Drone Management System for Hunting Unauthorized Drones

Suhair Mohammed Zeki Abd Alsammed

***Publication data**: 30 / 8 /2024*

***Keywords**: unauthorized Drones, monitor aircraft, threaten aircraft, radar, captured*

ABSTRACT

Drones, with their unauthorized path, threaten aircraft and airport systems, emergency procedures, and passenger safety. Therefore, an idea can be made that helps detect and monitor unauthorized drones, which are radars that monitor aircraft, where the aircraft is captured and its information is stored in a database. The information is the aircraft number and the name of the aircraft. And the name of the radar that captured the plane, the radar number, and the time the plane was captured with a picture of the plane. 4 radars can be used, each containing its own hard drive-in which information is stored, and the special hard drive for each radar is linked to the database of the main site, which in turn is linked to a special network for this purpose and to make a connection between it and the institution's website. Overall, this drone photo capturing system presents a valuable tool for improved security and efficiency in airspace management. However, addressing privacy concerns and ensuring robust cybersecurity are crucial for successful implementation.

1. Introduction

The flow of drones in our current area in the airspace has raised great concerns in countries, as their illegal use has led to an increase in danger and breach of safety meanings, and the development in the challenges of detection and identification of these aircraft has become very important for the advanced detection of unauthorized drones By entering countries for fear of reaching sensitive institutional areas.[1] Therefore, determining the identity of the plane and the legality of its entry, either through jamming or hunting according to a specific system, seemed to be an issue that occupies the interest of most countries in the world.[3]

Unauthorized drones refer to drones that are not legal or permitted for use in specific areas or under certain circumstances.

This can include flying drones in restricted airspace, such as near airports or government facilities, or using drones without the necessary permits of licenses. [5]

2. Related Works:

The search term "A Review on Software-Based and Hardware-Based Authentication Mechanisms for the Internet of Drones" touched Emmanouel T. Michailidis in 2022. Each component of the heterogeneous air as well as ground network is linked together and outfitted with cutting-edge sensors, communication modules, and processing power. IoD network evolution presumes mitigation of numerous privacy and security concerns. Therefore, for achieving secure operation within the IoD, strong authentication methods should be established. Yet, developing lightweight and effective authentication solutions is a difficult task because of the intrinsic characteristics of the IoD and the power, computational, and memory limitations of unmanned aerial vehicles (UAVs). Setting up sophisticated sensors that are connected to a communications device, an air and ground network, and an approach of elliptical encryption, public key encryption, or machine learning for reducing privacy and security risks.

The article "On the Detection of Unauthorized Drones - Techniques and Future Perspective" by Hamid Menouar, Muhammad Asif Khan, Adnan Abu-Dayya, Aisha Eldeeb, and Flora D. Salim originally appeared in 2022. In order to safeguard individuals' privacy from drones, drone detecting systems are essential. A system for detecting drones that is accurate, reliable, strong, and affordable is required. Owing to the significance of the issue, numerous drone detection techniques were put out over time. Because of the intrinsic shortcomings of the underlying detecting technology, none of them offer adequate performance. Numerous performance criteria exist, including robustness against environmental conditions, accuracy, detection range, and more. This encourages a thorough examination and critical evaluation of current methods, stressing both their advantages and

Department of Computer Science, University of Technology, Baghdad, Iraq.
E-mail: suhiar.m.abdllsammed@uotechnology.edu.iq

disadvantages. This study presents a critical analysis regarding the state of the art and provides a comprehensive overview of current drone detection technology. We offer important insights into upcoming drone detection systems based on the review. We think that such revelations will enable researchers and engineers in the field a thorough understanding of the larger environment around the drone detection problem.

In 2015 Chris Sandbrook" The social implications of using drones for biodiversity conservation "Unmanned aircraft and their contribution to mitigating problems, and for the conservation sector to agree on a reasonable framework for self-regulatory use of unmanned aircraft without authorization to fly in the air. Until such research and regulation is done, it would be wise to avoid spreading the widespread use of non-conservation-authorized drones.

3. Drone Management System (DMS)

A drone management system (DMS) for hunting unauthorized drones involves using a combination of hardware and software tools to detect, track, and neutralize unauthorized drones. One common tool used in such systems is the drone detection sensor, which can be either radar or a camera-based system. Those sensors are capable of detecting if there is a drone in the airspace and present real-time data about its speed, location, and altitude [18]

Usually, DMS is based upon UAV Tracking and Management System that utilizes the data that had been obtained by the detection sensors of the radar for tracking the movements of the drone and providing alerts to system operators. The software may be programmed as well for automatically taking action to neutralize the drone, for example, jamming its control signals or using an anti-drone system to physically intercept and disable it and after that, the DMS systems may be utilized in various settings, such as event security and border security.[17] It should be noted that the use of the anti-drone technology is conditional on strict regulations in several countries and it is of high importance to make sure that any DMS system operates according to the local rules and regulations.

4. Unauthorized drones

There are many common systems for drone control that are utilized in the DMS for neutralizing the unauthorized drones, examples include: [14]

Radio Frequency (RF) Jamming: This system of drone neutralization works through cutting off communications between the drone and the operator. The jamming system transmits signal on a similar frequency to the control signal of the drone’s, which is effective in blocking the ability of the drone in receiving commands from the operator.

GPS spoofing: Some of the antidote systems utilize the GPS spoofing for tricking a drone into thinking that it’s somewhere else or flying at an altitude that is not actually precise. Which might cause the drone to lose its bearings and crashing or plummeting.

Laser systems: those can be utilized for disabling drones through targeting their electronic mechanisms, like navigation systems or camera. Lasers can be utilized as well for blinding the pilot of the drone, which makes it quite difficult for them to control the drone. [10]

Net Cannon: which can be defined as anti-drone system involving shooting a net at the drone for the purpose of disabling it. The web can get entangled with the propellers of the drone, which causes it to lose the power and fall down.

5. Some local laws and regulations of the use of the counter-drone technology

Laws and regulations of utilizing the counter-drone technology range from one country to another and those could get complicated. On other hand, here are a few examples of the local laws and regulations in various locations:[16]

US: where the FAA (i.e., Federal Aviation Administration) is responsible for the regulation of the use of the drones and counter-drone technology. This administration established guidelines for counter-drone technology operation, which included the restrictions on utilizing specific counter-drone system types near the other sensitive locations such as airports.

European Union: In the EU, using counter-drone technology is regulated by GDPR (i.e., General Data Protection Regulation) as well as other laws concerned with privacy. Those laws require that any data that are collected by the anti-drone systems should be lawfully and transparently processed and that the individuals have rights of accessing and controlling their private data.

UK: where CAA (i.e., Civil Aviation Authority) is responsible for the regulation of the use of drones and counter-drone technology. CAA established the rules for counter-drone technology use, which included the restrictions on using specific types of systems near the airports as well as other sensitive locations. [15]

Canada: Transport Canada is responsible for the regulation of counter-drone technology uses, it had set up guide lines for counter-drone technology uses, and that includes restricting the use of specific system types near some locations like the airports.

6. Counter-drone Technology Guidelines

There are many differences concerning counter-drone technology guidelines, as those differ by different countries and the technology application itself. On the other hand, some general instructions are recommended, often in cases of the DMS implementations with the counter-drone technology:

Abiding by the local laws: It should be ensured that any DMS system is operated based on the local drone operation and counter-drone technology regulations. This could be including obtaining the important permissions from the authorities. [11]

Minimizing collateral damage risks: Counter-drone technologies must be designed for minimizing collateral damages to properties, people, and other aircraft. Using kinetic counter-drone systems, like the laser system sorbet guns, must be considered carefully in order to avoid accidental consequences.

Risk assessment: which should be performed for the identification of the possible threats from the unauthorized drones and for the determination of appropriate counter-drone technologies form litigating such threats.

Privacy considerations: Counter-drone technology must be designed for respecting the rights to privacy and have to be utilized only for purposes it was intended for. Data that is collected by the counter-drone systems must be transparently and lawfully processed, and people must have the right of accessing and controlling their own data.

Coordination with the local authorities: and that includes aviation authorities and law enforcement, which could be highly important for ensuring the safety and effectiveness of counter-drone technology uses.

Training and proficiency: counter-drone technology operators need to undergo the necessary training and must be skillful in using the technology for ensuring effective and safe operations.

7. Drone Regulations

Several countries implemented regulations for governing drone uses, which include requirements related to registration, restricted designations of air spaces, and a penalty for operating drones with no proper authorizations. [16]. Such regulations have the aim of deterring the unauthorized drone operations and facilitating drone owner tracking.

8. Radar (Radio Detection and Ranging)

Radar (which is referred to as the radio detection and ranging as well) operates through transmitting microwave radio waves that reflect back to radar antenna when colliding with some object, such as another aircraft. Subsequently, the radar system computes the object's velocity and distance by measuring the time it takes for the waves to return. The shape and size of the item could be ascertained by the radar system using the strength of reflected signal. After that, this data is shown on a screen for operators to review. Pulsed radar and continuous wave radar are the two main aircraft detection technologies used by radar systems. [21] Pulsed radar emits brief radio wave bursts, or pulses, and after that pauses until the signal is reflected before emitting another pulse. The distance to the item is determined by measuring the interval between the pulse's transmitting and receiving. The drone's direction and speed could be ascertained by the radar system by sequentially sending out several pulses. Furthermore, the continuous wave radar constantly generates radio waves while monitoring for variations in the frequency of reflected signal brought on by the Doppler Effect. The shift in frequency that happens as a drone target moves in relation to a wave source, like radar, is known as the Doppler Effect. The radar system measures the Doppler shift to ascertain the direction and speed of an object. [12]

Modern radar systems often use a combination of these technologies, as well as other advanced signal processing techniques, to achieve higher resolution and better target discrimination. In addition, many radar systems are now equipped with computer algorithms and machine learning techniques that can help identify and track multiple targets simultaneously and without interference.

9. Materials and Methods:

In this section include proposed system design, suggested drone detection model.

9.1. Proposed System Design

The major idea of the system refers to dividing the area that we want to monitor in to four sections. Each section has its own radar to monitor the drones pass through its sky.

Each radar contains a hard disk that stores information about the drones.

The hard disk is connected to the system database where the database imports data from the radar when picking up any new drone.

When any new drone is captured, notifications will appear including that anew drone has been captured.

9.2. The Suggested Drone Detection Model:

In this section involves many steps, send data from radar, show a pop-up to information, and inter to condition yes or no. show in Figure 1., Figure 2., and Figure 3.

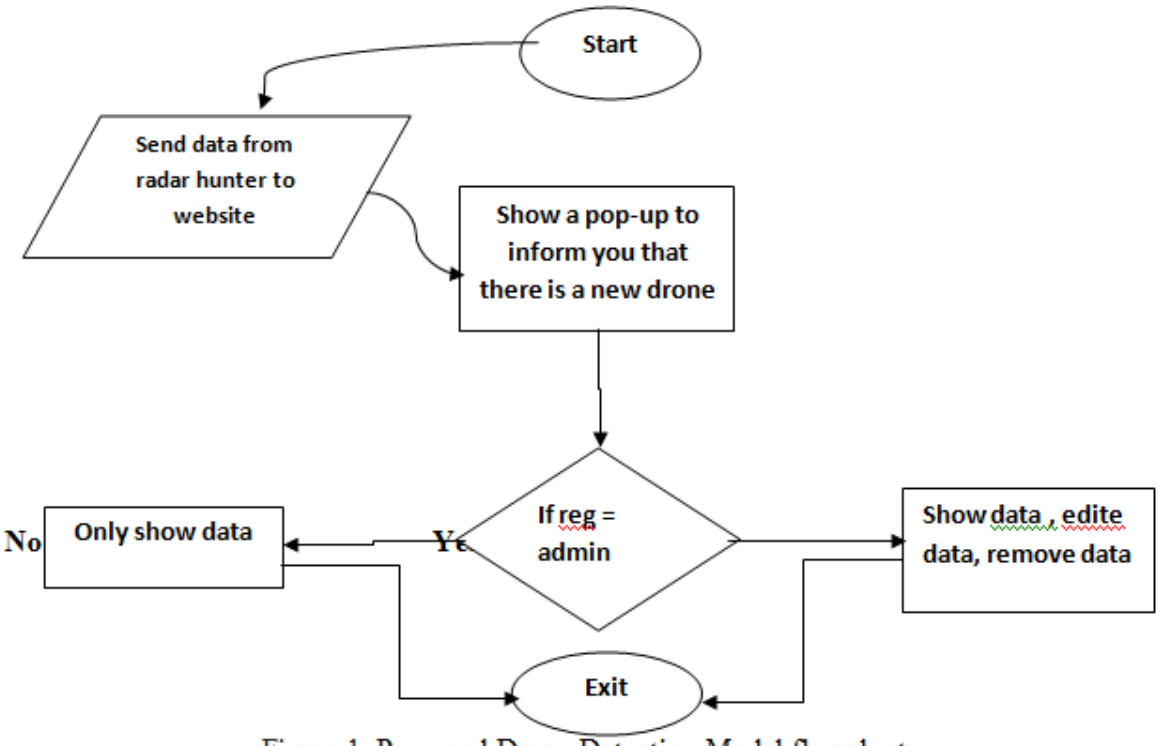

Figure 1. Proposed Drone Detection Model flowchart

Algorithm 1: Proposed system Algorithm.

Data: capture image drone
Result: Drone information
Initialization;
Perform drone detection and classification and payload recognition;
If capture image do not equals to the data in database program then
Perform perceived Threat Analysis;
Check Drone Data status
else
If object status harmful then
Show data;
Edit data;
Remove data;
Else
Just show data;
Show a pop-up that a new Drone;
end

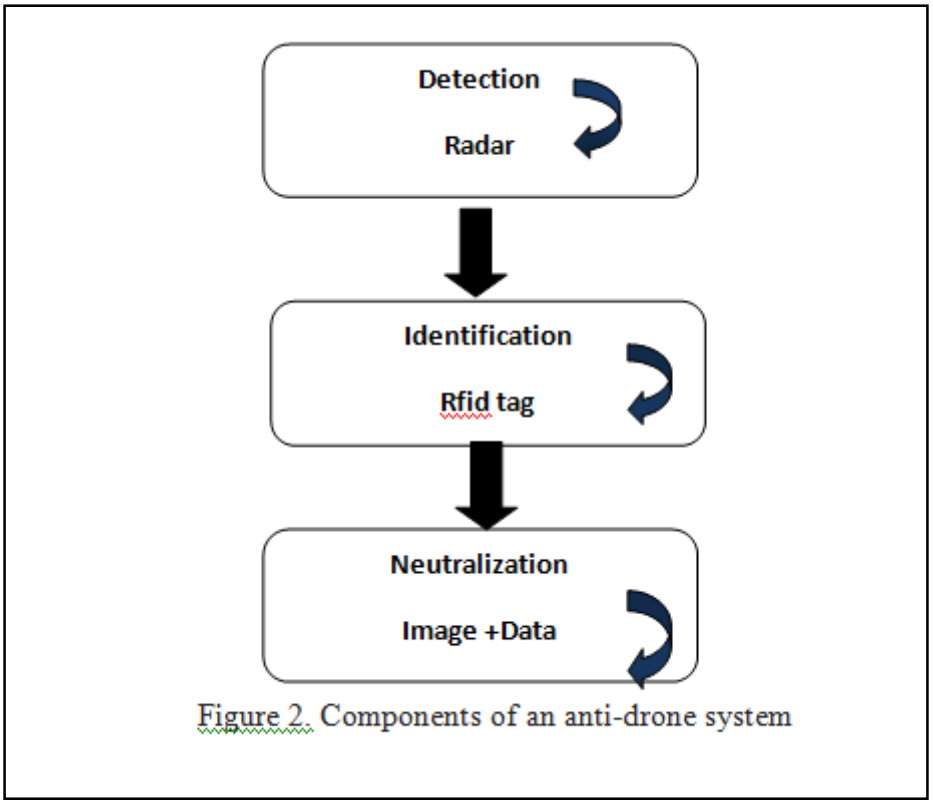

Figure 2. Components of an anti-drone system

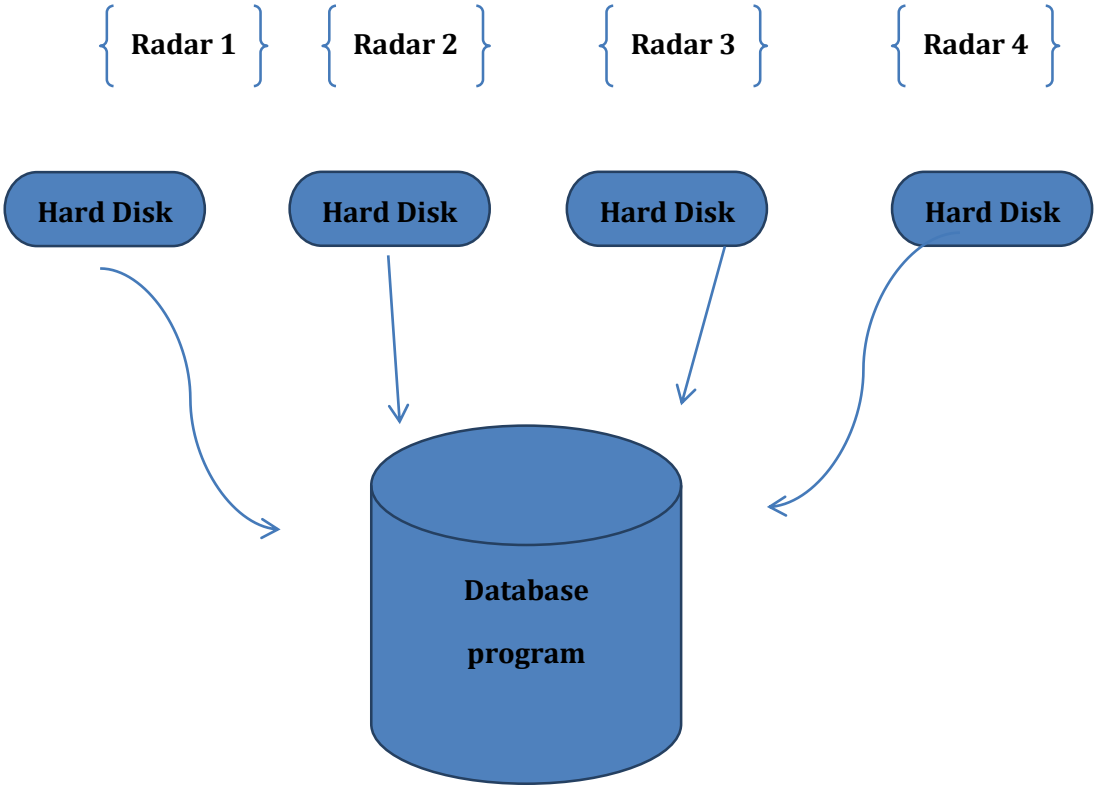

Figure 3. flowchart database program

9.3 Capture drone information

To capture drone information for use in radar chart, will need data on multiple variables that want to compare that could be relevant for a drone: as shown in Figure 4., Figure 5., Figure 6., Figure 7., Figure 8., and Figure 9.

Radar name	Image	Number	Name drone

Figure4.Information table

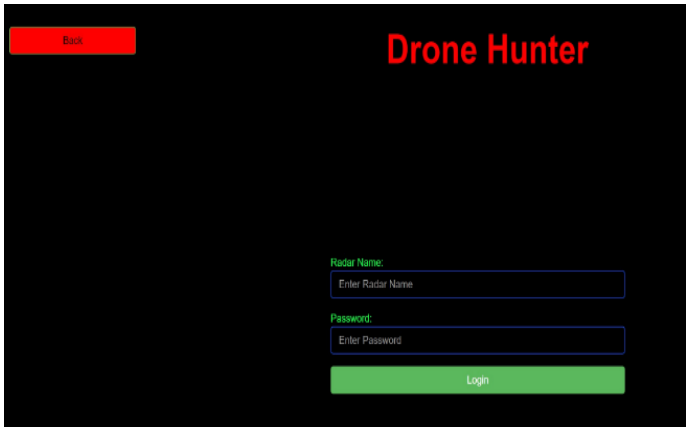

Figure5.Captured drone information

Figure 6 Information for Drones

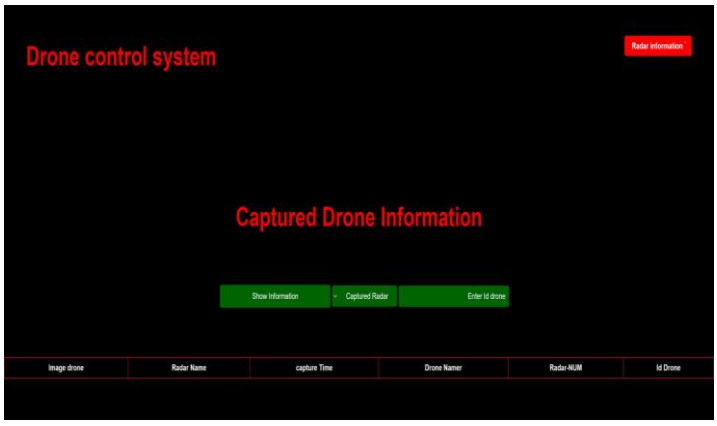

Figure 7 Login System

Figure 8 Radar System

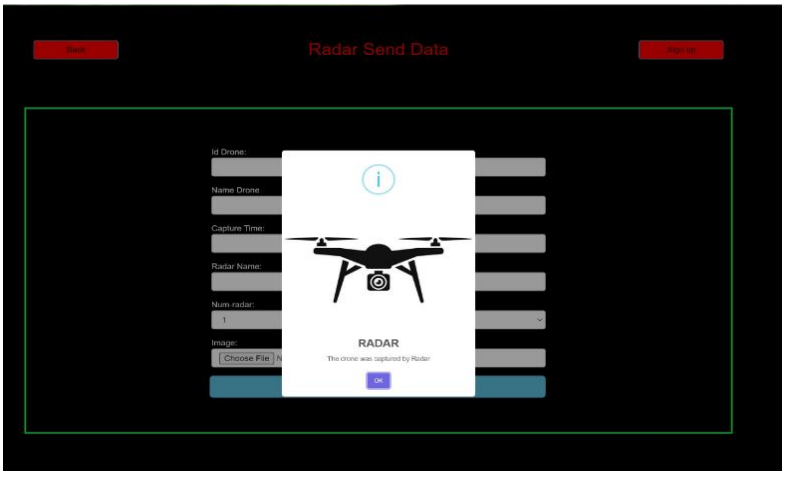

Figure 9 Radar saved Data

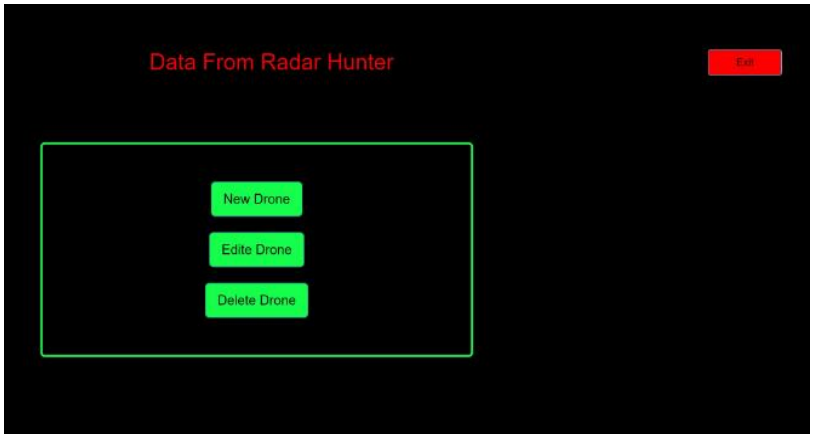

Figure 10 Radar Saved Data

9.4 Gather Data for the "Radar Hunter"

1- Manufactures 'Website by visiting the official website of the drone who captured by radar

2- Customer Reviews who have purchased and used the radar hunter

3- Check online drone retailers to find product descriptions and Specifications

4- Join drone enthusiasts and users to find discussions about the radar hunter as shown in Figure 10 Radar Hunter saved data.

10. Test and Result Methods:

In this section include the output of proposed drone management system radar hunter.

10.1 Output:

The output includes: sign up, how radar works, show data in system, analysis of system, challenges, improvements, value add, and author contributions.

10.1.1 Sign up

Authentication is essentially the process of verifying someone or something is who or what they claim to be. In the digital world, it's most commonly used to confirm a user's identity when trying to access a system or online account.

10.1.2 How a radar works

Detect drones When the radar senses a drone entering the area it is responsible for, it takes pictures of it and stores them on its hard drive.

Radar send data When the radar sends the captured drone data to the system database, the system will display notifications to the user that a new drone has been captured.

Data structuring The data is structured in tables containing the drone's name, its ID number, the time it was captured, the radar that captured it, and its ID number.

10.1.3 Show data in system

The data in the system is displayed in a table format. It is also possible to search for the data of each radar by its ID number.

10.1.4 Analysis of system

System Features:

- ✓ **Data Collection**: The system collects vital information about drones, such as their name, ID number, the ID number of the radar that captured the images, and photos of the drone.
- ✓ **Tracking**: The system allows for tracking the movements of drones within its designated airspace.
- ✓ **Security**: The system aids in monitoring the airspace and preventing unauthorized activities.
- ✓ **Data Analysis**: The collected data can be used to analyze drone traffic patterns and identify potential risks.

10.1.5 Challenges:

- **Privacy**: Collecting drone data may raise privacy concerns.
- **Cybersecurity**: The system must be secured against hacking and cyberattacks.
- **Integration**: Integrating the system with other systems, such as air traffic control systems, can be challenging.
- **Cost**: The cost of installing and maintaining the system can be high.

10.1.6 Improvements:

- **Integration of Artificial Intelligence Techniques**: AI can be used to analyze images automatically and identify suspicious drones.
- **Developing an Interactive User Interface:** A user interface can be developed to allow users to view and analyze data easily.
- **Enhancing Integration with Other Systems:** The system can be integrated with other systems, such as air traffic control systems, to enhance security and efficiency.

10.1.7 Value Added:

- **Improved Security:** The system helps improve security and prevent unauthorized activities.
- **Increased Efficiency:** The collected data can be used to enhance the efficiency of aerial operations.
- **Decision Support:** The collected data aids in better decision-making.

A drone photo capturing system is a valuable system that can be used to improve security and efficiency in various domains. However, certain challenges, such as privacy and cybersecurity, need to be addressed.

10.1.8 Author Contributions

- Conceptualization
- Data creation
- Formal analysis
- Funding acquisition
- Investigation
- Methodology
- Project administration
- Resources
- Validation
- Writing—original draft
- Writing—review and editing

11. Conclusions

To close such gap in current anti-drone system designs which concentrate only on drone detection with minimal effort for harmful screening, a 4-radar designed program for the purposes of attachment object identification, drone detection, and a secure channel neutralization model are presented in this work. Four radars have been utilized to upload drone images and capture several drone models of varying sizes in cloudy circumstances in order to provide superior detection and extensive coverage for identification. The image of the drone, its number, and the radar number that detected it are also recorded in a database along with other relevant information about the intended drone. This information is after that compared to the database that has been stored to ascertain whether or not the drone is listed as authorized to enter the airspace. Those results set important new standards for the development and design of anti-drone systems, which serve as a defensive mechanism to maintain safety and order in both international and domestic airspace and to restrict the use of drones for illicit purposes without permission or entry authorization.

However, there are still issues such as inaccurate identification associated with Drone identification ofDrone and other objects camouflaged in their surrounding environment, and identification of Drone in international airspace so the need to address remains for robust performance of spot-based counter vision and trapping Within unmanned aircraft system.

References

[1] Tao, J.; Han, T.; Li, R. Deep-Reinforcement-Learning-Based Intrusion Detection in Aerial Computing Networks. IEEE Netw. 2021, 35, 66–72.

[2] Taha, B.; Shoufan, A. Machine Learning-Based Drone Detection and Classification: State-of-the-Art in Research. IEEE Access 2019, 7, 138669–138682.

[3] Shi, X.; Yang, C.; Xie, W.; Liang, C.; Shi, Z.; Chen, J. Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges. IEEE Commun. Mag. 2018, 56, 68–74.

[4] Floreano, D.; Wood, R.J. Science, Technology and the Future of Small Autonomous Drones. Nature 2015, 521, 460–466.

[5] Park, S.; Kim, H.T.; Lee, S.; Joo, H.; Kim, H. Survey on Anti-Drone Systems: Components, Designs, and Challenges. IEEE Access 2021, 9, 42635–42659.

[6] Haviv, H.; Elbit, E. Drone Threat In addition, CUAS Technology: White Pape. Elbit Syst. 2019, 1, 1–20.

[7] Ripley, W. Drone with Radioactive Material found on Japanese Prime Minister's Roof. CNN.com. 2015. Available online: https://edition.cnn.com/2015/04/22/asia/japan-prime-minister-rooftop-drone/index.html (accessed on 31 January 2022).

[8] Reuters. Greenpeace Slams Superman-Shaped Drone into Nuclear Plant. New York Post, 3 July 2018; Volume 1, 1–2.

[9] Phillips, C.; Gaffey, C. Most French Nuclear Plants 'should be shutdown' over Drone Threat. Newsweek Magazine, 24 February 2015; Volume 1, 1–3.

[10] Hubbard, B.; Karasz, P.; Reed, S. Two Major Saudi Oil Installations Hit by Drone Strike, and US Blames Iran. The New York Times, 14 September 2019.

[11] Akter, R.; Doan, V.S.; Lee, J.M.; Kim, D.S. CNN-SSDI: Convolution Neural Network Inspired Surveillance System for UAVs Detection and Identification. Comput. Netw. 2021, 201, 108519.

[12] Gopal, V. Developing an Effective Anti-Drone System for India's Armed Forces. Obs. Res. Found. Issue Brief 2020, 1, 1–20.

[13] Çetin, E.; Barrado, C.; Pastor, E. Counter a Drone in a Complex Neighborhood Area by Deep Reinforcement Learning. Sensors 2020, 20, 2320.

[14] Bhatnagar, S.; Gill, L.; Ghosh, B. Drone Image Segmentation Using Machine and Deep Learning for Mapping Raised Bog Vegetation Communities. Remote Sens. 2020, 12, 2602.

[15] Bemposta Rosende, S.; Sánchez-Soriano, J.; Gómez Muñoz, C.Q.; Fernández Andrés, J. Remote Management Architecture of UAV Fleets for Maintenance, Surveillance, and Security Tasks in Solar Power

[16] Plants. Energies 2020, 13, 5712.

[17] Sun, H.; Yang, J.; Shen, J.; Liang, D.; Ning-Zhong, L.; Zhou, H. TIB-Net: Drone Detection Network With Tiny Iterative Backbone. IEEE Access 2020, 8, 130697–130707.

[18] Carrio, A.; Tordesillas, J.; Vemprala, S.; Saripalli, S.; Campoy, P.; How, J.P. Onboard Detection and Localization of Drones Using Depth Maps. IEEE Access 2020, 8, 30480–30490.

[19] Shi, Z.; Chang, X.; Yang, C.; Wu, Z.; Wu, J. An Acoustic-Based Surveillance System for Amateur Drones Detection and Localization. IEEE Trans. Veh. Technol. 2020, 69, 2731–2739.

[20] Dogru, S.; Marques, L. Pursuing Drones with Drones Using Millimeter Wave Radar. IEEE Robot. Autom. Lett. 2020, 5, 4156–4163.

[21] Alnuaim, T.; Mubashir, A.; Aldowesh, A. Low-Cost Implementation of a Multiple-Input Multiple-Output Radar Prototype for Drone Detection. In Proceedings of the 2019 International Symposium ELMAR, Zadar, Croatia, 23–25 [22] September 2019; pp. 183–186.

[23] Guvenc, I.; Koohifar, F.; Singh, S.; Sichitiu, M.L.; Matolak, D. Detection, Tracking, and Interdiction for Amateur Drones. IEEE Commun. Mag. 2018, 56, 75–81.