NOVEL RF-BASED DRONE RECOGNITION AND CLASSIFICATION

Dr. T. K. S. Rathish Babu[1], GoureddySrija[2], N. S. L. Harini[3], M. Madhu Shree[4]

Article History: Received: 14.02.2023 **Revised:** 31.03.2023 **Accepted:** 15.05.2023

Abstract

Unmanned aerial vehicles (UAVs) or drones have become a popular technology in various fields, including agriculture, delivery services, and surveillance. However, the use of drones in susceptible areas such as airport, armed forces bases, and critical infrastructure facilities has raised security concerns. Developing an efficient drone detection system has thus become a pressing need. In this editorial, we propose a drone discovery system that uses computer vision techniques to detect drones in real-time video streams. The proposed system is designed to work with different types of drones, regardless of their size, shape, and flight patterns. The system utilizes state-of-the-art object recognition algorithms, such as YOLOv5, and tracks the detected drones over time. The system's presentation is evaluated on a novel rf-based buzz detection dataset, and the results demonstrate the system's effectiveness in detecting drones in various environments. In similar way Deep Residual Neural Network (DRNN) framework used for drone detection as well as for categorization. The proposed system has the potential for use in a diversity of applications, such as security plus surveillance, public safety, and disaster management.

Keywords: UAV, sensor systems, and applications for signal detection and categorization.

[1]Professor, Computer Science and Engineering, Sridevi Women’s Engineering College Hyderabad, India
[2,3,4]Computer Science and Engineering, Sridevi Women’s Engineering College, B.Tech IV Year Hyderabad, India

Email address: [1]rathishbabu2013@gmail.com, [2]goureddysrija@gmail.com, [3]Nagireddiiharini@gmail.com, [4]shreemadhu948@gmail.com

DOI: 10.31838/ecb/2023.12.s3.329

1. INTRODUCTION

The growth of drone technology has been fast. Modern iterations come equipped with cutting-edge (SoA) drone parts including GPS, LIDAR, radar, and vision sensors. These developments make it possible to deploy drones for a range of tasks, including filmmaking, farming, monitoring, and recreational activities. Modern drone technology has great potential for search and rescue operations in hard-to-reach places, emergency aid delivery, and inspections of damaged infrastructure. In addition to these legitimate purposes, drones are also being used illegally, endangering public safety. Drug and weapon trafficking, as well as invasions of locations where security is a concern, such as nuclear power plants and airports, are all examples of criminal activity. A number of Counter Unmanned Aircraft Systems (C-UAS) have been developed to defend against drone attacks. Kinetic options for bringing down a buzz include using a skilled bird of prey, a net cannon, a laser beam, or a rifle. Non-kinetic methods such as (i) GPS spoofing [1] and (ii) RF jamming can be used to mislead a drone's localization system. No of the strategy, a drone ought to be present at all times. The automatic classification and identification of drones is a challenging task.

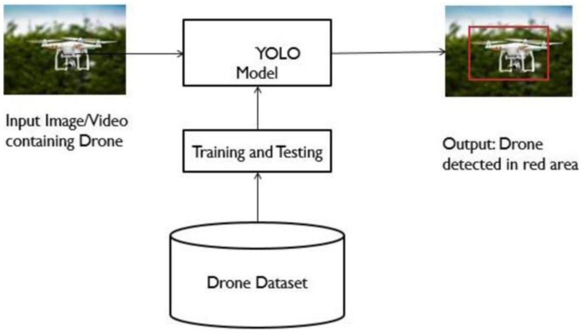

YOLO Model
Input Image/Video containing Drone
Training and Testing
Output: Drone detected in red area
Drone Dataset

Fig1: Module Diagram

These contain radar detection, video invention, acoustic finding, RF-based detection, and other prominent technological methods for drone detection and categorization. In addition to a thorough literature review, these technologies are used in the present SoA Machine Learning-based drone detection and categorization described in [2]. Multiple technologies may be used, according to research [3], in order to recognise and categorize UAVs. The backscattered RF signal is used by the radar detector to locate and classify drones. Due of its slight radar cross section (RCS), a mini-drone cannot be detected by conventional radar systems. Using a multistatic radar [4] or a Frequency Modulated Continuous Wave (FMCW) radar [5], [6] and relying on its micro-Doppler signature, researchers were able to spot and categorize a quadcopter or multi-rotor UAV.

Between [7] and [9], researchers used this technology to build a number of drone detection techniques that integrated optical and thermal detection into the video/image detection. This method uses information about the drone's colour, shape, and edges to identify it [7]. Line of sight (LOS) between the drone and camera is still necessary despite the detecting approach's precision. Performance is significantly impacted by the time of day and external variables such as clouds, rain, fog, and dust. It is more harder for a video detector given how similar a bird and a drone are to one another. The authors of [8] distinguished a drone from a bird using motion and trajectory data from the drone. In [10], a basic summary of the frameworks that can distinguish a drone from a bird is provided.

By listening to the sound the drones make as they fly, the acoustic detection technique uses microphones to find them.

2. LITERATURE REVIEW:

A evaluation of unmanned aerial vehicle security concerns and strategies to mitigate them:

Over the last ten years, the usage of unmanned aerial vehicles (UAVs) for a variety of purposes has increased. Small unmanned aerial vehicles (UAVs) of a new generation have just become commercially available, underscoring the rising threat that these devices pose. In respect to mid-air collisions, terrorist attacks, unauthorised observation and reconnaissance, smuggling, and electronic eavesdropping, this research explores the security threat posed by unmanned aerial vehicles (UAVs). It also covers various UAV invasions in terms of their objectives and operator proficiency. Geofencing, detection techniques (like radar, resonance, RF release, and electro-optical (EO) sensing), electronic barriers (like command link jamming and appropriation, GNSS blocking and spoofing), and kinetic barriers (like gunfire down UAVs and net imprison using interceptor UAVs) are all part of UAV intrusion mitigation.

Modern study on drone recognition and categorization using machine learning

This article provides a comprehensive evaluation of a recent study on machine learning-based drone recognition and categorization that utilises a number of modalities. This study area has just recently emerged as a result of the rapidly rising commercial and recreational drone use and the accompanying danger to the security of the airspace. Sensor devices with radio frequency, radar, optical, and acoustic capabilities are among the technologies discussed. The overall conclusion of the study is that machine learning-based drone categorization appears to have a lot of promise and has seen a number of noteworthy individual contributions. But because most research is experimental, it might be difficult to compare the findings of several articles. The challenge of drone detection and classification currently lacks a comprehensive requirement-driven specification as well as reference datasets that would make it easier to compare different solutions.

A home-built Internet of Things-based intelligent drone surveillance system

Since there are so many different ways drones, also known as mini-unmanned aerial vehicles, may be utilised for surveillance, photography, agriculture, communications, and other public services, their use has increased. However, the usage of amateur drones comes with a number of privacy, security, and safety risks. A important, largely unexplored answer to these issues is amateur drone surveillance. The first section of this essay provides a quick summary of the most current findings on amateur drone surveillance. The Dragnet concept is then shown utilising the recently established Cognitive Internet of Things architecture and is particularly designed for amateur drone surveillance. Following a discussion of the technological difficulties and unresolved problems, the major enabling techniques for Dragnet are addressed in great depth. Additionally, we offer a case study that illustrates how amateur drones that are legal and unlawful may be distinguished from one another. In this case, only approved drones are permitted to fly above a significant event.

Multistatic radar categorization of loaded and unloaded micro-drones

The preliminary results presented in this letter address the detection and categorization of hovering micro-drones shipping various payloads using multistatic radar and micro-Doppler analysis. The classification procedure makes use of two crucial variables relating to the centroid of the micro-Doppler signature, and the advantages of using data from a multistatic radar system as opposed to a traditional monostatic one are also looked at. With an accuracy rate of over 90%, the categorization of hovering micro-drones has done remarkably well.

Multirotor drone detection and categorization in radar sensor networks

Recent technology advancements have led to the development of a latest invention of unmanned aerial vehicles (UAVs) that are minute and affordable. Small UAVs, often known as drones, are expanding previously unimaginable possibilities while simultaneously creating new safety concerns due to the potential for abuse (such as for eavesdropping, drug trafficking, and terrorist strikes). The three main obstacles to drone identification—detection, potential verification, and classification—are looked at in this article. Modern surveillance systems employ a system of geographically scattered sensors, which are explained in more depth below, to ensure full coverage of the monitored region. The rate of recurrence modulated continuous wave (FMCW) radar sensor is the main focus. This vital technology is all the more crucial since it is low-cost, reliable across vast distances, and has excellent lighting and weather resistance. In this article, we examine the most effective techniques used at several identification phases, including the detection of potential drone presence, target confirmation, and categorization.

Intrusion detection techniques for vision-based sense-and-avoid systems

The detection of intruders is a significant point of contention for vision-based Sense and Avoid (SAA) systems. This research proposes a deep characteristic learning-based intrusion recognition system. Four steps make up the intruder detection method: collecting test samples, amassing an extremely broad vocabulary, deep feature learning, and pinpointing the invader's position. The procedure for gathering test samples involves sliding windows. The K-means Singular Value Decomposition (K-SVD) is used for extensive glossary training. We extract features based on the dictionary using the deep feature learning technique. The invasion region is eventually established by integrating the overlapping regions of interest (ROI) after the area of interest (ROI) has been chosen using the support vector machine (SVM). The experiment's findings show that the algorithm works well in a range of lighting, weather, and viewing situations.

Implementing a detection and tracking system for tiny unmanned aircraft systems:

Unmanned aircraft systems (UAS) are becoming more and more popular for video surveillance since they offer valuable video data while offering less hazards than human operators. Due to its advantages, UAS traffic roughly doubles in volume every year. However, there are additional risks associated with UAS. The FAA predicts that there will be constant increase and a doubling of aircraft traffic over the next 20 years. Along with the UAS traffic's exponential increase, collision risk and privacy issues are also increasing. For the safety of air traffic, a reliable UAS recognition and/or tracking mechanism is required. This project attempts to design a system that can sense or identify a UAS in order to be able to take action against one. The future system will locate a UAS using a variety of techniques, including as mechanical tracking and image analysis. Once a UAS has been detected, the tracking system may also be used in conjunction with a countermeasure. We present the system's design, algorithms, implementation specifics, and certain performance characteristics in this paper. The suggested approach will aid in preventing malicious or destructive UAS from penetrating residential zones or other restricted places.

3. METHODOLOGY

Deep Neural Network (DNN)-based classifiers can recognize and classify drones by examining their frequency signatures. Using a simple feed forward DNN and a given dataset, the author was able to recognize and discriminate between three commercial drones. By a convolutional neural network (CNN), the author showed how to detect, identify, and categorize the same dataset. More investigation on the effect of noise on detection accuracy was not possible due to the small dataset used in this study. Furthermore, it was not looked at how well detection works when there are plenty of signals or interference.

Disadvantages:
1. There is currently no valid approach in the literature for classifying and identifying drones.
2. A reduced categorization rate.
The YOLOV5 algorithm is used in our newly announced RF-based drone detection system to identify and classify drones. Here, we developed a dataset called RF that comprises of pictures taken from various perspectives of 6 commercial drones. In order to accurately detect and categorize drones, it uses GoF (Goodness of fit) spectrum sensors and the MUSIC algorithm to predict DoA (Dead-On-Arrival). Wideband CFAR-based energy detection is used to illustrate feature extraction and drone detection capabilities. We provide drone categorization using a DRNN architecture. The categorization was less well done.

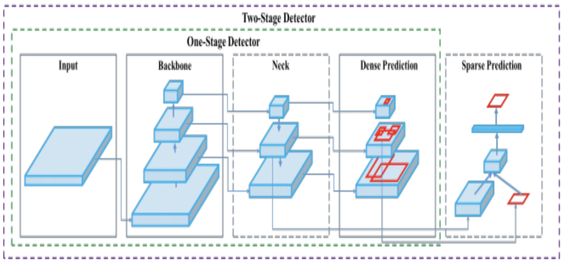


Fig2: System Architecture

Advantages:
1. We show how the YOLOV5 framework improves detection performance.
2. Using both techniques, we were able to acquire satisfactory detection and classification results. We particularly highlighted in the limitation discussion that while the classification is done under supervision, the performance may change when there are unidentified or more recent drone signals.
In order to complete the aforementioned project, we constructed the modules listed below.

- Data exploration: We will use this module to import data into the system.
- Processing: We shall read data in order to process it.
- Data splitting into train and test: Using this module, we will separate data into train and test.
- Model generation: We will construct the model using YOLOV5 and DRNN, with the accuracy of the algorithms determined.
- User signup & login: User registration and login are available using this module.
- User input: supplied via this module and
- Prediction: the final prediction is displayed.

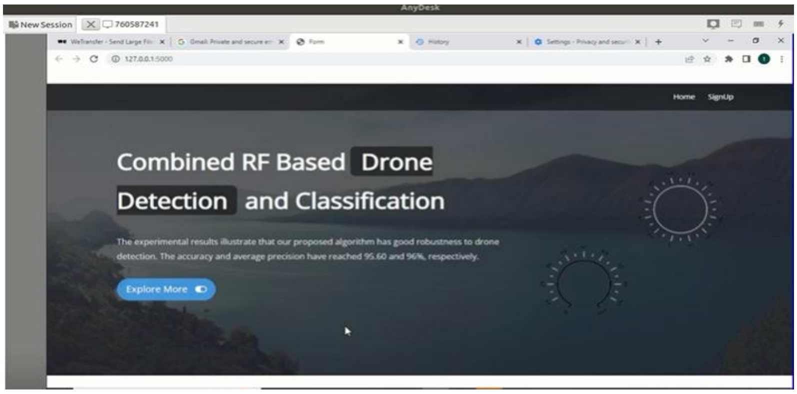
ALGORITHMS:
YOLOV5:
"You Only Look Once," or YOLO, is a metaphor for the object identification method, which divides images into grids. Finding the objects inside each grid cell is the cell's responsibility. YOLO is one of the most well-known methods for item recognition because of its accuracy and rapidity. Schematic representation of the YOLOv5-based Convolutional Neural Network (CNN). The head, neck, and backbone are the main parts. The BackBone uses CSPNet to mine features from the input photographs' images. The pyramid feature is created with The Neck. Additionally, it does not appear to be less accurate than YOLOR. Data labelling, data quality, and parameter optimization

have a significant impact on the mean average accuracy of YOLOR and YOLOv5.

DRNN:

Over the previous ten years, the usage of unmanned aerial vehicles (UAVs) for a variety of purposes has increased. Small unmanned aerial vehicles (UAVs) of a novel generation have just become commercially available, underscoring the rising threat that these devices pose. In respect to mid-air collisions, terrorist attacks, unauthorized observation and reconnaissance, smuggling, and electronic eavesdropping, this research explores the security threat posed by unmanned aerial vehicles (UAVs). It also covers various UAV invasions in terms of their objectives and operator proficiency. Geofencing, detection techniques (like radar, acoustic, RF emission, and electro-optical (EO) sensing), electronic barriers (like command link blocking and appropriation, GNSS jamming and spoofing), and kinetic barriers (like gunfire down UAVs and net capture using interceptor UAVs) are all part of UAV intrusion mitigation.

4. EXPERIMENTAL RESULTS



Combined RF Based Drone Detection and Classification

The experimental results illustrate that our proposed algorithm has good robustness to drone detection. The accuracy and average precision have reached 95.60 and 96%, respectively.

Fig3: Home Page

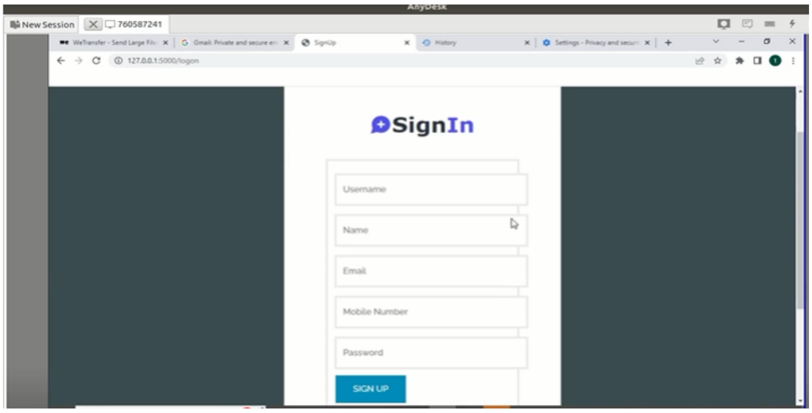


Fig4: User signup

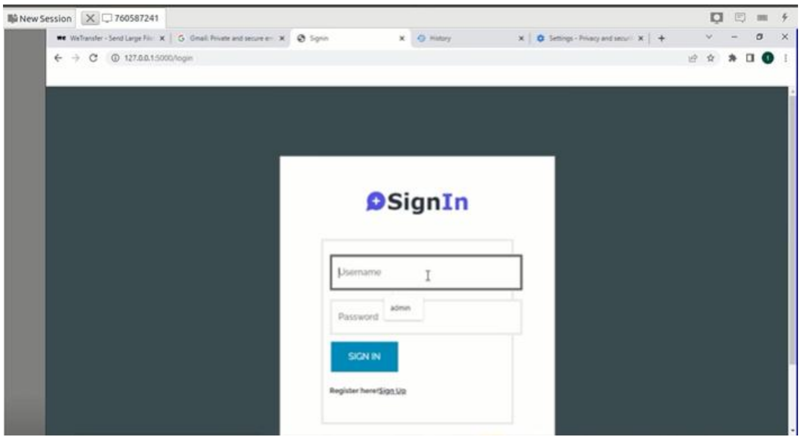


Fig5: User Signin

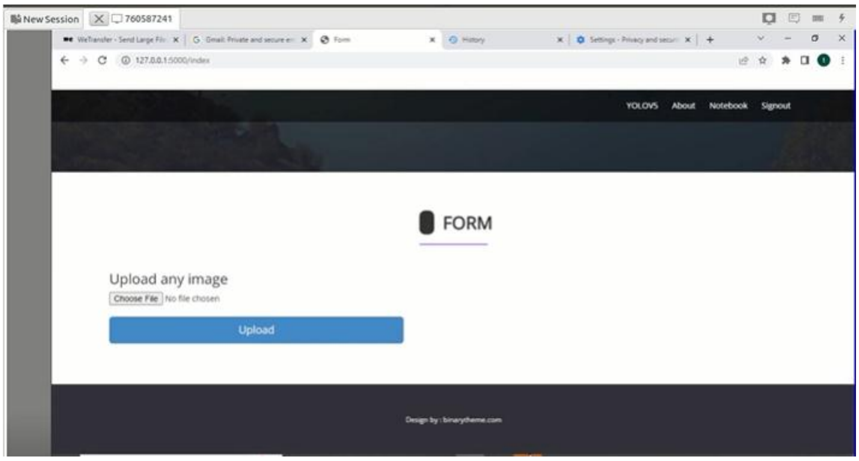


Fig6: Main screen

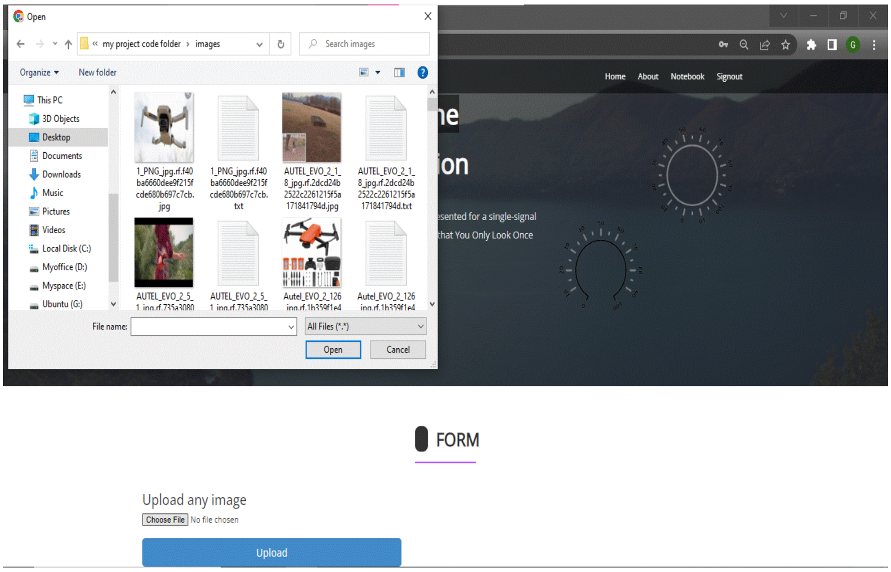


Fig7: User input

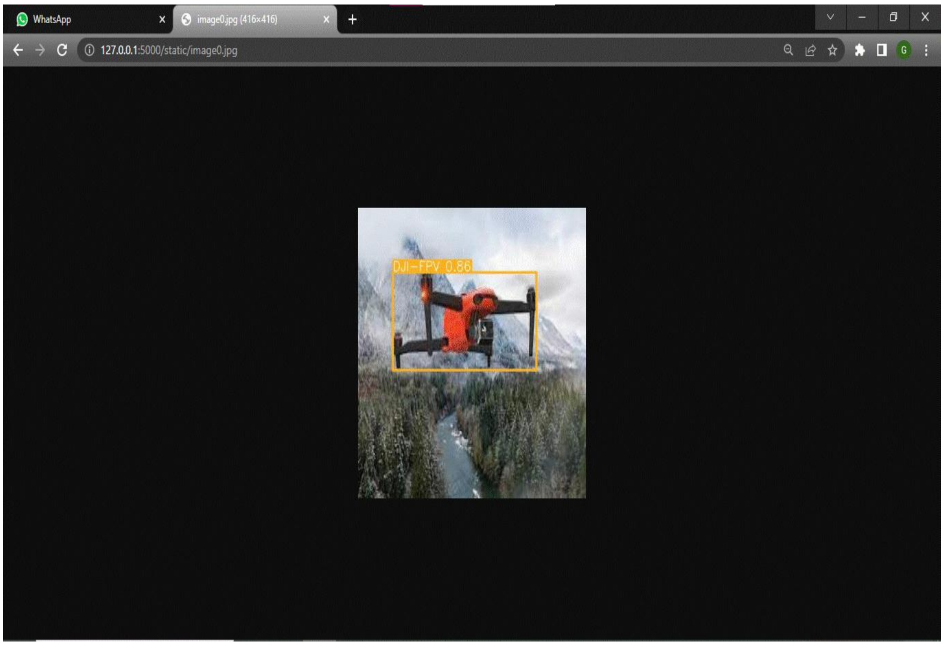


Fig8: Prediction Result

5. CONCLUSION AND FUTURE ENHANCEMENT

Conclusion:
Drones have been identified and recognized using YOLOV5 and DRNN algorithms. YOLOV5 makes use of state-of-the-art technology and recognizes drone photographs from various angles and sizes more successfully. While DRNN detects and classifies drones with less precision. In noisy datasets, YOLOV5 also classifies and recognizes drone photos. Therefore, we draw the conclusion that YOLOV5 recognizes and categorizes pictures more correctly than DRNN.

Future Enhancement:
Since we are eager in creating a strong system that can identify and categorize any drones regardless of the dataset it is provided with, we will study the unsupervised scenarios in the forthcoming work.

6. REFERENCES

D. Sathyamoorthy, “A review of security threats of unmanned aerial vehicles and mitigation steps,” J. Defence Security, vol. 6, no. 1, pp. 81–97, 2015.

B. Taha and A. Shoufan, “Machine learning-based drone detection and classification: State-of-the-art in research,” IEEE Access, vol. 7, pp. 138669–138682, 2019.

G. Ding, Q. Wu, L. Zhang, Y. Lin, T. A. Tsiftsis, and Y.-D. Yao, “An amateur drone surveillance system based on the cognitive Internet of Things,” IEEE Commun. Mag., vol. 56, no. 1, pp. 29–35, Jan. 2018.

F. Fioranelli, M. Ritchie, H. Griffiths, and H. Borrion, “Classification of loaded/unloaded micro-drones using multistatic radar,” Electron. Lett., vol. 51, no. 22, pp. 1813–1815, 2015. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/el.2015.3038 [5] J. Drozdowicz et al., “35 GHz FMCW drone detection system,” in Proc. 17th Int. Radar Symp. (IRS), 2016, pp. 1–4.

A. Coluccia, G. Parisi, and A. Fascista, “Detection and classification of multirotor drones in radar sensor networks: A review,” Sensors, vol. 20, no. 15, p. 4172, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/15/4172

Z. Zhang, Y. Cao, M. Ding, L. Zhuang, and W. Yao, “An intruder detection algorithm for vision based sense and avoid system,” in Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS), 2016, pp. 550–556.

S. R. Ganti and Y. Kim, “Implementation of detection and tracking mechanism for small uas,” in Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS), 2016, pp. 1254–1260.

R. Stolkin, D. Rees, M. Talha, and I. Florescu, “Bayesian fusion of thermal and visible spectra camera data for mean shift tracking with rapid background adaptation,” in Proc. IEEE SENSORS, 2012, pp. 1–4.

A. Coluccia et al., “Drone-vs-bird detection challenge at IEEE AVSS2019,” in Proc. 16th IEEE Int. Conf. Adv. Video Signal Based Surveillance (AVSS), 2019, pp. 1–7.

M. Nijim and N. Mantrawadi, “Drone classification and identification system by phenome analysis using data mining techniques,” in Proc. IEEE Symp. Technol. Homeland Security (HST), 2016, pp. 1–5.

M. Benyamin and G. H. Goldman, Acoustic Detection and Tracking of a Class I UAS with a Small Tetrahedral Microphone Array, Army Res. Lab., Adelphi, MD, USA, Sep. 2014.

J. Busset et al., “Detection and tracking of drones using advanced acoustic cameras,” in Proc. Unmanned/Unattended Sens. Sens. Netw. XI Adv. Free-Space Opt. Commun. Techn. Appl., vol. 9647, Oct. 2015, Art. no. 96470F.

P. Nguyen, M. Ravindranatha, A. Nguyen, R. Han, and T. Vu, “Investigating cost-effective RF-based detection of drones,” in Proc. 2nd Workshop Micro Aerial Veh. Netw. Syst. Appl. Civilian Use, 2016, pp. 17–22. [Online]. Available: https://doi.org/10.1145/2935620. 2935632

P. Kosolyudhthasarn, V. Visoottiviseth, D. Fall, and S. Kashihara, “Drone detection and identification by using packet length signature,” in Proc. 15th Int. Joint Conf. Comput. Sci. Softw. Eng. (JCSSE), 2018, pp. 1–6.

I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, and S. Zappatore, “Blind detection: Advanced techniques for WiFi-based drone surveillance,” IEEE Trans. Veh. Technol., vol. 68, no. 1, pp. 938–946, Jan. 2019.

M. F. Al-Sa’d, A. Al-Ali, A. Mohamed, T. Khattab, and A. Erbad, “RFbased drone detection and identification using deep learning approaches: An initiative towards a large open source drone database,” Future Gener. Comput. Syst., vol. 100, Nov. 2019, pp. 86–97.

S. Al-Emadi and F. Al-Senaid, “Drone detection approach based on radio-frequency using convolutional neural network,” in Proc. IEEE Int. Conf. Inform. IoT Enabling Technol. (ICIoT), 2020, pp. 29–34.

M. M. Azari, H. Sallouha, A. Chiumento, S. Rajendran, E. Vinogradov, and S. Pollin, “Key technologies and system trade-offs for detection and localization of amateur drones," IEEE Commun. Mag., vol. 56, no. 1, pp. 51–57, Jan. 2018.

P. Stoica, S. Basak, C. Molder, and B. Scheers, "Review of counter-uav solutions based on the detection of remote control communication," in Proc. 13th Int. Conf. Commun. (COMM), 2020, pp. 233–238.

T. K. S Rathish Babu et al., "MLPNN-RF: Software Fault Prediction based on Robust weight optimization and Jacobian Adaptive Neural Network", 'Concurrency and Computation Practice and Experience", DOI: 10.1002/cpe.7122 ISNN: 1532-0634(2021).