sustainability

MDPI

Review

Drone Forensics and Machine Learning: Sustaining the Investigation Process

Zubair Baig [1,*], Majid Ali Khan [2], Nazeeruddin Mohammad [3] and Ghassen Ben Brahim [2]

[1] School of Information Technology, Deakin University, Geelong 3216, Australia
[2] College of Computer Engineering and Science, Prince Mohammad Bin Fahd University, Khobar 34754, Saudi Arabia; makhan@pmu.edu.sa (M.A.K.); gbrahim@pmu.edu.sa (G.B.B.)
[3] Cybersecurity Center, Prince Mohammad Bin Fahd University, Khobar 34754, Saudi Arabia; nmohammad@pmu.edu.sa
* Correspondence: zubair.baig@deakin.edu.au

Abstract: Drones have been increasingly adopted to address several critical challenges faced by humanity to provide support and convenience . The technological advances in the broader domains of artificial intelligence and the Internet of Things (IoT) as well as the affordability of off-the-shelf devices, have facilitated modern-day drone use. Drones are readily available for deployment in hard to access locations for delivery of critical medical supplies, for surveillance, for weather data collection and for home delivery of purchased goods. Whilst drones are increasingly beneficial to civilians, they have also been used to carry out crimes. We present a survey of artificial intelligence techniques that exist in the literature in the context of processing drone data to reveal criminal activity. Our contribution also comprises the proposal of a novel model to adopt the concepts of machine learning for classification of drone data as part of a digital forensic investigation. Our main conclusions include that properly trained machine-learning models hold promise to enable an accurate assessment of drone data obtained from drones confiscated from a crime scene. Our research work opens the door for academics and industry practitioners to adopt machine learning to enable the use of drone data in forensic investigations.

Keywords: drones; criminal activity; machine learning; digital forensics

Citation: Baig, Z.; Khan, M.A.; Mohammad, N.; Brahim, G.B. Drone Forensics and Machine Learning: Sustaining the Investigation Process. *Sustainability* **2022**, *14*, 4861. https://doi.org/10.3390/su14084861

Academic Editor: Fabrizio D'Ascenzo

Received: 17 February 2022
Accepted: 15 April 2022
Published: 18 April 2022

1. Introduction

Drones are flying Internet of Things (IoT) objects that are an embodiment of hardware designed to be driven by software-based controls. Drones are programmed to fly according to user-defined specifications and have on-device IoT sensors and cameras augmented with a Global Positioning System (GPS) controller to facilitate their flight and all activity relevant to their operations. Drones are useful for several civilian applications. Some of the earlier work from the 1990s in unmanned aerial vehicle (UAV) technology [1] was specified for military applications alone. This comprised reconnaissance work for battlefields to enable military expeditions. However, contemporary drone utility in the civilian domain is gaining increasing acceptance by consumers.

Drone sales have only exponentially increased in the last five years, with sales topping eight million in 2021. According to [2], retail applications adopting drones will exceed 122,000 by 2023, with popular purposes being aerial photography, express delivery services, reconnaissance for disaster-hit zones, thermal sensing for rescue operations, building safety inspections, crop monitoring, storm tracking and border surveillance (law enforcement). Moreover, we live in an era of Generation 7 drones, which have the capability of intelligent operation, hazard avoidance, holistic airspace awareness and automated flight. Data that consequently are produced through drone flights are significant in volume.

Drones have been deployed to reach locations too hazardous for human access, such as facility observation at an altitude, surveillance and monitoring of high-rise buildings, anal-

ysis of mobile communication towers for anomalies and overhead electricity transmission line monitoring.

Smartphones play an integral role in the process of controlling drones. They serve dual purposes in the phone-to-drone interaction, where users can switch between manual and automatic/autonomous control modes. In [3], the studied drones sent light commands, drone status, images, and video over WIFI communication channels. Under this setup, a client smartphone may issue a set of predefined commands that vary the drone's rotors to change the drone's position while operating in the manual mode. Alternatively, image processing and machine-learning algorithms can run on the client smartphone, generating commands that return the drone to autonomous flight modes. For longer distance transmission of data between drones and smartphones, a different method of operation is employed. It relies on a 2.4 GHz radio communication channel between a transmitter and a receiver controller attached to a smartphone via a USB cable and a receiver mounted on the drone's assembly [4]. Autonomous navigation of the drone can be achieved by having the smartphone gain access to the drone's controls to issue commands based on flight calculations as a result of trajectory calculations and vision-based processing that run on the smartphone. The authors in [5] suggest building on top of these functions to deploy an autonomous landing system for drones.

Drones can breach airspace regulations of their jurisdictions as part of malicious attacks that can be perpetrated by a criminal, where the rogue agent can use a fake email address to log in to the mobile smart app of a drone and conceal its identity when it is carrying out some criminal action such as 'breach of airspace' or carrying out illegal activities such as taking photos of strategic or sensitive locales [6]. This threat is posed to vulnerable drones that have few or no security controls in place to prevent device compromise.

In the event of a drone being involved in criminal activities, its confiscation and subsequent analysis at a digital forensic investigation laboratory is a crucial part of evidence gathering and analysis. Such activity precedes any presentation of admissible evidence against the owner of a confiscated drone.

According to [7], challenges associated with drone forensics include:

1. Post-crash scattering of individual drone components encumbers routine association of parts to a drone seized at crash site.
2. The diverse types of on-device components for a drone imply that the use of a single digital forensic investigation tool will not serve the purpose of investigation; a full range of tools, both hardware and software, would be needed to run a thorough forensic procedure.
3. Physical data acquisition of forensic images from a drone may not be practicable as certain drones only permit wireless transfer of images.
4. Access control and protection mechanisms may prevent certain data elements from being acquired as part of the forensic image. Moreover, drone controller chips may be accessible only through an owner-signed remote controller, which can be difficult to emulate by law enforcement.;
5. Certain drones have multiple file systems on them, thus encumbering the process of identifying the right tool to be able to carry out data acquisition.
6. Add-on software makes it difficult to forecast the software platform, file system and the corresponding hardware configuration for a seized drone.
7. Flash memory and RAM can lose data after a crash, if the battery of the drone runs out;
8. Data logs may be partial or programmed to not hold any data depending on the drone model.
9. Deliberate attempts by a remote controller to wipe out data on a confiscated drone does not help the law enforcement procedure.

As enumerated in the above list of challenges for drone forensics, the introduction of artificial intelligence-based techniques for accurate modeling of evidence collation of drone-based criminal activities is anticipated to be a future direction for carrying out forensic investigations.

In this paper, we present a robust analysis of existing digital forensic frameworks and popular drone families in Section 2. The fundamental concepts of machine learning (branch of artificial intelligence) and adaptability of the same for drones is presented in Section 3. We propose a novel model for machine-learning-based drone forensics in Section 4. The paper is concluded in Section 5.

2. Background

2.1. Digital Forensics Frameworks

Several drone forensic frameworks exist in the literature. We summarize these and provide a gap analysis of existing solutions. Drone components are known to have distinct identification numbers. Such information may comprise serial numbers of the drone itself (manufacturer assigned), its propeller, motor, camera, and the on-board GPS device. Depending on the drone type, such information may or may not be available to the investigator, but if available, it is useful to foster a linkage between the drone and its potential ground user.

As part of drone forensics, data generated in flight, which are captured in log files, can be processed to reveal various aspects of the drone's movement and operations, such as, time stamps, flight duration, power speed, yaw, pitch and roll, altitude and drone type. Data need to be retrievable for analysis, and encryption encumbers such activity. A visualization of the drone flight can be performed to augment the forensic investigation if the data are in readable formats.

In [1], the drone forensic paradigm was bifurcated into the following: digital forensics and hardware or physical forensics. Furthermore, digital forensics was classified as the procedure conglomerate of network traffic analysis including analysis of drone to controller communication messages, system log analysis, file systems analysis and camera recordings.

Hardware forensics comprises drone type, payload description, fingerprinting and drone flight location/trajectory. The typical approach for drone data acquisition consists of confiscation of the drone from a crash scene and application of various techniques for careful recovery of hardware and stored data. The proposed drone forensic methodology comprised the following steps: data acquisition, digital forensics, hardware forensics and an overall forensic analysis framework. Additionally, forensic procedures entail evidence preservation and the assurance through a chain of custody of the integrity of confiscated components and resident data.

As part of hardware forensics, fingerprinting ascertains users who were in contact with the drone and its individual components such as the battery, propellers, payload and wings and are captured and subsequently analyzed where payloads may include illegal contents such as weapons, drugs and mobile devices, given the capability of commercial drones to carry anywhere between 2 and 20 kg [8,9].

In [10], the authors attempted to study the possibility of image retrieval from a drone's memory, flight path reconstruction, and linkage a confiscated drone to a suspected command and control (rogue) device. The analysis comprised the following drone attributes for the DJI Phantom 3 and 4 drone types: maximum flight time, maximum transmission distance, operating frequency, drone–controller connection type, mobile apps supported, memory definition and flight information. The authors were able to conclude that the communication standard adopted for drone to ground controller communication is significant in determining the data elements transferred, which can effectively lead to retrieval of admissible evidence from a confiscated drone.

In summary, existing work comprises proposals to retrieve all drone data in a safe manner to avoid tampering with evidence. The data vary from one proposed framework to another and is also contingent upon the availability of data within various drone families. With the advent of Generation 7 drones, the volume of data as well as their diversity will only increase over time.

2.2. Forensic Readiness for Popular Drone Families

Digital forensic examination of drones is reliant upon multiple sources of data that are acquired from various streams, applications (including mobile apps) and devices.

In [11], the contributors compared digital forensic preparedness for three drone families, namely 3DR Solo, Yuneec Typhoon H and DJI Phantom 4. All three commercial drones are popular for personal use. Analysis of the drone data extraction process and approach is as follows: 3DR Solo has a 16 GB SDCard, logs data in .txt format and flight path in .kmz format, which are viewable on the Google Earth application. On average, 20 log entries are created by the drone for on-device storage. Yuneec Typhoon H stores data in a .csv format when it is equipped with an SD card, otherwise, the data are streamed to the ground controller for storage. The DJI Phantom 4 holds flight logs in an encrypted format. Several third party applications such as DroneDeploy and Litchi facilitate decryption of log files. The contributors were able to analyze log files in a Java-based integrated development environment to study the drone flight paths by running these files on Google Earth for path visualization. Key parameters observed were drone type, flight duration, flight altitude, FAA notes, location, power, speed, yaw, pitch, roll, and importantly, date/time. One challenge noted was the inability of forensic investigators to accurately identify a drone model after it is recovered from a crash site unless a priori registration is made with the drone manufacturer before flying.

The DJI Mavic Air was developed by SZ DJI Technology Co., Ltd., Shenzen, China. The Mavic comprises four propellers, light sensors, GPS and Wi-Fi based communication. On-device memory includes 8 GB storage. The drone is operated from the ground through a ground controller station which interacts with a remote controller device. Mavic Air has a flight duration of roughly 21 min and a range of 10 km. The drone is equipped with software to render real-time images to the ground station, and the on-device flight path recording is also provisioned [6].

Experimental data extraction comprised retrieval of data from two file types: .dat captured by the drone for on-device storage and a .txt file, generated by the mobile remote controller app of the ground user. The contributors were able to analyze the .dat files by feeding these as inputs to CSVView and AirData apps. The media files were located at '/DCIM/100MEDIA' path in the drone's memory, comprising images in JPEG and videos in MP4 formats, respectively. Streaming of media files to the ground device app was also identified, however, the quality/resolution of the images was not as high in quality as those obtained from the on-device storage. Additionally, EXIF data were also retrieved from the JPEG images, comprising data and timestamps, file source, GPS coordinates of image, latitude and longitude. The contributors were able to note that the reference time used by the drone and captured in EXIF data, is provided by the group device smart app, and therefore, the timestamps of images captured by the drone are reliant upon the accuracy of the group device smart app [6]. It was also noted in [12] that drone data across the DJI Mavic 2 Pro, DJI Mavic Air, DJI Spark, and DJI Phantom 4 models were similar in type. The DJI GO 4 smartphone app stores .dat files that are retrievable in a decrypted manner to enable forensic investigations, whereas, except for DJI Spark, all other models stored data in an encrypted format.

In [13], a key observation noted by the contributors was that drone data emanating from data extraction of crashed drones can be correlated to data that are stored in mobile apps as part of a logical backup setup. Consequently, data across DJI drones can be associated with corresponding data items as stored on mobile devices. Such correlation can help investigators produce insights to aid in their forensic investigations. Data items for analysis can include log-in credentials, flight paths, multimedia file signatures and metadata that can also ascertain verification of data source, which is essential to hold evidence valid in the court of law. Lack of automated media file processing and data correlation (including intelligence analysis) tools encumbers the process, and the need for future work on development of such tools cannot be understated.

In [14], the contributors defined a methodology to adopt for examining a confiscated drone, namely a DJI Mavic Air 2. The tools adopted for their forensic investigation included 2D and 3D X-ray machines, DataCon, CSVView, EnCase/FTK Imager and Compact Forensic Imaging Device (CFID). Hardware retrieval comprises careful dismantling of the drone motherboard and the flash memory chip. As previously highlighted, if the drone model is known through user registration of the same, it is easier to identify the right technical datasheet for reference which in turn helps understand the data storage technique adopted by the drone's software as well as the data vs. control pins on the chip. The contributors identified the drone type by observing the model number as imprinted on the memory chip, which was intact after the crash. They subsequently used X-ray machines to trace circuit tracks and in-chip pins/points and to read data if they were unavailable to be read directly from the memory chip through a chip reader. Specific data on the the DJI Mavic Air 2 are not encrypted and include temporary folders and data on the total number of files. In summary, the forensically sound and viable data items included the blackbox folder (flight information), the system folder (operating system and process information), the upgrade folder (firmware information), the log file (system, disk and process details), the FTP file (commands, start time and logon information), the board serial number and the camera sensor serial number. Data encryption on the DJI Mavic family encumbers the forensic investigation process, and the process will thus have to rely upon those data assets that are offered through extraction in plaintext format.

In [7], the contributors were able to adopt a forensic investigation methodology on a Parrot AR drone. Data can be acquired through both a USB connection and a Wi-Fi access point, which is established by the drone at booting time. Flight path history was located within the '/data/video' folder and found to be timestamped. It was noted that the remote controller can also be used for acquiring the flight path data. Images and videos are stored in the internal flash memory of the device and can be downloaded via FTP. GPS coordinates were included in the EXIF files of images only when these were available during flight. Ownership information was not retrievable from this drone type unless the drone and its remote controller are both seized, at which time it is possible to match the drone serial number with the controller. A related contribution by the same authors is presented in [15], where a Parrot AR drone 2.0 was analyzed through an active file system access approach adopted for a serial or an FTP connection between the device and the forensic investigation system. An analysis of various techniques for retrieval of image and video capture data from the drone were reported. Specifically, wireless connections were on FTP, Telnet and wired connections through a USB port or a serial (UART) port. Full media access was accomplished through the wireless connections (Telnet and FTP), whereas the USB connection was unable to allow for a physical disc direct access. The serial (UART) connection yielded an advantage in terms of the amount of accessible data, namely media files as well as the drone system files and onboard data.

In Table 1, we provide a comparative analysis of various drone families in terms of the type of data available for conducting forensic investigations. Encrypted data confiscated from a drone encumber the investigation process, except if third party tools for decryption can be arranged. Moreover, the lesser the date for investigation, the lesser is the forensic readiness for a given drone type.

In [16], the authors provided a forensic analysis of two drone families, namely DJI Phantom 3 Professional and A.R. Drone 2.0. Both drones are commercial and provide good coverage relative to their costs; DJI Phantom 3 Professional can fly for 5 Km, whereas A.R. Drone 2.0 has a range of 50 m. The two drones were flown to deliberately participate in a simulated crime (operating within legally acceptable drone safety guidelines). The drones were made to fly on four way points over a 150 m radius across high-rise buildings as well as through open spaces. Data thus collected were analyzed in a digital forensics lab. The goal of the experiments was to provide evidence under the 'daubert' guidelines to confirm its admissibility [17]. Various operating systems, licensed and open source, were adopted for conducting the forensic examination of the drone data. These include

CyanogenMod, an open-source operating system, CSVView, Google API, Google Maps and DJI Go application. DJI Phantom was connectable to the forensic analysis workstation through a micro-USB port, whereas the A.R drone was connected through Wi-Fi as a wired option is not available for this drone type. DJI Phantom directories of interest contained flight data, activity logs, error logs, MP4 files with accompanying descriptor text files and GPS data. The A.R Drone data comprised system logs, drone serial number, drone name, SSID, GPD data,and footprint of the mobile platform. EXIF data obtained from the drones were analyzed using the Exiftool [18].

Table 1. Summary of drone data availability and forensic readiness.

Drone Family	Data Extracted	Encryption	Memory	Forensic Readiness
3DR Solo [1]	Text-based Logs and Flight path	No	16 GB	High
Yuneec Typhon H [1]	Text-based Logs and Flight Path	No	128 GB	Med
DJI Phantom 4, DJI Mavic DJI Spark [11]	.dat and .txt files EXIF for images Date/time stamps GPS Coordinates Flight Path	Yes (3rd party tools req.)	8 GB	High (if decryption enabled)
Parrot AR [7]	Flight Path Images and Video EXIF for images	No	8 GB	Med

In [19], it was noted that for Phantom 3 drones, in the absence of flight logs, EXIF data can yield GPS coordinates that can be used for reconstructing the flight. An IPv4 network is formed between drone and accompanying components/devices including the drone itself, the controller, the camera and the mobile smartphone. Through a reverse engineering (decompilation) of the DJI GO application, the SSID and accompanying password for this ad hoc IPv4 network can be revealed, which is a useful trait to foster the drone forensic procedure.

Whilst acknowledging that the DJI Phantom III drone has previously been involved in malicious activities such as drop bombs, plane watching and remote surveillance, the authors in [20] present their findings on the forensic analysis of this drone type. Contributions reported include a set of procedures for forensic examiners to follow, the binary file structure of the flight recording file, the design of a .dat file parser and the correlation procedure for extracted drone data. As reported previously, the DJI GO smartphone app stores flight data in.txt format alongside a date and timestamp. The payload of data is encrypted; however, several data components of the.txt file are readable, namely file length, file version, flight data including GPS, battery, flight status and general drone information including drone name, location, serial and model numbers.

In [21], the contributors presented flight recording data for the DJI Spark drone. Data obtained from the DJI GO mobile app comprised several traits reflective of the flight. These included photos taken during the flight in JPG format, videos during flight, flight data stored in the.dat file and .txt files generated during the flight. A correlation analysis was conducted by the authors to compare the date and timestamps obtained from the drone, SD card and the DJI GO app on the mobile phone. No significant findings were reported through their analysis for aiding in the forensic investigation, i.e., corroboration of results from the three sources was not possible.

In summary, existing literature in the field of digital forensics for drones is at a preliminary stage, and a significant opportunity exists for the proposal of novel digital forensic frameworks for drone data analysis. Moreover, the limitations in the amount of data accessible from a drone can be highlighted as the key impediment to undertaking any viable forensic investigation on a confiscated/crashed drone.

3. Machine Learning from Drone Forensics

3.1. Machine Learning Primer

Machine learning (ML) is a branch of artificial Intelligence that primarily focuses on making predictions (or forecasting) through the development of mathematical models. These models are designed in such a way that they explore abundant and massive amounts of data and attempt to exploit the inherent correlations within the various components of the data to identify repeating patterns. This helps with the process of decision making with little or no human intervention, i.e., automated decision making is made tangible. These models also try to learn from "experience" (also known as historic data) to improve prediction accuracy. Machine-learning algorithms comprise two parts: a training phase and a testing phase.

The process of improving prediction performance is carried out during the training phase of machine learning, where the algorithm is introduced with a large set of historic data typically in an iterative manner for producing mathematical values, to emulate an artificially trained brain. Applications of machine learning include speech recognition [22], natural language processing [23], robotic vehicles [24], fraud detection [25], text and handwriting classification [26], object classification [27], digital forensics [28] and systems security [29].

Machine-learning algorithms can also help uncover and learn hidden patterns embedded in the data under analysis or perform classification of observed data. This is the test phase of the process. Each of these algorithms implement a different philosophy on how data are analyzed. Example of such algorithms include decision trees, support vector machines, artificial neural networks, linear regression, K-nearest neighbor, naïve Bayes and random forest.

3.2. Machine Learning for Drone Data

Machine learning has been previously proposed to analyze several problem domains related to unmanned aerial vehicles (UAV). A detailed survey on ML techniques used for UAV-based communications is presented in [30]. The paper highlights how ML has been used for improving several communication concerns including channel modeling, resource management and positioning and security within UAV based communication. The paper classifies ML applications within four broader categories including: (1) physical layer aspects (channel modeling, interference management and spectrum allocation), (2) resource management aspects (such as network planning, power management, routing and data caching), (3) positioning (such as placement, detection and mobility), and (4) security (public safety, network jamming and eavesdropping). The paper then provides a summary of relevant work within each problem domain of these broader categories.

A jamming attack comprises an adversarial attempt to inject noise into a communication channel to cause disruption of routine communication exchange. In [31], a two classifier-based approach is proposed for detecting jamming attacks on a C-RAN network. The first classifer is a multilayer perceptron (MLP) and the second is a Kernlab support vector machine (KSVM). Jamming attacks were attested as not being linearly separable in a low dimension space. Therefore, the distinction between two classes of radio signal data is realizable through the adoption of a KSVM machine-learning solution for those jamming attack vectors that circumvent the MLP classifier. Results show promise and help prove the significance of adopting machine learning for classification of data to refer to a jamming or an eavesdropping attack.

In [32], an anomaly detection scheme is proposed for mitigating the effects of several attack vectors. The machine- learning-based anomaly detector is able to identify five attack types, namely constant position deviation attack (message modification), random position deviation attack (message modification), velocity drift attack (message modification), DOS attack (message deletion) comprising constructive and destructive interference, and the flight replacement attack (message injection). The use case analyzed is the air traffic surveillance system, ADS-B (automatic dependent surveillance-broadcast). The two-step anomaly detection scheme comprises preliminary reconstruction of ADS-B data, combined

presentation of the reconstructed and the actual values to the SVDD (support vector data description) for training, and the definition and implmenetation of a hypersphere classifier for anomaly detection.

Reinforced learning-based power provision approaches are used to protect UAV transmissions against attacks such as eavesdropping and jamming [33]. ML can also be used for detecting an eavesdropper by building a classifier based on the received signals associated with eavesdropping attacks and non-attacks [34]. This activity is based upon prior training of ML models through presentation of data that depict a radio signal jamming attack to the ML classifier.

Another survey paper [35] focused on deep-learning techniques used in UAV problem domains for feature extraction, planning and situational awareness. In [36], the authors first highlighted that drones typically fly at an altitude that is higher than traditional ground user equipment. Radio signal propagation is affected through flight through height and also line of sight of free space propagation. A scheme is proposed for the identification of rogue drones that may be found in a mobile network. Legitimate drones may be registered with ground equipment. However, unregistered rogue drones permeating the airspace in sensitive locales may prove to be a security risk. The authors emulated drone deployment scenarios comprising outdoor drones and ground user equipment for urban scenarios. The simulation setup included the following parameters: number of flying sites and sectors, inter-site distance, antennas for a base station (height, power) and carrier frequencies. Measurement data were collected from the simulations and split into a training and a testing set. Two machine-learning techniques were adopted, namely logistic regression (LR) and decision trees (DT). For LR, two categories (variables) were specified, drones and other user equipment, respectively. DT are supervised-learning models that work on feature-value tuples extracted from a dataset. In this case, four features were observed, namely received signal strength indicator (RSSI), standard deviation of the eight strongest reference signals, difference between top two strength reference signals and serving cell values. Classification results yielded a 100% accuracy in detection of rogue drones for >60 m altitudes, and 5% detection rate for lower altitudes. This was attributed to the radio frequency interference phenomenon, which is more significant at lower altitudes.

In [37], a deep-learning-based approach is presented for drone detection and identification. In particular, drone acoustic fingerprints were analyzed for detection and identification. Specifications on drone noise data comprised foot printing of drones to produce 1300 audio clips of drone sounds. Furthermore, to ascertain accuracy in detection, the datasets thus derived were an amalgamation of pure drone noise, silence and drone audio clips that were captured through drone propeller noise generated in an indoor setting. Audio clips were also balanced based on time intervals between captures. Each audio file was processed based on file type, data sampling rate and the bitrate of the channel. Additionally, audio files were also segmented into smaller chunks (which were further experimented on to deduce the most accurate segment size) to improve the performance of the deep-learning classifier. Classification of the processed drone data by the three adopted classifiers, namely recurrent neural networks (RNN), convolutional neural network (CNN) and convolutional recurrent neural network (CRNN), were subsequently reported by the contributors when these were tested on a three-class classification experiment (drone type one, drone type two and other noise). Results portrayed the superiority of the CNN technique over the other two.

Lee et al. provide a comprehensive drone detection system using machine learning in [38]. The authors were able to classify camera-equipped drone data, i.e., image data, through the adoption of a cascade classification of images using CNNs. Drone data were manually labeled, comprising 2099 drone images. A total of 1777 were used for training and the remainder 429 for testing. The system was able to deduce the location of a drone on a camera-captured image as well as the vendor model of a drone based on machine classification with reported accuracies of >90%. For feature extraction, the authors were

able to adopt the Haar feature processing method to extract drone sub-images from the image dataset obtained from [39].

In [40], an approach for identifying anomalies in a swarm flight comprising multiple flying drones, wherein certain drones may be deliberately controlled by the adversary to cause a possible sabotage, was proposed. Flight data from multiple streams were analyzed to identify such anomalies. Drone data comprising time-series sensory data are sampled at a certain frequency, with the authors generating 16 samples per time stamp. Data from normal and anomalous drones are prelabeled. Categories of anomalies were defined into three, namely noise caused through sensor generated signal disruption in flight, abnormal signals generated in actual flight but recoverable in flight and signal errors causing the aircraft to halt flight due to malfunction. The classifier selected for the experiments was the 1D signal unsupervised CNN based on a generative model.

In [41], a prediction technique for drone position is defined based on classification of drone data through the adoption of machine learning. Drone data captured at the ground controller are introduced to a naïve Bayes classifier to help predict the power utilization and current location of a drone, to potentially enable subsequent plans to continue or to interrupt drone flight. Data fields adopted for classification include drone altitude, switching status of the four transmitter coils and measured power transfer efficiency. Resulting drone position is compared against the actual drone position to verify the accuracy in classification. Training of the classifier is achieved through the introduction of past observations on drone flight trajectory, path and location as input to facilitate naïve Bayes model generation. Error rates in accuracy in the range 0.09% to 45%, were noted to depend upon the feature values such as the transmitter coil-switching values.

The authors in [42] proposed a methodology to detect the presence of a remotely operated drone, its current status and movement based solely on the communication between drone and the remote controller. They used random forest algorithms as the classifier. It also evaluates the effectiveness of the methodology in the presence of heavy packet loss and evasion attacks. The methodology is specifically designed and evaluated for remotely operated aircraft systems (RPAS) drones. They have shown a drone detection accuracy of 99.9% within 30 m without any packet loss and a detection accuracy >97% within 200 m with a packet loss up to 74.8%.

In [43], authors proposed UAV detection and identification based on radio frequency (RF) data using a hierarchical ensemble learning approach. The first classifier detects UAVs, the second one identifies the type of UAV, and the remaining two are used to identify the mode of operations. Each classifier used ensemble learning based on KNN and XGBoost algorithms. The proposed approach resulted in a classification accuracy of 99% with 10 classes. Each class uniquely identified the presence or absence of a UAV, its type (out of three different types of UAVs) and its mode of operation (ON mode, hovering mode, flying mode and recording mode). The paper also summarized the existing UAV detection using machine-learning approaches based on different data sources.

The authors in [44] provided a technique to identify the pilot of the drones based on radio control signals sent to a UAV using a typical transmitter. The dataset was collected from 20 different trained pilots flying the UAV through three different trajectories. The dataset consists of nine features including thurst, pitch, roll and yaw at time (t) and their derivatives at time (t). It also included control simultaneity variable at time (t) which describes the control signals available simultaneously at time (t). The proposed system used a random forest algorithm and resulted in an accuracy of 90%. The proposed technique can be used during forensic analysis to identify the pilot of the UAV and raise an alert in case of the suspected hijacking of a drone.

The authors in [45] proposed a methodology to detect drone status (flying or at rest) using just the encrypted communication traffic between the drone and the remote controller. The dataset was collected using communication from a drone running ArduCopter firmware. The encrypted packet information (without using its contents) was converted into six features (inter-arrival time, packet size, mean and standard deviation computed

over a certain number of samples of inter-arrival time and packet size). Three different classifiers were used for classification (decision tree, random forest and neural networks). The random forest classifier provided better results for drone detection.

In [46], the authors identified the issue of inter-drone communication reliability, wherein transmitted packets may not reach the intended target successfully. The authors attempted to apply machine learning for accurate prediction of transmission patterns. The success/failure probabilities are computed using a Monte Carlo simulation setup comprising modeling channel design for transmission. The linear regression machine-learning technique was adopted alongside a comparative analysis with support vector machines (SVMs) with a quadratic kernel. The first property observed was the inverse proportionality between inter-drone distance and probability of a successful packet transmission. To foster measurement data collection, a total of 20 drones were simulated. Communication channel success in packet transmission was fixed at a 0.05 probability factor. Specific features identified for training of linear regression were transmission probability, node locations, transmission probability within a channel and time. For the SVM-QK classifier, features comprised quantization factor values, transmission probabilities, times, and locations of nodes in the network. Average prediction rates were found to yield a very low error rate of 0.00597

3.3. Machine Learning for Drone Data

There has been relatively less work on digital forensics for drones using machine-learning techniques. In [47], the authors conducted a survey on existing work in drone forensic domain (DRFs). They highlighted the challenges and opportunities in drone forensics. They also presented a methodology for drone-related event investigation. The existing work on forensic analysis for drone data has quite limited work focused on using machine-learning techniques for forensic analysis.

In [48], the authors proposed a methodology for drone forensic analysis and to identify suitable tools for performing digital forensics on drone data. Their work focused on the data acquired from the DJI Mavic air drone, and they compared three different tools including Airdata, CsvView and Autopsy. The acquired data included deleted files, attached devices information, emails and images along with audio and video files stored on the SD card. They presented their findings on the usage of these tools for forensic analysis and considered Airdata and Autopsy to be more suitable for drone data forensic analysis. The authors had earlier also provided a methodology based on a self-organizing map (SOM) for digital forensic analysis in [49]. The experiments were conducted using images acquired from ArduPilot DIY drone and DJI Phantom 4 drones. As part of the investigation, flight paths were extracted, and their associated datasets were obtained from both the drones. These datasets were further subjected to SOM-based clustering. The results obtained identify DJI Phantom 4 drones to hold more evidence and be forensically sound when compared with ArduPilot DIY drones.

In digital forensics, through clustering of common data samples into a single cluster and through subsequent visualization of the data clusters, commonalities between data elements can be observed, which can subsequently be labeled. Through the definition of such clusters for drones and the generated data during flight, it is possible to predict the trajectory of drones in flight and to label these as either legitimate flight paths or compromised ones that are typically exhibited by rogue/compromised drones [50,51].

Machine-learning techniques are beneficial in analyzing diverse datasets with variable volumes to generate inferences on the likelihood of an event occurring. Drone data analysis would benefit from such inferences as also evidenced in the recent literature that includes proposals to adopt machine-learning-based analysis of confiscated drones [38,39,42].

Table 2 provides a summary of the work presented in this section highlighting the different usages of machine-learning techniques for drone data and forensic analysis.

Table 2. Summary of machine-learning techniques used for drone data and forensics.

Paper	Year	Short Description	Scope	Evaluation Type
[30]	2019	Machine-Learning Techniques used for UAV-based Communications	ML use to address communication concerns including channel modeling , resource management, positioning and security within UAV-based communication.	Survey Paper
[35]	2017	Deep-Learning Techniques used in UAV problem domain	Survey paper highlighting work performed on use of deep learning for feature extraction, planning, situational awareness and motion control aspects of UAV systems based on Aerostack architecture.	Survey Paper
[36]	2019	Rogue drone detection	A novel machine-learning approach to identify the rogue drones in mobile networks based on radio measurements	In Lab (Simulated data)
[37]	2021	Deep-Learning-based technique for drone detection and identification using acoustic data	Uses CNN, RNN and CRNN-based architectures to identify drones using acoustic fingerprints of flying drones.	In Lab (Real data with augmentation)
[38]	2018	Drone detection and identification system using Artificial Intelligence	Uses Haar classifier to detect a drone in an image and then uses CNN model to identify the type of drone.	In Lab (Real data)
[40]	2020	Deep-learning-based anomaly detection for a vehicle in swarm drone system	The proposed anomaly detection model uses a deep neural network-based generation model to create a training model with normal data and perform tests with abnormal data.	In Lab (Real data)
[41]	2017	Novel wireless power transfer system for drones using machine-learning techniques	Machine-learning model (using naïve Bayes) is used to identify position of the drone for enhancing wireless power transfer efficiency.	In Field
[42]	2020	Drone detection via network traffic analysis	Detect presence, status and movement of drones by applying standard classification algorithms to the eavesdropped traffic, analyzing features such as packets inter-arrival time and size.	In Field
[43]	2021	RF-Based UAV Detection and Identification	UAV detection and identification based on radio frequency (RF) data using hierarchical ensemble learning approach. The first classifier detects UAVs, second one identifies the type of UAV and the remaining two are used to identify the mode of operations.	In Lab (Real data)
[44]	2018	Drone Pilot Identification based on Radio Control Signals	Describes an approach where radio control signal sent to an unmanned aerial vehicle (UAV) using a typical transmitter can be captured and analyzed to identify the controlling pilot using machine-learning techniques.	In Lab (Real data)
[45]	2019	Detecting drones status via encrypted traffic analysis	Detect the current status of a powered-on drone (flying or at rest), leveraging just the communication traffic exchanged between the drone and its remote controller (RC) analyzing features such as packets inter-arrival time and size.	In Field
[47]	2021	Research Challenges and Opportunities in Drone Forensics Models	It provides a detailed review of existing digital forensic models. It highlights the research challenges and opportunities through which an effective investigation can be carried out on drone-related incidents.	No evaluation
[49]	2019	Digital forensics for drone data using SOM	Proposes a methodology based on self-organizing map (SOM) for digital forensic analysis of drone data.	In Lab (Real data)
[46]	2016	Prediction of information propagation in a drone network by using machine learning	The packet transmission rates of a communication network with 20 drones were simulated, and results were used to train the linear regression and support vector machine with quadratic kernel (SVM-QK).	In Lab (Simulated data)
[48]	2020	Digital Forensics for Drones: A Study of Tools and Techniques	Proposes a methodology that can help forensic investigators identify the most pertinent forensic investigation tools	In Lab (Real data)

4. A Machine-Learning-Based Drone Forensics Framework

We propose a drone forensics framework to comprise several components that refer to a robust and forensically ready design to foster an accurate depiction of criminal activity. In Figure 1, we illustrate the high-level components of the framework.

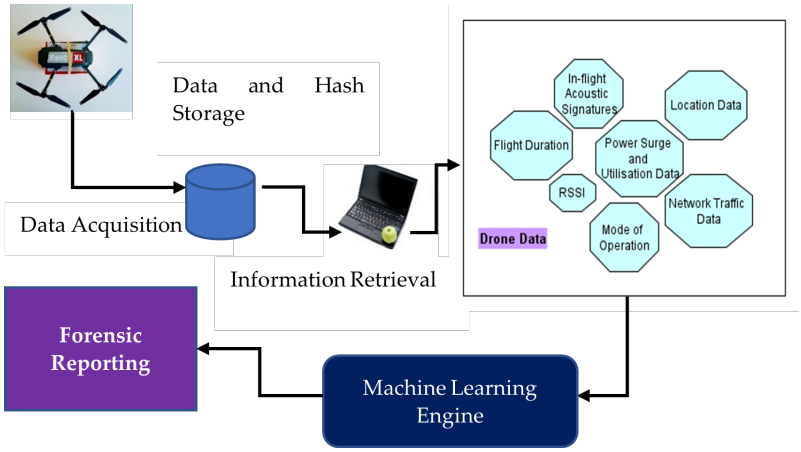

Figure 1. Proposed machine-learning-based drone forensics framework.

Drone configuration is essential in defining the data elements that are captured by a drone during flight as well as the amount and frequency of data transmissions that are made between the drone and a ground remote controller. Drone configuration can be specified to include log files that contain descriptions of the following key parameters:

- Drone coordinates;
- Flight trajectory;
- Flight duration;
- Battery life;
- Drone-to-controller communication frequency;
- Drone-to-controller data exchange definitions.

Drone data acquisition can be defined to ensure that two copies of drone data are defined and stored, with the potential to hold a third copy in the Cloud. Real-time analysis of drone data on the ground controller can also be enabled while it is being transmitted from the drone to the receiving unit. Through such real-time analysis, only those elements of the data being captured would be logged, which will prove to be beneficial for digital forensic procedures that will subsequently be undertaken for forensic analysis. If all data transmitted to a drone ground controller is logged, it will present an unusually high volume of data to the machine-learning system, which will also include insignificant data for forensics. Through such a rapid analysis mechanism, the data volume can be condensed before it is stored to foster a subsequent forensic procedure. This constitutes the concept of live forensics [52], wherein, while a system is still operational, the data being generated is being filtered and intelligently logged to foster a subsequent forensic investigation process. Additionally, by designing systems that comprise previously seen data models of routine and suspicious drone data, the overall forensic readiness of such systems is increased.

In Figure 2, we illustrate the machine-learning-based model for drone forensics. As part of training, raw drone data is transmitted to the ground controller and is stored in log files for subsequent analysis. All stored data will have to be preprocessed first. The preprocessing of data can follow one of the following techniques as found in the literature: entropy analysis, group method for data analysis, Chi-squared feature ranking and k-means clustering. The training data is generated through test flights that are conducted in various modes: altitudes, distances and heterogeneous payloads (if the drones have this capacity). After several runs, the data collected would be representative of actual drone flights. The process can be repeated with anomalous trajectories representative of a compromised drone or a drone being involved in criminal activity. An example of such training data includes drones flying outside acceptable flying zones despite having a clear zone specification in place.

The application of ML for training and model generation can be subsequently carried out, where parameters are defined for the ML system that is adopted. The testing phase comprises the deliberate anomalous behavior of a drone in flight, so that the data generated

by the drone represents a real-life incident based on a criminal motive. The purpose of machine-learning algorithm testing is the definition of a robust and high accuracy system for evaluating real-time drone data, which is being generated by inflight drones and captured by a ground-based remote controller.

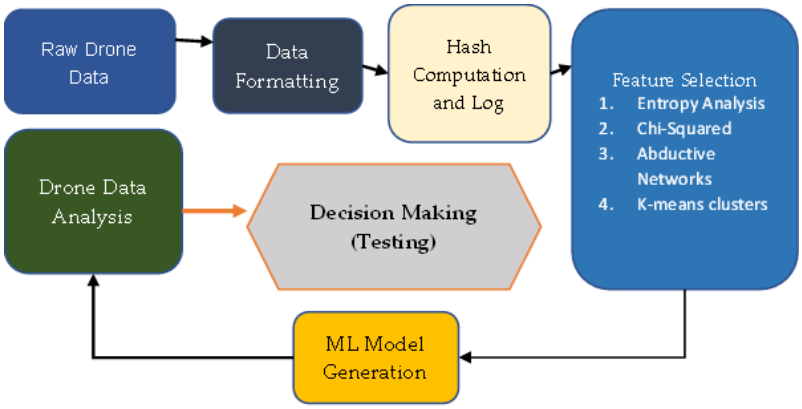

Figure 2. Machine-learning process applied to raw drone data (training) and life drone data (testing).

Following the ML step, the trained and tested models for classification can be placed in production mode awaiting actual drone data from a confiscated drone from a crash site to be presented for subsequent classification into normal (routine crash) vs. anomalous (deliberate attempt by a criminal). As part of the forensic procedure, the confiscated drone data is subject to the following steps:

1. Data is securely extracted without affecting its integrity;
2. Data is securely stored through validation and cross examination, in order to maintain a chain of custody;
3. Preprocessing of data is then conducted based on those techniques that were adopted for preprocessing of the training data;
4. ML-based data classification is then conducted to identify whether or not the drone was involved in a malicious event.

Though the ability of the ML-based classification systems is very much reliant upon the quality of training data, the efficacy of the digital forensic procedure can be elevated through the definition of robust flight paths that a specific drone model can undertake to emulate a normal flight pattern. For example, a drone that performs temperature sensing in a given fly zone can be operated with specific characteristics that represent the 'routine' flight. Depending upon the use case, this may include altitude ranges, flying zone coordinates, distance from the remote controller, triggering sensor usage in-flight, etc. By flying a drone within these predefined bounds, routine operations and associated data can be generated. By having the drone violate these parameters, obviously without breaching the aviation policy of the jurisdiction where the flight takes place, a range of anomalous drone flight data can be generated and collected for subsequent analysis.

Through such preincident activity, the ML-based digital forensic model can be defined with a high degree of precision, as the training models will have insights on both routine and malicious flight paths. The other possibility for drone investigators to produce valid training models from routine flight data only is to use machine-learning techniques such as single-class SVM that are capable of producing models from training data belonging to a single class [53]. It may be noted that the adoption of machine learning to identify suspicious drone flight data may not be acceptably accurate if the training data is not robust enough. As reported in [51], several pitfalls in the type of data presented to the classifier should be avoided to prevent a skew in the classification accuracy between true positives/negatives and false positives/negatives. It is therefore significant to generate preincident drone data that is both robust and complete to eliminate the chance of inaccuracies in data classification.

Data acquisition of drone data is dependent upon its accessibility after an inciden tsuch as a drone crash has occurred, . The process of data acquisition is dependent upon availability of a USB connection (port access) to the drone or through a live Wi-Fi network card that has not been damaged in the crash.

Once the data acquisition process is initiated, a free traversal of all on-device data to the data acquisition device is carried out.

The second source for data acquisition is the remote controller. As discussed in Section 2, real time flight data is captured by the remote controller if the preflight firmware configuration enables such a process. This is practicable in the Parrot AR drone. Moreover, postincident, the remote controller data can be retrieved through a FTP connection if it is still accessible. In case it was turned off by the criminal, this data source is unreachable. However, for purposes of training, model generation and testing, this data is to be presented to the ML engine.

The next step comprises secure storage of the drone data through a hash computation of all data elements and subsequent storage of both the fully acquired data and the associated hash values. It may be noted that the data will comprise audio, video, and generic data in the form of bits and bytes that can be readily hashed using a known hash function such as the secure hash algorithm (SHA-3). The purpose of computing the hash value is to mark the digital forensic procedural register with a description of the personnel who are handling the investigation and through whose hands the acquired evidence is passed. The third step in the forensic investigation is the deployment of common software-based tools to carry out an analysis of the acquired data. These tools include CSVView, Google API, Google Maps, ExifTool and CyanogenMod. The extracted data is then presented to the trained machine-learning engine for classification.

Based upon our analysis of drone families (Table 1), we proposed that the following data elements can be presented to the machine-learning algorithm to enable robust training for drone forensic readiness:

1. Received signal strength indicator (RSSI)–normal ranges;
2. Drone in-flight acoustic signatures—noise;
3. Flight data as time-series sensory values;
4. Power surge or utilization data;
5. Location data;
6. Network traffic–packet loss data, interarrival times of data packets, packet lengths;
7. Mode of operation data–ON, hovering, flying or recording.

Drone signals lost through longer flights that traverse beyond acceptable limits into no-fly zones can be referred through higher RSSI (weaker) signals. In-flight acoustic signatures can refer to a cyberattack, where malicious software may have been successfully installed on a drone to sabotage its flight. Time series-based collection of IoT sensory data from drone sensors is essential in the diagnosis of the various value ranges. Subsequent comparison of sensory data with normal ranges at the receiver's end will support drone data analysis to refer to anomalous locales visited by the drone or unusual value ranges that can confirm the compromise of the drone. Similarly, power surges in a drone can either occur through malfunction or through deliberate sabotage. Drone location data is essential in identifying the location coordinates visited by a drone in-flight. We postulate that network traffic data is also essential in identifying the proximity of a drone to the ground receiver. This data can subsequently be corroborated with in-flight data obtained from the drone. Operations data will also be representative of routine flight paths adopted by the drone.

The drone forensic process comprising machine-learning-based model generation and analysis may suffer from several limitations listed as follows:

1. Limits to the volume of training data that may be available during the training phase of the machine-learning process;
2. Unclear demarcation in the classes of normal and anomalous data retrieved from previously crashed/confiscated drones;

3. Inability of the machine-learning algorithm to accurately classify live drone data into normal or anomalous (with a high degree of admissible accuracy)

5. Conclusions

Drones are prone to compromise as well as to adoption by malicious actors to carry out criminal activities. Drones confiscated from a crash site or from a suspect need to be examined for evidence that may be presented in a court of law to implicate the perpetrators. We have provided a review of existing forensic frameworks suited for drone forensics, machine-learning techniques as found in the literature and their adaptability for drone data analysis, and finally, a model for implementation of machine-learning-based analysis of captured drone data to support digital forensics investigation. The future direction of this work would comprise hands-on activities for drone data generation, data collection, and adoption of the posed machine-learning techniques for conducting a robust digital forensic investigation.

Author Contributions: Conceptualization, Z.B. and N.M.; methodology, Z.B.; validation, M.A.K., G.B.B. and Z.B.; project administration, Z.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Prince Mohammad Bin Fahd University, PCC-Grant-202103.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Renduchintala, A.; Jahan, F.; Khanna, R.; Javaid, A.Y. A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework. *Digit. Investig.* **2019**, *30*, 52–72. [CrossRef]
2. Drone Technology Uses and Applications for Commercial, Industrial and Military Drones in 2021 and the Future. 2021. Available online: https://www.businessinsider.com/drone-technology-uses-applications (accessed on 14 April 2022).
3. Hummel, K.A.; Pollak, M.; Krahofer, J. A distributed architecture for human-drone teaming: Timing challenges and interaction opportunities. *Sensors* **2019**, *19*, 1379. [CrossRef] [PubMed]
4. Yanmaz, E.; Quaritsch, M.; Yahyanejad, S.; Rinner, B.; Hellwagner, H.; Bettstetter, C. Communication and coordination for drone networks. In *Ad hoc Networks*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 79–91.
5. Tanaka, H.; Matsumoto, Y. Autonomous Drone Guidance and Landing System Using AR/high-accuracy Hybrid Markers. In Proceedings of the 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), Osaka, Japan, 15–18 October 2019; pp. 598–599.
6. Yousef, M.; Iqbal, F. Drone forensics: A case study on a DJI Mavic Air. In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 3–7 November 2019; pp. 1–3.
7. Bouafif, H.; Kamoun, F.; Iqbal, F.; Marrington, A. Drone forensics: Challenges and new insights. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–6.
8. Flynt, J. How Much Weight Can a Drone Carry? Available online: https://3dinsider.com/drone-payload/ (accessed on 14 April 2022).
9. Flynt, J. 5 Best Heavy Lift Drones-Large Drones That Have High Lift Capacity. Available online: https://www.dronethusiast.com/heavy-lift-drones/ (accessed on 14 April 2022).
10. Al-Room, K.; Iqbal, F.; Baker, T.; Shah, B.; Yankson, B.; MacDermott, A.; Hung, P.C. Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models. *Int. J. Digit. Crime Forensics (IJDCF)* **2021**, *13*, 1–25. [CrossRef]
11. Renduchintala, A.L.S.; Albehadili, A.; Javaid, A.Y. Drone forensics: Digital flight log examination framework for micro drones. In Proceedings of the 2017 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 14–16 December 2017; pp. 91–96.
12. Yousef, M.; Iqbal, F.; Hussain, M. Drone forensics: A detailed analysis of emerging DJI models. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; pp. 66–71.
13. Iqbal, F.; Alam, S.; Kazim, A.; MacDermott, Á. Drone forensics: A case study on DJI phantom 4. In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 3–7 November 2019; pp. 1–6.
14. Lan, J.K.W.; Lee, F.K.W. Drone Forensics: A Case Study on DJI Mavic Air 2. In Proceedings of the 2022 24th International Conference on Advanced Communication Technology (ICACT), Seoul, Korea, 13–16 February 2022; pp. 291–296.

15. Bouafif, H.; Kamoun, F.; Iqbal, F. Towards a better understanding of drone forensics: A case study of parrot AR drone 2.0. *Int. J. Digit. Crime Forensics (IJDCF)* **2020**, *12*, 35–57. [CrossRef]
16. Barton, T.E.A.; Azhar, M.H.B. Forensic analysis of popular UAV systems. In Proceedings of the 2017 Seventh International Conference on Emerging Security Technologies (EST), Canterbury, UK, 6–8 September 2017; pp. 91–96.
17. Carrier, B. Open Source Digital Forensics Tools: The Legal Argument. 2002. http://www.atstake.com/ (accessed on 14 April 2022).
18. Harvey, P. Exiftool for Linux. Available online: http://www.sno.phy.queensu.ca/phil/exiftool/ (accessed on 14 April 2022).
19. Trujano, F.; Chan, B.; Beams, G.; Rivera, R. Security analysis of dji phantom 3 standard. *Mass. Inst. Technol.* 2016. Available online: https://courses.csail.mit.edu/6.857/2016/files/9.pdf (accessed on 14 April 2022).
20. Clark, D.R.; Meffert, C.; Baggili, I.; Breitinger, F. DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. *Digit. Investig.* **2017**, *22*, S3–S14. [CrossRef]
21. Kao, D.Y.; Chen, M.C.; Wu, W.Y.; Lin, J.S.; Chen, C.H.; Tsai, F. Drone forensic investigation: DJI spark drone as a case study. *Procedia Comput. Sci.* **2019**, *159*, 1890–1899. [CrossRef]
22. Alhawiti, K.M. Advances in artificial intelligence using speech recognition. *Int. J. Comput. Inf. Eng.* **2015**, *9*, 1432–1435.
23. Nadkarni, P.M.; Ohno-Machado, L.; Chapman, W.W. Natural language processing: An introduction. *J. Am. Med. Inform. Assoc.* **2011**, *18*, 544–551. [CrossRef]
24. Murphy, R.R. *Introduction to AI Robotics*; MIT Press: Cambridge, MA, USA, 2019.
25. Abdallah, A.; Maarof, M.A.; Zainal, A. Fraud detection system: A survey. *J. Netw. Comput. Appl.* **2016**, *68*, 90–113. [CrossRef]
26. Kulik, S. Neural network model of artificial intelligence for handwriting recognition. *J. Theor. Appl. Inf. Technol.* **2015**, *73*, 202–211.
27. Voronin, V.; Marchuk, V.; Semenishchev, E.; Makov, S.; Creutzburg, R. Digital inpainting with applications to forensic image processing. *Electron. Imaging* **2016**, *28*, 1–7.
28. Francisca, O.; Ogbuju, E.; Alayesanmi, F.; Musa, A. The State of the Art in Machine Learning-Based Digital Forensics. *SSRN Elec. J.* **2020**, doi: 10.2139/ssrn.3668687. [CrossRef]
29. Bertino, E.; Kantarcioglu, M.; Akcora, C.G.; Samtani, S.; Mittal, S.; Gupta, M. AI for Security and Security for AI. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, Virtual, 26–28 April 2021; pp. 333–334.
30. Bithas, P.S.; Michailidis, E.T.; Nomikos, N.; Vouyioukas, D.; Kanatas, A.G. A survey on machine-learning techniques for UAV-based communications. *Sensors* **2019**, *19*, 5170. [CrossRef] [PubMed]
31. Hachimi, M.; Kaddoum, G.; Gagnon, G.; Illy, P. Multi-stage jamming attacks detection using deep learning combined with kernelized support vector machine in 5g cloud radio access networks. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 20–22 October 2020; pp. 1–5.
32. Luo, P.; Wang, B.; Li, T.; Tian, J. ADS-B anomaly data detection model based on VAE-SVDD. *Comput. Secur.* **2021**, *104*, 102213. [CrossRef]
33. Xiao, L.; Xie, C.; Min, M.; Zhuang, W. User-centric view of unmanned aerial vehicle transmission against smart attacks. *IEEE Trans. Veh. Technol.* **2017**, *67*, 3420–3430. [CrossRef]
34. Hoang, T.M.; Duong, T.Q.; Tuan, H.D.; Lambotharan, S.; Hanzo, L. Physical layer security: Detection of active eavesdropping attacks by support vector machines. *IEEE Access* **2021**, *9*, 31595–31607. [CrossRef]
35. Carrio, A.; Sampedro, C.; Rodriguez-Ramos, A.; Campoy, P. A review of deep learning methods and applications for unmanned aerial vehicles. *J. Sens.* **2017**, *2017*, 3296874. [CrossRef]
36. Rydén, H.; Redhwan, S.B.; Lin, X. Rogue drone detection: A machine learning approach. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–6.
37. Al-Emadi, S.; Al-Ali, A.; Al-Ali, A. Audio-Based Drone Detection and Identification Using Deep Learning Techniques with Dataset Enhancement through Generative Adversarial Networks. *Sensors* **2021**, *21*, 4953. [CrossRef]
38. Lee, D.; La, W.G.; Kim, H. Drone detection and identification system using artificial intelligence. In Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 17–19 October 2018; pp. 1131–1133.
39. CVOnline-Image Databases. Available online: https://homepages.inf.ed.ac.uk/rbf/CVonline/Imagedbase.htm (accessed on 14 April 2022).
40. Ahn, H. Deep learning based anomaly detection for a vehicle in swarm drone system. In Proceedings of the 2020 International Conference on Unmanned Aircraft Systems (ICUAS), Athens, Greece, 1–4 September 2020; pp. 557–561.
41. Jeong, S.; Bito, J.; Tentzeris, M.M. Design of a novel wireless power system using machine learning techniques for drone applications. In Proceedings of the 2017 IEEE Wireless Power Transfer Conference (WPTC), Taipei, Taiwan, 10–12 May 2017; pp. 1–4.
42. Sciancalepore, S.; Ibrahim, O.A.; Oligeri, G.; Di Pietro, R. PiNcH: An effective, efficient, and robust solution to drone detection via network traffic analysis. *Comput. Netw.* **2020**, *168*, 107044. [CrossRef]
43. Nemer, I.; Sheltami, T.; Ahmad, I.; Yasar, A.U.H.; Abdeen, M.A.R. RF-Based UAV Detection and Identification Using Hierarchical Learning Approach. *Sensors* **2021**, *21*, 1947. doi: [CrossRef]
44. Shoufan, A.; Al-Angari, H.M.; Sheikh, M.F.A.; Damiani, E. Drone Pilot Identification by Classifying Radio-Control Signals. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2439–2447. doi: [CrossRef]

45. Sciancalepore, S.; Ibrahim, O.A.; Oligeri, G.; Di Pietro, R. Detecting Drones Status via Encrypted Traffic Analysis. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning (WiseML 2019), Miami, FL, USA, 15–17 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 67–72. doi: [CrossRef]
46. Park, J.; Kim, Y.; Seok, J. Prediction of information propagation in a drone network by using machine learning. In Proceedings of the 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 19–21 October 2016; pp. 147–149.
47. Al-Dhaqm, A.; Ikuesan, R.A.; Kebande, V.R.; Razak, S.; Ghabban, F.M. Research Challenges and Opportunities in Drone Forensics Models. *Electronics* **2021**, *10*, 1519. doi: [CrossRef]
48. Viswanathan, S.; Baig, Z. Digital Forensics for Drones: A Study of Tools and Techniques. In *International Conference on Applications and Techniques in Information Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 29–41.
49. Mekala, S.H.; Baig, Z. Digital Forensics for Drone Data–Intelligent Clustering Using Self Organising Maps. In *Future Network Systems and Security*; Doss, R., Piramuthu, S., Zhou, W., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 172–189.
50. Fei, B.; Eloff, J.; Venter, H.; Olivier, M. Exploring forensic data with self-organizing maps. In *Ifip International Conference on Digital Forensics*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 113–123.
51. Feyereisl, J.; Aickelin, U. Self-organizing maps in computer security. In *Computer Security: Intrusion, Detection and Prevention*; Hopkins, R.D., Ed.; University of Melbourne: Melbourne, VIC, Australia, 2009; pp. 1–30.
52. Adelstein, F. Live forensics: Diagnosing your system without killing it first. *Commun. ACM* **2006**, *49*, 63–66. [CrossRef]
53. He, H.; Ma, Y. *Imbalanced Learning: Foundations, Algorithms, and Applications*; Wiley-IEEE Press: Hoboken, NJ, USA, 2013.