



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.165



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

Anti – Drone System using Image Processing

Yogapriya Thirumurthy, Yasmin Immaculate. S, Dr. G. Rohini

UG Student, Dept. of E.C.E., St. Joseph's Institute of Technology, Chennai, Tamil Nadu, India

UG Student, Dept. of E.C.E., St. Joseph's Institute of Technology, Chennai, Tamil Nadu, India

Professor & Supervisor, Dept. of E.C.E., St. Joseph's Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: An unmanned aerial vehicle (UAV), commonly known as a drone, is an aircraft without any human pilot, crew, or passengers on board. UAVs are a component of an unmanned aircraft system (UAS), which includes adding a ground-based controller and a system of communications with the UAV. The flight of UAVs may operate under remote control by a human operator, as remotely-piloted aircraft (RPA), or with various degrees of autonomy, such as autopilot assistance, up to fully autonomous aircraft that has no provision for human intervention. Consider connecting the use of the darknet framework for discovery and constructing a drone detection system to get to know a machine by utilizing drone detection based on deep learning. The device recognizes drones largely based on a live feed received from a USB camera or an uploaded photo on the Raspberry Pi using the darknet, the YOLOv3 algorithm, and OpenCV. The device captures drones when it is placed in a specific environment. Assembling the dataset, annotation, device education, and device testing are the four stages of the project technique. The challenge changed into being capable of picking out the drones with an average achievement rate of 99% and 100% from live films and uploaded photos, respectively. The task showed that because of deep learning strength, the detection changes into sturdy against modifications in light intensity, and the lifestyles of the background result in special environment situations.

KEYWORDS: Drone detection, detection system, detection using deep-Learning, UAVs, and Drones

I. INTRODUCTION

In recent years, drones have had tremendous development due to their low price and ease of use. Drones have been widely utilized in many application scenarios, which potentially pose great threats to public security and personal privacy. To mitigate these threats, it is necessary to deploy anti-drone systems in sensitive areas to detect, localize, and defend them against invading drones. This project provides a comprehensive overview of the technologies utilized for drone surveillance and the existing anti-drone systems. Then develop an anti-drone system with image processing, which combines multiple passive surveillance technologies to realize drone detection and localization. Furthermore, we discuss the challenges and open research issues of such a system.

Drones, that is, small unmanned aerial vehicles (UAVs), are experiencing explosive growth nowadays, and they have been widely used in many areas (aerial photography, traffic monitoring, disaster monitoring, etc.). They have attracted much research interest concerning path planning, secure communication, attack detection, and so on. Nevertheless, the increasing use of drones poses great threats to public security and personal privacy. For example, an attacker might strap explosives or other dangerous materials to a drone to carry out an attack; criminals can use drones to smuggle illicit materials across borders; an operator can control a drone carrying a high-fidelity camera to fly over walls and spy on inhabitants' private information. The increasing frequency of incidents caused by drones makes it necessary to regulate drone air traffic. A few drone manufacturers (e.g., DJI) have embedded geofencing software into their drones to prevent them from flying over security-sensitive areas (government buildings, airports, etc.). However, it is unrealistic for geofencing to cover every place and every drone. Therefore, it is of great significance to deploy an anti-drone system in a geofenced-free but security-sensitive area. Such an anti-drone system can detect a drone at the time it flies into a sensitive area and estimate its location for drone defense. Recent years have shown a noticeable rise in the number of incidents involving drones, related to both civilian and military installations. While drone neutralization techniques have become increasingly effective, detection most often relies on professional equipment, which is too expensive to be used for all critical nodes and applications. Therefore, there is a need for drone detection systems that could work on low-performance hardware. Its critical component consists of an object detection system.



In the past ten years, drone generation improvement for the reason that the first commercial drone was released at CES 2010 has created a couple of individuals and institutions to apply drones for a couple of functions. We are presently living in a time in which drones are being used for food shipping, the shipment of goods, and film filming and they may probably involve an extra factor in our lives close to destiny. Nonetheless, drones also pose an amazing project in terms of security and privacy inside the society (for both people and groups), and plenty of drone-associated incidents are reported each day. These events have become known as the focus of the need to locate and disable drones used for malicious intentions and began up a new research and development region for academia and enterprise, with a marketplace that is anticipated to cost \$1.85 billion by 2024. Computer vision is a method of the use of imagery, each pic, and video, to recognize devices. Computer vision obligations require techniques to accumulate, keep, interpret and recognize the facts in the photos. There are several strategies for laptop vision, which include image reputation, item localization, item identification, semantic segmentation, segmentation of times, etcetera, and falls under the Architectures of Object Detection. You Only Look Once (YOLO), is an approach to object detection the use of co-evolutionary neural networks for object detection. YOLO's key benefit is that it helps the tracking of artifacts in real-time. "YOLO" only looks at the complete picture as soon as, hence the name, "you only look once. This paper is an examination of the design and function of YOLO.

II. RELATED WORK

In 2020 Real World object detection dataset for Quadcopter unmanned aerial vehicle detection published in October, by Maciej L.Pawelczyk and Marek Wojtyra. In this paper, the entire 51446 training image dataset is used for training. While this number seems to be large enough to generalize the drone detection task with sufficient model performance, the exact number of images to be used seems large for a single class task. As such, multiple different training dataset configurations will be run to establish a point in which adding more images to the dataset does not provide sufficient improvement based on the testing dataset performance (the testing set will remain the same for comparison). Every model runs for 1 million iterations minimum for direct comparison with a model set established during research used for this paper. Artificial Neural Networks with many hidden layers, also called Deep Learning, have been known for decades, but 2012 ImageNet successes have shown a resurgence in their use with multiple successful industrial applications. For object detection purposes pretrained convolutions based (CNN) models can be used as the starting point to be fine-tuned on a drone dataset in a process called transfer learning

In 2021 Drone detection sensor with continuous 2.4 Ghz ISM band coverage based on cost effective SDR platform published in August, by Przemyslaw Flak. In this paper, a cost-effective RF sensor with data pre-processing for commercial dronedetection and its hard-ware implementation was presented. The single receiver was used to deliver a spectrum estimator of the entire 2.4 ISM GHz frequency band by the USB interface instead of raw IQ data. Therefore, the entire processing power of the companion computer software can be utilized for neural network-based or similar calculations without the need to pre-evaluate any time-frequency domain transformation. Besides, after selecting the binarized output mode for the STFT detection approach, the computing power requirement can be reduced even further. The verification results showed no significant impact on the observed signal shape obtained by the adapted approximation techniques over accurate calculations and reference device indications. This leads to the conclusion that the proposed sensor can be used for creating the new drone RF classification dataset. In terms of dwell time measurement, good performance was noted even in low SNR conditions, thanks to the advanced adaptive thresholding. The most relevant limitation of the proposed sensor compared to the USRP B210 is the lower gain of the RF chain inside the LimeSDR-USB, which results in a 9 dB sensitivity reduction.

In 2021 Survey on Anti-Drone systems: Components, Designs and Challenges" published in March, 2021 by Seongjoon Park, Hyeong Tae Kim, Sangmin Lee and Hwangnam Kim. Modern detection solutions guarantee a certain level of drone detection accuracy by integrating multiple detection systems. Each methodology has performance limitations in terms of detection range, functionality, weather dependency, etc., so the anti-drone industry tends to construct hybrid detection systems. However, administrators should analyze the defense area to design optimal detection systems and improve drone detection efficiency. This survey suggests a guideline for installing an anti-drone detection system considering efficiency and priority. The proposed guidelines include abstract classifications for detection equipment, priority classification for defended areas, and actual system deployment examples for airports, industrial

facilities, and airspaces. Detection systems should be tightly coupled with fine grained drone identification networks to provide a viable drone tracking and neutralization solution.

In 2018 Anti-Drone system with multiple surveillance technologies: Architecture, Implementation and Challenges published in April, by Xiufang Shi, Chaoqun Yang, Weige Xie, Chao Liang, Zhiguo Shi and Jiming Chen. This article gives a comprehensive review of four of the most widely used surveillance technologies in drone detection and localization, and also summarizes existing anti-drone systems. Then an anti-drone system, called DEZJU, is developed which combines three passive surveillance technologies. Experimental results show that our system can detect and localize the intruding drone in a campus environment. RF jamming to the detected drone is also available if necessary. Furthermore, it discusses the challenges and open research issues in such a system.

In 2020 Drone detection experiment based on Image Processing and Machine Learning published in February, by Giao N.Pham. This paper proposes an effective solution to detect drones based on image processing. The proposed solution used the Haar-like features to detect drones from frames captured by a single camera. The proposed solution is implemented and experimented with both indoor and outdoor environments. It could accurately detect almost all cases. The proposed solution is simple and easy to implement for personal purpose applications for any place. The proposed solution is also flexible to developers. Because developers can use their training dataset to develop their applications for specific purposes. This is an advantage of this solution. In the future, big datasets can be collected to improve the accuracy of the proposed solution and experiment with the proposed solution with many places.

III. PROPOSED ALGORITHM

A. Design Software:

A darknet is an Internet overlay network that may handiest be accessed with special software, settings, or permissions, and additionally uses a completely unique protocol for personalized verbal exchange. Social networks (normally used for document website hosting with a peer-to-peer link) and anonymity proxy networks such as Tor through anonymous connection collection are not unusual darknet forms. The phrase 'darknet' changed into popularized by means of fundamental news shops to connect services with Tor Onion, while it became used by the notorious Silk Road drug bazaar, regardless of the language being unofficial. Technologies which include Tor, I2P, and Freenet had been advanced to guard virtual rights thru encryption, anonymity, or resistance to censorship, and are used for each unlawful and valid functions. Darknets additionally, promote anonymous contact among whistleblowers, activists, newshounds and information media through the usage of packages along with Safe Drop. It is open supply and written in C/CUDA and serves as the premise for YOLO. Darknet is a platform for schooling neural networks. Darknet is used as the YOLO schooling platform, which means it sets the network structure. Darknet is a neural network architecture written in C and CUDA is open source. The Darknet, but is neural community architecture written in C and CUDA that is open supply. It is fast, easy to put in and helps computations for the CPU and GPU. Each of those cells is chargeable for predicting 5 bounding boxes: YOLO splits the picture right into a grid of 13 by way of 13 cells. It applies the complete picture to a single neural community. For each region, this community splits the image into regions and predicts bounding packing containers and probabilities. The regions concerned are selected for the use of co-evolutionary neural networks and are graded. Like YOLO, which comes underneath the regression organization, the set of rules in a single run, it predicts object instructions and makes use of a single neural community to stumble on a couple of objects inside the photos. It is simpler to make much less localization mistakes because YOLO looks at the whole picture to expect artifacts at the man or woman cells. The set of rules has the capability to deal with 45 frames per second. YOLO consists of a neural community structure, Darknet, for training. Three current versions of YOLO are to be had. The variants of YoloV1, YoloV2 and YoloV3 are the Yolo versions. There are 24 layers in overall inside the very first model of Yolo, with 24 convolutional layers followed by means of 2 absolutely related layers. When detecting small objects, the algorithm become now not successful, and this turns out to be the huge hassle of YoloV1. There are 30 layers in total in YoloV2 without completely related layers. A batch normalization layer is accompanied by any Convolution layer and Anchor bins are introduced in this model. This algorithm also did not detect small items and became located to be a multi-class problem as nicely. The new edition that makes use of 106 neural community layers is YoloV3. Considering nine anchor packing containers, three are expected according to class.

And as a result extra bounding packing containers. In this the multiclass problem is translated into a multipliable trouble. For small artifacts, the algorithm works nicely, and this turns out to be an amazing result. OpenCV (Open Source Computer Vision Library) is a software program library for open supply pc vision and machine mastering. OpenCV has been created to provide a shared infrastructure for programs for laptop vision and to speed up using system perception in consumer merchandise. It has interfaces which include C++, Python, Java and MATLAB and helps Windows, Linux, Android and Mac OS. OpenCV leans typically toward actual-time vision applications and wherein to be had, takes advantage of MMX and SSE commands. Right now, a complete CUDA and OpenCV interface is being actively evolved. There are over 500 algorithms that compose or suggest those algorithms and about 10 times as many features. OpenCV is natively written in C++ and has a templated interface that works with STL boxes seamlessly.

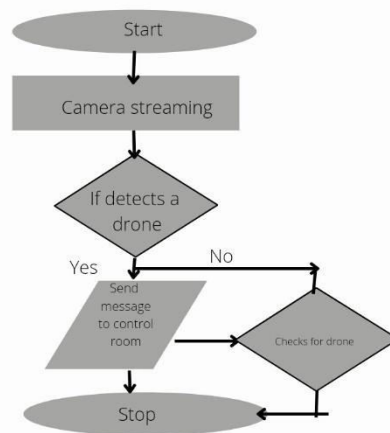


Fig 1. Drone detection circuit flow chart

B. Description Hardware:

The main signal processing chip unit used in the Raspberry Pi system is a Broadcom 2835 700MHz Chip in which the CPU core is a 32-bit ARM1176JZF-S RISC processor designed by Advanced RISC Machines. This main processing chip connects a camera and display. The Raspberry Pi design does not include a built-in hard disk or solid-state drive, instead of using an SD card for booting and long-term storage. This board is intended to run Linux Debian-based operating systems. This Raspberry Pi module has a Samsung class 4 micro SD card preloaded with the Raspberry Pi NOOBS (New Out of Box Software) package, and a printed Micro SD card adaptor. Raspberry Pi board (Model B). B.Camera Interface The camera module used in this paper is the raspberry pi camera module as shown The camera module plugs into the CSI connector on the Raspberry Pi. It's able to deliver a clear 5MP resolution image or 1080p HD video recording at 30fps. The camera module attaches to Raspberry Pi by a 15-pin Ribbon Cable, to the dedicated 15-pin MIPI Camera Serial Interface (CSI), which was designed especially for interfacing to cameras. The CSI bus is capable of extremely high data rates, and it exclusively carries pixel data to the BCM2835 processor.

The proposed method uses the raspberry pi board as the main controller. The latest version of raspbian wheezy is used on the board. After installing the OS to the board connect all the necessary hardware components and switch on the power supply. It starts booting up the Board and log in to the raspberry pi by username and password. It operates on the Linux Debian arch operating system. It mainly works on the python software and checks the network settings to update the python software by commands in the terminal window. Following packages are to be installed for implementing the proposed model. Installation commands have been listed below.

```

Sudo apt-get install python-matplotlib
Sudo apt-get install python-numpy
Sudo apt-get install python-scipy
Sudo apt-get install python-imaging
    
```

Enable the camera settings on the board to capture the image and save it on the folder. Run the python code to check the enhancement algorithms and remove the noise present in an image. The proposed method implementation is shown in the flow chart.

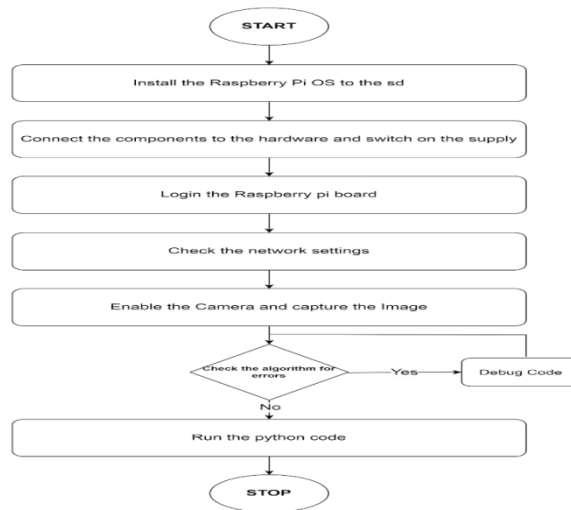


Fig 2. Drone detection setup Flowchart

IV. SIMULATION RESULTS

In this paper, we have developed an image processing system, which is operated using OpenCV and Raspberry-pi. A software code embedded into the microcontroller controls the working of various camera modules and buzzers on the system. Receivers receive the video signals from the camera and will be able to record the video. The camera mounted with Raspberry Pi performs face recognition to identify the intruder. At last, a software component is used to alert the caught intruder. Alert emails are also generated by the system.

Data Collection

The collected and amassed dataset of more than 3,three hundred pics from the motion pictures and images changed into divided by 20% for checking out and eighty% for the detection device training which might be amassed from the field. This became targeted on the majority doing the best exercise. During this procedure, deletion of the unwanted pics become additionally executed. We have completed multiple frames and snapshots in more than five one-of-a-kind locations with distinct light settings, to support us through feeding the system with the detection of the drone and increasing the accuracy of the detection for the drones. The heritage in filmingthe drone plays a huge function of the detection and enhancing the accuracy for the drone detection

Converting the videos into photos:

By the use of the OpenCV, we were capable of saving the film frames as an Image every five frames, wherein we're using the equation $x=30/5$ where x is the saved body. This is a vital step to assist us to gather an increasing number of photographs for the drone to feed or insert into the system. Whereas, the OpenCV can smash these videos into body photos Annotation: We had been able to annotate the drone's photos via using labeling, and every photo accrued turned into annotated the usage of labeling as proven in discern 6. The label used to become "drone" for every photograph. The output changed into an XML record containing the drone's coordinates. LabelIng is an annotation method for graphical pics. It's written in Python and its graphical interface uses Qt. Annotations are saved in PASCAL VOC, the layout used by ImageNet, as XML files. In addition, the YOLO layout is likewise supported.

Annotating Images by way of Using YOLOv3 Format Training the system:

After we've gathered the movies and images with one-of-a-kind backgrounds, breaking them into hundreds of frame photos and labeling every one of them with the drone, we used eighty % of the accrued dataset for the education of the gadget to help identify the photographs/photographs of the drones. Moreover, 80% of the selected pixels have been randomly selected so that it will help us in selecting extra backgrounds, lights, and the distances of the drone captured from the camera, without focusing on one precise standard.

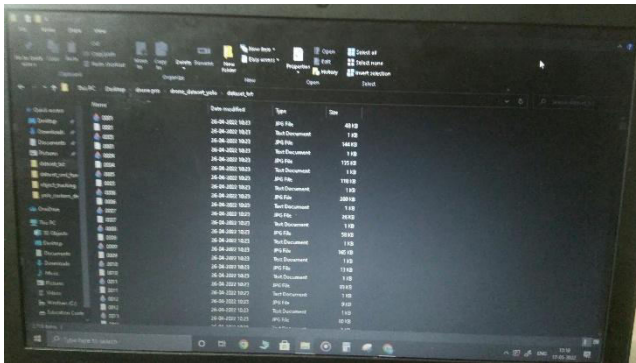


Fig 3. Drone Dataset



Fig 4. Drone detection output

V. CONCLUSION AND FUTURE WORK

We propose an end-to-end, complete autonomous drone surveillance system based on RGB cameras and computer vision. Considering the needs of this two-camera system, a detailed framework has been built, consisting of algorithms and policies for detection, tracking, and recognition. The proposed scheme can be used partially or fully for other video surveillance tasks rather than counter-drone activity, after proper modifications. Our system, in collaboration with a static wide-angle camera and a rotating low-angle camera, has been proven to provide plausible results based on simulations and field tests. One advantage of the system is the limited GPU memory requirement which makes it affordable.

After in-depth experimentation, it has been concluded that separating the resource exhaustion detector architecture from the lower input size classifier can be a conceivable strategy. A lightweight version of the YOLOv3 architecture is used for detection tasks with several filters as small as possible. We have observed that even with this significantly thinner architecture, small drones can be detected with a drastically low false alarm rate. However, this strategy would not always detect only intended objects; therefore, this part of the system should be treated as a primary filter for candidate targets.

In addition to this, we have developed and presented an autonomous intelligent tracking policy, where suspicious airborne targets are examined in detail with a lower-angle camera. Probably, the most innovative contribution of this paper is the proposal of a basic method, where frames coming from multiple cameras are overlaid with a proper configuration, and an object detection algorithm with deep learning is executed once. To the best of our knowledge, this is the first similar attempt in the literature.

Our multi-camera scheme can be accompanied by more complex re-identification (ReID) algorithms in the future, which offer significant performance augmentation. Literature on ReID primarily has been focused on person/pedestrian tracks. In future developments, we would like to apply a similar approach to track drones (and other airborne objects), starting from their initial detection on primary, static wide-angle cameras, until the end of the recognition process with secondary zoomed cameras.

To draw a conclusion, we can firmly state that using a very lightweight (in terms of filter count) deep YOLO architecture (properly and adequately trained with a voluminous dataset) shall give high performance in terms of precision and accuracy compared to conventional object detection methods while attaining a similar FPS and memory consumption. As mentioned previously, this architecture would not be a front-end recognition system, but serve as a primary candidate target location finder.

REFERENCES

1. U. GHEORGHE, D. ALEXANDRA, AND O. MIHAELA, —UNMANNED AERIAL VEHICLE IN MILITARY OPERATIONS, SCIENTIFIC RESEARCH AND EDUCATION IN THE AIR FORCE-AFASES, pp. 199-205, 2016.
2. S. Pedrozo, —Swiss Military Drones and the Border Space: A Critical Study of the Surveillance Exercised By Border Guards, Geogr. Helv., vol. 72, pp. 97–107, 2017.
3. A. Restas, —Drone Applications for Supporting Disaster Management, World Journal of Engineering and Technology, vol. 3, pp. 316-321, 2015.
4. How to Fly a Drone. UAV Coach Company. <https://uavcoach.com/how-to-fly-a-quadcopter-guide/> (accessed on 5 September 2019).



5. S. Lee, and Y. Choi, —Reviews of Unmanned Aerial Vehicle (Drone) Technology Trends and its Applications in the Mining Industry,| Journal Geo-system Engineering, vol. 19, pp. 197-204, 2016.
6. G. David, —Drone Applications for Environmental Management in Urban Spaces: A Review,| International Journal of Sustainable Land Use and Urban Planning, vol. 3, pp. 1-14, 2016.
7. Could Airbus drone detection system help protect planes?
<https://www.dailypost.co.uk/business/businessnews/could-airbus-drone-detection-system-11200748>, (accessed on 5 September 2019).
8. Drone Detection Systems. <https://coherentreceiver.com/1094/drone-detection-systems> (published 5 September 2019).
9. B. Nuss, L. Sit, M. Fennel, J. Mayer, T. Mahler, and Z. Thomas, —MIMO OFDM Radar System for Drone Detection,| Proc. of 18th International Radar Symposium, pp. 1-10, Prague, June 2016.
10. K. W. Lee, K. M. Song, J. H. Song, C. H. Jung, W. K. Lee, M. J. Lee, and Y. K. Song, —Implementation of Radar Drone Detection Based on ISAR Technique,| The Journal of Korean Institute of Electromagnetic Engineering and Science, vol. 28, pp. 159-162, 2017.



INNO  SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

 **doi**[®]
CROSS **ref**

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details