Unmanned Aerial Vehicle Forensics Investigation Performance under Different Attacks

Taiwo Ojo
Dept. of Computer & info Sciences
Florida A&M University
Tallahassee, FL, USA
taiwo1.ojo@famu.edu

Hongmei Chi
Dept. of Computer & info Sciences
Florida A&M University
Tallahassee, FL, USA
hongmei.chi@famu.edu

Samuel Kofi Erskine
Dept. of Computer & info Sciences
Florida A&M University
Tallahassee, FL, USA
samuel.erskine@famu.edu

***Abstract*—Unmanned Aerial Vehicles (UAVs), also called drones, have grown tremendously in recent years and have been adopted in various sectors. With the continuous development of machine learning algorithms to detect various attacks on UAVs. The attackers also focused on utilizing this machine-learning algorithm to disrupt the UAV's activities by using predictions to generate the attack route. In digital forensics, the forensics experts focus on the communication data between the controller and the drones, the multimedia files, and the flight data to make a complete cybersecurity report. This paper reviews various ways the drone may be compromised and its performance evaluation using the existing machine learning detection algorithm to make the forensics report about the drones. The machine learning algorithms investigated in this study include Multilayer Perceptron (MLP) for the detection technique.**

Keywords—Drones, Machine Learning, Cyber-Attacks, Digital forensics

I. INTRODUCTION

In recent years, the application of Unmanned Aerial Vehicles (UAVs) to day-to-day activities has improved tremendously. These applications are not limited to military use alone but include plant protection, parcel delivery, medical rescue, entertainment, etc. Fig. 1 below shows the various applications of drones in this current age and not just the general knowledge; these drones can be used specifically as IoT devices to carry out investigations and analyses of various operations they set to accomplish. This application makes its usage more popular among the masses, making it susceptible to attacks.

With this increase in usage comes many complications ranging from direct physical attacks in the form of natural weather issues to cyber-attacks, which significantly undermine the efficiency of drones in performing specific tasks. According to the statistics of the registered UAVs with the FAA [1], we can see an increment in the number of commercial drones. In contrast, recreational drones have the highest number registered in the United States of America. These drones can be used under various scenarios to serve as evidence for criminal investigation if they are present at the crime's location.

For the UAVs designs, investigations have primarily focused on the communication aspect of the UAV designs, which only amounts to the attack-level element of the cybersecurity field. Several authors have examined how drones can be compromised to investigate attacks, such as spoofing, hacking, generative adversarial attacks, etc. This attack only focused on the misdirection of the drone to a particular place or scenario. Investigating these scenarios requires the knowledge of a forensics expert to check the type of evidence needed from the drone, whether the flight log, the GPS position, or the data from any of the sensors, such as lidar, images, videos, and point cloud data. This data is then adopted as evidence in a chain of events or criminal investigations.

The importance of UAVs in day-to-day activity has significantly improved from what the military and government agencies used them. The recent survey of the use of UAVs in developing countries and war region requires drones to be deployed to monitor the situation around the camp or the area. Investigating these scenarios for various reasons and decisions requires the knowledge and technique of a forensics expert. This data can be used as an evidence chain and in planning and strategizing for the wars around them.

Contributions to this paper will include:

i. The review of various machine learning algorithms adopted on drone technology.
ii. The application of ML application to the E Bee X drones to generate an attack
iii. The forensic performance report from detecting compromised drones.
iv. Case study of attack on traffic monitoring with the E - Bee X drone under the ML-generated attack on multimedia and flight data.
v. A review for current digital forensic technology in drones

This paper is organized as follows: The introduction in Section I, followed by the background in Section II. The literature review is in Section III. Section IV discusses the new methodology and implementation. After the implementation is structured, the result and discussion are presented in Section V. Section Vi, and the final section is the conclusion and future work.

979-8-3503-2028-2/22/$31.00 ©2022 IEEE
DOI 10.1109/CSCI58124.2022.00235

II. BACKGROUND

Drone forensics plays a critical role in various investigation and modern society and lacks efficacy studies. From the cyber-crime investigation's view, drone forensics is high demanded. Drone forensics needs a thorough examination: for example, how the drone is being used and what purpose they are being used for. Table 1 shows the statistics on the registered drone in the United States. Due to the increased usage of drones, there will be different scenarios in which these drones are applied.

Table 1: Drones by the Numbers

Types of registration	Total Number
Drones Registered	861,669
Paper registration	3,569
Commercial drones registered	321,611
Remote Pilots Certified	290,369
Recreational drones registered	536,489
TRUST Certificates Issued	316,340

This research paper primarily focuses on investigating the use of the commercial vehicle using digital forensics expertise by utilizing machine learning algorithms. Several research papers have been done on manipulating multimedia data, such as deepfakes [3 - 6], attacking the communication links between drones and operators. The deepfake technology allows images and videos to be manipulated, greatly reducing its effectiveness as a source of evidence for any legal use [8].

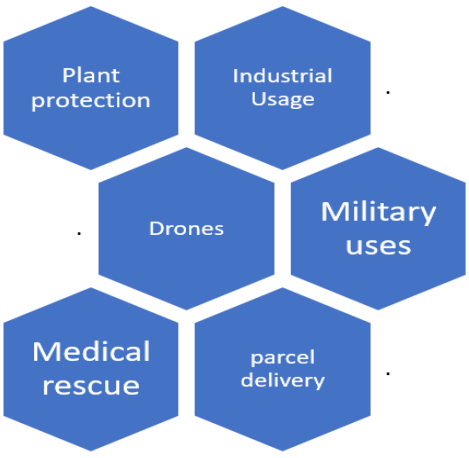


Fig. 1: Applications of UAVs

Drones are readily available for deployment in hard-to-access locations for delivery of critical medical supplies, surveillance, weather data collection, and home delivery of purchased goods.

The various applications of these drones are shown in Fig. 1, which makes monitoring and policy-making essential. As stated earlier, the increase in registered drones in the united states shows that the technology of drones is advancing. With advancing technology, the forensics framework in investigating these scenarios also changes. The various uses of drones include search and rescue, surveillance, traffic monitoring, weather monitoring, firefighting, personal use, drone-based photography, and videography. The two basics of drones are flight mode and navigation.

The drone's usage depends on which assignment or category of need it is addressing. The features of each drone are varied based on the components and sensors that are attached to it. The popular feature of drones based on their applications is artificial intelligence (AI) which makes the drones to be able to perform the following assignment:

- Augmented reality that virtualizes real-time object
- Object identification during flight time
- Media storage format based on the connection
- Hover Accuracy
- Obstacle sensory range

All these activities listed above require applying machine learning techniques to function effectively. Using machine learning in these drone applications, even though it increases efficiency, makes it difficult for digital forensics as there are various ways in which these techniques can be attacked or tampered with. Another scenario is the case of a shortage in storage capability or direct interference in the flight logs, which makes it difficult to trace the evidence-gathering aspect of the drones.

Investigating the drone forensics not only relied on just applicable tools such as Autopsy, FTK imager, OSforensics, etc. but machine learning algorithms can also be used to check the performance of the result and evidence gathered from the drones. Since the inception of deepfakes, there are many ways in which the drone result can be manipulated which make it difficult to be accepted in the aerial crime investigations. Also, the altitude of the drone also play significant roles in perfectly identifying or portraying the scenarios on a minute level.

The increase in the usage of generative adversarial network (GAN) shows that, if the distance of the drone is far and the speed of flying is increased, the evidence acquired can be tampered. To address these issues, several machine learning algorithm such as [5 – 7] have been employed to investigate the performance and the authenticity of the evidence acquired for digital forensics investigation. Also, Deep learning, Artificial Neural Networks (ANN) are primarily used with the drones for detecting far and near object and makes it easy for the drone to scan a region and a good use for transport monitoring and evidence capture in various traffic crime investigation. Not only traffic investigation, it was also employed in agriculture in

identifying different stalks of plantation for diseases and pest control mitigations [2].

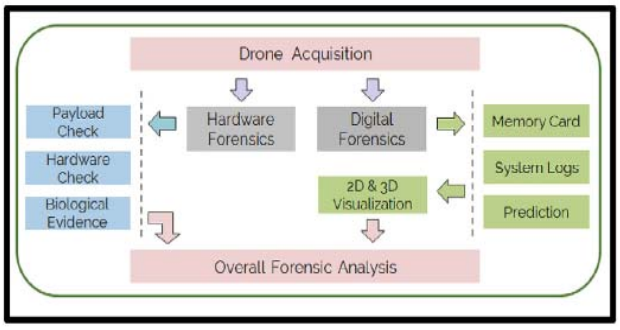
III. Related Work

Unmanned aerial vehicles (UAVs) are aircraft with self-piloting capabilities. The UAVs are considered under the autonomous system designs and can be remotely controlled. Flight time can go for an extended period depending on the UAV's speed and height, and it plays a vital role in aviation.

UAVs have come to the limelight in any smart city environment and monitoring. Several applications of it have been adopted by many industries, not limited to Agriculture, Transportation, Delivery, etc. Digital forensics is essential in investigating UAVs for security and accountability. Most of the use of digital forensics for UAVs systems is majorly in academic works [7, 8, 9, 10].

AI and ML have significant advantages and hold a bright future ahead. But the same technology can inevitably be used to craft, automate, and execute some serious crimes that can also be deadly for people. For instance, hackers can develop an ANN that scans new versions of popular apps for unknown vulnerabilities, exploit them, and report the vulnerability to the hacker. If this process is done manually, it can take a long time to pretest an app. But with the help of ML, it can be done quickly and can be done on multiple different apps at the same time with machine efficiency. It makes the job for hackers easy and quick [10].

Renduchintala [11] proposed the drone forensic framework to analyze flight log data. This shows in Fig. 2, which explains the process of performing the digital forensic acquisition and investigation on the drone. The first step is to acquire the data directly from the hardware chip; then the software from which the drone is being controlled.



Fig, 2: Drone Forensic Framework [11]

Investigating how your drone attacked has become the primary focus since the inception of adversarial networks. Controls and electrical engineers have proposed multiple models showing how these attacks are carried out.

A review of the literature revealed that scholars and developers have generally approached the DRFs field through various categories such as (1) forensic analysis, (2) non-forensic analysis, (3) forensic framework, and (4) application in forensic analysis. A total of 29 models were found in the literature review process, as shown in mantas et al., which were entirely centered upon the DRFs topic. For example, [1] discusses how to recover the required evidence in case a drone is investigated under digital forensics circumstances. These studies mainly focused on the wireless forensic aspects, whereas [1] centered on all drone parts.

In this paper of drone forensics, Hana B. et al. [5] propose a case study on parrot AR drones where he utilizes the general acquisition techniques for regular IoT devices to extract the data and recreate the event based on the data acquired.

Similarly, a study in [1] forensically analyzed the DJI Phantom 2 Vision Plus to answer the following critical question: "Can the flight path of a UAV be reconstructed with the use of positional data collected from a UAV?". In addition, a concise investigation of counter forensic methods was conducted to ascertain the flight path record. In another research, a preliminary forensic analysis of the Parrot Bebop [2]. The Parrot Bebop can be named the only UAV comparable with the Parrot AR Drone 2.0. From the research in [1], the author addressed the critical challenges in UAV forensic analyses and then carried out his investigation on two separate parts: the UAV and the flight controller. The flight-related data were retrieved from the device in '.pud' file folder.

Along with the growing number of novel solutions for wireless networks during the last few years, several recent surveys focusing on the interplay of AI/ML and wireless communications have been provided. Findings from [5] showed that if a UAV is turned on, the integrity of the data kept in its internal storage can be impacted. New .dat file was generated each time the UAV was turned on. Moreover, it was found that in case the SD card was at or near its total capacity, turning on the UAV caused the immediate removal of the oldest data in a way that was not coverable later. As stated by [5], although their research offered an appropriate point to start UAV forensic analysis, further research is required to cover the broad range of UAVs obtainable presently.

In addition, the study in [7] provides a comprehensive discussion regarding the ways the GPS coordinates can be applied as location evidence when investigating crimes committed using drones. The authors, as mentioned above, attempted to extract the system logs. They also visualized GPS coordinates on maps, where web-based third-party platforms were employed to plot the flight path. In another project, a forensic model was introduced by [6] to determine and authenticate different drone components that can be employed in committing unlawful deeds. They were centered on the analysis of physical evidence gathered by investigators from the crime scene along with GPS-related data and any multimedia found on board. Their research was carried out on five commercial drones and their components once seized at crime scenes.

IV. METETHOLOGY

To investigate drone forensics, the framework introduced in this research is to utilize the communication network between the drone and the sender to develop the drone path. The method employed in this study was to use the knowledge of machine learning to identify discrepancies in the evidence gathered. The scenarios for these studies were focused primarily on gathering evidence based on object identification of the machine learning method. Knowing the increase in the technology of the deepfake, how can drone forensics be identified without using any existing tools and focusing on developing an algorithm from the standard known machine learning techniques?

Based on paper reviews [14] and the needs in the current drone forensics, Multilayer perceptron was applied in extracting the evidence out from the drones. These extraction techniques are based on the drone successfully identifying objects while not storing them in the primary storage of the drone. The connection for the drone was on the eMotion app, which is mainly used to plan and deploy the drones for their various uses.

A. Datasets

The dataset used in this research was an eBee X drone, a lightweight mapping drone for broad coverage and sharp data. It is designed to provide 1.5 cm / 0.6 in of absolute accuracy with available RTK / PPK and to cover an area up to 500 ha/1,235 ac. Offering up to 90 minutes of flight time, the3.6 lbs fixed-wing photogrammetry drone meets the highest standards of various industries.

The picture of the drone is shown in Fig. 3 below, and the dataset is based on the installed camera type presented on the drone during the flight, which can be a 3D, RGB, multispectral or thermal camera. For this investigation, the data was stored in RGB format. The dataset was taken from the transportation environment.

Fig. 3 The eBee-X fixed-wing drone

The drone setup is on deciding on what type of data is being analyzed. The network signal needs to be unobstructed, as shown in Fig 4 below.

Fig. 4: The drone setup

B. Flight Information

The flight information was planned with the eMotion app, which is displayed in Fig. 4 below. It is mainly used to form the path in which the drone will fly. This area was set to the Campus environment based on its radius and altitude and heavily relied on the latitude and longitudes for its positioning.

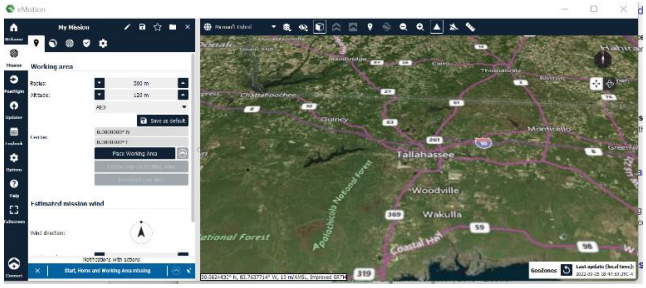


Fig. 5: The eMotion Outlook

C. Scenario Preparation.

The scenario for the investigation was that the drone could detect the car moving in the neighborhood during a specific period. The investigation avoided heavy trees to cover the camera to picture the object better. This investigation was focused more on object detection to provide evidence for the investigator.

D. Multi-Layer Perceptive (MLP) for Drone Forensics

The MLP algorithm solved the problem of examining the latitude and longitudinal data of the drones to check if it was swapped while the evidence was ongoing. The process of the method is seen in Fig. 5, and it explains the basics of how the operation was performed.

The MLP algorithm focuses on detecting specific evident chains from the collected data and verifying with the existing system if the data have been collected. The environment is set up on the eMotion app and is also the drone's main controller. The communication link is based on the signal receiver, and the drone is expected to fly for approximately 50 minutes for one duration.

The first step in the detection algorithm is to identify the number of moving objects, and after the object is identified, it checks to see what type of moving object it is after the identification is made, it marks the position of the object, and the time at which the object was taken.

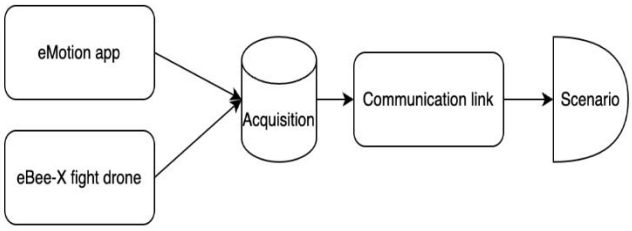


Fig. 6: The project guideline step in investigating

The approach to deploying the drone is shown in Fig. 6, which explains the steps of data acquisition for any drone. We establish a connection between the drone and the software application, and this scenario is planned according to the GPS position or using the longitude and latitude. These details are communicated to the drone, which then aids its flight path. The data stored in the drone comprises the communication log files, the flight log data, the video, and the pictures of the specific region. The multilayer perceptron is then applied through the eMotion app for detection.

In the eMotion app, the data stored can allow for the spatial manipulation of the actual position of the drones, which can render the evidence acquired from such drones ineffective. The postflight data and the logbook are also part of the analysis to determine how effectively the result is acquired.

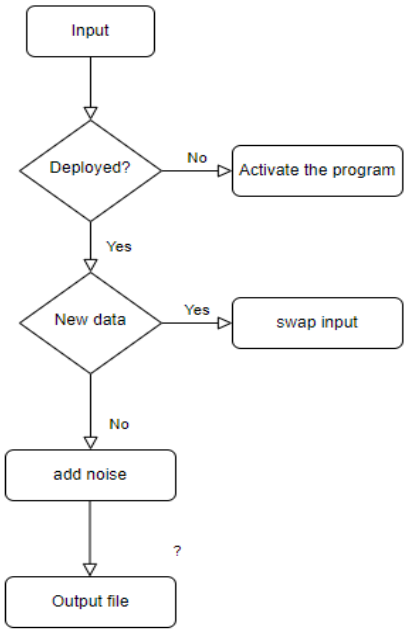


Fig. 7: The process of data verification with MLP

V. Results and Discussion

The use of UAVs in forensic applications for evidence detection can be beneficial for small law enforcement office or organizations since these low-cost and easy-to-use platforms can help in crime scene or accident investigation and serve as legal evidence for prosecuted offenders.

In specific, considering the results of natural image recording, it should be highlighted that drone deployment can achieve high detection rates of nearly 100%. However, it should be noted that the degree of drone's accuracy depends on the flight settings. Therefore, for the detection of such small objects in the environment have to do with the height of the drone deployed and at what speed the drone is moving. It was decided the drone would fly at the height of 6 m, at a speed of up to 7 kph, and with a window overlap of 33% where the changes result in an increase of the flight speed or altitude and a decrease of the degree of scan, overlap could have a negative impact on achieving extremely high detection rates.

The result of the investigation is shown below in Fig. 7 by showing the position of the drone and the selected object as

shown in Fig 8 about the spatial displacement of the object and their correspondence positions.

Fig. 8: The positioning

The machine learning algorithm was used to investigate how accurate the detection algorithm was. The result presented in Fig 9 shows the success rate of the drone object detection based on the height of the drone and different terrains in which the drone was flown. The blue plot shows the field location while the red shows just the drone detection accuracy based on the distance of the drone to the ground level and what type of object needed to be identified.

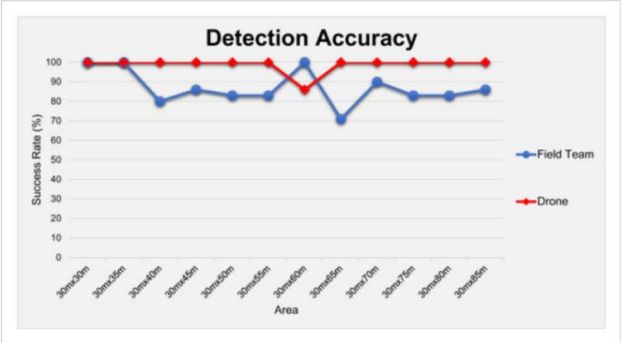


Fig. 9 The accuracy of the image data successfully identified

However, it should be noted that color-based detection method using computer vision techniques can increase rates of false alarms when, for example, a shadow is detected as a black object. The rate of false alarms depends on the ground complexity. In specific, a terrain of red clay soil with green vegetation, white stones, and shades of adjacent trees can lead to increased false alarms. (i.e., red due to soil, green due to vegetation, white due to stones, black due to shadows) if the sensitivity settings (i.e., the color detection threshold) are not properly adjusted. Nevertheless, there are advanced software tools, such as the "TensorFlow Object Detection" [7], which can detect various objects such as vehicles, TV monitors, chairs, or even people. If these tools are enriched with forensic-valuable objects (e.g., weapons and bomb components), and they can be used to facilitate evidence detection without confronting the false alarms resulting from color-based detection algorithms.

Furthermore, from the above, it should be noted that drone deployment is adherent to communication data links since a connection loss or signal degradation results in a spatial discontinuity in the coverage of the area of interest. This was the case with the two missing detections in the single-colored scenarios. Specifically, a blur disturbance occurred as a result of the degradation of the RF signal between the drone and the eBee X (eMotion) remote controller, mostly due to the distance between them or secondarily due to interference from other nearby signals (Wi-Fi IEEE 802.11 also operates in the same bandwidths with the controller, i.e., 2.4 GHz [3, 5, 6]).

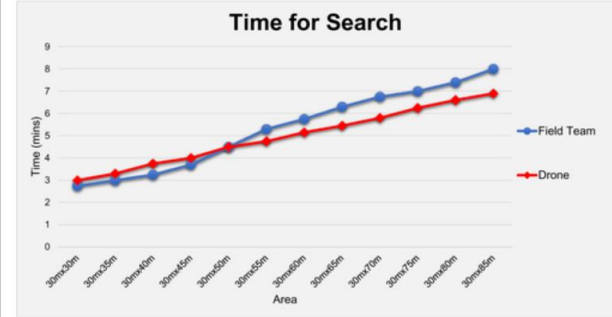


Fig. 10: The time required to complete the process

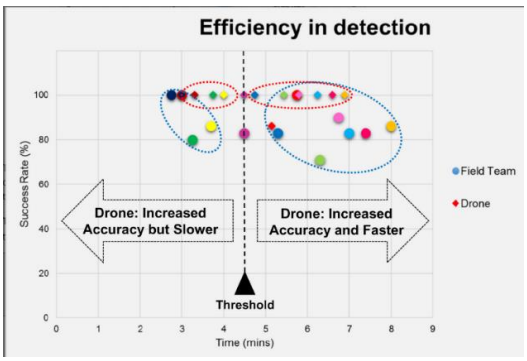


Fig. 11: Performance evaluation of various object

The performance of the MLP algorithm reflects the position of the object with respect to the location of the evidence site. The cluster shown in Fig. 10 explains the time it takes for evidence to be identified. Fig 11 shows that the initial stage of the drone flying, the detection accuracy is high but it takes longer time to identify the authenticity of the image acquired and this improved as the drone flew for longer periods. The learning rate of the algorithm is based on the level of data the drones acquired and it is learning as it is flowing over the area of investigation. The longer time in the same area, the higher the efficiency of the drone detecting the objects accurately.

VI. Conclusion & Future Work

The current research project investigated the usefulness of MLP in real-time evidence detection and gathering using UAVs for crimes and traffic investigation. The method selected shows 100% in detecting the type of object or the specific model of the vehicles being used, but in identifying the car plate, the detection is about 80% which was greatly influenced by the type of camera being used and the angle at which the monitoring was done.

To further investigate the plate number and identify the object in the moving vehicle for high-level detailing. More ML models will also be investigated to see if we can have a high-level success rate in determining the vehicle owner by focusing on the vehicle plate number and running it through the city database system.

More scenarios will also be examined to test more about the efficiency of the detection by grouping the data collected. Since this article only focused on object detection and grouping.

Acknowledgment

This research was partly funded by the National Centers of Academic Excellence in Cybersecurity Grant (H98230- 21-1-0326), which is part of the National Security Agency. The research was partly sponsored by the Army Research Office and was accomplished under Grant Number W911NF-21-1-0264. The views and conclusions contained in this document are those of the authors. They should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes, notwithstanding any copyright notation herein.

References

[1] https://www.faa.gov/uas, Accessed on 09-03-2022,

[2] Alotaibi, F. M., Al-Dhaqm, A., Al-Otaibi, Y. D., & Alsewari, A. A. (2022). A Comprehensive Collection and Analysis Model for the Drone Forensics Field. *Sensors*, *22*(17), 6486.

[3] Baig Z, Khan MA, Mohammad N, Brahim GB. Drone Forensics and Machine Learning: Sustaining the Investigation Process. *Sustainability*. 2022; 14(8):4861. https://doi.org/10.3390/su14084861

[4] Jafar, Mousa Tayseer, et al. "Forensics and analysis of deepfake videos." *2020 11th international conference on information and communication systems (ICICS)*. IEEE, 2020.

[5] Ferreira S, Antunes M, Correia ME. A Dataset of Photos and Videos for Digital Forensics Analysis Using Machine Learning Processing. *Data*. 2021; 6(8):87. https://doi.org/10.3390/data6080087

[6] Mantas, Evangelos, and Constantinos Patsakis. "Who watches the new watchmen? The challenges for drone digital forensics investigations." *Array* (2022): 100135.

[7] Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection: A survey." *Computer Vision and Image Understanding* 223 (2022): 103525.

[8] Clark, D., Meffert, C., Baggili, I., and Breitinger, F. (2017). "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III", Digital Investigation, vol.22, pp.3-14. doi:10.1016/j.diin.2017.06.013.

[9] Horsman, G. (2016). "Unmanned Aerial Vehicles: A Preliminary Analysis of Forensic Challenges". Digital Investigation, vol.16, pp.1-11.

[10] Jain, U.; Rogers, M.; Matson, E.T. Drone forensic framework: Sensor and data identification and verification. In Proceedings of the 2017 IEEE Sensors Applications Symposium (SAS), Glassboro, NJ, USA, 13–15 March 2017; pp. 1–6.

[11] Renduchintala, A.L.P.S., Albehadili, A., Javaid, A.Y., 2017. Drone forensics: digital flight log examination framework for micro drones, 2017. In: International Conference on Computational Science and Computational Intelligence (CSCI). Presented at the 2017 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, Las Vegas, NV, USA, pp. 91e96. https://doi.org/10.1109/CSCI.2017.15

[12] Taeb, M., & Chi, H. (2022). Comparison of Deepfake Detection Techniques through Deep Learning. *Journal of Cybersecurity and Privacy*, *2*(1), 89-106.

[13] Taeb, M., Chi, H., & Bernadin, S. (2022). Digital Evidence Acquisition and Deepfake Detection with Decentralized Applications. In *Practice and Experience in Advanced Research Computing* (pp. 1-2).

[14] Baig Z, Khan MA, Mohammad N, Brahim GB. Drone Forensics and Machine Learning: Sustaining the Investigation Process. *Sustainability*. 2022; 14(8):4861. https://doi.org/10.3390/su14084861