IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Machine Learning Based Optical Surveillance System for Detection & Neutralization of Rogue Drones

Vijilesh Krishnan V.K(Assistant Professor, KMCTITM- Kuttippuram), MinuV S-(Former Assistant Professor, MESCE)

Sidharth K.P, Naeem Abullaise, Mohamed Faris RS, (Former Students of MESCE, Kuttippuram)

Abstract- Rogue Drones can potentially pose great threats to public security and personal privacy. To mitigate these threats, it is necessary to deploy an anti-drone system in the sensitive area to detect, localize and defend against the intruding drones. Our Drone detection System combines optical passive surveillance technology with machine learning to realize drone detection, localization, alarm alert system and radio frequency jamming. Anti-Drone Technology or drone defence system allows neutralization of any kinds of Drones in the area. Drones or Unmanned Aerial Vehicles (UAV) systems have been utilized by military forces for years. An Anti-Drone Technological implementation can play a vital role in the security of some countries and territories. Especially today, the terrorist threat is increasing and these threats have to be taken seriously. The low cost of Drones today could easily be used for everything from spying and surveillance to actually delivering terror from the sky. Big attention is now turning to proactive defence systems and Anti-drone technology. There is already a big choice on the market in this technology. It is possible to spot the drone targets from a range of 10km to 20km. fortunately, until now, there have not been any major attacks utilising drones. But as technology is developing more and more, the question is when, rather than if, a major incident will occur.

Keywords- Drones, Open-CV, Haar cascade, Arduino.

I. INTRODUCTION

Drones are small unmanned aerial vehicles (UAVs), experiencing explosive growth nowadays and they have been widely used in many areas, like aerial photography, traffic monitoring, disaster monitoring, etc. They have attracted many research interests with regard to path planning, secure communication, attack detection, and so on [1]-[4]. Nevertheless, the prevalent 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 the border; an operator can control a drone carrying a high- fidelity camera to fly over walls and spy inhabitants' private information. The increasing frequency of incidents caused by drones makes it necessary to regulate drone air traffic. A few drone manufactures, like DJI, have embedded geofencing software into their drones to prevent them from flying over security-sensitive areas, like 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 geofencing-free but security-sensitive area. Such a system should be able to detect the drone at the moment it flies into the sensitive area, and estimate its location and potentially flight path for drone defence, like jamming, triggering a siren or an alarm, or to seize control of the detected drone.

II. SYSTEM DESIGN

A. OpenCV

OpenCV (Open-source computer vision) is a library of programming functions mainly aimed at real time computer vision. It supports deep learning frameworks Tensor Flow, Torch or PyTorch and Caffe. OpenCV was built to provide a common infrastructure for computer vision applications and to accelerate the use of machine perception in the commercial products. OpenCV-Python makes use of NumPy, which is a highly optimized library for numerical operations with MATLAB-style syntax. All the OpenCV array structures are converted to and from NumPy arrays. We can see an example of drone detection using OpenCV in Fig 1.

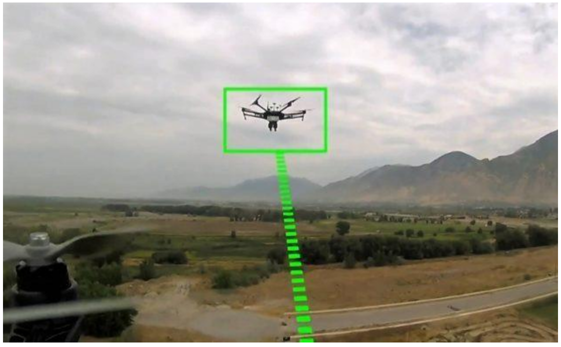

Fig 1: Drone detection

B.ARDUINO

Arduino is an open-source platform composed of hardware and software that allows for the rapid development of interactive electronics projects. The emergence of Arduino drew the attention of professionals from many different industries, contributing to the start of the Maker Movement. With the growing popularity of the Maker Movement and the concept of the Internet of Things (IoT), Arduino has become one of the main platforms for electronic prototyping and the development of MVPs. The Arduino Uno board, shown in Fig 2 contains several pins which can be programmed to operate using Arduino IDE. Arduino uses its own programming language, which is similar to C++. However, it's possible to use Arduino with Python or another high-level programming language. In fact, platforms like Arduino work well with Python, especially for applications that require integration with sensors and other physical devices. All in all, Arduino and Python can facilitate an effective learning environment that encourages developers to get into electronics design. We can control the Arduino by using python language. Firmata is an intermediate protocol that connects an embedded system to a host computer, and the protocol channel uses a serial port by default. The Arduino platform is the standard reference implementation for Firmata. The Arduino IDE comes with the support for Firmata. This could work perfectly with Odyssey-X86 with its onboard Arduino Core meaning that you can control the Arduino Core simply using Firmata protocol with different programming languages too. The Firmata library implements the Firmata protocol for communicating with software on the host computer. This allows you to write custom firmware without having to create your own protocol and objects for the programming environment that you are using. You would have to write lots of code on the Arduino to handle the requests coming across from python using pyserial, with pyfirmata the Arduino code is upload once and forget. The only code you would need to change is the python code on the python device.

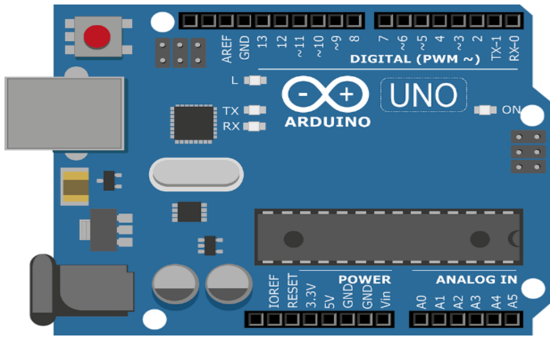

Fig 2: Arduino Uno

III. IMPLEMENTATION

A. Surveillance Technologies

Video: Drone detection based on video images is essentially an object detection problem in the area of computer vision and pattern recognition. An object can be detected based on its appearance features [8], colours, contour lines, geometric forms or edges, etc., or/and its motion features across consecutive frames [9]. Appearance feature-based methods have great difficulty in distinguishing drones from other similar small objects, like birds, in cluttered backgrounds without motion information. By comparing consecutive images, position and moving direction of a moving object can be determined by motion-based methods, which are also utilized for object tracking. It was suggested to distinguish a drone from birds by looking at the flight patterns, since a bird will fly in a more random pattern than a drone will. However, such method might fail when the bird is gliding. For drone detection, it is best to combine both motion features and appearance features, which would enable the detection with higher accuracy. On the other hand, even though object detection and tracking are based on video images, they still suffer from many issues, like occlusions, which also exist in drone detection and tracking.

Radio Frequency: The existing drones in the market or customized drones usually communicate with their controllers at some specific frequency bands, like 2.400-2.483GHz and 5.725-5.825GHz for DJI Phantom 4. However, in a practical environment, the existence of many other radio frequency signals, like Wi-Fi, which share the same frequency band with the drones, makes radio frequency-based drone detection challenging. One simple way is to monitor a wide range of radio frequency, like 1MHz-6.8GHz, and take any transmitter of unknown radio frequency signals as a drone. This method will induce a high probability of false alarms, since an unknown radio frequency transmitter is not necessarily a drone. It should be noted that the detection ranges are obtained from the existing systems, and they might vary with the type of drones, the surveillance environments, the hardware parameters and the corresponding algorithms.

B. Existing Anti-Drone Systems

There are already several commercial/military anti-drone systems, Orelia Drone-Detector1 are an audio-based detector, and are able to detect both fixed-wing and rotary wing drones. Its detection range can reach 100m when the background noise is less than 40dB. Another system, DroneDetector2, which was developed by Dronelabs, utilizes audio and radio frequency surveillance for drone detection and its detection range is reported to be 1km. Dedrone3 has several products including Drone Tracker, radio frequency sensor and Drone Jammer, etc. Drone Tracker combines microphones, optical cameras and Wi-Fi sensors, and it can detect a drone within 500m. Radio frequency sensor can detect all drones connected through radio frequency and Wi-Fi within 1km. Drone Jammer transmits radio frequency signals at multiple frequency bands via omni-directional antennas to disrupt the drone communication. ARDRONIS4, which was developed by Rohde&Schwarz, is based on radio frequency surveillance. For the drones using Frequency-Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) transmission systems, ARDRONIS builds a radio frequency library for drone detection. The detection range of ARDRONIS can be up to 1km-2km, which depends on radio frequency transmission power, radio condition and antenna gain. Apart from drone detection, ARDRONIS can realize localization of both the drone and its operator via direction finding. DroneShield5 provides an integrated detection and defence solution. It utilizes radar, audio, video and radio frequency surveillance for drone detection with nominal detection ranges being: 1.5km for radar, 200m for audio, 600m for video and 1km for radio frequency. Regarding drone defence, DroneShield also uses radio frequency jamming to cease the video transmission from the drone back to its operator. The nominal maximum jamming distance is 2km. Falcon Shield6 utilizes three surveillance technologies, radar, video and radio frequency, and can realize drone detection, localization and defence. However, the maximum effective range is unclear. AUDS7 combines radar and video surveillance. With radar, AUDS can detect a drone with a distance up to 3.6km. With radio frequency inhibition, AUDS can defeat drone communication at multiple frequency bands, like 433MHz, 915MHz, 2.4GHz, 5.8GHz and GNSS bands. We can see that most of these systems take more than one surveillance technologies, since multiple surveillance technologies can provide much more information for drone detection and localization. With regard to the realized functions, all of them can realize drone detection; some of them can realize both detection and localization; only two of them, Falcon Shield and AUDS, can simultaneously realize detection, localization and defence. Both Falcon Shield and AUDS have taken advantage of radar surveillance, which however is unsuitable to deploy in urban areas for all day and night monitoring. Motivated by the above observations, our objective is to develop a system which is suitable to deploy in urban areas and can timely detect, localize and defend against the intruding drones. Falcon Shield6 utilizes three surveillance technologies which are radar, video and radio frequency, and can realize drone detection, localization and defence. However, the maximum effective range is unclear. AUDS7 combines radar and video surveillance. With radar, AUDS can detect a drone with a distance up to 3.6km.

With radio frequency inhibition, AUDS can defeat drone communication at multiple frequency bands, like 433MHz, 915MHz, 2.4GHz, 5.8GHz and GNSS bands.

IV. ARCHITECTURE

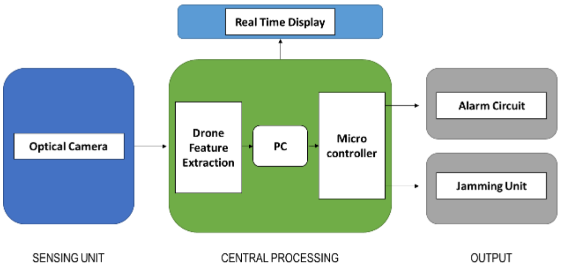

Fig 3: Architecture of Anti-Drone System

In this section we develop an anti-drone system, called which uses optical camera and sensing unit for surveillance. Fig. 3 shows the architecture of Anti-Drone System, which consists of four parts: sensing unit, central processing unit, output unit and real-time display unit. In the following, each part is explained in detail.

A. Sensing Unit. In sensing unit, sensors are adopted to capture the information for drone detection. This primarily includes optical camera, which is responsible for capturing the data that is to be processed.

B. Central Processing. This part is essentially the brain of entire operation and it is responsible for extracting data and processing it. The data is forwarded to it via sensing unit. Central processing has 3 main components.

a. **Drone Feature extraction**: Drone feature extraction is essential for drone detection. We analyse the drone's features based on the received video images by using Open CV image detection. Image Feature: Fig 4 shows an example of face detection using the process of Image detection Using Haar cascade. By using same methodology, we use drone detection using Haar cascade.

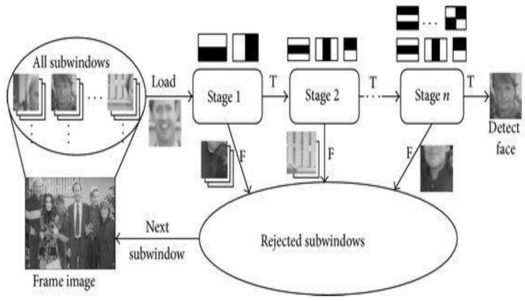

Fig 4: Process of Image Detection Using OpenCV Haar cascade

b. **Personal Computer**: We use normal Personal Computers for our project, with some essential software and Hardware. We use the MSI GF63F, which is powered by an Intel Comet Lake i5-10500H processor, NVIDIA® GeForce RTX™ 3050 graphics, 8 GB DDR4memory. And the system should require python platform like PyCharm and Arduino Ide for Arduino board. The system should contain a webcam for image capturing.

c. **Micro-Controller:** Here we use Arduino for controlling the siren/alarm or jamming circuit according to image detection. As shown in the Fig 6 we will connect our output devices for surveillance as mentioned above. Rather than that, for manual radio frequency jamming, we use ESP8266 Wi-Fi module. The pin out diagram of ESP8266 Wi-Fi module is shown in the fig 5.

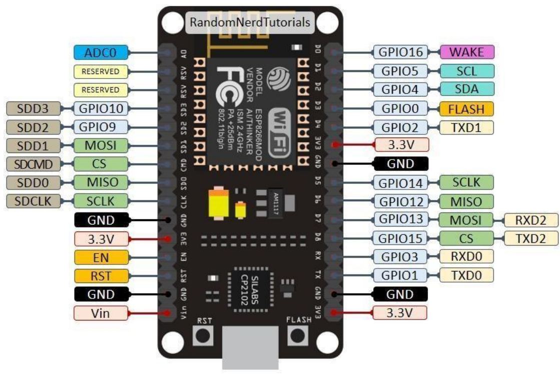

Fig 5: ESP 8266 microcontroller

C. Output.

As show in the fig 6, we can see that a servo motor is placed by connecting its wires on GND, +5V and a pin out which is connected according to the program or algorithm given.

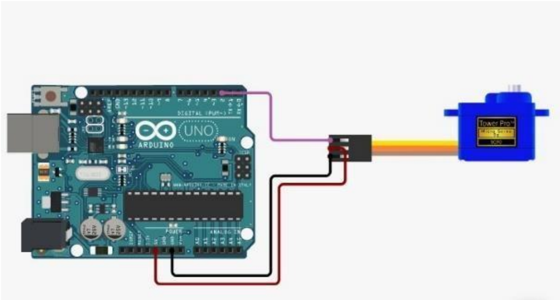

Fig 6: Assembled board visualisation

This is just an example of output given to the Arduino according to the object detection using Haar cascade. We can use Jamming circuits or manual jamming circuits like ESP8266 Wi-Fi module or a siren/alarm for surveillance. When the object is identified, at the same time without any lag, the python code will work and gives input to Arduino board using the library named as Pyfirmata.

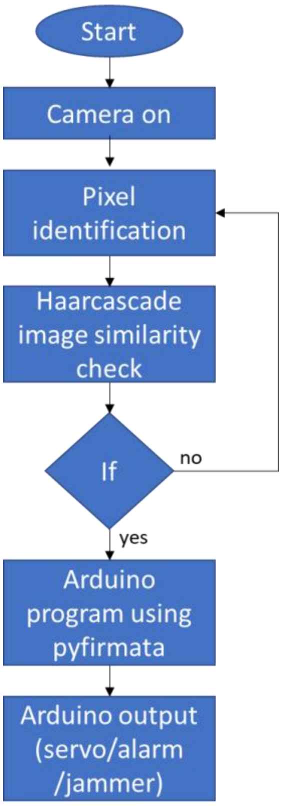

Fig 7: A basic idea of the implemented code

V. CHALLENGES

Although we have realized basic functions for drone surveillance in our anti-drone system, new challenges have been raised and there are still some open research and legality issues to be addressed:

- **Multiple drone detection and localization.** Most of the existing anti- drone systems tackle one drone. When multiple drones appear in the area of interest, one key problem is data association, how to associate the data from optical sensors with the corresponding drones. Both clutters and similar drones in the environment will bring challenges to data association, and then affect drone detection and localization. A solution to which is more sophisticated algorithm but such endeavours are computationally expensive.
- **Power control of radio frequency jamming**. The automatic jamming unit transmits radio frequency signals to interfere with the communication between the detected drone and its controller, which however may also interfere with the ambient wireless communications. It remains to be addressed how to control the transmission power of the radio frequency jamming signals so that the detected drone can be effectively defended without interfering with the ambient wireless communications.
- **Legality**. Many regions consider jamming circuits, or jammers, as it is commonly known illegal. This is because as aforementioned jammers are not specific, which means, the interference signals can block other communication devices, especially aviation and emergency communications. As such and also because authorities are afraid of misconduct, jammers are illegal to own, manufacture or even operate without a licence.

VI. CONCLUSION

A comprehensive review of Anti-Drone system is established. We use machine learning to identify and visualise an incoming unmanned aerial object. Experimental results will show that our system can detect and localize the intruding drone in a campus or similar environment using Image AI and OpenCV python library. This system can also be used for face detection, vehicle detection, pedestrian counting and security systems, jamming of the detected drone is also available, if necessary. Although due to legal reasons it might not be feasible in all scenarios. Furthermore, we discussed the challenges, especially the legal aspect as aforementioned and the ways in which this type of system can be improved.

REFERENCES

1. X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi and J. Chen, "Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges," in IEEE Communications Magazine, vol. 56, no. 4, pp. 68-74, April 2018, doi: 10.1109/MCOM.2018.1700430.
2. H. Sedjelmaci, S. M. Senouci, and N. Ansari, “Intrusion detection and ejection framework against lethal attacks in UAVaided networks: A bayesian game-theoretic methodology,” IEEE Trans. Intell. Transport. Syst., vol. 18, no. 5, May 2017,pp. 1143–1153.15
3. J. Su, et al. “A Stealthy GPS Spoofing Strategy for Manipulating the Trajectory of an Unmanned Aerial Vehicle.” IFACPapersOnLine, vol. 49, no. 22, 2016, pp. 291–296.
4. A. Sanjab, W. Saad, and T. Bas?ar, “Prospect theory for enhanced cyber-physical security of drone delivery systems: A network interdiction game,” arXiv preprint arXiv:1702.04240, accessed on Jul. 18, 2017.
5. C. Zhao, J. He, J. Chen, “Resilient Consensus with Mobile Detectors against Malicious Attacks,” IEEE Trans. Signal Inf. Process. Netw., doi. 10.1109/TSIPN.2017.2742859,2017.http://ieeexplore.ieee.org/abstract/document/8013830/, accessed on Sep. 7, 2017.
6. F. Hoffmann, et al., “Micro-doppler based detection and tracking of UAVs with multistatic radar,” Proc. IEEE RadarConf, Philadelphia, PA, USA, May 2016, pp. 1–6.
7. J. Farlik, et al., “Radar cross section and detection of small unmanned aerial vehicles,” Proc. 17th IEEE Int’l. Conf. Mechatronics–Mechatronika, Prague, Czech Republic, Dec. 2016, pp.1–7.
8. F. Christnacher, et al., “Optical and acoustical UAV detection,” Proc. of SPIE Security+ Defence, vol. 9988, 2016, pp. 99880B-1–99880B-13.
9. Z. Zhang, Y. Cao, M. Ding, L. Zhuang, and W. Yao, “An intruder detection algorithm for vision-based sense and avoid system,” Proc. IEEE ICUAS, Arlington, VA, USA, Jun. 2016, pp. 550–556.
10. S. R. Ganti and Y. Kim, “Implementation of detection and tracking mechanism for small UAS,” Proc. IEEE ICUAS, Arlington, VA, USA, Jun. 2016, pp. 1254–1260.
11. DDC, “Domestic drone countermeasures,” http://www.ddcountermeasures.com/products.html, accessed on Apr. 17, 2017.
12. M. Peacock and M. N. Johnstone, “Towards detection and control of civilian unmanned aerial vehicles,” Proc. 14th Australian Information Warfare and Security Conf., Edith Cowan University, Perth, Western Australia, Dec. 2013, pp. 9–15.
13. P. Nguyen, et al., “Investigating cost-effective RF-based detection of drones,” Proc. 2nd ACM Wksp. Micro Aerial Vehicle Networks, Systems, and Applications for CivilianUse, Singapore, Singapore, Jun. 2016, pp. 17–22.
14. N. Dalal and B. Triggs, “Histograms of oriented gradients for human detection,” Proc. IEEE CVPR, San Diego, CA, USA, Jun. 2005, pp. 886–893.
15. H. Tang, “DOA estimation based on MUSIC algorithm,” 2014, https://pdfs.semanticscholar.org/5ff7/806b44e60d41c21429e1ad2755d72bba41d7.pdf, accessed on Sep. 7, 2017.
16. S. Wang, B. R. Jackson, and R. Inkol, “Hybrid RSS/AOA emitter location estimation based on least squares and maximum likelihood criteria,” Proc. 26th IEEE QBSC, Prague, Czech Republic, May 2012, pp. 24–29.[16] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi and J. Chen, "Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges," in IEEE Communications Magazine, vol. 56, no. 4, pp. 68-74, April 2018, doi: 10.1109/MCOM.2018.1700430.

Fig 1: Drone detection

(https://cdn.geekwire.com/wp-content/uploads/2019/02/190201-dronehunter-630x386.jpg)

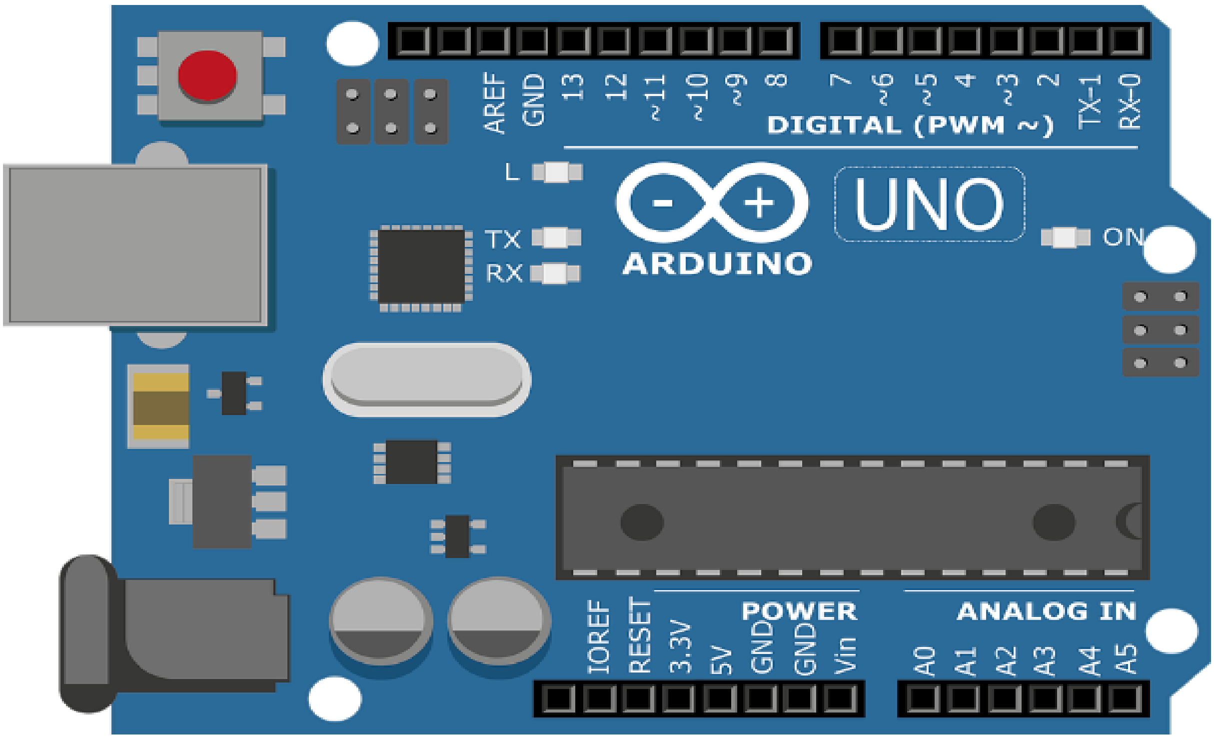

Fig 2: Arduino Uno

(https://blog-c7ff.kxcdn.com/blog/wp-content/uploads/2017/02/Blog-Featured-Image.png)

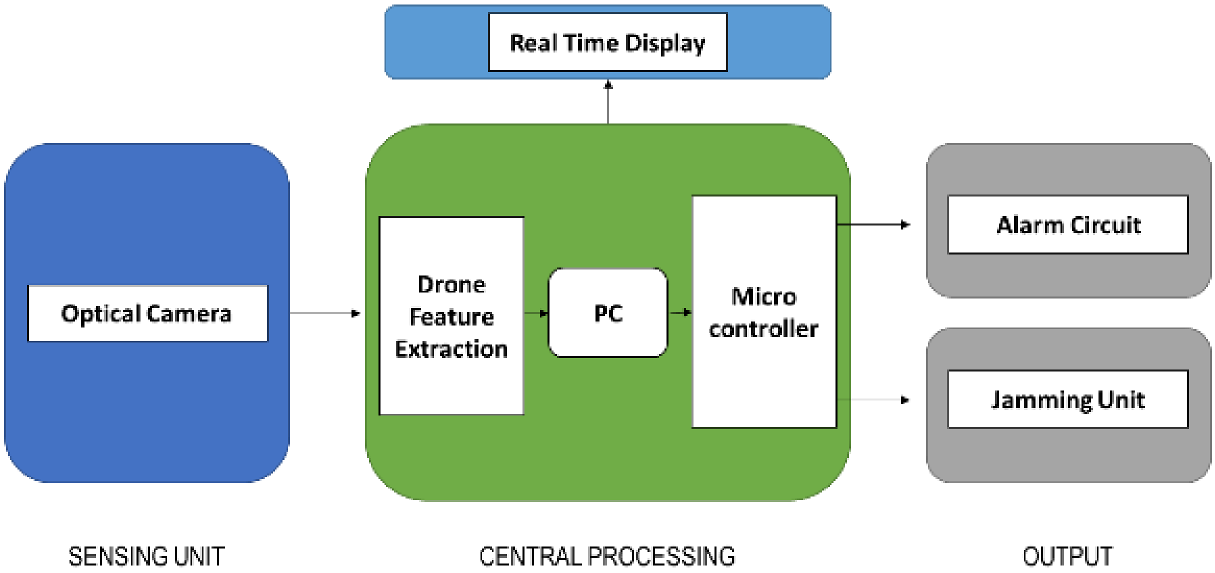

Fig 3: Architecture of Anti-Drone System

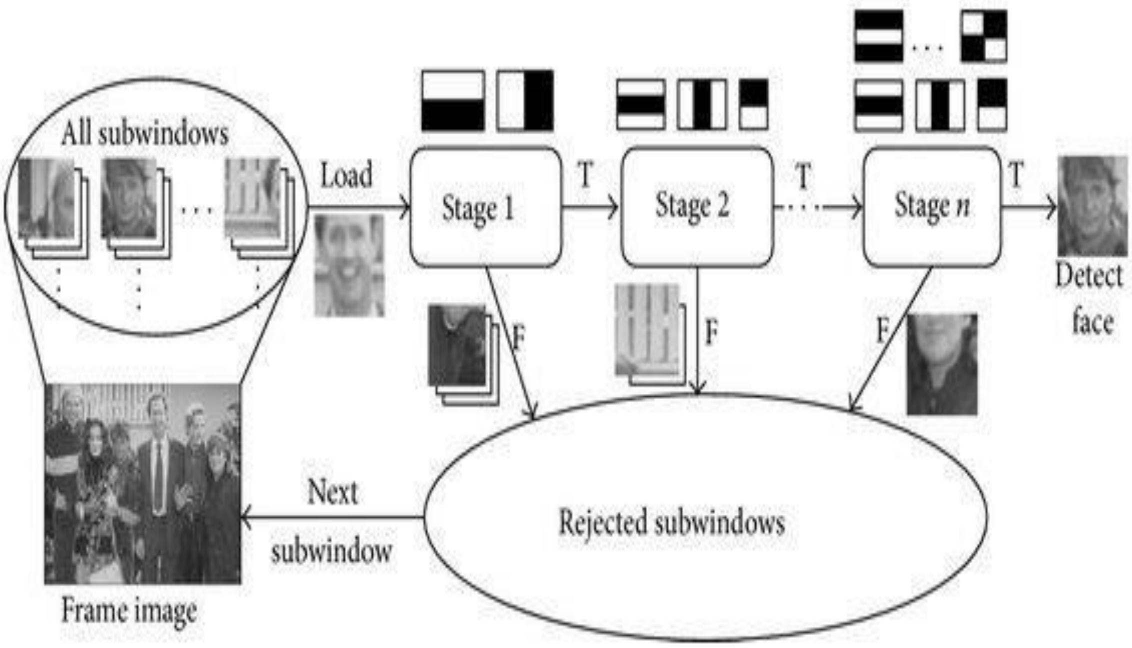

Fig 4: Process of Image Detection Using OpenCV Haar cascade

(https://machinelearningknowledge.ai/ezoimgfmt/www.researchgate.net/publication/277929875/figure/fig9/AS:329583183319048@1455590162849/Cascade-structure-for-Haar-classifiers.png?ezimgfmt=rs:600x260/rscb1/ng:webp/ngcb1

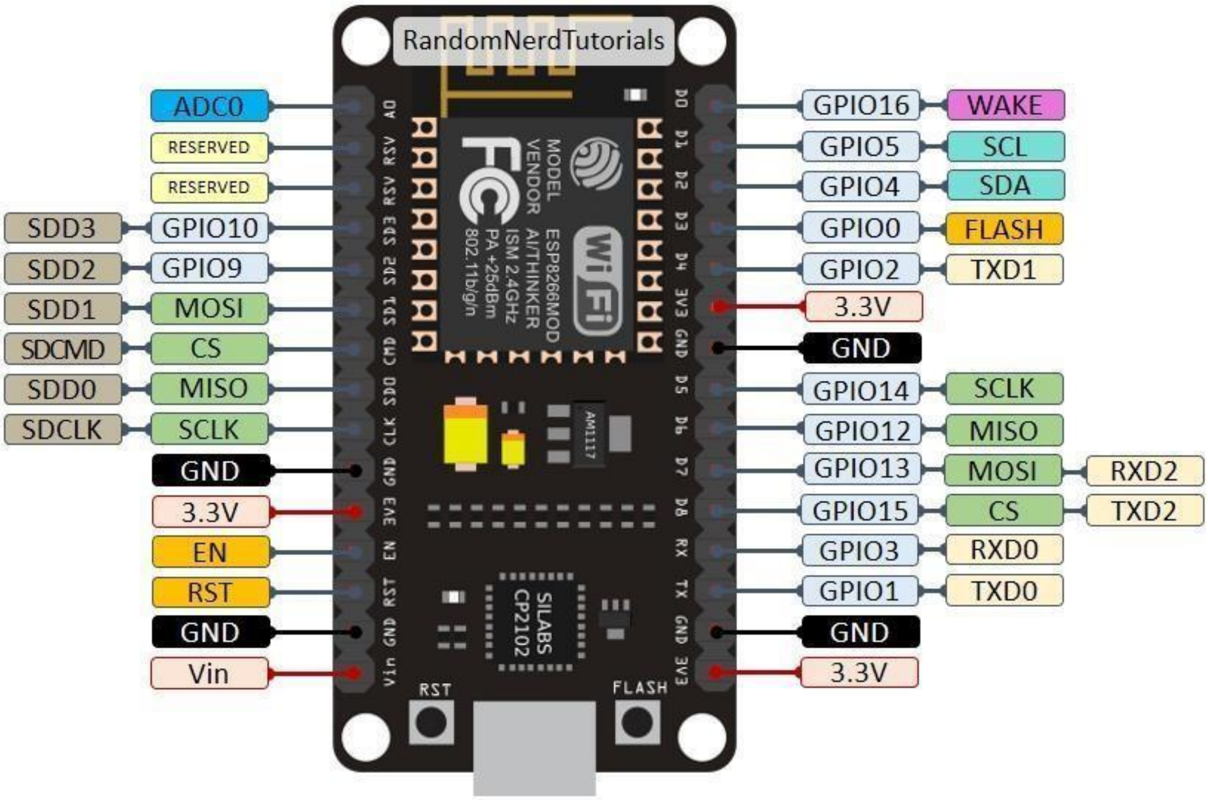

Fig 5: ES8266 Microcontroller
(https://i0.wp.com/randomnerdtutorials.com/wp-content/uploads/2019/05/ESP8266-NodeMCU-kit-12-E-pinout-gpio-pin.png?w=817&quality=100&strip=all&ssl=1)

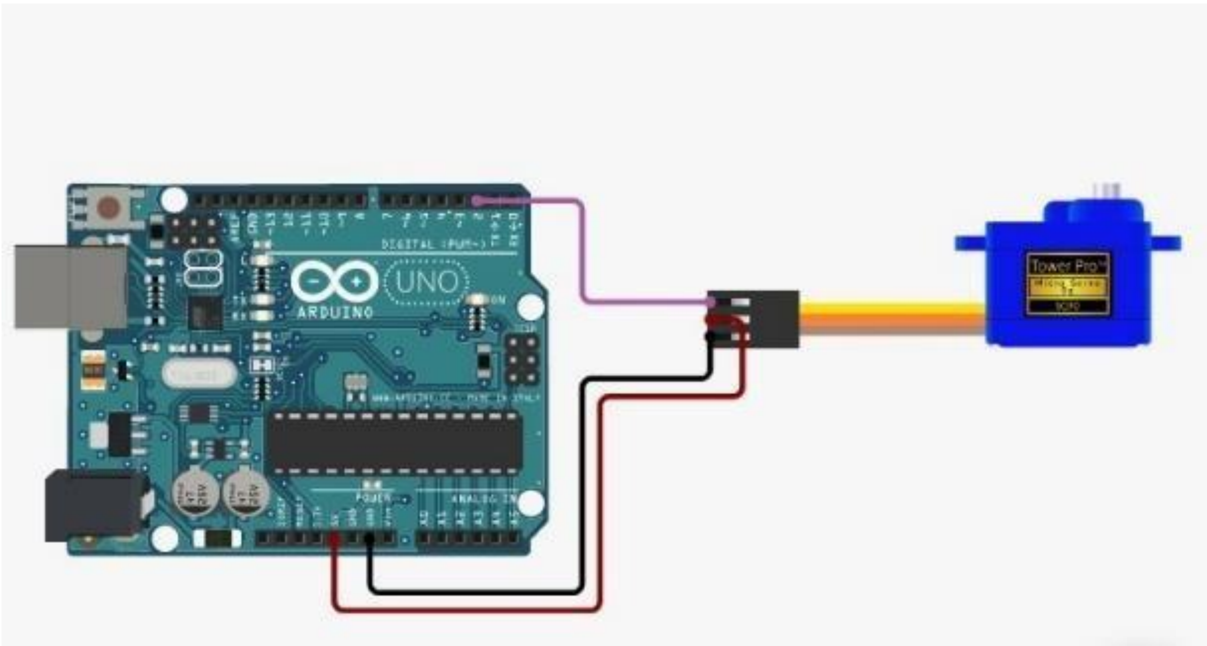

Fig 6: Assembled board visualisation (https://www.circuito.io/)

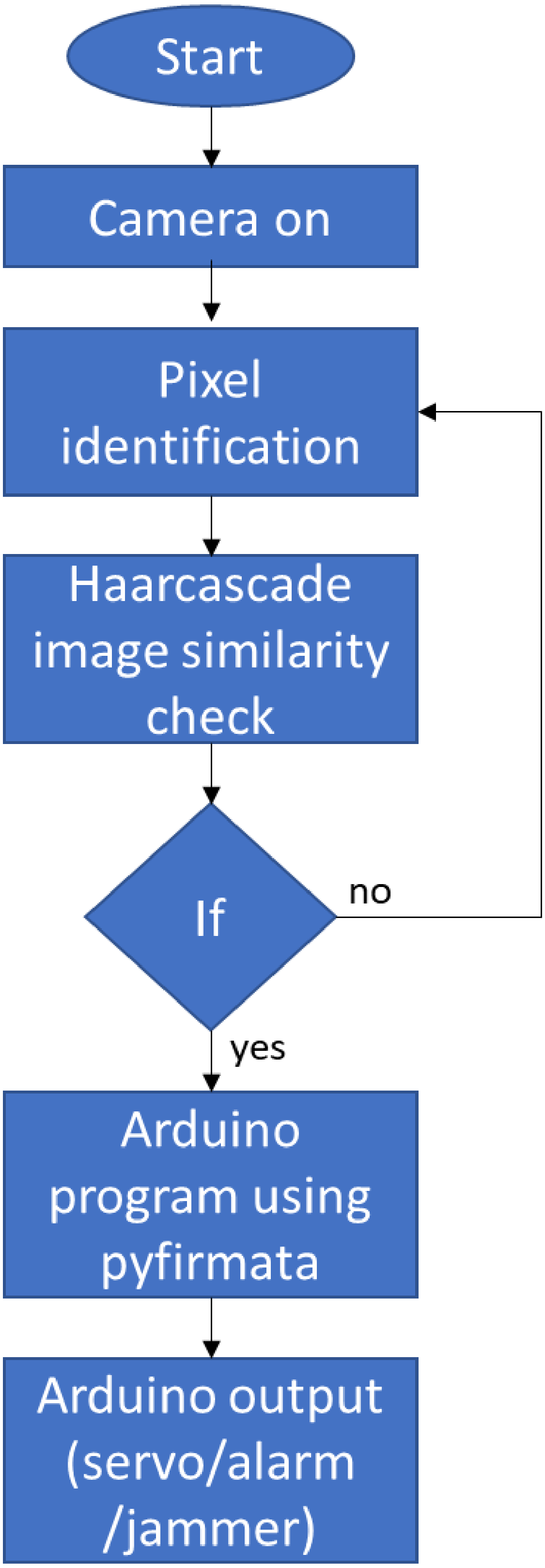

Fig 7: Algorithmic representation