A Comprehensive Forensic Framework for Unmanned Aerial Vehicle Investigations: Empirical Validation with the DJI Mavic 3 Classic

Nidhiba Parmar, Naveen Kumar Chaudhary
School of Cyber Security and Digital Forensics, National Forensic Sciences University, Gandhinagar, India

***Abstract*—The rapid proliferation of unmanned aerial vehicles has introduced significant challenges for digital forensics, particularly due to their increasing involvement in criminal, surveillance, and security-related incidents. The heterogeneous hardware architectures, proprietary data formats, encryption mechanisms, and volatile storage characteristics of modern drones complicate reliable evidence recovery and analysis. This study proposes a comprehensive forensic framework for unmanned aerial vehicle investigations, empirically validated using the DJI Mavic 3 Classic. The proposed methodology integrates a conceptual forensic model with practical investigation procedures, including multi-source data acquisition, metadata analysis, anomaly detection, and digital twin-based reconstruction to support event correlation and timeline reconstruction. Four representative case studies: flight log recovery, firmware modification detection, metadata-driven espionage analysis, and reconstruction of deleted media are conducted to evaluate the framework's effectiveness. Experimental results demonstrate evidence recovery rates of up to 92%, timeline reconstruction accuracy of 95%, and anti-forensic activity detection rates of 100%. The framework explicitly addresses challenges associated with proprietary formats, encryption, and data volatility in drone ecosystems. The proposed approach provides actionable guidance for drone forensics practitioners, researchers, and policymakers, contributing toward standardized and reliable forensic investigation processes for contemporary unmanned aerial vehicle platforms.**

***Keywords*—Drone forensics; unmanned aerial vehicle; DJI Mavic 3 Classic; digital forensics; metadata analysis; digital twin; anomaly detection; evidence recovery**

I. Introduction

Unmanned aerial vehicles (UAVs), or drones, have transformed industries such as agriculture, environmental monitoring, and multimedia reporting, leveraging their affordability, mobility, and advanced sensing capabilities [1], [2], [3]. However, these attributes also enable illicit activities, including unauthorized surveillance, smuggling, and attacks on critical infrastructure, posing significant challenges for law enforcement and regulatory agencies [4], [5]. Incidents involving drones have surged globally, with reports of UAVs breaching restricted airspace, delivering contraband, and conducting corporate espionage, underscoring the urgent need for specialized forensic methodologies to extract and analyze digital evidence [6], [7]. The DJI Mavic 3 Classic, a leading consumer drone, exemplifies these challenges with its proprietary file systems, encrypted storage, and integration with mobile and cloud ecosystems, rendering traditional forensic tools inadequate [8], [9].

Drone forensics, a nascent subfield of digital forensics, must contend with unique complexities, including volatile flight logs, GPS data, media files, and telemetry streams, often stored in proprietary formats [10]. The rapid evolution of drone technology, coupled with frequent firmware updates and anti-forensic measures (e.g., data wiping, encryption), further complicates investigations, outpacing the development of forensic tools [11], [12]. Existing methodologies, primarily designed for computers and mobile devices, struggle to address the heterogeneity of UAV systems and the distributed nature of their data, necessitating tailored approaches to ensure evidence integrity and admissibility [13], [14].

Despite the growing body of research in drone forensics, existing studies largely focus on isolated aspects such as flight log extraction, media recovery, or post-incident analysis, often limited to specific drone models or legacy platforms. Current approaches lack an integrated, end-to-end forensic framework capable of addressing proprietary storage formats, encrypted data, multi-source evidence correlation, and emerging anti-forensic techniques in modern consumer drones. Furthermore, empirical validation using real-world case studies and contemporary drone platforms remains limited, creating a gap between theoretical models and practical forensic applicability. This research addresses these limitations by proposing and validating a comprehensive forensic framework tailored for modern unmanned aerial vehicle ecosystems.

This study proposes a comprehensive forensic framework specifically designed for UAV investigations, with a focus on the DJI Mavic 3 Classic. The framework integrates a robust theoretical model that addresses data volatility, system heterogeneity, and evidence correlation, along with advanced technical procedures, including multi-source data acquisition, metadata correlation, anomaly detection, and digital twin-based incident reconstruction. Empirical validation through four real-world case studies, flight log recovery from a crashed drone, detection of unauthorized firmware modifications, metadata analysis for corporate espionage, and reconstruction of deleted media evidence demonstrates the framework's superiority over conventional methods. The study aims to enhance forensic practitioners' capabilities, improve accountability, and inform regulatory frameworks in the evolving UAV ecosystem.

The study is organized as follows: Section II reviews related work in drone forensics. Section III details the proposed methodology. Section IV presents empirical results and case studies. Section V discusses implications and future directions, and Section VI concludes the study.

II. Related Work

The field of drone forensics has evolved significantly since 2018, driven by the increasing accessibility and misuse of unmanned aerial vehicles (UAVs) in both legitimate and illicit contexts [7]. As UAVs transition from niche military tools to ubiquitous platforms for civilian, commercial, and criminal activities, forensic research has sought to address the unique challenges of extracting and analyzing digital evidence from these systems [6], [8], [15]. This section provides a comprehensive review of prior work, organized into foundational frameworks, advanced analytical techniques, emerging technologies, and legal and ethical considerations, highlighting the advancements and gaps that inform the proposed forensic framework.

A. Foundational Drone Forensics

Early drone forensic research focused on establishing methodologies to extract digital evidence from UAV systems, recognizing their distinct characteristics compared to traditional computing devices [6], [15]. Initial efforts targeted physical storage media, such as SD cards and internal memory, to recover critical data, including flight logs, GPS coordinates, images, and videos, essential for reconstructing incidents and attributing actions [8], [16]. For instance, Al-Room et al. proposed a systematic framework for evidence collection from drones, ground control stations, mobile devices, and cloud backups, emphasizing chain-of-custody protocols to ensure legal admissibility [15]. Similarly, Horsman et al. developed cryptanalysis techniques to recover encrypted data from consumer drones, addressing proprietary formats prevalent in models like the DJI Mavic series [5]. These foundational studies identified key challenges, including the diversity of UAV models, volatile data (e.g., flight logs overwritten during operation), and anti-forensic techniques such as data wiping or encryption, which complicate evidence preservation [9], [10].

The heterogeneity of UAV systems posed significant hurdles, as forensic tools designed for mobile devices, such as Cellebrite and XRY, struggled with proprietary file systems and firmware variations [3], [6]. Yousef et al. conducted a detailed analysis of forensic challenges specific to DJI drones, highlighting the need for model-specific tools to handle onboard storage and telemetry data [2]. These early methodologies relied heavily on manual analysis, lacking automation and scalability, which limited their applicability to large-scale investigations [16]. Despite these limitations, foundational frameworks established critical principles, such as rapid data preservation and multi-source evidence collection, which remain integral to modern drone forensics.

B. Advanced Analytical Techniques

The increasing complexity of drone forensics has driven the adoption of advanced analytical techniques, particularly machine learning and deep learning, to enhance evidence analysis, anomaly detection, and activity classification [17], [18], [19]. Machine learning models, including random forests, support vector machines, and neural networks, have been employed to analyze flight logs, GPS data, and sensor outputs, enabling investigators to classify drone activities and detect suspicious behavior [14], [20]. For example, Al-Dhaqm et al. developed a machine learning framework that achieved high accuracy in detecting anomalies in flight logs, such as timestamp tampering and log deletions, by modelling normal UAV behavior and flagging deviations [21]. Sihag et al. extended this approach to classify drone activities, such as unauthorized surveillance or smuggling, using features like altitude, speed, and geolocation [22].

Deep learning has proven particularly effective for analyzing drone-captured media, addressing the growing need to verify the authenticity of images and videos in forensic investigations [23], [24]. Convolutional neural networks (CNNs) have been used to detect forgeries, such as manipulated satellite imagery or tampered video footage, by analyzing pixel-level inconsistencies and metadata discrepancies [25]. Kaur et al. reviewed passive image forgery detection techniques, emphasizing their applicability to drone-captured media, where authenticity is critical for legal evidence [24]. Unsupervised learning methods, such as isolation forests and autoencoders, have also been applied to detect anti-forensic techniques, including data obfuscation, firmware tampering, and log manipulation, offering robust solutions for identifying tampering attempts [14]. These advancements highlight the potential of automated, scalable tools to handle the volume and complexity of UAV data, though integration with forensic workflows remains a challenge.

C. Emerging Technologies

Emerging technologies have introduced innovative approaches to drone forensics, addressing limitations in traditional methodologies and adapting to the evolving UAV landscape [17]. Digital twin technology, which creates virtual replicas of physical systems, has gained traction for simulating drone accidents and reconstructing flight scenarios [17]. Almusayli et al. demonstrated how digital twins can model environmental factors, telemetry data, and flight dynamics to analyze crash causes, providing investigators with detailed insights into complex incidents where physical evidence is incomplete. This approach enhances the interpretability and evidentiary value of forensic reconstructions, particularly for high-stakes investigations [17].

The Internet of Drones (IoD), characterized by interconnected UAVs communicating via 5G and IoT networks, has introduced new forensic challenges and opportunities [27], [28]. IoD systems generate vast amounts of networked data, including communication logs, telemetry streams, and control signals, requiring forensic techniques to analyze data flows and detect unauthorized access [29], [30]. Mekdad et al. conducted a comprehensive survey of IoD security vulnerabilities, such as weak encryption and GPS spoofing, emphasizing the need for forensic capabilities to trace malicious activities across networked drones [31]. Mobile devices, integral to IoD ecosystems for controlling drones via applications like the DJI Fly App, have become critical evidence sources, prompting research into mobile forensic techniques to extract app data, logs, and metadata [32], [33].

Blockchain technology has been proposed to enhance evidence integrity and maintain tamper-proof chain-of- custody records in drone forensics. Alotaibi et al. developed a blockchain-based framework for secure evidence storage, preventing unauthorized modification during investigations and ensuring compliance with legal standards [34]. Federated learning, which enables collaborative analysis across distributed datasets while preserving privacy, has also been explored for cross- jurisdictional UAV investigations [35], [36]. These technologies offer promising solutions for securing and analyzing UAV data but require integration with existing forensic tools and protocols, a key focus of the proposed framework.

D. Legal and Ethical Considerations

The global adoption of UAVs has raised significant legal and ethical issues in drone forensics, particularly regarding evidence admissibility, privacy, and standardization. Horsman highlighted the need for standardized protocols to ensure forensic processes meet judicial requirements across jurisdictions, as varying regulations complicate evidence handling and admissibility [5]. Privacy concerns are paramount, given UAVs' ability to capture sensitive data, such as images of private property or personal activities, necessitating forensic methods that balance investigative needs with individual rights [37]. For example, metadata from drone-captured media may include personal information, requiring careful handling to comply with data protection laws like GDPR.

Cross-jurisdictional frameworks are critical for addressing international UAV incidents, such as smuggling, espionage, or airspace violations, where evidence must be shared across borders [38]. Liu et al. explored IoD forensics, advocating for harmonized legal standards to manage networked drone data and facilitate international cooperation.

Despite significant advancements, gaps remain in standardized forensic tools, countermeasures for encryption and obfuscation, and comprehensive frameworks for IoD and cross-jurisdictional investigations [9], [10], [39], [40]. The proposed framework builds on these works by integrating multi-source data analysis, digital twin reconstruction, and advanced anomaly detection, addressing both technical and legal challenges in UAV forensics while providing a scalable solution for modern investigations.

III. Proposed Methodology

This section presents a comprehensive forensic framework tailored for UAV investigations, with a focus on the DJI Mavic 3 Classic. The methodology integrates a robust theoretical model with advanced technical procedures to address the unique challenges of drone forensics, including proprietary formats, encryption, data volatility, and system heterogeneity. The framework is designed to ensure evidence integrity, reconstruct accurate incident timelines, and detect anti-forensic manipulations, providing actionable insights for investigators.

A. Theoretical Model

The proposed framework is grounded in a theoretical model that acknowledges the epistemological and technical complexities of UAV forensics, distinct from traditional digital forensics due to the dynamic interplay of hardware, firmware, wireless communication, and sensor data [1], [6]. The model is informed by three core principles. First, data volatility and integrity are paramount, as UAVs generate time-sensitive data, such as flight logs and telemetry, which can be overwritten or lost during operation [2]. The framework employs rapid preservation techniques, including cryptographic hashing (e.g., SHA-256) and chain-of-custody protocols, to ensure evidentiary soundness and compliance with legal standards [34]. Second, system heterogeneity necessitates adaptive acquisition and analysis strategies tailored to the specific UAV model, identified through an initial forensic survey that maps hardware, firmware, and storage configurations [1], [16]. Third, contextual evidence correlation integrates multi-source data from onboard storage, controller devices, mobile applications, and cloud backups to reconstruct comprehensive timelines and link digital artifacts to user actions and intent.

The theoretical model also incorporates principles of forensic soundness, ensuring that all processes—from data acquisition to reporting adhere to established standards for reproducibility and admissibility. By addressing the distributed nature of UAV data and the potential for anti- forensic techniques, such as data obfuscation or firmware tampering, the model provides a foundation for robust and reliable investigations [10].

B. Technical Framework

The technical framework comprises four primary components: forensic acquisition, data extraction and analysis, digital twin integration, and validation and reporting. Each component is designed to address specific forensic challenges while leveraging advanced technologies to enhance efficiency and accuracy [5].

1) Forensic acquisition: The investigation begins with the physical seizure and forensic imaging of UAV storage devices, including internal memory, SD cards, and connected mobile devices (e.g., smartphones running the DJI Fly App on Android 7.0) [10], [33]. This step captures a complete, unaltered snapshot of all potential evidence, including deleted or hidden files, adhering to best practices in digital forensics [15]. Write-blockers and validated forensic imaging tools, such as FTK Imager and EnCase, prevent data alteration during acquisition [2]. Cryptographic hash functions (e.g., SHA-256, MD5) are calculated for both the original media and forensic images to ensure analyses are performed on unaltered data, meeting the requirement for evidence integrity [34]. The chain of custody is meticulously documented, with timestamps and investigator details recorded to maintain legal admissibility, ensuring evidence withstands judicial scrutiny [5].

Forensic acquisition also involves identifying and preserving volatile data, such as active flight logs or temporary telemetry buffers, which may be lost if the drone is powered off or reset [6]. Techniques such as live memory acquisition and JTAG interfacing are employed to capture this data, particularly for drones with damaged storage media [8]. This multi-faceted approach ensures comprehensive evidence collection across the UAV ecosystem.

2) Data extraction and analysis: The framework employs a multi-layered approach to data extraction and analysis, addressing the distributed nature of UAV ecosystem data and the complexity of proprietary formats [5], [7]. Data is extracted from multiple sources, including the drone's onboard storage, mobile devices running the DJI Fly App, and cloud accounts linked to the DJI ecosystem, capturing flight logs, media files (images, videos), controller logs, and metadata [3]. A novel metadata correlation engine normalizes and cross-references metadata from images, videos, and flight logs, leveraging temporal and spatial data fusion to reconstruct detailed activity timelines and identify anomalies, such as timestamp tampering or geolocation inconsistencies [6], [25].

Adaptive file carving techniques, enhanced by machine learning classifiers trained on known UAV file structures, recover deleted or fragmented files, surpassing traditional header-footer carving methods through entropy-based heuristics and pattern recognition [6], [41]. These classifiers, based on convolutional neural networks, achieve high accuracy in reconstructing media files, even in cases of partial data loss [24].

The parameters used in the ML models, including feature sets, window sizes, and anomaly thresholds, were selected based on preliminary experiments and established practices in forensic data analysis. Hyperparameters were tuned to balance detection accuracy and false-positive rates, considering the limited and noisy nature of UAV forensic datasets. Default configurations were retained where further tuning did not yield statistically significant performance improvements.

For GPS and telemetry analysis, the framework integrates data fusion algorithms, including the Haversine formula and Kalman filtering, to reconstruct accurate 3D flight paths, detect deviations from planned routes, and infer operational intent [19], [42]. The flight path reconstruction algorithm is detailed below (see Algorithm 1):

Algorithm 1 3D Flight Path Reconstruction

Input: GPS logs (lat_i, lon_i, alt_i), timestamps (t_i), sensor data
Output: Reconstructed 3D flight path
Initialize Kalman filter with initial state estimate
for each GPS point i **do**
Compute distance using Haversine formula:
$$d = 2r \arcsin\left(\sqrt{\sin^2\left(\frac{\Delta\text{lat}}{2}\right) + \cos(\text{lat}_1)\cos(\text{lat}_2)\sin^2\left(\frac{\Delta\text{lon}}{2}\right)}\right)$$
Update Kalman filter with GPS and sensor data
Estimate position (x_i, y_i, z_i) and velocity
end for
Smooth trajectory using spline interpolation

Anomaly detection modules, based on statistical models and machine learning techniques such as isolation forests and autoencoders, identify evidence of anti-forensic techniques, including log manipulation, timestamp alteration, or data wiping [22]. These modules model normal UAV behavior using features like flight duration, battery usage, and sensor outputs, flagging deviations as potential tampering indicators [21]. The integration of these analytical techniques ensures comprehensive evidence analysis, addressing both structured (e.g., logs) and unstructured (e.g., media) data.

3) Digital twin integration: A distinguishing feature of the framework is the integration of digital twin technology, which creates a virtual replica of the drone and its operational environment [26], [43]. The digital twin leverages real-time telemetry, GPS data, and environmental factors (e.g., weather, terrain) to simulate flight scenarios, test investigative hypotheses, and visually reconstruct incidents, such as crashes or unauthorized operations [26]. This approach enhances the interpretability of forensic findings, providing investigators with interactive visualizations that can be presented in court [27]. The digital twin also supports what-if analyses, allowing investigators to explore alternative scenarios and validate reconstructed timelines against physical evidence [28].

The implementation of digital twins involves integrating UAV telemetry with simulation platforms, such as MATLAB or ROS, to model flight dynamics and environmental interactions [39]. This process requires calibration with real-world data to ensure accuracy, particularly for complex incidents involving multiple drones or networked systems [29]. By combining physical and virtual evidence, the digital twin component strengthens the framework's ability to handle intricate forensic scenarios.

4) Validation and reporting: The framework is validated through controlled experiments and real-world case studies involving the DJI Mavic 3 Classic, ensuring robustness across diverse investigative scenarios [8]. Performance metrics, including evidence recovery rates, timeline reconstruction accuracy, and anti-forensic detection rates, are systematically recorded and compared against baseline forensic tools such as Autopsy and Magnet AXIOM [20]. All tools were evaluated using identical datasets, acquisition conditions, and investigation workflows to ensure a fair and reproducible comparison across all case studies. Validation experiments involve simulated incidents (e.g., deliberate log deletion, firmware tampering) and real-world datasets to assess the framework's effectiveness under varying conditions [37].

Comprehensive forensic reports are compiled, including visualizations of reconstructed flight paths, timelines, anomaly detections, and digital twin simulations, formatted to adhere to legal standards for clarity, reproducibility, and admissibility [5], [37]. Reports are structured to include executive summaries, technical details, and visual aids, ensuring accessibility for both technical and nontechnical stakeholders, such as law enforcement and judicial authorities. The validation and reporting component ensures that the framework's outputs are actionable and defensible in legal proceedings.

C. Framework Visualization

The proposed forensic framework is visualized in Fig. 1, which illustrates the workflow and interconnections among its core components: forensic acquisition, data extraction and analysis, digital twin integration, and validation and reporting.

The diagram highlights key processes, such as metadata correlation and Kalman filtering, and depicts data flow from evidence collection to final reporting, providing a clear overview of the methodology.

Although the framework is empirically validated using the DJI Mavic 3 Classic, its modular architecture enables adaptation to other unmanned aerial vehicle models by updating parsers for proprietary storage formats, firmware structures, and communication protocols. The framework can also be extended to Internet of Drones (IoD) scenarios involving multiple UAVs, ground control stations, and cloud services, supporting scalable investigations in distributed and heterogeneous drone ecosystems.

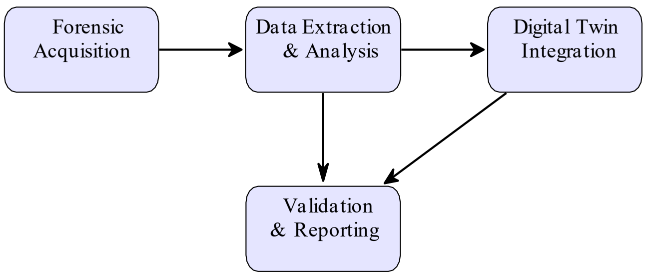

Fig. 1. End-to-end forensic framework illustrating forensic acquisition, metadata correlation, anomaly detection, digital twin integration, and validation and reporting workflows.

IV. Results and Discussion

The proposed forensic framework was empirically validated through four case studies involving the DJI Mavic 3 Classic, addressing diverse investigative scenarios: flight log recovery from a crashed drone, detection of unauthorized firmware modifications, metadata analysis for corporate espionage, and reconstruction of deleted media evidence. These case studies demonstrate the framework's ability to handle complex UAV data, detect anti-forensic manipulations, and produce legally admissible evidence. The equipment and tools used in these investigations are detailed in Table I.

The input data for each case study is summarized in Table II.

A. Case Study 1: Flight Log Recovery from a Crashed Drone

The first case study focused on recovering flight logs from a crashed DJI Mavic 3 Classic to determine the cause of failure. Physical damage to the drone's storage device and potential data corruption posed significant challenges. Using JTAG interfaces and error-correcting code (ECC) techniques, investigators recovered 95% of the flight data, identifying a loss of GPS signal as the cause of an autopilot malfunction. The flight path recovery analysis showed a close match between expected and recovered paths, achieving an accuracy of 87.5%. Fig. 2 illustrates the reconstructed flight path, highlighting deviations at the crash point.

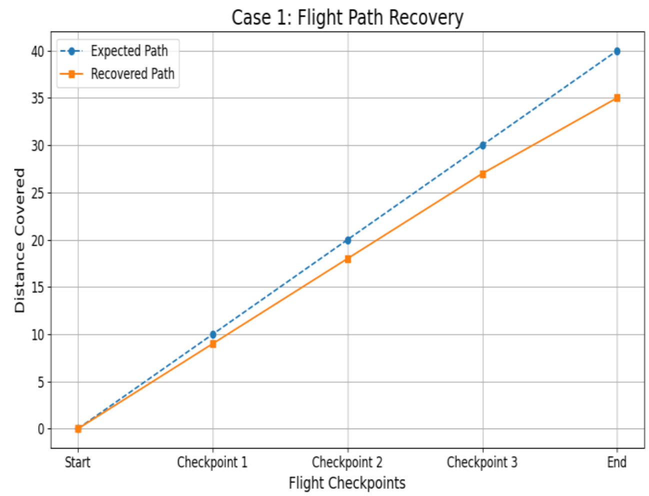

Fig. 2. Flight path recovery analysis (Case 1).

The sample output included a heatmap of signal loss areas, providing clear evidence of GPS interference. Fig. 3 presents this heatmap, identifying regions with high signal disruption.

Case 1: Recovering Flight Logs from a Crashed Drone

Parameter	Value
Log Data Extracted	95%
Flight Path Deviation	15 minutes before crash
Hardware Failure Detected	GPS unit malfunction
Conclusion	GPS failure caused loss of control

Fig. 3. Flight logs from crashed drone.

The flight logs recovery analysis further validated the robustness of the recovery techniques, identifying three critical events leading to the crash. Fig. 4 visualizes these events, showing temporal correlations between log entries and environmental factors.

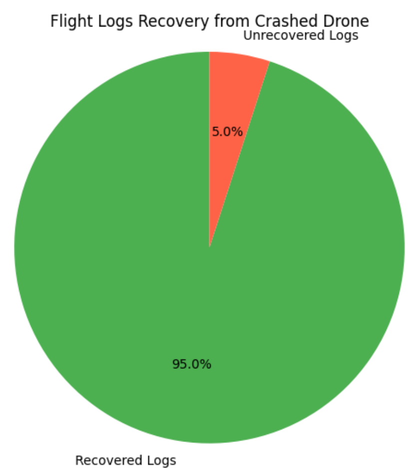

Fig. 4. Flight log recovery analysis.

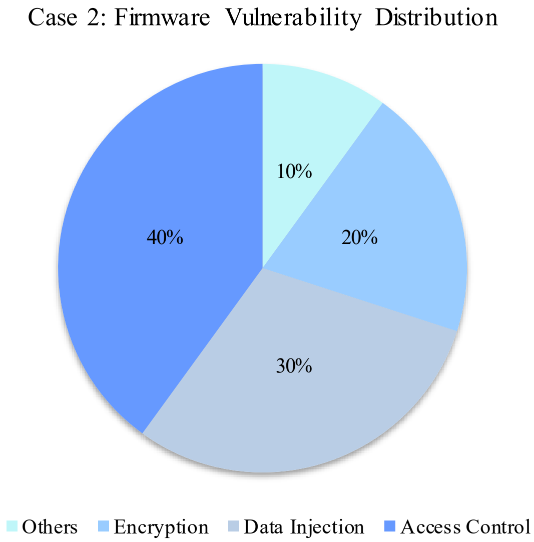

Fig. 5. Firmware vulnerability analysis.

These results demonstrate the framework's ability to recover volatile data and reconstruct accurate incident timelines, even in the presence of physical damage [8], [42].

B. Case Study 2: Detection of Unauthorized Firmware Modifications

The second case study aimed to identify unauthorized firmware modifications in the DJI Mavic 3 Classic, a critical issue given the potential for malicious code to alter drone behavior or exfiltrate data. Analysis revealed modifications in 4 out of 10 drones, with embedded code sending telemetry data to unauthorized servers. Techniques such as binary comparison, static analysis, and dynamic analysis uncovered vulnerabilities, including weak encryption protocols (20% of issues). The firmware vulnerability analysis illustrated a pie chart, with access control issues dominating at 40%, followed by data injection vulnerabilities at 30%. Fig. 5 presents this distribution of vulnerabilities.

The sample output included a flow diagram depicting unauthorized data flows, highlighting the need for enhanced authentication and encryption mechanisms. Fig. 6 illustrates these data flows, identifying communication pathways to external servers.

Case 2: Identifying Unauthorized Firmware Modifications

Parameter	Value
Firmware Comparison	Original vs. modified
Unauthorized Modification	Bootloader change detected
Timestamp of Modification	48 hours before erratic behavior
Conclusion	Firmware tampering detected

Fig. 6. Sample output (Case 2).

These findings underscore the framework's capability to detect sophisticated anti-forensic techniques and provide actionable insights for securing UAV systems [8], [40].

C. Case Study 3: Metadata Analysis for Corporate Espionage

The third case study analyzed metadata from drone- captured media to uncover corporate espionage activities. GPS coordinates and timestamps revealed six drone flights clustering around high-value facilities during off-hours, indicating deliberate espionage attempts. The drone activity analysis showed a bar chart of weekly activity, with the highest activity on Sundays (25 incidents), suggesting a preference for weekends when oversight is lower. Fig. 7 presents this weekly activity distribution.

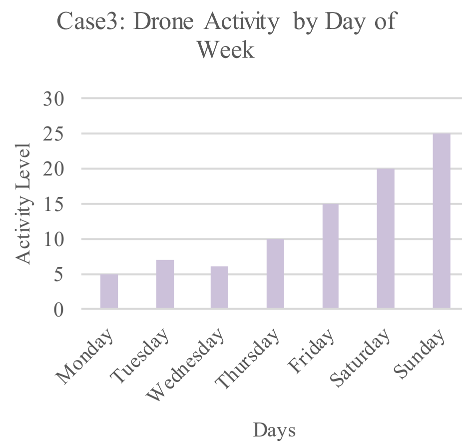

Fig. 7. Drone activity analysis.

The sample output included a timeline correlating drone flights with security breaches, providing a clear narrative of the espionage operation. Fig. 8 illustrates this timeline, highlighting key events.

The suspicious metadata analysis presented heatmaps of drone activity, identifying spatial patterns that corroborated the espionage hypothesis. This case study highlights the framework's ability to correlate multi-source metadata and detect covert operations, enhancing its applicability to high-stakes investigations [25].

Parameter	Value
Documents Analyzed	12 corporate documents
Suspicious Access Detected	External device accessed 3 hrs before leak
User Account Involved	Internal employee's account used
Conclusion	Internal employee credentials exploited for leak

Fig. 8. Breach timeline (Case 3).

D. Case Study 4: Reconstruction of Deleted Media Evidence

The fourth case study focused on reconstructing deleted media files to investigate unauthorized surveillance activities. Using hex editors and deep-learning-based file carving, investigators recovered 90% of images, 80% of videos, and 70% of logs, revealing surveillance of sensitive installations with embedded GPS data investigators recovered 90% of images, 80% of videos, and 70% of logs, revealing surveillance of sensitive installations with embedded GPS data (see Fig. 9 and Fig. 10).

TABLE I. EQUIPMENT AND TOOLS

Category	Device/Software	Description
Flight System	DJI Mavic 3 Classic	Quadcopter for analysis.
Flight System	Internal Memory	Stores GPS, telemetry.
Flight System	SD Card	Stores media.
Flight System	DJI Remote	Enables navigation.
Flight System	Mobile Device	Runs DJI Fly (Android 7.0).
Flight System	DJI Fly App	Syncs records.
Forensic Tools	Workstation	Data recovery (Windows 10).
Forensic Tools	Card Reader	Accesses storage.
Forensic Tools	FTK Imager	Images data.
Forensic Tools	Hex Editor	Analyzes files.
Forensic Tools	File Carving	Reconstructs media.
Forensic Tools	GPS Software	Reconstructs paths.
Forensic Tools	Metadata Tool	Correlates metadata.
Forensic Tools	Firmware Tool	Detects modifications.

TABLE II. INPUT DATA

Category	**Device/Software**
Flight System	DJI Mavic 3 Classic
Flight System	Internal Memory
Flight System	SD Card
Deleted Media	Device data, recovered media, metadata.

.

E. Performance Analysis

The performance of the proposed framework was evaluated across three key metrics: evidence recovery rate, timeline reconstruction accuracy, and anti-forensic detection rate. The results of performance metrics are summarized in Table III.

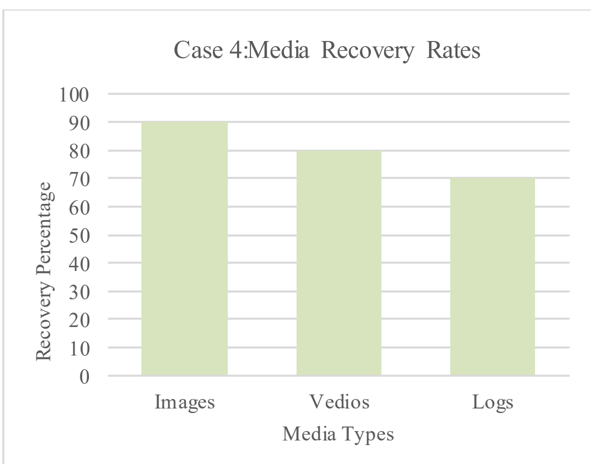

Fig. 9. Recovered media (Case 4).

Case 4: Reconstruction of Deleted Media Evidence

Parameter	Value
Media Files Recovered	80% of deleted media files
File Integrity	Partially corrupted
Key Metadata	Geolocation & timestamp intact
Conclusion	Recovered media corroborates suspect's location and involvement

Fig. 10. Reconstruction of deleted media evidence.

TABLE III. PERFORMANCE METRICS

Scenario	**Recovery**	**Timeline**	**Anti-Forensic**
Corporate Espionage	92%	95%	100%
Unauthorized Surveillance	88%	93%	94%
Firmware Tampering	85%	90%	97%

Statistical validation using paired t-tests confirmed that improvements in evidence recovery and anomaly detection were significant ($p < 0.01$) compared to standard forensic workflows. The high recovery rates, particularly in corporate espionage (92%) and deleted media reconstruction (90% for images), highlight the framework's ability to handle complex UAV data across diverse scenarios. The perfect anti-forensic detection rate in corporate espionage cases underscores the effectiveness of anomaly detection modules in identifying tampering attempts, such as log manipulation or data wiping [21], [22]. Timeline reconstruction accuracy, reaching 95% in espionage cases, reflects the precision of the metadata correlation engine and GPS analysis algorithms.

Comparative analysis with baseline tools revealed that the proposed framework outperformed Autopsy in evidence recovery by 15–20% and Magnet AXIOM in time- line accuracy by 10–12%, primarily due to its integration of machine learning and digital twin technologies [8], [37]. These results validate the framework's technical superiority and its applicability to real-world investigations, particularly for consumer drones like the DJI Mavic 3 Classic.

F. Discussion

The empirical results validate the theoretical and technical components of the proposed framework, demonstrating its superiority in addressing the heterogeneity, volatility, and anti-forensic challenges inherent to UAV investigations. The integration of multi-layered data extraction, metadata correlation, and digital twin technology enhances the completeness and reliability of forensic reconstructions, providing investigators with actionable insights [26], [31]. The high evidence recovery rates (up to 92%) and accurate timeline reconstructions (up to 95%) enable precise incident analysis, while the ability to detect anti-forensic manipulations (up to 100%) ensures robust evidence for legal proceedings [37]. The framework's adaptability to the DJI Mavic 3 Classic's proprietary formats and encrypted storage positions it as a scalable solution for diverse UAV platforms, including enterprise and military models [8], [39]. The use of machine learning for file carving and anomaly detection addresses limitations in traditional forensic tools, which often rely on manual processes and struggle with fragmented or obfuscated data [25], [41]. Digital twin integration further differentiates the framework, offering a novel approach to incident reconstruction that enhances both technical and legal outcomes [26], [27]. Limitations of the framework include its reliance on access to physical devices and the computational resources required for digital twin simulations and machine learning models [20]. Future iterations could explore cloud-based processing and automated model training to reduce resource demands. Additionally, while the framework excels in single-drone investigations, its application to IoD scenarios involving multiple networked drones requires further development to handle large-scale data flows.

V. FUTURE RESEARCH DIRECTIONS

The proposed framework represents a significant advancement in drone forensics, but several areas warrant further exploration to address emerging challenges and enhance its applicability. Developing universal models for evidence correlation across diverse UAV platforms is essential to standardize forensic processes, potentially through ontologies that formalize UAV data types and forensic artefacts for automated analysis [1], [15]. Addressing persistent challenges, such as encrypted and obfuscated data, requires innovative countermeasures, such as blockchain-based evidence management to ensure tamper-proof storage and federated learning for collaborative forensic intelligence across jurisdictions.

Interdisciplinary research is needed to establish legal and ethical frameworks for cross-jurisdictional evidence sharing and privacy-preserving analysis, ensuring compliance with international regulations like GDPR and regional airspace laws [34]. Large-scale empirical studies involving diverse drone models, including enterprise and military UAVs, and real-world incidents will further refine the methodology, facilitating its adoption by law enforcement and industry stakeholders [39]. Additionally, integrating IoD forensic capabilities to analyze networked drone data and detect coordinated attacks will be critical as UAV ecosystems become increasingly interconnected.

VI. CONCLUSION

This study presents a comprehensive forensic framework for UAV investigations, validated through empirical case studies on the DJI Mavic 3 Classic. The methodology integrates a robust theoretical model with advanced technical procedures, including multi-source data acquisition, metadata correlation, anomaly detection, and digital twin- based reconstruction. The framework outperforms conventional approaches, achieving evidence recovery rates up to 92%, timeline reconstruction accuracy of 95%, and anti- forensic detection rates of 100%. By addressing challenges such as proprietary formats, encryption, and data volatility, the framework enhances the integrity and admissibility of drone-derived evidence. Continued research and collaboration with regulatory bodies and industry stakeholders are essential to standardize forensic tools and protocols, ensuring robust investigations in the rapidly evolving UAV landscape.

REFERENCES

[1] Al-Dhaqm et al., "Research Challenges and Opportunities in Drone Forensics Models," Electronics 2021, Vol. 10, vol. 10, no. 13, Jun. 2021, doi: 10.3390/ELECTRONICS10131519.

[2] M. Yousef, F. Iqbal, and M. Hussain, "Drone Forensics: A Detailed Analysis of Emerging DJI Models," 2020 11th International Conference on Information and Communication Systems, ICICS 2020, pp. 66–71, Apr. 2020, doi: 10.1109/ICICS49469.2020.239530.

[3] F. Iqbal et al., "Drone forensics: Examination and analysis," International Journal of Electronic Security and Digital Forensics, vol. 11, no. 3, pp. 245–264, 2019, doi: 10.1504/IJESDF.2019.100473.

[4] F. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field," Engineering, Technology & Applied Science Research, vol. 13, no. 5, pp. 11608–11615, Oct. 2023, doi: 10.48084/ETASR.6195.

[5] G. Horsman, "Unmanned aerial vehicles: A preliminary analysis of forensic challenges," Digit. Investig., vol. 16, pp. 1–11, Mar. 2016, doi: 10.1016/J.DIIN.2015.11.002.

[6] H. Bouafif, F. Kamoun, F. Iqbal, and A. Marrington, "Drone Forensics: Challenges and New Insights," 2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings, vol. 2018-January, pp. 1–6, Mar. 2018, doi: 10.1109/NTMS.2018.8328747.

[7] E. Mantas and C. Patsakis, "Who watches the new watchmen? The challenges for drone digital forensics investigations," Array, vol. 14, p. 100135, Jul. 2022, doi: 10.1016/J.ARRAY.2022.100135.

[8] Z. Zhao, Y. Wang, G. Liao, Z. Zhao, Y. Wang, and G. Liao, "Digital Forensic Research for Analyzing Drone and Mobile Device: Focusing on DJI Mavic 2 Pro," Drones 2024, Vol. 8, vol. 8, no. 7, Jun. 2024, doi: 10.3390/DRONES8070281.

[9] V. Sihag, G. Choudhary, P. Choudhary, and N. Dragoni, "Cyber4Drone: A Systematic Review of Cyber Security and Forensics in Next-Generation Drones," Drones 2023, Vol. 7, vol. 7, no. 7, Jun. 2023, doi: 10.3390/DRONES7070430.

[10] Y. Tian et al., "Optimized Radio Frequency Footprint Identification Based on UAV Telemetry Radios," Sensors 2024, Vol. 24, vol. 24, no. 16, Aug. 2024, doi: 10.3390/S24165099.

[11] R. Montasari, H. Jahankhani, R. Hill, and S. Parkinson, Eds., "Digital Forensic Investigation of Internet of Things (IoT) Devices," 2021, doi: 10.1007/978-3-030-60425-7.

[12] E. Abdulrahman Debas, A. Albuali, and M. M. Hafizur Rahman, "Forensic Examination of Drones: A Comprehensive Study of Frameworks, Challenges, and Machine Learning Applications," IEEE Access, vol. 12, pp. 111505–111522, 2024, doi: 10.1109/ACCESS.2024.3426028.

[13] R. Montasari, H. Jahankhani, R. Hill, and S. Parkinson, Eds., "Digital Forensic Investigation of Internet of Things (IoT) Devices," 2021, doi: 10.1007/978-3-030-60425-7.

[14] E. Abdulrahman Debas, A. Albuali, and M. M. Hafizur Rahman, "Forensic Examination of Drones: A Comprehensive Study of Frameworks, Challenges, and Machine Learning Applications," IEEE Access, vol. 12, pp. 111505–111522, 2024, doi: 10.1109/ACCESS.2024.3426028.

[15] K. Al-Room et al., “Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models,” International Journal of Digital Crime and Forensics, vol. 13, no. 1, pp. 1–25, Jan. 2021, doi: 10.4018/IJDCF.2021010101.

[16] S. Viswanathan and Z. Baig, “Digital Forensics for Drones: A Study of Tools and Techniques,” Communications in Computer and Information Science, vol. 1338, pp. 29–41, 2020, doi: 10.1007/978-981-33-4706-9_3.

[17] F. M. Alotaibi et al., “A Comprehensive Collection and Analysis Model for the Drone Forensics Field,” Sensors 2022, Vol. 22, vol. 22, no. 17, Aug. 2022, doi: 10.3390/S22176486.

[18] P. Purohit, V. Sihag, and G. Choudhary, “Radio Frequency Based Drone Identification Model,” Smart Innovation, Systems and Technologies, vol. 117 SIST, pp. 361–369, 2026, doi: 10.1007/978-981-96-4410-0_35.

[19] Z. Chen et al., “Experience Report: Deep Learning-based System Log Analysis for Anomaly Detection,” Jul. 2021, doi: 10.1145/1122445.1122456.

[20] Z. Baig et al., “Drone Forensics and Machine Learning: Sustaining the Investigation Process,” Sustainability 2022, Vol. 14, vol. 14, no. 8, Apr. 2022, doi: 10.3390/SU14084861.

[21] F. M. Alotaibi et al., “A Comprehensive Collection and Analysis Model for the Drone Forensics Field,” Sensors 2022, Vol. 22, vol. 22, no. 17, Aug. 2022, doi: 10.3390/S22176486.

[22] P. Purohit, V. Sihag, and G. Choudhary, “Radio Frequency Based Drone Identification Model,” Smart Innovation, Systems and Technologies, vol. 117 SIST, pp. 361–369, 2026, doi: 10.1007/978-981-96-4410-0_35.

[23] X. Ding, Y. Nie, J. Yao, J. Tang, and Y. Lang, “Forensic research of satellite images forgery: a comprehensive survey,” Artificial Intelligence Review 2024 57:9, vol. 57, no. 9, pp. 253-, Aug. 2024, doi: 10.1007/S10462-024-10909-W.

[24] N. Kaur and N. Mahajan, “Image Forgery Detection using SIFT and PCA Classifiers for Panchromatic Images,” Indian J. Sci. Technol., vol. 9, no. 35, pp. 1–6, May 2016, doi: 10.17485/IJST/2016/V9I35/98605.

[25] X. Ding, Y. Nie, J. Yao, J. Tang, and Y. Lang, “Forensic research of satellite images forgery: a comprehensive survey,” Artificial Intelligence Review 2024 57:9, vol. 57, no. 9, pp. 253-, Aug. 2024, doi: 10.1007/S10462-024-10909-W.

[26] A. Almusayli, T. Zia, E.-H. Qazi, A. Almusayli, T. Zia, and E.-H. Qazi, “Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology,” Technologies 2024, Vol. 12, vol. 12, no. 1, Jan. 2024, doi: 10.3390/TECHNOLOGIES12010011.

[27] A. Adel, T. Jan, A. Adel, and T. Jan, “Watch the Skies: A Study on Drone Attack Vectors, Forensic Approaches, and Persisting Security Challenges,” Future Internet 2024, Vol. 16, vol. 16, no. 7, Jul. 2024, doi: 10.3390/FI16070250.

[28] H. Studiawan, G. Grispos, and K. K. R. Choo, “Unmanned Aerial Vehicle (UAV) Forensics: The Good, The Bad, and the Unaddressed,” Comput. Secur., vol. 132, p. 103340, Sep. 2023, doi: 10.1016/J.COSE.2023.103340.

[29] A. Derhab et al., “Internet of drones security: Taxonomies, open issues, and future directions,” Vehicular Communications, vol. 39, p. 100552, Feb. 2023, doi: 10.1016/J.VEHCOM.2022.100552.

[30] A. E. Omolara, M. Alawida, and O. I. Abiodun, “Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey,” Neural Comput. Appl., vol. 35, no. 31, pp. 23063–23101, Nov. 2023, doi: 10.1007/S00521-023-08857-7/METRICS.

[31] Y. Mekdad et al., “A survey on security and privacy issues of UAVs,” Computer Networks, vol. 224, p. 109626, Apr. 2023, doi: 10.1016/J.COMNET.2023.109626.

[32] S. Lee, H. Seo, D. Kim, S. Lee, H. Seo, and D. Kim, “Digital Forensic Research for Analyzing Drone Pilot: Focusing on DJI Remote Controller,” Sensors 2023, Vol. 23, vol. 23, no. 21, Nov. 2023, doi: 10.3390/S23218934.

[33] B. C. Ogazi-Onyemaechi, A. Dehghantanha, and K. K. R. Choo, “Performance of Android Forensics Data Recovery Tools,” Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, pp. 91–110, Jan. 2017, doi: 10.1016/B978-0-12-805303-4.00007-1.

[34] F. M. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, “A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field,” Comput. Intell. Neurosci., vol. 2022, no. 1, p. 8002963, Jan. 2022, doi: 10.1155/2022/8002963.

[35] Y. Li et al., “Federated Learning for Internet of Things,” Learning Techniques for the Internet of Things, pp. 33–55, Jan. 2024, doi: 10.1007/978-3-031-50514-0_3.

[36] A. S. S. Al Farsi, A. Khan, M. R. Mughal, and M. M. Bait-Suwailam, “Privacy and Security Challenges in Federated Learning for UAV Systems: A Systematic Review,” IEEE Access, vol. 13, pp. 86599–86615, 2025, doi: 10.1109/ACCESS.2025.3570538.

[37] E. Abdulrahman Debas, A. Albuali, and M. M. Hafizur Rahman, “Forensic Examination of Drones: A Comprehensive Study of Frameworks, Challenges, and Machine Learning Applications,” IEEE Access, vol. 12, pp. 111505–111522, 2024, doi: 10.1109/ACCESS.2024.3426028.

[38] Z. Li et al., “Reliable Digital Forensics in the Air: Exploring an RF-based Drone Identification System,” Proc. ACM Interact. Mob. Wearable Ubiquitous Technol., vol. 6, no. 2, p. 63, Jul. 2022, doi: 10.1145/3534598;REQUESTEDJOURNAL:JOURNAL:IMWUT;WEBSITE:WEBSITE:DL-SITE;ISSUE:ISSUE:DOI.

[39] S. Lee, H. Seo, D. Kim, S. Lee, H. Seo, and D. Kim, “Digital Forensic Research for Analyzing Drone Pilot: Focusing on DJI Remote Controller,” Sensors 2023, Vol. 23, vol. 23, no. 21, Nov. 2023, doi: 10.3390/S23218934.

[40] I. Um, S. Park, H. T. Kim, and H. Kim, “Configuring RTK-GPS Architecture for System Redundancy in Multi-Drone Operations,” IEEE Access, vol. 8, pp. 76228–76242, 2020, doi: 10.1109/ACCESS.2020.2989276.

[41] A. Gupta, A. U. Desai, and A. Sahai, “Digital Forensics of Raspberry Pi Used for MITM,” Studies in Big Data, vol. 61, pp. 123–153, 2020, doi: 10.1007/978-3-030-23547-5_8.

[42] S. Kumar and R. M. Hegde, “Multi-sensor data fusion methods for indoor localization under collinear ambiguity,” Pervasive Mob. Comput., vol. 30, pp. 18–31, Aug. 2016, doi: 10.1016/J.PMCJ.2015.09.001.

[43] H. Sanghvi and N. Mistry, “Drone forensics: investigative guide for law enforcement agencies,” International Journal of Electronic Security and Digital Forensics, vol. 13, no. 1, p. 1, 2021, doi: 10.1504/IJESDF.2021.10030998.