EasyChair Preprint

№ 9608

A Machine Learning Based Adaptive Approach to Detect and Identify Drone Activities

Ankush Agarwal and Shikha Verma

January 21, 2023

A machine learning based adaptive approach to detect and identify drone activities

Ankush Agarwal[1], Shikha Verma[2]
[1]*Department of Computer Engineering and Application, GLA University, Mathura, India - 281406*
[2]*Indian Meteorological Department, Ministry of Earth Sciences, New Delhi, India – 110003*
ankushak28@gmail.com, shikha.crest@gmail.com

***Abstract*—Drones or Unmanned Aerial Vehicles (UAVs) are flying objects with sizes ranging from a few centimeters to a few meters and payloads ranging from a few grams to a few kilograms. As their use has increased in recent years, small size drones are constantly being used to perform a variety of activities. Simultaneously, the threat posed by drones to society, public security, and personal privacy is growing significantly. From the security point of view, drones allow the attacker to reach any target in any location and their applications range from weapon carriers to espionage capabilities. To mitigate and negate the impact of drones, there is an urgent requirement to develop and deploy counter-drone systems for the detection of incoming drone threats. Before going into details, let us understand why drone detection is such a challenging task. Considering the unique characteristics of drones in terms of speed, size, hovering and resemblance to birds, no standalone unique system will be able to provide sufficient detection, tracking and identification capabilities to ensure a reliable and effective approach against threats from drones. Therefore, the integration of several types of detection strategies is essential to detect and identify drones.**

Keywords—Anti-drone, Artificial Intelligence, Defence, Drone, Machine Learning

I. INTRODUCTION

Unmanned aerial vehicles (UAV) also known as drones are a class of aircraft that is suitable for outdoor operation and can fly at reasonable altitude without the onboard presence of a pilot. They can be controlled remotely using a reliable wireless communication system from the Ground Control Station (GCS).

The basic version of drones comes with a single camera along with a GPS unit, but nowadays they can be assembled with multiple visual sensors on a single drone with separate GPS units. With the emerging technology, drones are designed with advanced GPS mode, intelligent autopilot systems and advanced stabilization technology along with high-resolution visual sensors. These advanced drones are extremely dangerous when it comes to the security of the country. One of the major inescapable security concerns of advanced drones is surveillance by unauthorised people without seeking the permission of concerned authorities. The vision sensors mounted on surveillance drones are scalable and flexible, providing extensive surveillance coverage. They can perform unauthorised search operations to identify the target, and track and monitor its movement even in a hostile environment. The drones fitted with high-precision cameras can steal classified information even from high altitude in the form of still images and videos of a specific target, built-up or location, and sensitive area posing a serious threat to the country. The drone provides very high-resolution imagery along with the geotag information which depends on the sensor width, sensor height and focal length [1]. Some of the drones come with 'Follow me technology' which is programmed to automatically follow around an intruder, providing ample opportunities to film aerial shots of any location including prohibited areas. These drones are capable of tracking the subject by remaining stationary in the sky, following the motion of the subject and by rotating around its axis. This kind of advanced technology can be operated remotely by using GPS enabled devices such as mobile phones, tablets or GSC. By default, integrated GPS unit in drones geotags the visual outputs that include some essential parameters like geo-coordinates, timestamp, altitude etc.

Drones have now become an integral part of modern warfare [2]. Although border security forces are always on high alert to disrupt any malicious plans, the conventional approaches to monitor national borders have proven to be complicated. Many incidents from smuggling and narcotics to life-threatening attempts by the enemy using drones have been reported by officials. Drone surveillance from across the border is an alarming security indicator. These drones are programmed to identify patterns using artificial intelligence to cross the borders and conduct critical perimeter surveillance. Moreover, these drones can be equipped with a variety of payloads to fulfil the wide range of dangerous security threats.

A. Work done with drone

In recent years, drones have undergone substantial development. They have giant potential in the public and private domains. Drones have gained popularity due to low production and deployment cost, ease of use and their limitless applications in agriculture, surveillance, monitoring, disaster management and other important public services.

In agriculture, drone has been used to critically evaluate the performance of various classification techniques and to compute optimal vegetation index that helps to minutely classify the field classes with higher accuracy [3], [4]. Drone had also been used to minimize the effect of shadow in agriculture filed so that the field classes can be segregated correctly [5]. For the detection of joggled fishplate in railroad track, feature based template matching had been used on drone images [6]. A vision based approach had been used to monitor the track gauge with the help of drone images [7]. A neural network based change detection was computed for land terrain monitoring with the help of drone and satellite data [8]. They can also be used to monitor real time scenarios by providing the aerial view in terms of the live streaming. Now a days, it is used to evaluate the before and after condition and hence to compute the loss incur during disaster [9], [10].

With the rapid expansion of the drone industry, civilians are overtly exposed to this technology and their pervasive drone operations have surpassed the rules and regulations of security guidelines. This activity has become more common and causing potential privacy, safety and security threats to the country.

B. Work done in anti-drone

Nowadays, the access and use of drones becoming common raising a chance of stealing the private or secret information. There are certain scenarios where the drones can be used effectively to capture the vital information like in war zones, secret air-bases and similar other places. Thus, there is a need of anti-drone technology for the security measures. It can help to detect and identify the unknown drone that may breach the security by stealing the information at various red zones, sensitive and high tension areas like borders, air-bases, no-flying zone area etc.

Phillips et. al., observed that in case of tension at the borders, rapidly formed coalitions magnify the risk of sharing classified information [11]. This provides stealth drones with an plentiful opportunity to carry forward the desired task without being noticed. Utsav et. al. enhanced the working mechanism of the drone to monitor and control the high-altitude geographical region using IoT. It can also detect unwanted signals to increase the level of security and holds importance from the military point of view [12].

The framework of an autonomous drone is heavily influenced by Artificial Intelligence (AI) and Machine Learning (ML). Sriram et al. have suggested the implementation of a quad-copter in the Line of Control (LOC) for defence machinery maintenance and surveillance using AI/ML. With the help of autonomous operation in the defence sector, high sensitive borders and latest generation military machinery can be put under high accuracy top-notch surveillance [2]. Ma'sum et al., implemented a simulation of a warzone using AR. Drone quadrotor and Robot Operating System (ROS) platform that detected target and its position [13].

The extensive use of drones poses great threats to security and privacy. These security concerns call for an immediate emergence of anti-drone technology in sensitive areas. There is an urgent need to create diverse strategies for countering drones utilising various anti-drone techniques [14]. Therefore, we need to implement a robust framework across borders that can adopt state-of-the-art anti-surveillance technology to ensure security and peace.

Anti-drone systems are designed to address robust and sustainable systems that can detect, defend and neutralise intruding drones. Jurn et al. have used CNN deep learning algorithms to recognise and classify the drone, DOA (direction of arrival) algorithms and AOA (angle-of-arrival) algorithms for localisation [14]. In a study, Faster Region-based Convolutional Neural Network (R-CNN) with Residual Neural Network-101 (ResNet-101) was used to detect drones in simulation that gave 93.40% accuracy [15]. Dogru and Marques came up with the proposal of a ground-based aerial target detection system using Light Detection And Ranging (LiDARs), that was centred on sparse detections rather than dense point clouds, to identify drones along with the estimation of their motion and active track [16]. Another successful attempt was made to develop Field Programmable Gate Arrays (FPGA) based vision processing system for a low-cost UAV with a total flying weight of less than 3kg, which was tested using simulated and real aerial footage with a mission to detect distinct objects on the ground [17].

Although drones have numerous advantages, the biggest issue in these drones is their distinctive buzzing noise due to the spin of propellers, as it can blow the cover of spy drones. Such issues and limitations of drones can be taken into consideration to detect and neutralise them using the anti-drones system. To develop the undetectable stealth capabilities of drones, their noise is needed to be reduced significantly which can be done by using an affordable LiDAR sensor and 3D printed propellers [16].

Therefore, the objective is to detect, defend and neutralise the intruding drones to mitigate the infiltration attempts. The major challenges in drone operations are geo-rectification, ortho-rectification and calibration. The geo-rectification directly affects the positional accuracy of pixels within georeferenced remote sensing data and hence requires adjustment of those relative positions of points with one another. Geo-rectification applied to remote sensing imagery significantly improves the accuracy of geo-referencing by removing terrain, platform, and sensor-induced distortions [18]. Ortho-rectification removes the effects of image perspective (tilt) and relief (terrain) effects intending to provide a planimetrically correct image. This is important because with the increase in geometric resolution of modern visual sensors, the requirement for the geometric accuracy of ortho-rectification has also increased. The resultant ortho-rectified image allows for the accurate direct measurement of distances, angles and areas [19]. Regardless of how advanced drone technology has evolved, all drones require periodic calibration to assure accuracy. Calibrating a drone creates a massive difference in its operation and functionality. It is extremely important to calibrate if a drone is flying inconsistently or flying in a new location or if errors are encountered [20]. Therefore, the motivation of this paper is to provide a secure system that can detect, identify and helps to neutralise intruders' drones with less human intervention. This will help real-time monitoring of border areas round the clock and will help decision-makers to formulate security measures with minimum resources.

II. Dataset

The dataset for this study was created manually with more than 140 images of two distinct drones with varying backdrop features such as sky, ground and crop. The images of drone were shot during the daytime, which is at various altitudes. The dimension of the images was 4000 x 3000 pixels. To evaluate the performance of our machine learning model, we split the image dataset of drones into 70% and 30% for training and testing set respectively.

III. Methodology

The workflow of the proposed methodology is shown in the Figure 1. It is depicted from the figure that the live stream is taken as input from the vision camera, then the frames are extracted from the associated live stream. After extracting the frames, they are provided as an input to the machine learning model whose task is to detect and identify drones. A machine learning model is trained with various flying object that flew at low altitude such as birds, drones, and other similar objects. If a model detects the activity and identifies that activity as a drone, it will trigger an alarm and show a warning message to the authorities on the drone activity.

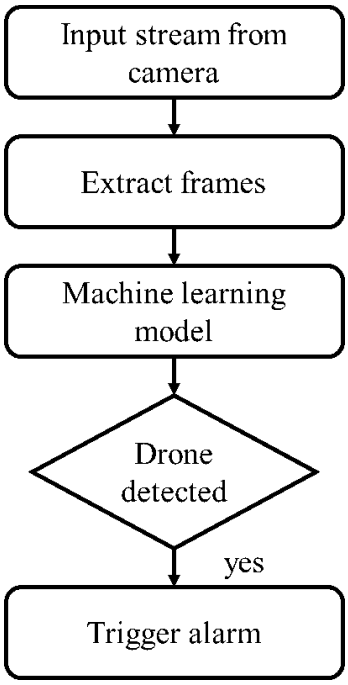

Figure 1: Workflow of the proposed approach

IV. Result and Discussion

The frames are extracted from the live stream that are given as input to the trained model. The model was trained using the pre-defined data to detect theft activity across the security regions. The model detected and identified the presence of a drone with an accuracy of more than 95%. The model was also able to distinguish between drone and other flying objects like birds, airplanes, etc. The model may be configured by the authorized user to set the threshold of confidence level as per the requirement. The model was tested to raise an alert with the threshold greater or equals to 80%, which triggered an alarm in terms of the warning message. The result obtained for the detection and identification of the drone along with the warning message is shown in Figure 2.

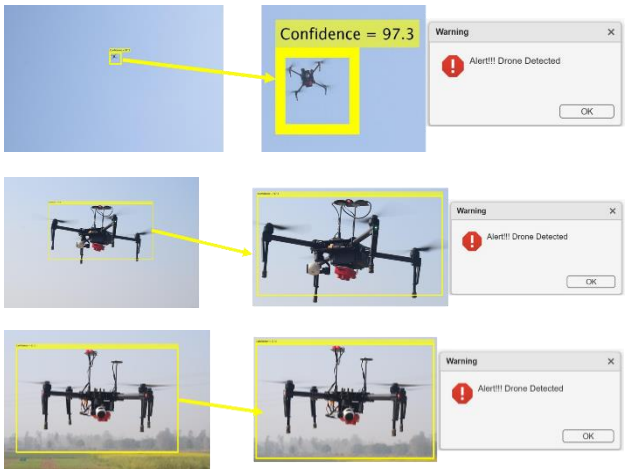

Figure 2: Output of the proposed approach

V. Conclusion

The work is devoted to the development of an anti-drone system using machine learning which is an effective approach of monitoring and tracking the activities of intruders' drones at national borders. We have proposed an approach that would ensure the detection of distinct objects and identification of drones, which automatically trigger the alarm to alert the authorities with the confidence of more than 80%.

Acknowledgement

We would like to thank all our colleagues, friends and family members who always inspired and motivated us to excel in this research.

References

[1] "GSD Calculator," *Propeller*. https://www.propelleraero.com/gsd-calculator/ (accessed Jun. 16, 2022).

[2] P. R. Sriram, S. K. Ramani, R. V. Shrivatsav, M. M.Mankiandan, and N. Ayyappaa, "Autonomous Drone for Defence Machinery Maintenance and Surveillance," in *2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4)*, Jul. 2019, pp. 288–292. doi: 10.1109/WorldS4.2019.8904014.

[3] A. Agarwal, A. K. Singh, S. Kumar, and D. Singh, "Critical analysis of classification techniques for precision agriculture monitoring using satellite and drone," in *2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS)*, 2018, pp. 83–88.

[4] A. Agarwal, S. Kumar, and D. Singh, "Development of Machine Learning Based Approach for Computing Optimal Vegetation Index with the Use of Sentinel-2 and Drone Data," in *IGARSS 2019-2019 IEEE International Geoscience and Remote Sensing Symposium*, 2019, pp. 5832–5835.

[5] A. Agarwal, S. Kumar, and D. Singh, "An adaptive technique to detect and remove shadow from drone data," *J. Indian Soc. Remote Sens.*, vol. 49, no. 3, pp. 491–498, 2021.

[6] A. Saini, A. Agarwal, and D. Singh, "Feature-based template matching for joggled fishplate detection in railroad track with drone images," in *IGARSS 2020-2020 IEEE International Geoscience and Remote Sensing Symposium*, 2020, pp. 2237–2240.

[7] A. K. Singh, A. Swarup, A. Agarwal, and D. Singh, "Vision based rail track extraction and monitoring through drone imagery," *Ict Express*, vol. 5, no. 4, pp. 250–255, 2019.

[8] A. Agarwal, S. Kumar, and D. Singh, "Development of Neural Network Based Adaptive Change Detection Technique for Land Terrain Monitoring with Satellite and Drone Images," *Def. Sci. J.*, vol. 69, no. 5, p. 474, 2019.

[9] A. Restas, "Drone Applications for Supporting Disaster Management," *World J. Eng. Technol.*, vol. 03, no. 03, p. 316, 2015, doi: 10.4236/wjet.2015.33C047.

[10] T. J. Tanzi, M. Chandra, J. Isnard, D. Camara, O. Sébastien, and F. Harivelo, "Towards 'drone-borne' disaster management: future application scenarios," Jul. 2016, vol. III–8, pp. 181–189. doi: 10.5194/isprs-annals-III-8-181-2016.

[11] C. E. Phillips, T. C. Ting, and S. A. Demurjian, "Information sharing and security in dynamic coalitions," in *Proceedings of the seventh ACM symposium on Access control models and technologies*, New York, NY, USA, Jun. 2002, pp. 87–96. doi: 10.1145/507711.507726.

[12] A. Utsav, A. Abhishek, P. Suraj, and R. K. Badhai, "An IoT Based UAV Network For Military Applications," in *2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Mar. 2021, pp. 122–125. doi: 10.1109/WiSPNET51692.2021.9419470.

[13] M. A. Ma'sum *et al.*, "Simulation of intelligent Unmanned Aerial Vehicle (UAV) For military surveillance," in *2013 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, Sep. 2013, pp. 161–166. doi: 10.1109/ICACSIS.2013.6761569.

[14] Y. N. Jurn, S. A. Mahmood, and J. A. Aldhaibani, "Anti-Drone System Based Different Technologies: Architecture, Threats and Challenges," in *2021 11th IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, 2021, pp. 114–119.

[15] A. J. Garcia, J. Min Lee, and D. S. Kim, "Anti-Drone System: A Visual-based Drone Detection using Neural Networks," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct. 2020, pp. 559–561. doi: 10.1109/ICTC49870.2020.9289397.

[16] J. Oh, D. Choe, C. Yun, J. Kim, and M. Hopmeier, “Towards the development and realization of an undetectable stealth UAV,” in *2019 Third IEEE International Conference on Robotic Computing (IRC)*, 2019, pp. 459–464.

[17] A. Price, J. Pyke, D. Ashiri, and T. Cornall, “Real time object detection for an unmanned aerial vehicle using an FPGA based vision system,” in *Proceedings 2006 IEEE International Conference on Robotics and Automation, 2006. ICRA 2006.*, 2006, pp. 2854–2859.

[18] University of New Mexico and C. Lippitt, “Georeferencing and Georectification,” *Geogr. Inf. Sci. Technol. Body Knowl.*, vol. 2020, no. Q3, Jul. 2020, doi: 10.22224/gistbok/2020.3.3.

[19] “orthorectification – OSSIM.” https://trac.osgeo.org/ossim/wiki/orthorectification

[20] “How to Calibrate a drone?,” *Fly Robotics*. https://www.fly-robotics.com/how-to-calibrate-a-drone/