

Drone Forensics

Subjects: Computer Science, Interdisciplinary Applications

Contributor: Fahad Mazaed Alotaibi , Arafat Al-Dhaqm , Yasser D. Al-Otaibi , Abdulrahman A. Alsewari

Unmanned aerial vehicles (UAVs) are adaptable and rapid mobile boards that can be applied to several purposes, especially in smart cities. These involve traffic observation, environmental monitoring, and public safety. The need to realize effective drone forensic processes has mainly been reinforced by drone-based evidence. Drone-based evidence collection and preservation entails accumulating and collecting digital evidence from the drone of the victim for subsequent analysis and presentation.

drone forensics

smart cities

UAV

1. Introduction

Unmanned aerial vehicles (UAVs) are flexible and rapid mobile boards applicable to different purposes, especially in smart cities, including traffic observation, environmental monitoring, and public safety, as shown in **Figure 1**. UAVs have received tremendous attention since these vehicles can be controlled and monitored without pilots, based on pre-programming flight paths. In the start, this technology was adopted for military purposes, but it has been recently used even to facilitate common people's lives.

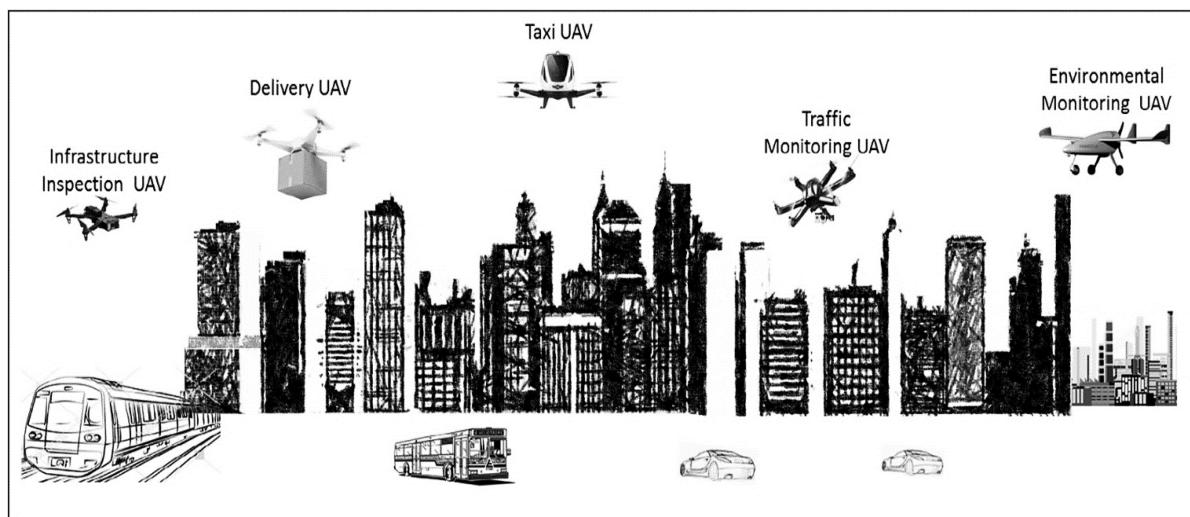


Figure 1. Using UAVs for various purposes in the smart environment [\[1\]](#).

This technology is most commonly used in area monitoring, inspection, surveillance, and cargo purposes [\[2\]\[3\]](#). It improves life quality, especially by monitoring special public events and using shared space [\[4\]](#). It is observed that the airspace is loaded with a great deal of traffic, and collision accident reports are increasing day by day [\[5\]](#). Due to UAVs' traffic patterns and technology, tackling the congestion and any incident is more challenging compared to

traditional networks [6][7]. The increasing trend of congestion leads to high interference, data dropping, overhead, and other abnormalities in the control system. Various types of UAVs are currently available, including small drones, aircraft, or weapon-enabled drones [8][9]; small drones fly like small insects; they can fly around an area of interest to monitor vital signs and inform the base station for further decision-making. However, the nature of data is scattered in these networks where different types of devices are involved, including routers, switches, sensor nodes, and SD cards [10][11][12]. The data are located in different places, and there is a need for proper investigation and planning to extract the forensic features.

The drone functionalities involve several items such as the ground-station controller, onboard power management system (PMS), onboard flight control board (FCB), (multi)rotor system, electronic speed controller (ESC), and transceiver control unit (TCU) [13][14]. Regarding the potential digital forensic items, the ground-station controller, ESC, FCB, TCU, and PMS offer potentially reliable sources of evidence [15]. The information of log and memory could be taken out of the ground-station controller unit. It can be a software platform or a customized base-station design, which can interact with FCB. As drones are unmanned, TCU plays a crucial role by providing a medium for communication and control between the base station and FCB as well as a medium of communication for different sensors installed on the drone. FCB acts as the drone brain [16][17] by integrating and coordinating the information received from the functional drone units (including the mounted sensors), the inertial measurement and controls, and the flight trajectory and navigation control, and also by the management of power and being in communication with the station on the ground. Additionally, ESC is the core functionality in a drone: an electronic circuit house responsible for managing the speed and overall efficiency of a drone's movement [18].

Thus, drone forensic items of drone devices could be observed in the form of data stored in the memory (practical use of memory forensics), electromagnetic (EM) wave data, and contents of different log files. ESC and FCB are the potential sources of memory items, which could be directly taken out of the components of ESC and FCB, respectively. The components include flight control data, flight record data, information from the drone's internal monitoring unit, and data from the mounted transceivers and sensors. Generally, the signal processing methodologies complement the process of forensically identifying and extracting the data. Nevertheless, the digital items, which appear in the form of EM signals from the respective transceivers and mounted sensors, can make further corroborative information available to the investigation process. In this sense, TCU could be leveraged to extract primary EM signals, which could be processed further to extract the secondary corroborative digital items. **Figure 2** illustrates a UAV's architecture and the protocols supporting its communications, which may help investigators use it during the investigation of drone crimes.

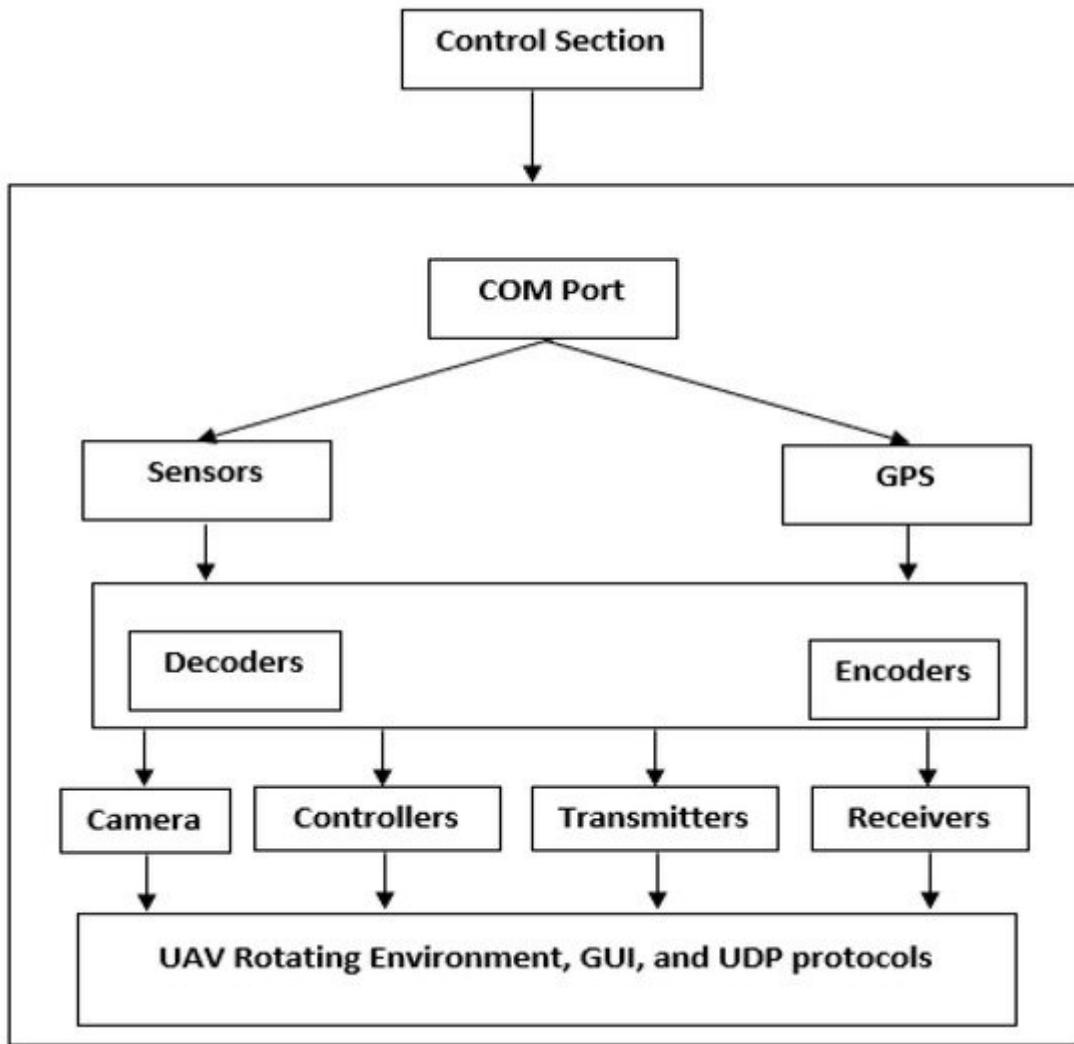


Figure 2. A UAV architecture composition.

2. Drone Forensic Models and Frameworks

The literature on drone forensics has been loaded with different models and frameworks proposed by various scholars. They consider four perspectives in common: forensic analysis, non-forensic analysis, forensic framework, and application in the forensic analysis [16]. For instance, in [8][9], the researchers focused on the ways to improve the evidence needed in cases where a drone is examined under digital forensics conditions. They concentrated upon the wireless forensics aspects. On the other hand, in [19], the authors discussed all components of a drone. They all emphasized the use of the Linux operating system and its potential to gather evidence on the Linux file system. Note that to work properly, drones need to use an OS. The researchers in [20] attempted to build a tool using Java-FX to visualize the real-time flight control. Their designed tool is not directly applicable to the DF field; however, it can create efficient connections between a drone and its controller to transfer data. In addition, this tool can display sensor parameters, including GPS, IMU, and altitude for pilots, providing a great level of flight safety [21][22]. In the same way, the researchers in [23] forensically examined the DJI Phantom 2 Vision Plus to find out whether the flight path of a UAV can be reconstructed using positional data collected from the UAV. They also

carried out a brief examination of counter-forensic methods to discover whether the record of a flight path can be detected. In [24], the authors conducted a preliminary forensic analysis on the Parrot Bebop, known as the only UAV similar to the Parrot AR Drone 2.0. In [14], the most important challenges in UAV forensic analyses were addressed; then, two separate parts, i.e., UAV and flight controller, were investigated. In that study, the author retrieved the flight-related data from the device in the form of ".pud" files and then created a novel ".pud" file at each session between the UAV and the controller. In the case of each ".pud" file, at the opening point of the file, a set of metadata was found, comprising the UAV's serial number, the date and time of the flight, the flight controller model, and the flight controlling application. After that, the author attempted to determine the images and videos recorded by the UAV's onboard camera. In the images, there were the EXIF data showing information about the latitude and longitude coordinates of the sites from which the images had been taken. However, the owner of the device could be identified only if the UAV and controller are seized by determining the serial number of the device.

In [19], a general review was performed on drone forensics using the DJI Phantom 2. The breakdown analyses of the drone's software and hardware components were conducted; then, the way the components could be used when implementing drone forensics was examined. The results obtained in that study established a belief in the persistence and scope of drone forensics. In addition, the study findings could facilitate having deeper insight into this concept and enhance its quality. Furthermore, in [25], working on the Parrot AR Drone 2.0, the authors attempted to integrate the visualizing data recovered from drones with a non-forensic approach. They designed an application to visualize the log parameters from flight data. However, only a small number of drones were evaluated in their study. The researchers in [26] analyzed the drones' vulnerabilities and applications and their relationships with issues that generally arise in the cybersecurity domain. They asserted that if a drone is hacked and abused by opponents, serious risks or consequences may arise. That study primarily focused on identifying the benefits of using drones in numerous conditions, from employing these devices as children's toys to using them as mass destruction weapons.

The authors in [27] proposed a 12-phase forensic framework to offer an innovative approach to the systematic investigation of UAVs. Wide-ranging tests were carried out on five commercial UAVs, for instance, the Parrot AR Drone 2.0, to identify the relationships amongst various components. They also executed an experiment to validate their developed framework. All the UAVs tested in the study were modified by adding and removing some parts. These modifications were done to check whether the framework involved all of the various elements in any basic commercial UAV and to examine whether it could be applied to a comprehensive UAV analysis. They found out that an important issue that does not allow for mitigating the attacks effectively is the deficiency of law enforcement training processes in UAVs. None of the UAVs were exposed to forensic analyses; however, an effective framework was finally constructed, which applied to the examination and analysis of the stages involved.

The authors in [28] were the first researchers that comprehensively analyzed the DJI Phantom 3 Standard. The examined UAV was flown towards two different sites. Then, the collected data were separated into three parts: controller, drone, and phone/tablet. Eventually, they explored two types of files of interest: the ".dat" files produced by the UAV and the ".txt" files produced by the DJI GO application. The files were first subjected to the decryption and decodification processes; after that, the information about the GPS locations, flight status, Wi-Fi connections,

remote control, motors, etc., was extracted. When the obtained data were analyzed, and the proprietary file structures were well-understood, the researchers developed the DROP tool for the analysis of the evidentiary files. They also developed a forensically-sound open-source drone parser (DROP) tool.

In [29], the researchers comprehensively discussed how the GPS coordinates could be used as location evidence while examining the crimes committed with the help of a drone. They attempted not only to extract the system logs but also to visualize GPS coordinates on maps, where the web-based third-party platforms were used to plot the flight paths.

In [30], the authors explored the flight data correlation among drones, SD cards, and mobile phones. Finding a connection between a drone and a suspect significantly facilitates criminal inspections. The application of specific software to private UAV devices could provide many digital items such as GPS timestamps and waypoints, several connected satellites, barometer, pitch, roll, battery status, azimuth, distance, photos, and videos.

In [31], the essential major log parameters of the autonomous drone were analyzed, and it was suggested to employ comprehensive software architecture related to drone forensics with preliminary results. The researchers expected that their developed software could provide a user-friendly graphical user interface (GUI) based on which the users could extract and investigate the onboard flight information. In addition, they claimed their findings would contribute to the body of the drone forensics field by designing a new tool that greatly helps run investigations effectively on criminal deeds executed with the help of drones.

As reported in [32], open-source tools, e.g., ExifTool and CsvView, have been used in different studies to extract items from mobile applications of drones using mobile forensic techniques. The researchers in that paper used Windows and Kali (a Linux distribution) as forensic workstations to conduct the needed analyses on A.R Drone and DJI Phantom 3. Different open-source tools such as Geo-Player have been used primarily to visualize the data related to the flight path. Due to the absence of a proper built environment, including a package manager, configuration tools, and a compiler within the UAV system, this option entails making a serious change to the data existing in the UAV. Therefore, it was terminated in favor of the logical level acquisition. This was carried out by mounting a forensic mass storage device onto a UAV; the existing files were copied entirely from the mounted “/data” partition using the “cp” command.

Ref. [33] discussed the challenges that might arise during a UAV/drone forensic analysis. For this purpose, the currently employed forensic guidelines were evaluated for their efficiency when used in the DRF domain. After that, the authors offered their own set of guidelines in this regard. To end with, they explained how their procedures could be effectively implemented when analyzing a drone forensically. They employed DJI Phantom 3 drone as their case study. A key limitation in UAV forensics is that there is not any confirmed forensically useful tool (this indeed recommends a direction for future research). For example, the subsequent logical step is the creation of different parsing tools that can analyze original data and make available readable and reliable information. In addition, UAVs are expected to attain the capacity needed for being properly integrated with radio communication services in the future.

In [34], a novel architecture was introduced using the ID-based Signcryption to guarantee the authentication process and privacy preservation. In the initial step, the authors defined the key elements that the architecture relies on. After that, they investigated the interactions between these elements to explore how the process goes on. Next, they elaborated on their proposed authentication scheme. Thus, the RFID tags were applied to tracking the drones and the temporary identity to preserve privacy. In addition, they simulated the calculation of the average renewal of temporary identity by testing the drones' different times and speeds.

The researchers in [35] made a forensic analysis of a captured UAV. Security forces may capture suspected UAVs using different techniques or tools such as a shotgun; these devices may break into private properties. It is necessary to determine what software/hardware modules are used to examine a UAV. After that, the investigator needs to perform three activities: gathering accessible evidence, providing the chain of custody, and analyzing the media/artifact loaded on the UAV. The increasing incidence of unlawful utilization of UAVs reflects legal ambiguity and uncertainty in the existing aviation regulations. This problem has resulted in a shortage of evidence and fundamental standards.

In [36], the authors attempted to identify the potential cyber-physical security threats and address the current challenges attributed to UAV security before a time in the future when UAVs are the predominant vehicles used by ordinary people. Furthermore, in that study, there is a suggestion about using a certain method that can be applied effectively to examining large-scale cyber-security attack vectors of such systems concerning four classes of systems, which are highly important to UAV operations. Furthermore, the authors elaborated on the contributions of their findings and suggested the appropriate ways to defend against such attacks. The researchers in [37] designed arbitrary software and then applied it to a locked target to gain access to the device's interior sensors and logs with the help of neutralization and hardening strategies to predict the effectiveness. The researchers in [38] designed an innovative scheme called distributed, agent-based secure mechanism for IoT and smart grid sensors monitoring (DASMIS). They aimed to test a hybrid of peer-to-peer (P2P) and client-server (C/S) network architecture with reduced protocol overheads for immediate and bandwidth-efficient communication. Each node within this system is assigned with an initial status and provided with a python-based agent that can scan and detect in read-only node IDs, node MAC address, system calls made, node IP address, all running system programs and applications, installed applications, and modifications. The agent securely authenticates the nodes, puts communications in a coded form, and approves inter-node access. This can prevent and detect different attacks, e.g., modification, masquerading, and DoS attacks. In addition, it can execute data encryption and hashing and report the changes to other peer nodes and the server located at the C&C center. In [39], the researchers attempted to facilitate the processes such as generating, analyzing, validating, and optimizing data to trace evidence recovery. To do this, they introduced and explained the approach adopted for solving this problem considering the target fiber retrieval context using self-adhesive tapes.

In [40], the authors attempted to adapt digital forensic processes to enhance drone incident response plans by implementing the drone forensic analysis process. The authors in that study provided more detailed information about the developed Drone Forensics and Incident Response Plan. They concluded that the Federal Aviation Administration (FAA) could update what unmanned aerial systems (UAS) require based on two classifications of

UAS. In addition, they performed an inclusive review of the existing literature. They found that it lacks research concentrating on incident responses and forensic analysis frameworks designed specifically for remotely piloted aerial systems. Then, they attempted to bridge this gap. The researchers in [41] introduced the concept of "electromagnetic watermarking" as a technique exploiting the IEMI impacts to embed a watermark into civilian UAVs so that forensic tracking could be done well. In [42], many aircraft accident investigators and drone forensics investigators were surveyed to find out how they employ forensic models to carry out forensic analyses on drones. The authors analyzed the data using the chi-square test of independence; it revealed no significant connection between the drone investigations of the groups of respondents and the techniques they use to perform UAS forensics. [43] introduced a new method to accurately and quickly determine whether a drone is lying on the ground or in the sky. These results are attained just by eavesdropping on the radio traffic and processing it using standard machine learning techniques (instead of using any active approach). The authors in that study asserted that if the network traffic is classified properly, the exact status of a drone could be accurately determined using the overall operating system of ArduCopter (for instance, several DJI and Hobbyking vehicles). Furthermore, a lower bound was created on the detection delay when using the aforementioned method. It was confirmed that their proposed solution could discriminate against a drone's state (moving or steady) with approximately 0.93 SR in 3.71 s. The researchers in [44] assessed and discussed the security vulnerabilities of Parrot Mambo FPV and Eachine E010 drones. They then suggested proper countermeasures to enhance their resilience against possible attacks. The findings showed that Parrot Mambo FPV was vulnerable to de-authentication and FTP service attacks, while Eachine E010 was susceptible to radio frequency (RF) replay and custom-made controller attacks.

The authors in [45] discussed the overall legal processes that need to be taken into action to collect drones from the crime scene and investigate them in the laboratory. In addition, in [46], a model was introduced for collecting and documenting digital data from the flight items and the related mobile devices to aid investigators in forensically examining two common drone systems, i.e., the Mavic Air and DJI Spark. Recently, several studies have been conducted in the drone forensics domain. For example, in [47], a novel drone forensic readiness framework was proposed; however, it lacked a real implementation. Moreover, the authors addressed several issues and challenges in the drone forensics domain in [16][48][49][50][51][52][53].

The variety of drone infrastructures makes drone forensics a diverse, complex, and unclear domain. Researchers and developers typically deal with the drone forensics domain from three perspectives: drone infrastructures perspective and technical perspective as well as drone incident perspective. However, they vary in covering the perspectives. For example, some models covered all three drone forensics perspectives, whereas others covered two, and others covered only one.

The comprehensive review of all drone forensic models reveals that the drone forensics domain lacks a unified model/framework for data collection and analysis. There is a lack of a post-investigation stage that can facilitate evaluating the investigation stage and overcoming previous mistakes.

3. Machine Learning Techniques Used in the Drone Forensics Field

Machine learning (ML) is an artificial intelligence (AI) area that deals with developing mathematical predictive models. These models are created in a way to analyze large volumes of data and uncover repeated patterns by using the underlying correlations among the various components of the data. This aids in the decision-making process without human interference. Such techniques also attempt to increase the forecast accuracy by learning from “experience” (also known as historical data). A training phase and a testing phase are both included in machine learning algorithms. The process of enhancing prediction performance is closely based on the process of training the model, when these models are given a large amount of historical data to produce mathematical values, simulating an artificially trained brain. Systems security [54], natural language processing [55], robotic vehicles [56], fraud detection [57], text and handwriting classification [58], object categorization [59], digital forensics [60], and speech recognition [61] are some of the areas of ML. ML models may also be applied to the discovery and detection of hidden patterns in the data being analyzed as well as the classification of the data. This is where the process is tested. Each of these algorithms follows a different approach to data analysis. Random forest, naïve Bayes, KNN, linear regression, artificial neural network (ANN), SVM, and decision tree are examples of such techniques. ML has been applied to studying a variety of issues linked to UAV. The authors in [62] presented a comprehensive study of machine learning algorithms for UAV-based communications. The study discussed how machine learning has been used to improve numerous phases of UAV-based communication, including channel modelling, resource management, positioning, and security. The paper divided the ML applications into four categories: (1) security (public safety, network jamming, and eavesdropping), (2) positioning (placement, detection, and mobility), (3) resource management (network planning, power management, routing, and data caching), and (4) physical layer (channel modelling, interference management, and spectrum allocation). The article then summarized the relevant work in each of these domains. An aggressive attempt to inject noise into a communication channel to disrupt ordinary communication exchange is known as a jamming attack. A two-classifier-based technique for identifying jamming attacks on a cloud radio access network (C-RAN) network was proposed in [63]. The multilayer perceptron (MLP) was the first classifier, and the Kernlab support vector machine (KSVM) was the second. In a low-dimensional space, jamming attacks were found to be non-linearly separable. As a result, for certain jamming attack vectors that bypass the MLP classifier, the differentiation between two classes of radio signal data can be achieved by the use of a KSVM machine learning solution. Their results were promising; they assisted to demonstrate the importance of using machine learning to classify data in order to refer to a jamming or eavesdropping attempt.

The authors in [64] proposed an anomaly detection model to reduce several attack vectors' consequences. Their ML-based anomaly detector can detect five attack types: constant position deviation (message modification), random position deviation (message modification), velocity drift attack (message modification), DOS attack (message deletion) with constructive and destructive interference, and flight replacement attack (message injection). The automatic dependent surveillance-broadcast (ADS-B) air traffic surveillance system was the case study in their research (automatic dependent surveillance-broadcast). Preliminary ADS-B data reconstruction, combined presentation of the reconstructed and actual values to the SVDD (support vector data description) for training, and the definition and implementation of a hypersphere classifier for anomaly detection are parts of the two-step anomaly detection scheme. Reinforced learning-based power provisioning techniques are used to protect

UAV transmissions from attacks such as eavesdropping and jamming [65]. ML can be used to detect an eavesdropper by building a classifier based on the received signals connected to eavesdropping attacks and non-attacks [66]. They developed the ML classifier by feeding it with data that showed a radio signal jamming attack.

Deep-learning algorithms proposed for feature extraction, planning, and situational awareness in UAV-related domains were the subject of another review article [65]. In [66], first, the researchers noted that drones frequently fly higher than typical ground user equipment. Flight altitude and line of sight propagation in open space both have an impact on radio signal transmission. They suggested a technique for locating rogue drones that could be found in a mobile network. Ground-based technology can be used to register drones that are lawful. On the other side, unregistered rogue drones that enter restricted airspace could be a security risk. The authors created virtual drone deployment scenarios for urban settings that included outside drones and ground-based equipment. The simulation scenario took into account the quantity of flying sites and sectors, inter-site distance, antennas for a base station (height and power), and carrier frequencies. Data obtained from the simulation were gathered and split into two categories: training and testing. The logistic regression (LR) and decision trees (DTs) were employed as two ML techniques. Other user equipments and drones were chosen as the two categories (variables) for LR. DT is a supervised learning model that learns by accessing feature-value tuples from a dataset. In this instance, the following items were noted: the serving cell data, the received signal strength indicator (RSSI), the standard deviation of the eight strongest reference signals, and the difference between the top two reference signals for strength. The classification results demonstrated a 100% accuracy in detecting rogue drones at heights more than 60 m and a 5% detection rate for lower altitudes. This had to deal with radio frequency interference, a more common phenomenon at lower altitudes.

Ref. [67] proposed a deep-learning-based method for detecting and identifying drones. Particular attention was paid to the identification and detection of drone acoustic fingerprints. Drones were used to create 1300 audio samples for the drone noise data standards. Additionally, to assure the accuracy of detections, the datasets included a combination of drone audio recordings recorded in an interior environment employing drone propeller sounds, stillness, and pure drone noise. To equalize audio clips, time gaps between captures were also utilized. Processing was done based on the file type, data sampling rate, and channel bitrate of each audio file. The deep-learning classifier became more successful by segmenting audio samples into more manageable portions (which were then experimented to determine the most accurate segment size). In a three-class classification experiment, the three selected classifiers—recurrent neural networks (RNN), convolutional neural networks (CNN), and convolutional recurrent neural networks (CRNN)—reported the classification of the processed drone data (drone type one, drone type two, and other noise). The CNN method was proven to produce better results than the other two.

A full drone identification approach based on ML was presented by Lee et al. in [68]. Using a CNN-based cascade classification method, the authors could classify picture data (data produced by drones with cameras) for their study. A total of 2206 drone pictures had their tags manually added. In total, 1777 were utilized for training, and the remaining 429 were used for testing. The system was able to determine the location of a drone on a camera-captured image and the vendor model of a drone based on machine classification, with stated accuracy rates of

more than 90%. In [69], using the Haar feature processing method, the authors were able to extract drone sub-images with the help of the pictures collected.

The researchers in [67] offered a way to spot anomalies in a swarming flight with numerous flying drones, where the adversary might purposefully influence some drones to sabotage. Flight data from several streams were examined in order to discover these irregularities. The authors produced 16 samples per time stamp when sampling the drone data, which was made up of time-series sensory data. Prelabeled data were gathered from both normal and unusual drones. Three types of anomalies were identified: noise produced by sensor-induced signal interruptions in flight, anomalous signals generated in flight but recoverable in flight, and signal faults that force an aircraft to land as a result of a malfunction. A generative model-based 1D signal unsupervised CNN classifier was chosen for the studies.

In [68], based on the classification of drone data using ML, a drone position prediction method was defined. A naïve Bayes classifier may predict a drone's power usage and current location using drone data gathered at the ground controller, which may allow later plans to continue or cease flying. Drone altitude, the four transmitter coils' switching status, and the measured power transfer efficiency are among the data fields used for classification. To confirm the correctness of the classification, the resulting drone position was contrasted with the actual drone position. To create a naïve Bayes model, the classifier was trained utilizing the prior observations of the drone flight trajectory, path, and position as input. The accuracy error rates ranged from 0.09 to 45%, which were shown to be dependent on feature parameters such as transmitter coil-switching values. Based simply on the communication between the drone and the remote controller, the authors in [69] developed a methodology to detect the presence of a remotely operated drone, its current condition, and its movement. As a classifier, they used the random forest technique. It also assesses the methodology's efficacy in the face of high packet loss and evasion attempts. The methodology was created and tested exclusively for RPAS (remotely piloted aircraft systems) drones. They showed a detection accuracy of 99.9% within 30 m without packet loss and detection accuracy of >97% within 200 m with up to 74.8% packet loss.

The authors of [70] suggested a hierarchical ensemble learning technique for radio frequency (RF) data-based UAV detection and identification. UAVs are initially detected, then their types and modes of operation are identified by the second and third classifiers. Each classifier used ensemble learning based on the KNN and XGBoost algorithms. The proposed method attained a classification accuracy of 99% with ten categories. There are three different types of UAVs, and each class indicates its nature and manner of operation (ON mode, hovering mode, flying mode, or recording mode). Additionally, in [68], the current machine-learning-based methods were examined to find a way to identify UAVs from diverse data sources.

In [71], a method was described for identifying the drone pilots via radio control signals broadcast to a UAV using a standard transmitter. Twenty trained pilots who flew the UAV on three different routes were contacted to collect the data required. There were nine characteristics in the dataset, including thrust, pitch, roll, and yaw at the time (t) and their derivatives at the time (t) (D). Additionally, a control simultaneity variable at a time (t) was provided, describing the control signals available at the time (t). The proposed system was shown to have an accuracy rate of 90% and

used the random forest algorithm. The suggested method can be applied to forensic analysis in the event of a suspected drone hijacking to locate the UAV's pilot and raise the alarm.

In [43], the authors proposed using only the encrypted communication traffic between the drone and the remote controller to determine the drone's status (flying or at rest). A drone equipped with ArduCopter firmware was used to collect the data. Six features were produced without using the contents of the encrypted packet (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, i.e., decision tree, random forest, and neural networks, were used to classify data. The random forest classifier yielded superior results for drone detection.

The authors of [72] recognized inter-drone communication reliability as a concern, where transmitted packets may not arrive at their intended locations. To effectively predict the transmission patterns, the authors employed ML. Utilizing a Monte Carlo simulation setup that incorporates transmission channel modeling, the success/failure probability was determined. The ML method for linear regression was combined with a comparative analysis using support vector machines (SVMs) with a quadratic kernel. The first property identified was the negative link between inter-drone distance and the likelihood of a successful packet transfer. A total of 20 drones were simulated to encourage measurement data collection. In packet transmission, the chance of communication channel success was set to 0.05. Transmission probability inside a channel, node locations, and time were all recognized as specific features for linear regression training. Quantization factor values, transmission probabilities, timings, and network node locations were among the features used by the SVM-QK classifier. The average prediction rates yielded an extremely low error rate of 0.00597.

The literature showed that digital forensics for drones utilizing ML algorithms had received less attention. Very little research focuses on employing ML techniques for forensic analysis of drone data. The authors of [16] surveyed existing drone forensics (DRF) studies. They discussed the difficulties and possibilities in drone forensics. They also developed an approach to investigating drone-related events.

On the other hand, several models and frameworks have been proposed in the literature for drone and digital forensics to solve the challenges and issues of drone forensics [73][74][75][76][77][78][79][80][81][82].

References

1. Mohamed, N.; Al-Jaroodi, J.; Jawhar, I.; Idries, A.; Mohammed, F. Unmanned aerial vehicles applications in future smart cities. *Technol. Forecast. Soc. Chang.* 2020, 153, 119293.
2. Yu, K.-P.; Tan, L.; Aloqaily, M.; Yang, H.; Jararweh, Y. Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. *IEEE Trans. Ind. Inform.* 2021, 17, 7669–7678.
3. Yu, K.; Arifuzzaman, M.; Wen, Z.; Zhang, D.; Sato, T. A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid. *IEEE*

Trans. Instrum. Meas. 2015, 64, 2072–2085.

- 4. Tan, L.; Yu, K.; Shi, N.; Yang, C.; Wei, W.; Lu, H. Towards secure and privacy-preserving data sharing for covid-19 medical records: A blockchain-empowered approach. *IEEE Trans. Netw. Sci. Eng.* 2021, 9, 271–281.
- 5. Tan, L.; Yu, K.; Ming, F.; Cheng, X.; Srivastava, G. Secure and resilient artificial intelligence of things: A HoneyNet approach for threat detection and situational awareness. *IEEE Consum. Electron. Mag.* 2021, 11, 69–78.
- 6. Tan, L.; Yu, K.; Lin, L.; Cheng, X.; Srivastava, G.; Lin, J.C.-W.; Wei, W. Speech emotion recognition enhanced traffic efficiency solution for autonomous vehicles in a 5G-enabled space-air-ground integrated intelligent transportation system. *IEEE Trans. Intell. Transp. Syst.* 2021, 23, 2830–2842.
- 7. Awan, S.; Ahmed, S.; Ullah, F.; Nawaz, A.; Khan, A.; Uddin, M.I.; Alharbi, A.; Alosaimi, W.; Alyami, H. IoT with blockchain: A futuristic approach in agriculture and food supply chain. *Wirel. Commun. Mob. Comput.* 2021, 2021, 5580179.
- 8. Li, H.; Yu, K.; Liu, B.; Feng, C.; Qin, Z.; Srivastava, G. An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things. *IEEE J. Biomed. Health Inform.* 2021, 26, 1949–1960.
- 9. Saif, A.; Dimyati, K.; Noordin, K.A.; C, D.G.; Shah, N.S.M.; Abdullah, Q.; Mohamad, M. An efficient energy harvesting and optimal clustering technique for sustainable postdisaster emergency communication systems. *IEEE Access* 2021, 9, 78188–78202.
- 10. Feng, C.; Liu, B.; Guo, Z.; Yu, K.; Qin, Z.; Choo, K.-K.R. Blockchain-based cross-domain authentication for intelligent 5g-enabled internet of drones. *IEEE Internet Things J.* 2021, 9, 6224–6238.
- 11. Feng, C.; Liu, B.; Yu, K.; Goudos, S.K.; Wan, S. Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs. *IEEE Trans. Ind. Inform.* 2021, 18, 3582–3592.
- 12. Ullah, F.; Pun, C.-M. The Role of Internet of Things for Adaptive Traffic Prioritization in Wireless Body Area Networks. In *Healthcare Paradigms in the Internet of Things Ecosystem*; Elsevier: Amsterdam, The Netherlands, 2021; pp. 63–82.
- 13. Feng, C.; Yu, K.; Aloqaily, M.; Alazab, M.; Lv, Z.; Mumtaz, S. Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV. *IEEE Trans. Veh. Technol.* 2020, 69, 13784–13795.
- 14. Ding, F.; Zhu, G.; Alazab, M.; Li, X.; Yu, K. Deep-learning-empowered digital forensics for edge consumer electronics in 5G HetNets. *IEEE Consum. Electron. Mag.* 2020, 11, 42–50.

15. Ding, F.; Yu, K.; Gu, Z.; Li, X.; Shi, Y. Perceptual enhancement for autonomous vehicles: Restoring visually degraded images for context prediction via adversarial training. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 9430–9441.
16. Al-Dhaqm, A.; Ikuesan, R.; Kebande, V.; Razak, S.; Ghabban, F. Research Challenges and Opportunities in Drone Forensics Models. *Electronics* **2021**, *10*, 1519.
17. Ding, F.; Zhu, G.; Li, Y.; Zhang, X.; Atrey, P.K.; Lyu, S. Anti-forensics for face swapping videos via adversarial training. *IEEE Trans. Multimed.* **2021**, *24*, 3429–3441.
18. Zhou, Z.; Dong, X.; Li, Z.; Yu, K.; Ding, C.; Yang, Y. Spatio-Temporal Feature Encoding for Traffic Accident Detection in VANET Environment. *IEEE Trans. Intell. Transp. Syst.* **2022**, *1*–10.
19. Kovar, D.; Dominguez, G.; Murphy, C. UAV (aka drone) Forensics. In Proceedings of the SANS DFIR Summit, Austin, TX, USA, 23–24 June 2016; pp. 23–24.
20. Mhatre, V.; Chavan, S.; Samuel, A.; Patil, A.; Chittimilla, A.; Kumar, N. Embedded video processing and data acquisition for unmanned aerial vehicle. In Proceedings of the 2015 International Conference on Computers, Communications, and Systems (ICCCS), Kanyakumari, India, 2–3 November 2015; pp. 141–145.
21. Yu, K.; Tan, L.; Lin, L.; Cheng, X.; Yi, Z.; Sato, T. Deep-learning-empowered breast cancer auxiliary diagnosis for 5GB remote E-health. *IEEE Wirel. Commun.* **2021**, *28*, 54–61.
22. Yu, K.; Tan, L.; Mumtaz, S.; Al-Rubaye, S.; Al-Dulaimi, A.; Bashir, A.K.; Khan, F.A. Securing critical infrastructures: Deep-Learning-Based threat detection in IIoT. *IEEE Commun. Mag.* **2021**, *59*, 76–82.
23. Roder, A.; Choo, K.-K.R.; Le-Khac, N.-A. Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study. *arXiv* **2018**, arXiv:1804.08649.
24. Horsman, G. Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digit. Investig.* **2016**, *16*, 1–11.
25. Procházka, T. Capturing, Visualizing, and Analyzing Data from Drones. Bachelor Thesis, Charles University, Staré Město, Czech Republic, 2016.
26. Mohan, M. Cybersecurity in Drones; Utica College: Utica, NY, USA, 2016.
27. 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, NY, USA, 13–15 March 2017; pp. 1–6.
28. 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.

29. Prastyo, S.E.; Riadi, I.; Luthfi, A. Forensic Analysis of Unmanned Aerial Vehicle to Obtain GPS Log Data as Digital Evidence. *Int. J. Comput. Sci. Inf. Secur.* 2017, 15, 280–285.

30. Llewellyn, M. DJI Phantom 3-Drone Forensic Data Exploration; Edith Cowan University: Perth, Australia, 2017.

31. Renduchintala, A.L.P.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.

32. Barton, T.E.A.; Bin Azhar, M.H. 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.

33. Maune, K.G. A Project Completed as Part of the Requirements for BSc (Hons) Computer Forensic Investigation. 2018. Available online: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1025.4878&rep=rep1&type=pdf> (accessed on 3 March 2021).

34. Benzarti, S.; Triki, B.; Korbaa, O. Privacy preservation and drone authentication using Id-Based Signcryption. *Front. Artif. Intell. Appl.* 2018, 303, 226–239.

35. 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.

36. Dawam, E.S.; Feng, X.; Li, D. Autonomous Arial Vehicles in Smart Cities: Potential Cyber-Physical Threats. In Proceedings of the 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, 28–30 June 2018; IEEE: New York, NY, USA, 2018; pp. 1497–1505.

37. Esteves, J.L.; Cottais, E.; Kasmi, C. Unlocking the Access to the Effects Induced by IEMI on a Civilian UAV. In Proceedings of the 2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE), Amsterdam, The Netherlands, 27–30 August 2018; pp. 48–52.

38. Fitwi, A.; Chen, Y.; Zhou, N. An Agent-Administrator-Based Security Mechanism for Distributed Sensors and Drones for Smart Grid Monitoring; SPIE: Philadelphia, PA, USA, 2019; p. 11018.

39. Jones, Z.V.; Gwinnett, C.; Jackson, A.R. The effect of tape type, taping method and tape storage temperature on the retrieval rate of fibres from various surfaces: An example of data generation and analysis to facilitate trace evidence recovery validation and optimisation. *Sci. Justice* 2019, 59, 268–291.

40. Salamh, F.E.; Rogers, M. Drone Disrupted Denial of Service Attack (3DOS): Towards an Incident Response and Forensic Analysis of Remotely Piloted Aerial Systems (RPASs). In Proceedings of

the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019; pp. 704–710.

41. Esteves, J.L. Electromagnetic Watermarking: Exploiting IEMI effects for forensic tracking of UAVs. In Proceedings of the 2019 International Symposium on Electromagnetic Compatibility-EMC EUROPE, Barcelona, Spain, 2–6 September 2019; pp. 1144–1149.
42. Mei, N. Unmanned Aircraft Systems Forensics Framework an Approach to Unmanned Aircraft Systems Forensics Framework. Ph.D. Thesis, Capitol Technology University, South Laurel, MD, USA, 2019.
43. Sciancalepore, S.; Ibrahim, O.A.; Olinger, G.; Di Pietro, R. Detecting drones status via encrypted traffic analysis. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning, Miami, FL, USA, 14 May 2019; pp. 67–72.
44. Yihunie, F.L.; Singh, A.K.; Bhatia, S. Assessing and Exploiting Security Vulnerabilities of Unmanned Aerial Vehicles. *Smart Innov. Syst. Technol.* 2020, 141, 701–710.
45. Mistry, N.R.; Sanghvi, H.P. Drone forensics: Investigative guide for law enforcement agencies. *Int. J. Electron. Secur. Digit. Forensics* 2021, 13, 334–345.
46. Yang, C.-C.; Chuang, H.; Kao, D.-Y. Drone Forensic Analysis Using Relational Flight Data: A Case Study of DJI Spark and Mavic Air. *Procedia Comput. Sci.* 2021, 192, 1359–1368.
47. Alotaibi, F.M.; Al-Dhaqm, A.; Al-Otaibi, Y.D. A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. *Comput. Intell. Neurosci.* 2022, 2022, 1–13.
48. Atkinson, S.; Carr, G.; Shaw, C.; Zargari, S. Drone Forensics: The Impact and Challenges. In Digital Forensic Investigation of Internet of Things (IoT) Devices; Springer: Berlin/Heidelberg, Germany, 2021; pp. 65–124.
49. 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), Virtual Conference, 13–16 February 2022; pp. 291–296.
50. Husnjak, S.; Forenbacher, I.; Peraković, D.; Cvitić, I. UAV Forensics: DJI Mavic Air Noninvasive Data Extraction and Analysis. In Proceedings of the 5th EAI International Conference on Management of Manufacturing Systems, Krynica-Zdrój, Poland, 5–7 October 2022; pp. 115–127.
51. Parghi, P.; Dhamija, R.; Agrawal, A.K. Innovative Approach to Onboard Media Forensic of a Drone. In IOT with Smart Systems; Springer: Berlin/Heidelberg, Germany, 2022; pp. 307–314.
52. Alhussan, A.A.; Al-Dhaqm, A.; Yafooz, W.M.S.; Emara, A.-H.M.; Razak, S.B.A.; Khafaga, D.S. A Unified Forensic Model Applicable to the Database Forensics Field. *Electronics* 2022, 11, 1347.
53. Alhussan, A.A.; Al-Dhaqm, A.; Yafooz, W.M.S.; Razak, S.B.A.; Emara, A.-H.M.; Khafaga, D.S. Towards Development of a High Abstract Model for Drone Forensic Domain. *Electronics* 2022, 11,

1168.

54. 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.
55. Nadkarni, P.M.; Ohno-Machado, L.; Chapman, W.W. Natural language processing: An introduction. *J. Am. Med. Inform. Assoc.* 2011, 18, 544–551.
56. Murphy, R.R. *Introduction to AI robotics*; MIT Press: Cambridge, MA, USA, 2019.
57. Abdallah, A.; Maarof, M.A.; Zainal, A. Fraud detection system: A survey. *J. Netw. Comput. Appl.* 2016, 68, 90–113.
58. Kulik, S.D. Neural network model of artificial intelligence for handwriting recognition. *J. Theor. Appl. Inf. Technol.* 2015, 73, 1–10.
59. Voronin, V.V.; Marchuk, V.I.; Semenishchev, E.A.; Makov, S.V.; Creutzburg, R. Digital inpainting with applicataions to forensic image processing. *Electron. Imaging* 2016, 28, 1–7.
60. Oladipo, F.; Ogbuju, E.; Alayesanmi, F.S.; Musa, A.E. The State of the Art in Machine Learning-Based Digital Forensics. *SSRN* 2020.
61. Alhawiti, K.M. Advances in artificial intelligence using speech recognition. *Int. J. Comput. Inf. Eng.* 2015, 9, 1432–1435.
62. 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.
63. 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.
64. Luo, P.; Wang, B.; Li, T.; Tian, J. ADS-B anomaly data detection model based on VAE-SVDD. *Comput. Secur.* 2021, 104, 102213.
65. 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.
66. 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.
67. 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.

68. 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.

69. Sciancalepore, S.; Ibrahim, O.A.; Olinger, G.; Di Pietro, R. PiNch: An effective, efficient, and robust solution to drone detection via network traffic analysis. *Comput. Netw.* **2020**, *168*, 107044.

70. 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.

71. 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.

72. 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 Island, Korea, 19–21 October 2016; pp. 147–149.

73. Al-Dhaqm, A.; Razak, S.; Ikuesan, R.A.; Kebande, V.R.; Othman, S.H. Face Validation of Database Forensic Investigation Metamodel. *Infrastructures* **2021**, *6*, 13.

74. Kebande, V.R.; Ikuesan, R.A.; Karie, N.M. Review of Blockchain Forensics Challenges. In *Blockchain Security in Cloud Computing*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 33–50.

75. Kim, J.; Kim, M.-Y.; Kwon, H.; Kim, J.-W.; Im, W.-Y.; Lee, S.M.; Kim, K.; Kim, S.J. Active Machine Learning Adversarial Attack Detection in the User Feedback Process. *Forensic Sci. Int. Rep.* **2020**, *3*, 36908–36923.

76. Al-Dhaqm, A.; Razak, S.; Othman, S.H.; Choo, K.-K.R.; Glisson, W.B.; Ali, A.; Abrar, M. CDBFIP: Common database forensic investigation processes for Internet of Things. *IEEE Access* **2017**, *5*, 24401–24416.

77. Kebande, V.R.; Karie, N.M.; Choo, K.R.; Alawadi, S. Digital forensic readiness intelligence crime repository. *Secur. Priv.* **2021**, *4*, e151.

78. Al-Dhaqm, A.; Razak, S.A.; Ikuesan, R.A.; Kebande, V.R.; Siddique, K. A Review of Mobile Forensic Investigation Process Models. *IEEE Access* **2020**, *8*, 173359–173375.

79. Makura, S.; Venter, H.S.; Kebande, V.R.; Karie, N.M.; Ikuesan, R.A.; Alawadi, S. Digital forensic readiness in operational cloud leveraging ISO/IEC 27043 guidelines on security monitoring. *Secur. Priv.* **2021**, *4*, e149.

80. Philomin, S.; Singh, A.; Ikuesan, A.; Venter, H. Digital forensic readiness framework for smart homes. In Proceedings of the International Conference on Cyber Warfare and Security, Albany, NY, USA, 17–18 March 2022.

81. Kebande, V.R.; Ikuesan, R.A. Virtual sensor forensics. In Proceedings of the 2nd International Conference on Intelligent and Innovative Computing Applications, Plaine Magnien, Mauritius, 24–25 September 2020.
82. Al-Dhaqm, A.; Razak, S.A.; Siddique, K.; Ikuesan, R.A.; Kebande, V.R. Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field. *IEEE Access* 2020, 8, 145018–145032.

Retrieved from <https://encyclopedia.pub/entry/history/show/66654>