong, M. A Deep-Learning-Based GPS Signal Spoofing Detection Method for Small UAVs. *Drones* **2023**, *7*, 370. [CrossRef]
41. Dang, Y.; Benzaïd, C.; Yang, B.; Taleb, T.; Shen, Y. Deep-ensemble-learning-based GPS spoofing detection for cellular-connected UAVs. *IEEE Internet Things J.* **2022**, *9*, 25068–25085. [CrossRef]
42. Zheng, Q.; Zhao, P.; Zhang, D.; Wang, H. MR-DCAE: Manifold regularization-based deep convolutional autoencoder for unauthorized broadcasting identification. *Int. J. Intell. Syst.* **2021**, *36*, 7204–7238. [CrossRef]
43. Zheng, Q.; Saponara, S.; Tian, X.; Yu, Z.; Elhanashi, A.; Yu, R. A real-time constellation image classification method of wireless communication signals based on the lightweight network MobileViT. *Cogn. Neurodyn.* **2024**, *18*, 659–671. [CrossRef]
44. Banu, A.S.; Padmavathi, G. Taxonomy of UAVs GPS spoofing and jamming attack detection methods. In *Computational Intelligence for Unmanned Aerial Vehicles Communication Networks*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 167–201.
45. Gasimova, A. Performance Comparison of Weak and Strong Learners in Detecting GPS Spoofing Attacks on Unmanned Aerial Vehicles (UAVs). Ph.D. Thesis, The University of North Dakota, Grand Forks, ND, USA, 2022.

46. Ibrahim, M.; Safa, N.S. Detecting message spoofing attacks on smart vehicles. *Comput. Fraud Secur.* **2023**, *2023*. [CrossRef]
47. Zhang, Y.; Hou, X.; Hou, X. Combining Self-Supervised Learning and Yolo v4 Network for Construction Vehicle Detection. *Mob. Inf. Syst.* **2022**, *2022*, 9056415. [CrossRef]
48. Cimarelli, C. Perception for Surveillance: Learning Self-Localisation and Intruders Detection from Monocular Images of an Aerial Robot in Outdoor Urban Environments. Ph.D. Thesis, University of Luxembourg, Luxembourg, 2022.
49. Meng, L.; Yang, L.; Ren, S.; Tang, G.; Zhang, L.; Yang, F.; Yang, W. An approach of linear regression-based UAV GPS spoofing detection. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 5517500. [CrossRef]
50. Chen, Y.; Peng, H.; Huang, L.; Zhang, J.; Jiang, W. A Novel MAE-Based Self-Supervised Anomaly Detection and Localization Method. *IEEE Access* **2023**, *11*, 127526–127538. [CrossRef]
51. Talaei Khoei, T.; Ismail, S.; Kaabouch, N. Dynamic selection techniques for detecting GPS spoofing attacks on UAVs. *Sensors* **2022**, *22*, 662. [CrossRef]
52. Aissou, G.; Benouadah, S.; EL ALAMI, H.; Kaabouch, N. A DATASET for GPS Spoofing Detection on Autonomous Vehicles. *Mob. Inf. Syst.* **2022**, *2022*, 9056415.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.