USE OF AI TO DIVERSIFY AND IMPROVE THE PERFORMANCE OF RF SENSORS DRONE DETECTION MECHANISM

Fahad Alsifiany

Department of Information Technology and Communications, King Fahad Security College, Riyadh, Saudi Arabia

ABSTRACT

Drone terrorism may seem elementary and efforts in its mitigation may seem painless. The fact is that security bodies in many countries are still grappling with this growing security concern. The autonomous nature of drones and the unpredictable nature of drone attacks remain to be some of the unforeseen challenges undermining the mitigation efforts in combating drone terrorism. The need to upskill our security forces and the general public on the operational practices and security capabilities in the drone world cannot be overemphasized. This paper explores a futuristic solution to the current challenges encountered in the war against drone terrorism. In its design, it delves into the possibility of utilizing Artificial Intelligence (AI) in characterizing the features of drones identified in our airspace to determine their authenticity. It further enriches the employees of the security services and the general public with information on combating drone terrorism by benefiting from the accumulated experiences of the relevant and specialized affiliates.

KEYWORDS

Drone terrorism, Drone, Radio Frequency (RF), Unmanned Aerial Vehicles (UAV), Artificial Intelligence (AI), Computer Vision (CV), Machine Learning (ML)

1. INTRODUCTION

Drones are autonomously flying robots, which are controlled remotely using flight-planning software in their embedded systems. Drones can fly in altitudes from as low as 400 feet to as high as 33,000 feet, which is equivalent to 10 kilometers [1]. The altitudes of choice are dependent on regulations of unmanned aerial vehicle (UAV) flights, which vary across different countries [2]. The altitude of flight is mainly characterized by the size, weight, and purpose for which the drone is used [1]. The major types of drones include multi-rotor drones, single-rotor drones, fixed-wing drones, and fixed-wing hybrid VTOL drones. The fixed-wing hybrid VTOL drones combine the efficiencies of fixed-wing drones and multi-rotor drones by switching between the two modes of operation during their flights. The sizes of these drones are different and their weight can range from 5 kg up to 100 kg. In addition to their basic weight, drones can carry variable loads during their flight [2].

Drones have been used for different purposes. One of the pioneering applications of drones was in photography and image collection. Photographers have employed drones to collect photos at family events, sporting events, and nature [1]. Drones have also been used for recreational purposes. This is common with tourists who engage in drone racing competitions. Commercial

David C. Wyld et al. (Eds): CCSEA, AIFU, EMSA, NLCAI, NCOM, SIPRO, SEA, DKMP, BDML, BIoT, CLOUD - 2023
pp. 29-40, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.130504

drones have also been used by large-scale logistic firms in management and delivery processes to save on the cost of human labor. The use of drones has also gained popularity in the field of security. In this field, commercial drones have been used for surveillance, inspection, monitoring, and data collection and most recently have been misused in drone terrorism [3].

1.1. Theoretical Framework

The invention of drones was a culmination of the second world war in the 20th century. The drones were used in military ventures and it was not until the year 2006 that the Federal Aviation Administration (FAA) issued the first commercial drone licenses. Since then, the use of drones has been embraced across different countries and one of the sectors that have majorly benefitted from their use is the security sector. The applications of drones in the security sector range from surveillance purposes to reconnaissance, monitoring, inspection, and data collection. The use of drones in terror attacks is slowly gaining popularity over the last four years. Drones have been used to fire missiles, drop bombs, or crash into the territories of target terrorists [3].

To mitigate drone terrorism, various technologies have been embraced. Radio Frequency (RF) has been the most prevalent technology in use [4]. The RF spectrum is between the range of 20 kHz and 300 GHz. Drones are autonomous and their controllers use the RF spectrum [3]. A varied range of RF equipment has been developed for detecting and analyzing drones in airspaces to determine their authenticity and identify rogue drones, which may have been deployed by terrorists. This equipment includes RF sensors, RF analyzers, RF jammers, and radar. Apart from RF technology, there has been an exploration of other approaches such as the use of acoustic sensors, use of optical sensors, and use of high energy lasers [5]. These efforts have however not attained the threshold we envision in the fight against drone terrorism. The need for exploration of more agile technologies in this course is undebatable.

1.2. Background

Artificial Intelligence (AI) is a flexible and agile technology, which serves to resolve most of the challenges revolving around the world of drone terrorism. AI involves emulating human behavior and thinking in computers or computer-controlled devices. Drone terrorism is rapidly evolving and drone terrorists have scaled up both technically and tactically. Drone attacks experienced today are therefore more sophisticated and require high-end efforts to combat them. AI was developed in the 20th century. For a while, the technology grew unnoticed as it had low levels of creativity. Today technology has however evolved to serve most of our needs with development in support technologies and the emergence of new technical skills. Companies offering drone defense solutions such as Dedrone in the United States of America are beginning to develop AI-based solutions for combating drone terrorism [11]. Exploration of the different aspects in which this technology can be utilized in combating drone terrorism will help in realizing optimal security measures for use by both members of the security service and civilians.

2. ANALYSIS

Artificial Intelligence (AI) leverages computer capabilities to realize human intelligence in computers. The technology draws a comparison between a prevalent situation and a vast range of databases with data parameters related to this task. Data utilized in AI is mainly sourced from similar occurrences in the past or formulated as a set of ideal parameters desired in a given course. In performing this comparison, AI classifies different events and their associated characteristics.

Radio Frequency (RF) technology served as the initial solution for countering drone terrorism. It has been the most prevalent technology in use, and it offers a futuristic pathway in the war against drone terrorism. RF sensors, RF analyzers, radars, and RF jammers utilize this technology [3]. RF sensors couple the efficiency of magnetic susceptibility and electrical permittivity to detect drones in their vicinity. The core components of these sensors are a monitoring circuit, a coil-shaped RF antenna, and an RF oscillator circuit. The sensors are also used in determining the proximity of attacking drones. RF analyzers are used in airspaces to determine the frequency utilization and detect different forms of interferences in the radio spectrum [4]. This way, they can detect enemy drones operating at divergent frequencies.

Radar detection systems utilize RF technology to range the distance, measure the angle and calculate the radial velocity of drones detected by sensors, to populate information relevant to the classification of the detected drones [4]. RF jammers are used at advanced stages after detection, where they generate waves similar to those of attacking drones to create interference and prevent signal relays between these drones and their controller stations [3]. Other technologies coupled with RF technology in countering drone terrorism include the use of acoustic sensors, use of optical sensors, and use of high energy lasers.

The dynamism associated with drone attacks is overwhelming the aforementioned RF technologies [5]. Table 1 details the dynamic features of attacking drones, which are posing technical complexity to the fight against drone terrorism.

Table 1. Dynamic features of attacking drones.

Parameter	Complexity
Size	Variation and unpredictability in the sizes of commercial drones in use by drone terrorists
Weight	Variation in the weights of different drones and establishing the credibility of drones of a specific weight
Shape	Varying shapes of commercial drones being utilized by drone terrorists
Number	Migration of drone attackers from conventional attacks using a single drone to using swarms of drones
Altitude	Variation and unpredictability in altitudes of flight for drones used in drone terrorism
Flight pattern	Variable flight patterns by different drones make it difficult to differentiate between authentic and rogue drones
Takeover and fend off	Lack of technical tools to execute takeover and fend off identified rogue drones
Speed	Variable speeds of flight for different drones, some exceeding the defined levels

To counter the dynamism, AI is being embraced in the war against drone terrorism. This technology is promising and as it’s in the initial stages of exploration, huge research efforts are required in this field. By coupling AI technology with RF technologies, greater efficiencies will be realized across this field. This way, the underlying dynamism will be contained as follows:

2.1. Size and Shape

AI utilizes different algorithms, modeled to perform specific roles. Computer vision (CV) is a sub-branch of AI, which utilizes object detection and object recognition algorithms [7]. Object detection algorithms use multiclass classification to define the type of objects and establish their characteristics. The size and weight of drones vary depending on the manufacturer, the purpose for which the drones are used, or the type of load carried by the drone [1]. Digging deep into these drone parameters can help in the primary steps of detecting rogue drones weaponized by terrorists [1]. RF sensors can be used in conjunction with AI technology to analyze the shapes and sizes of drones.

RF sensors solely detect the presence of any type of UAV in the air space [5]. While they do not single out instances of drones, it would be efficient to utilize Computer Vision to single out instances of drones and derive their associated parameters. This could be achieved by embedding AI processors in the sensors and equipping the RF sensors with quality camera systems to work in synchrony. On detecting a UAV, the camera would be enabled to take images of the UAV and the image will be sent to the AI processors for recognition. A colossal amount of data is required for training the AI model to support differentiation of the UAVs to primarily support the detection of drones and to characterize the shape and sizes of these drones. A sound understanding of the local UAV regulations will help in formulating data for use in this context. We can derive the most commonly used or licensed drone sizes and their corresponding shape and use this data to train our AI model. This way, classification after drone detection and recognition may point out an anomalous size or shape for a given drone, which can further be monitored to determine whether it is an attacking drone. Figure 1 shows the conceptualization of the hybrid AI and RF model.

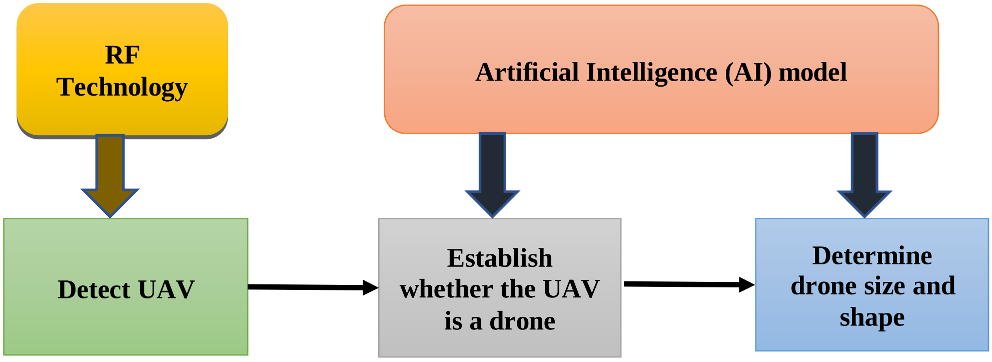

RF Technology
Artificial Intelligence (AI) model
Detect UAV
Establish whether the UAV is a drone
Determine drone size and shape

Figure 1. The hybrid AI and RF model workflow

2.2. Weight

The weight of a drone is a critical parameter in the war against drone terrorism. Weaponized drones often carry variable loads with them, which may be in the form of missiles or bombs. While RF technologies can barely identify the weights of drones in airspaces [1], it is essential to embrace AI for this use. We can once again leverage the benefits of Computer vision to determine the weight of drones. While we cannot achieve an AI model that blatantly tells us the weight of a hovering drone, we can develop models that can measure the volume and density of these drones.

To establish the volume of the hovering drone, we would use a 3D reconstruction algorithm in the AI model. Here, a camera is needed to work in synchrony with the RF sensors and the embedded AI system. Multiple images of the drone under scrutiny will be taken from different angles and the algorithm will reconstruct the 3D view of the drone and determine its volume. RF technologies cannot however establish the density of drones under scrutiny [4]. To derive the material density of the drone components, active thermography will be used [6]. A laser controller will be incorporated into the AI model to activate the laser beaming over each drone under scrutiny. The thermal gradient created by the incident laser on the drone surface will be taken as data input by the AI model. Continued scanning will be done to achieve a series of thermal frames with which the AI model will estimate the material density.

The model can consequently calculate the weight using the aforementioned parameters with the relationship below [6]:

$$Weight = v \times \rho \times g ,$$

Where v is the volume of the drone, ρ is the density of the drone, and g is the acceleration due to gravity.

2.3. Number and Altitude

RF technologies currently in use in rogue drone detection are being challenged by the drastic tactical approaches that terror attackers are using. Attackers are accustomed to using one drone to fire missiles, drop bombs, or to even crash into a target premise. Nowadays, attackers have resolved to use a swarm of drones which makes it hard to use RF technology in scrutinizing the drones [1].

AI can help us in establishing the number of drones in a particular swarm. Computer vision is efficient with such processes. By using a quality camera that can relay to an embedded AI system, we can determine the number of drones in the swarm. Computer vision algorithms can also be employed in determining the altitude of each drone in the swarm. Conventionally, radar ranging is efficient in establishing the altitude of flight in cases of isolated drones. Radar ranging uses frequencies between 400 MHz to 36 GHz [4].

Complexity arises in establishing the heights of multiple drones in a swarm and AI poses a solid solution to this challenge, through its high-end algorithms. By establishing the number of drones and their corresponding altitude of flights, our developed AI model would draw from a huge set of primary data on local UAVs flight trends and alert of any observed anomalies to take action on any rogue drones.

2.4. Flight Pattern

Ideally, drones used by attackers are likely to have suspicious flight patterns as they surveil their targets. Such suspicious patterns may include circling a given target or making multiple return flights over a target to establish its state. Such anomalies in flight patterns cannot be established by RF technologies currently in use. There is a need for an intelligent model, which can perform an analysis and raise alerts in cases of suspicion. This can be achieved through a combination of Computer Vision and Machine Learning (ML), which are sub-branches of AI.

ML algorithms provide us with an opportunity to define human-like behavior in a system [2]. A model can be developed and trained with data on common flight patterns of different commercial drones. In this approach, Computer vision will ensure the relay of drone images and videos to the embedded AI system. The ML model will then raise alerts on any anomalies detected in the flight patterns of the drones and appropriate action can be taken on any rogue drone.

2.5. Speed

Every country has its own defined maximum speed of flight for UAVs in its airspace. Drones operating at a speed greater than the maximum defined speed are rogue drones as they do not operate under the stipulations of their licenses. Computer vision can be used to monitor the speeds of drones to single out instances of rogue drones.

2.6. Takeover and Fend Off

In the war against drone terror attacks, fend-off has previously been employed using RF technologies. Fend off is the process of identifying the signal source of the drone controller and disabling the signal [10]. The drone consequently flies back to its original position or hovers around. This way, the drone can be monitored easily to determine whether it is an attacker's drone. The development of AI technology brings us the possibility of achieving drone takeover. In a takeover, after fend off has been achieved, the scrutinizer can establish autonomous control of the drone and combine the efficiencies of Computer vision and light detection and ranging (LiDAR) to land the attacker drone safely [10]. LiDAR is important as it helps in establishing the presence of objects or vegetation, and when combined with Computer vision, the scrutinizer can bring down the drone safely without causing any harm to people, structures, or vegetation. The proposed drone detection lifecycle for the hybrid AI, RF, and LiDAR system is shown in figure 2 below. Moreover, the proposed hybrid system is shown in figure 3 below

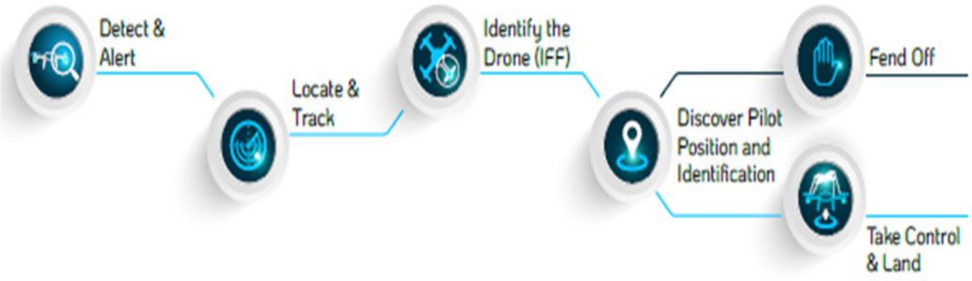


Figure 2. The proposed rogue drone detection lifecycle

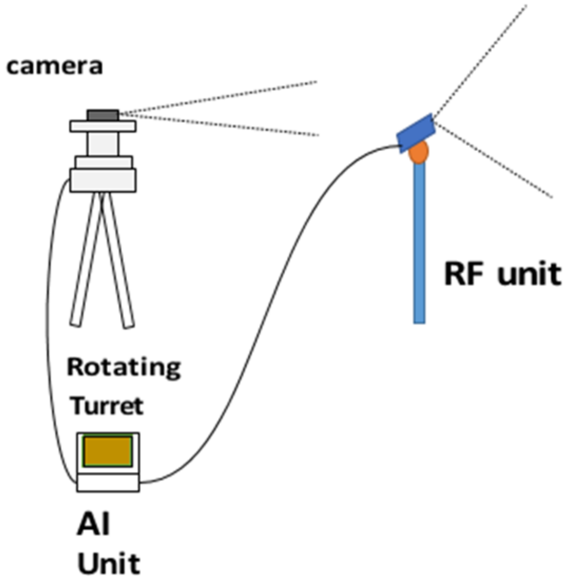


Figure 3. Proposed hybrid system

2.7. Mathematical System Model

The developed AI model for use will derive a wide range of parameters from the acquired images for regression analysis to determine the volume, weight, altitude, and flight patterns of the drones under scrutiny. These parameters will include area, shape, perimeter, eccentricity, axis length, radial distance, altitude, and instantaneous displacement of the drones over different angles and directions. The conceptualized algorithm is depicted in figure 4 below.

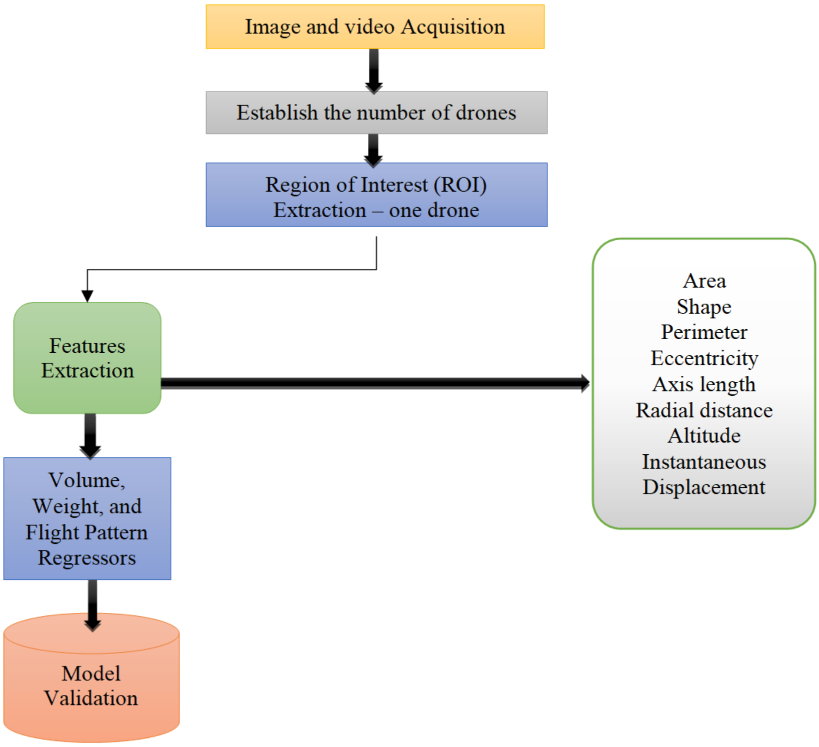


Image and video Acquisition
Establish the number of drones
Region of Interest (ROI) Extraction – one drone
Features Extraction
Area
Shape
Perimeter
Eccentricity
Axis length
Radial distance
Altitude
Instantaneous Displacement
Volume, Weight, and Flight Pattern Regressors
Model Validation

Figure 4. Conceptualized algorithm.

The proposed model will utilize 2D image feature extraction from the areas of a drone projected across different angles and directions. The 2D image features will then be used for 3D image reconstruction. The key parameters of interest are represented in table 2 below.

Table 2. Key parameters of interest.

Parameter	Representation
Y_A	Area
Y_p	Perimeter
Y_E	Eccentricity
Y_1	Major axis length
Y_2	Minor axis length
Y_d	Radial Distance
H_1	Average swarm altitude

Feature extraction in AI models relies on counting the number of pixels bound by contours identified in the images under analysis [9]. Taking a random vertex (x_n, y_n) for the captured drone image and constructing an ellipse of coordinates (X_1, Y_1), (X_2, Y_2), we deduce (M_2, N_2) and

(M_1, N_1) to be the endpoints of our major and minor axis respectively. We then proceed to extract the features of interest using the following regressions [9]:

$$Area, \qquad Y_A = \frac{1}{2}\sum_{n-1}^{N-1}(y_{n+1}x_n - x_{n+1}y_n)$$

$$Perimeter, \qquad Y_p = \frac{1}{2}\sum_{n-1}^{N-1}(x_{n+1}, y_{n+1}) - (x_n, y_n\ )$$

$$Eccentricity,\ Y_E = \frac{Y_1}{Y_2}$$

$$Major\ axis\ length, Y_1 = \sqrt{((X_2 - X_1)^2 + (Y_2 - Y_1)^2)}$$

$$Minor\ axis\ length, Y_2 = \sqrt{((M_2 - M_1)^2 + (N_2 - N_1)^2)}$$

$$Radial\ distance, Y_d(n) = \sqrt{\{X(n) - \bar{X}\}^2 + \{Y(n) - \bar{Y}\}^2}$$

$$Average\ swarm\ altitude, \qquad H_1 = \frac{Radar\ height_{(ROI1)} + \ \dots + Radar\ height_{(ROIn)}}{Number\ of\ ROIs(Drones)}$$

The AI model utilizes statistical Regressors to give an estimate of the volume, weight, and flight pattern of the drones once the 2D images have been reconstructed into 3D images. The volume obtained after a 3D reconstruction of the images is then used in determining the weight of the drone under scrutiny using the relation [8].

$$Weight = v\ \times\ \rho\ \times g$$

The density of the drone material is obtained by scanning the region of interest, initially defined to be the drone under scrutiny at that time. The altitude of flight for a single drone is obtained using radar ranging. In the case of a swarm of drones, however, the AI model works in synchrony with the radar ranging system to find the individual altitudes of the different regions of interest and find the average height of the swarm for further characterization of the flight behavior and variation from ideal flight parameters to determine whether they are rogue drones.

$$Rogue_{ROI} = \left|(\sum(ROI_s + ROI_H))\right|_{size,shape,volume,weight,flight\ pattern}$$

Where ROI represents a single drone, $ROI_s$is the speed of a single ROI, and $ROI_H$is the altitude of a single ROI.

The characterization of the magnitude of the speed and altitude of a single ROI is then done for the specific instances of size, shape, volume, weight, and flight patterns. The correlation between this characterization and the prevalent data in the AI model is then established, to detect any inconsistencies in the ROI under scrutiny. Below is the algorithm utilized for the above classification:

$$Rogue_{ROI} = \left|\left(\sum(ROI_s + ROI_H)\right)\right|_{size,shape,volume,weight,flight\ pattern}$$

```
        If altitude > 400
        Or speed > 100 mph
        Or length > 3.5:
            Rogue drone
            Fend off
            Take over
Else:
            Licensed drone
End
```

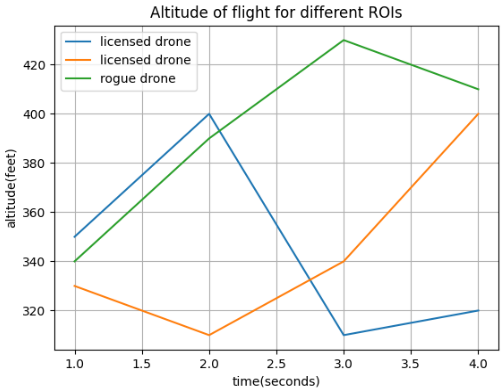
The algorithm for identifying a swarm of drones was as detailed below. The maximum difference in the Line of Sight (LoS) distance between different drones in a swarm was assumed to be 10m.

$$The\ separation\ between\ ROI, x = LoS_{ROI_n} - LOS_{ROI_{n-1}} \leq 10m$$

```
If x > 10m:
            Not a swarm
            Else:
            Swarm
            Fend off
            Take over
        End
```

3. Results and Recommendations

The developed AI model was simulated for different drones to determine the model's efficiency levels in detecting rogue drones. The sets of data used for training and correlation analysis were however limited and were drawn from basic laws regarding the operations of UAVs in Saudi Arabia. The maximum height of flight for UAVs in Saudi Arabia is stipulated to be 400 feet above the ground. 3 drones were scrutinized and characterized as shown in figure 5 below. Figure 6 shows the characterization of 4 drones based on their speed of flight.



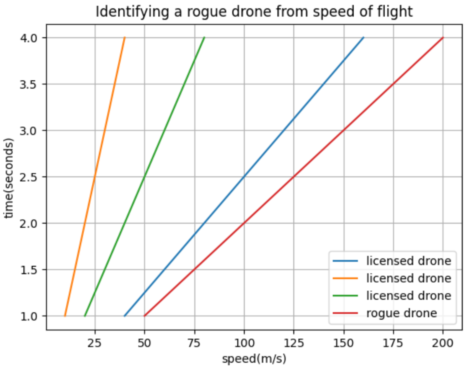


Figure 6: Speed-based characterization

Figure 5: Altitude-based characterization

In figure 5, two drones were identified as licensed drones as their average altitude of flight was below the stipulated maximum height of 400 feet. One drone was characterized as a rogue drone with its altitude of flight extending to about 430 feet above the ground. In figure 6, 3 drones were characterized as licensed drones with their speed of flight being less than the maximum stipulated speed of 100 mph. One drone was characterized as a rogue drone with its speed momentarily surpassing the maximum stipulated speed.

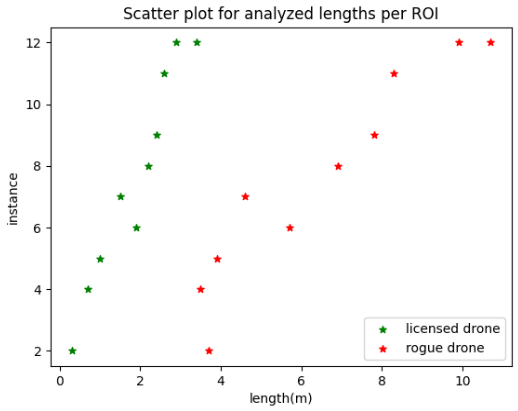


Figure 7: Length per ROI

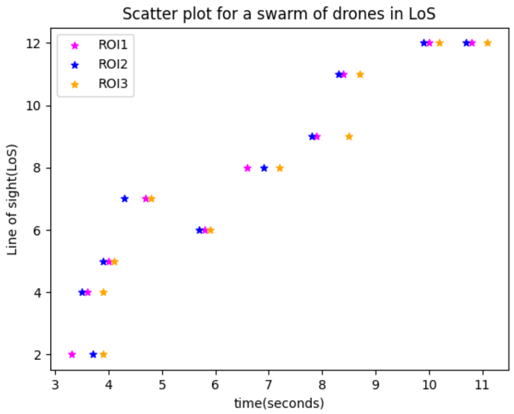


Figure 8: Identified swarm

In figure 7, a scatter plot is presented for two classifications based on the sizes of the drones. Ideally, the training data consider licensed local UAVs to have a prevalent length of up to 3.5 m. A series of drones whose lengths ranged between 3.7 m and 10.5 m were characterized as rogue drones. In figure 8, the AI model was used to identify a swarm of drones. The distance of the drones across the lines of sight was monitored over a given time and the scatter plot reveals a similarity in their pattern of flight, which proves the set of drones to be in a swarm. According to Saudi Arabia laws on UAV flights, only one drone should be flown by a controller at a given time. The identified swarm would therefore fall in the rogue drone characterization category.

Figure 9 depicts a fend-off process inflicted on the rogue drone identified in figure 5 from the unusual altitude of the flight. In the fend-off process, the RF unit disabled the RF signal from the remote controller of this drone. This resulted in the drone hovering around without further propagation in the LoS. The takeover process is depicted in figure 10 where data was populated for a rogue drone flying at unusual altitudes and lowered to the ground.

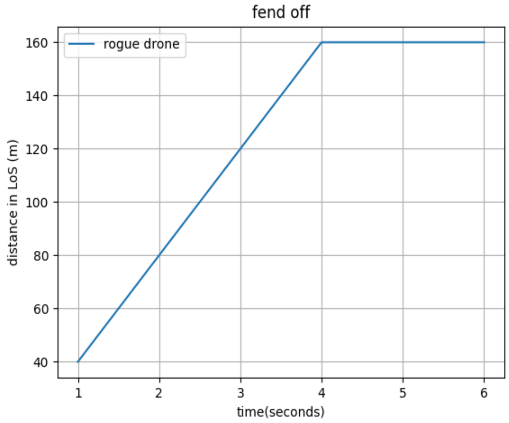


Figure 9: Rogue drone fend-off

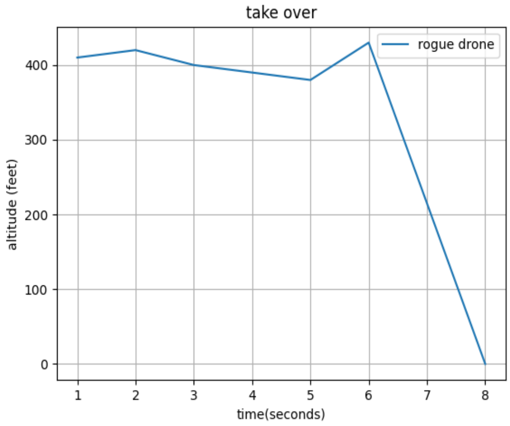


Figure 10: Rogue drone takes over

Characterization based on shape, volume, weight, and flight patterns however requires huge sets of data. The data should ideally be sourced from market stakeholders and commercial drone vendors. While this simulation involved minimal data sets, more market research to derive more market data can help in developing an ideal hybrid AI and RF system for use in the fight against drone terrorism.

4. CONCLUSION

With drone terrorism continually on the rise, there is a dire need to gear up in the war against drone-related attacks. Improvement in technical and technological skills will serve to be pivotal in this process. This research work puts across AI as a key futuristic technology for use in mitigating drone-terror attacks. From the proceedings, this technology merits in terms of its flexibility and efficiency for use in deriving the key features of interest in drone identification and classification. A good development trajectory is required for this technology and this calls for an optimal investment of financial, physical, and human resources by our security services. While the big chunk of this war against drone terrorism can be rested on the hands of our security service men, we cannot downplay the role civilians need to play. Civilians should be wary of suspicious drone activities in their environments and they should report such instances to local law enforcement officers on time. This way, we can achieve optimal drone terror mitigation practices.

4.1. Future Work

These future explorations would help in realizing a robust hybrid AI and RF model for use in rogue drone detection.

- Developing Deep Neural Networks (AI) algorithms and combining their use with infrared cameras to enable rogue drone detection at night, a realization that was not feasible with the developed model.
- Establishing a high-performance software platform, which can be used for deploying the hybrid AI and RF model to enable its remote control in both Line of Sight (LoS) and Non-Line of Sight (NLoS) rogue drone detection approaches.

REFERENCES

[1] Rico Merkert, James Bushell (2020). Managing the drone revolution: A systematic literature review into the current use of airborne drones and future strategic directions for their effective control. *Journal of Air Transport Management*, 89(1).

[2] Syed Agha HassnainMohsan, Muhammad Asghar Khan, Fazal Noor, Insaf Ullah & Mohammed H. Alsharif (2022). Towards the Unmanned Aerial Vehicles (UAVs): A Comprehensive Review. *MDPI*, 2(3).

[3] Jean-Paul Yaacoub, Hassan Noura, Ola Salman, Ali Chehab (2020). Security analysis of drones' systems: Attacks, limitations, and recommendations. *Elsevier - Internet of Things (IoT)*, 3(4).

[4] Erdemli, Mustafa Gokhan (2009). General use of UAS in EW environment--EW concepts and tactics for single or multiple UAS over the net-centric battlefield. *Naval Postgraduate School*, Monterrey, California.

[5] Alexander Farrow (2016). Drone Warfare as a Military Instrument of Counterterrorism Strategy. Air and Space Power Journal, 3(4), 7-12.

[6] Tamas Aujeszky, Georgios Korres, Mohamad Eid and Farshad Khorrami, (2019). Estimating Weight of Unknown Objects Using Active Thermography. MDPI, Robotics.

[7] Ahmed Reda Amin EL-Barkouky (2014). Mathematical modeling for partial object detection. The University of Louisville, Theses and Dissertations.

[8] Baohua Zhang, Ning Guo, Jichao Huang, Baoxing Gu, and Jun Zhou (2020). Computer Vision Estimation of the Volume and Weight of Apples by Using 3D Reconstruction and Noncontact Measuring Methods. Hindawi, 17(3).

[9] Innocent Nyalala, Cedric Okinda, Qi Chao, Peter Mecha, TchallaKorohou, Zuo Yi, Samuel Nyalala, Zhang Jiayu, Liu Chao & Chen Kunjie, (2021). Wight and volume estimation of single and occluded tomatoes using machine vision. International Journal of Food Properties, 24(1)

AUTHOR

Fahad Alsifiany received a B.Sc. degree in electrical and electronic engineering from King Abdulaziz University, Jeddah, Saudi Arabia, in 2001. He received an M.Sc. degree in telecommunications and networking engineering from the University of Pittsburgh, Pittsburgh, USA, in 2011. He received his Ph.D. degree in wireless communications from Newcastle University, Newcastle upon Tyne, U.K, in 2020. He is a lecturer now with the Faculty of King Fahad Security College, Riyadh, Saudi Arabia. His current research interests include noncoherentmimo systems, physical layer security, massive mimo, artificial intelligence, and machine learning.