Digital Forensics Issues of Unmanned Aerial Vehicle Operations

Orkhan Valikhanli
Institute of Information Technology, Baku, Azerbaijan
orkhanvalikhanli@gmail.com

***Abstract*— Recently, Unmanned Aerial Vehicles (UAVs) have become increasingly important in everyday life. It's possible to see their use in different fields, including agriculture, photography, surveillance, rescue operations, etc. However, as their use grows, concerns about misuse, safety, and privacy are also increasing. Due to this reason, UAV forensics has emerged as a specialized field. In order to investigate incidents, UAV forensics focuses on identifying, collecting, and analyzing data from UAVs. The article examines digital forensics issues related to UAVs.**

Keywords*— *UAV forensics; drone forensics; evidence sources; digital forensic extraction; forensic challenges;

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs) or drones have become an important part of our modern life. They are reliable, cheaper, and can complete tasks efficiently. For surveillance, authorities can monitor large areas in real time without risking human life. For agriculture, farmers can monitor crop health, detect diseases early, and use pesticides or fertilizers with the help of UAVs. For delivery, UAVs make it possible to transport goods more quickly. This is very useful for remote areas and locations that are hard to reach. They are also used to deliver medical supplies like vaccines and pills. For infrastructure, UAVs are used to inspect buildings, monitor projects, etc. This helps to reduce the need for physical labor. Overall, UAVs improve productivity, reduce risks, and make many tasks more effective.

But in addition to these advantages, UAVs have brought with them new privacy, security, and criminal misuse issues. UAVs can be used for harmful tasks. They can be used to violate people's privacy by spying on them without their consent [1]. Also, UAVs may be used by some people to interfere with busy public spaces or airports. This can lead to fear and safety concerns. In December of 2018, Gatwick Airport was forced to close due to the UAV disruptions [2]. As a result, many flights were cancelled. UAVs may also target critical infrastructure such as global supply chains and power systems. In September of 2019, two Saudi Arabian oil installations were hit by drone attacks. It damaged sites responsible for processing most of the country's crude oil production [3]. UAVs may also be used to carry out cyberattacks. This is possible by equipping them with specialized hardware components. They can fly near target devices or networks. UAVs can then jam signals, spoof communications, and inject malicious packets. UAVs may also be used to deliver illegal substances such as drugs and explosives. For instance, police say there have been recent reports of drug smugglers using drones in Punjab, India [3]. Due to these problems, governments around the world are actively developing frameworks and policies.

In this context, one of the issues of UAVs is related to their digital forensics. Unlike regular systems, UAVs work in different environments and have many components. These include flight controller, various sensors, navigation systems, actuators, cameras, communication links, etc. Due to these distinct features, gathering and analyzing evidence becomes much more difficult for UAVs.

In this work, various digital forensics issues of UAVs are discussed. The paper is organized as follows. In Section II, general information about UAVs and their various types is demonstrated. In Section III, the digital forensic investigation process and evidence sources in UAV systems are discussed. In Section IV, main forensic challenges are presented. In Section V, tools which are used in UAV forensics are demonstrated. In Section VI, existing approaches in UAV digital forensics are discussed. Section VII concludes this work.

II. UNMANNED AERIAL VEHICLE SYSTEMS

UAV systems consist of the aircraft itself as well as the equipment required to control and monitor it. They are designed to perform flight operations using onboard sensors, navigation system, and various control mechanisms.

A. Basic components of UAVs

UAVs consist of various components. It is necessary to understand these components before discussing more advanced topics. The main components are listed below:

- **Airframe:** The primary structural component of a UAV is its airframe. It comprises all of the system's structural components, such as fuselage, landing gear, wings, etc.
- **Flight controller (FC):** It stabilizes the UAV, processes data from sensors, controls the motors, records flight logs, and performs other important tasks.
- **Motor and propeller:** Generates mechanical energy from electrical energy to turn the propellers.
- **Electronic Speed Controller (ESC):** It receives control signals from FC to regulate the speed of the UAV's motors.
- **Communication module:** It is used to transmit and receive data between the UAV and the remote controller or between the UAV and other UAVs.

DOI: 10.25045/forensic.gov.2026.20

- **Navigation module:** It is used to determine UAV position and orientation.
- **Battery:** Supplies power to the UAV.
- **Power Distribution Board (PDB):** Distributes battery power to various UAV components.
- **Camera:** It is used to capture aerial images and record videos.

B. Types of UAVs

There are different types of UAVs. Each of them is designed for specific tasks and applications. These types differ according to their intended use, size, and range. The main types of UAVs are listed below [4]:

- **Fixed-wing:** This type of UAV has stationary wings and resembles conventional airplanes.
- **Single-rotor:** Similar to conventional helicopters.
- **Multi-rotor:** UAVs with multiple rotor systems. These include quadcopters, hexacopters, octocopters, etc.
- **Vertical Take-Off and Landing (VTOL):** It combines features of fixed-wing and multi-rotor UAVs.

C. Remote Controller of UAVs

UAVs are monitored and controlled by remote controllers. They usually consist of several components such as control sticks, buttons, communication modules, displays, and antennas. Additionally, remote controllers may include specialized software or firmware. Operators (pilots) use the remote controller to send commands to the UAV, adjusting its altitude, speed, and direction. They also receive real-time data such as aerial images, video feeds, telemetry, and other flight information. Moreover, some UAVs can also be controlled via tablets or mobile devices.

III. Digital Forensic Investigation Process and Evidence Sources in UAV Systems

As UAVs become more common in commercial and military use, they also create new problems. These include smuggling, cyberattacks, privacy violations, and other illegal uses. Digital forensic investigators analyze data stored within UAVs and their related systems. This procedure helps in identifying operators, reconstructing flight paths, and finding out the purpose of a UAV's actions.

A. Digital forensics investigation process in UAV systems

UAV digital forensics is a specialized branch of digital forensics which consists of various steps, including identification, preservation, collection, examination, analysis, reporting, and presentation. It's necessary to understand each step and these are given below:

- **Identification:** This is the initial step. It is used to determine the UAV, remote controller, and any potential data sources, such as internal memory, removable storage, and cloud storage.
- **Preservation:** This means to protect the UAV and all its data from any kind of change or loss. This includes special measures to block radio signals to prevent remote memory erasure. In most cases, it's also necessary to take pictures of the scene.
- **Collection:** In this step, all relevant data are collected from the UAV itself, the remote controller, and related systems. It includes images, videos, various flight logs, etc.
- **Examination:** Digital forensic investigators process and prepare data. They convert data into understandable formats, filter out unnecessary information, and even recover deleted media files.
- **Analysis:** Based on the data processed during examination, forensic investigators interpret that data to answer questions. For example, they may answer which path the UAV took, when, how fast, etc.
- **Reporting:** The entire procedure and its conclusions are documented by digital forensic investigators. This includes what was found, how it was discovered, which methods were used, and what tools were used during the investigation.
- **Presentation:** Digital forensic investigators present the findings from the report to the intended audience in an understandable manner. This could involve providing technical results to legal teams and informing law enforcement.

B. Evidence sources in UAV systems

During an investigation, a variety of possible digital evidence sources associated with UAV systems could offer useful forensic artifacts. Fig. 1 demonstrates the main evidence sources in the UAV ecosystem. Let's discuss each evidence source separately.

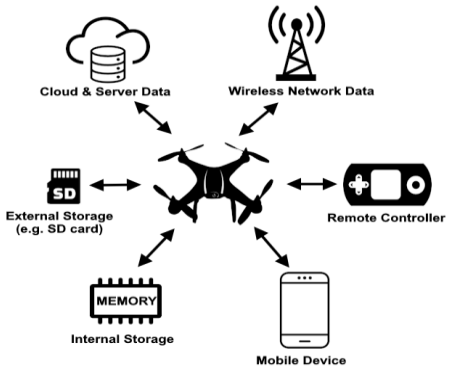

Figure 1. Evidence sources in UAV ecosystem

Cloud and server data can contain backup media files, user account information, synchronized flight logs, and firmware update logs. Wireless network data may provide connection timestamps and telemetry transmission information. It is also possible to locate a UAV if it uses cellular data. This method is called triangulation. The remote controller of the UAV also contains a lot of information, including flight command logs, configuration data, telemetry caches, event, and error logs. Mobile devices which running UAV specific applications usually contain user account data, flight history, captured

images, and recorded video files. Internal storage contains telemetry information, sensor data, system configuration files, device identification data, firmware files, and system error logs. External storage, like an SD card may contain captured images, recorded videos, telemetry files, flight logs, and other important data.

IV. MAIN FORENSIC CHALLENGES

The main forensic issues with UAVs are related to the way these systems store and protect data. One of the issues is data volatility. UAVs rely on both volatile and non-volatile memory. When power is interrupted, volatile data can be lost instantly [5].

UAV forensics is further complicated by limited hardware and software access. Many manufacturers build UAVs with proprietary firmware. They may also use custom file formats. This means digital forensic investigators may have difficulties to understand how data is stored or processed. Furthermore, accessing UAV's internal components may require special hardware and applications.

The use of encryption poses another significant obstacle. Most UAV manufacturers encrypt private data, including flight logs and user information. Because of this, it is challenging for investigators to understand the data without decryption keys. To bypass these protections, experts must either find a technical flow or ask for help directly from the manufacturer.

There are also legal and ethical considerations. The information gathered from personal devices may lead to terrible violations of personal privacy, even when digital investigations are carried out by qualified experts [6]. In many cases, UAVs also require owner permission to access their data, which complicates the situation even more.

Anti-forensic methods add another level of complexity. These are intentional acts to hide, modify, or even destroy evidence. For example, UAV operator may delete flight logs, aerial images, and videos. Timestamps and other user data may also be intentionally altered. It's also possible for UAV operator to trigger remote memory erasure, or even overwrite data.

This action may be unrecoverable and can result investigation to fail. In some cases, GPS spoofing may also be used to falsify UAV location. Table I summarizes the major challenges associated with UAV forensics.

TABLE I. UAV FORENSIC CHALLENGES

Forensic Issues	Description	Implications
Data Volatility	Temporary data disappears when power is interrupted.	Important evidence could disappear before being collected.
Restricted Access	UAV systems use proprietary architectures, firmware, and data formats.	Data extraction and interpretation are challenging without specialized tools.
Encryption	Stored data is protected with cryptography.	Data cannot be examined without the proper decryption keys.
Legal and Ethical Issues	Data access is regulated and private.	Permission and legal approval may be necessary for investigations.
Anti-Forensics	Users may intentionally hide or manipulate evidence.	Data can be altered, removed, or made misleading.

V. TOOLS FOR UAV FORENSİCS

The main goal of UAV forensics is to collect and analyze digital as well as physical evidence from UAVs. This helps to understand incidents like crashes, illegal flights, or intrusions. There are specialized tools used for digital forensics. While some are designed specifically for UAVs, others are general-purpose alternatives. These forensic tools are demonstrated in Table II.

TABLE II. FORENSIC TOOLS

Tools	Description
Autopsy	An open-source tool and can be used to examine system files, recover deleted files, etc.
MD-DRONE	A forensic tool for extracting and analyzing data from various UAV manufacturers including Pixhawk, DJI, and Parrot.
CSVView / DatCon	It is used for parsing and visualizing DJI flight log files into readable formats.
DroneXtract	An open-source forensic tool made especially for DJI UAVs to examine flight maps, telemetry, and sensor values.
UAV-1200	Provides data extraction and analysis for a variety of drone models including DJI, XIRO and FreeFlight.
Belkasoft X	It supports digital forensics analysis of data from various UAVs including DJI, ArduPilot, Parrot, etc.
Cellebrite	It can be used to extract flight logs, multimedia files, GPS information from UAVs.
Magnet AXIOM	It is digital forensics tool that can extract and analyze data from the mobile devices used to control the UAV, rather than directly from the UAV.
ExifTool	It can be used to read metadata from images and videos captured by UAVs.

VI. EXISTING APPROACHES IN UAV DIGITAL FORENSICS

Renduchintala et al. [7] present a comprehensive forensic framework for investigating UAVs. The paper suggests an integrated drone forensic model combining both hardware/physical and digital forensic investigation techniques for post-flight analysis. The hardware forensic component focuses on examining drone parts and physical evidence at the crime scene. Additionally, the digital forensic framework includes a JavaFX based application for extracting and analyzing critical onboard flight log parameters. Moreover, the tool supports 3D flight trajectory visualization through a file converter. This enables investigators to reconstruct drone flight paths effectively. According to the paper, research was conducted using DJI Phantom 4 and Yuneec Typhoon H drones. Overall, research provides a simple and reliable way to improve drone forensic investigations. Clark et al. [8] present the forensic analysis of the DJI Phantom III drone. The researchers identify proprietary DAT and TXT flight log files stored on both the drone and the controlling mobile device. According to the paper, the DRone Open source Parser (DROP) is introduced as an open source forensic tool which is capable of decoding the DAT flight log files of DJI. The study shows that investigators can retrieve important pieces of evidence from the drone, such as telemetry records, GPS coordinates,

flight status, and battery information. It's also demonstrated how a particular user can be linked to a specific drone by correlating data from the drone and the mobile device. The paper also highlights the need for appropriate forensic procedures because turning on the drone during acquisition could modify or remove evidence. Bouafif et al. [9] examine the forensic analysis of the Parrot AR Drone 2.0. According to the paper, a variety of technical issues related to drone forensics are identified. These include proprietary file systems, encrypted flight data, dependence on volatile memory, and challenges proving ownership. For UAV investigations, the study suggests a structured forensic methodology based on acquisition, analysis, and reporting. It is demonstrated that forensic investigators can access drone data through wireless, USB, Telnet, FTP, and serial connections. Moreover, it is shown that flight path data, media files, EXIF metadata, etc. can be recovered. Prastya et al. [10] examine the forensic analysis of unmanned aerial vehicles with a focus on extracting GPS log data from the DJI Phantom 3. The study investigates forensic acquisition techniques for the drone, camera memory card, and smartphone controller using both static and live methods. According to the findings, flight log data with GPS coordinates is kept in TXT log files within the DJI app on the smartphone and DAT files on the UAV. It is also found that GPS and flight data are recorded even when the UAV operates in flight modes that do not rely on GPS. The authors demonstrate that image and video metadata can also provide GPS coordinates. Roder et al. [11] propose a forensic investigation process for UAVs using the DJI Phantom 3 as a case study. According to the paper, the distinct architecture and evidence sources of UAV systems make traditional digital forensic frameworks (e.g., ACPO and NIST) guidelines not sufficient for UAV investigations. To solve this problem, a UAV forensic investigation process consisting of multiple steps was proposed. The methodology includes UAV-specific considerations such as identifying modifications, locating hidden storage media, etc.

CONCLUSION

In this work, various digital forensic issues of UAVs are discussed. Based on the discussion, it can be concluded that the digital forensics of UAVs plays an important role in modern criminal investigations. It helps investigators to recover, analyze, and interpret data from UAVs which involved in incidents or illegal activities. UAV forensics is important for ensuring accountability, improving security, and helping with legal investigations. To keep up with the evolving capabilities of UAV technology, new forensic standards and tools will be needed.

REFERENCES

[1] J. O. Uchidiuno, J. Manweiler, and J. D. Weisz, "Privacy and Fear in the Drone Era: Preserving Privacy Expectations Through Technology," in Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal QC Canada: ACM, Apr. 2018, pp. 1–6.

[2] B. Kotkova, "Defence systems against drone attacks," in SGEM International Multidisciplinary Scientific GeoConference EXPO Proceedings, 2022, vol. 22, pp. 19–26.

[3] M. Z. Chaari and S. Al-Maadeed, "The game of drones/weapons makers' war on drones," in Unmanned Aerial Systems, Elsevier, 2021, pp. 465–493.

[4] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," Ad Hoc Netw., vol. 111, no. 102324, p. 102324, 2021.

[5] V. Sihag, G. Choudhary, P. Choudhary, and N. Dragoni, "Cyber4Drone: A systematic review of cyber security and forensics in next-generation drones," Drones, vol. 7, no. 7, p. 430, 2023.

[6] A. Nieto et al., "Privacy-aware digital forensics," in Security and Privacy for Big Data, Cloud Computing and Applications, Institution of Engineering and Technology, 2019, pp. 157–195.

[7] A. Renduchintala, F. Jahan, R. Khanna, and A. Y. Javaid, "A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework," Digit. Investig., vol. 30, pp. 52–72, 2019.

[8] D. R. Clark, C. Meffert, I. Baggili, and F. Breitinger, "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III," Digit. Investig., vol. 22, pp. S3–S14, 2017.

[9] H. Bouafif, F. Kamoun, F. Iqbal, and A. Marrington, "Drone forensics: Challenges and new insights," in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018.

[10] S. E. Prastya, I. Riadi, A. Luth, "Forensic analysis of unmanned aerial vehicle to obtain gps log data as digital evidence", Int. Jour. of Comp. Sci. and Infor. Sec., vol. 15, no. 3, pp. 280-285, 2017.

[11] A. Roder, K.-K. R. Choo, N.-A. Le-Khac, "Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study", arXiv preprint arXiv:1804.08649.