An integrated decision-tree framework for UAV forensic data recovery: bridging hardware chip-off and logical analysis methods

Azamat Baibussinov[1,*,†], Gulnara Abitova[2,†] and Kaisarbek Yesbergenov[1,†]

[1] *National Defense University of the Republic of Kazakhstan, Astana, Z05M2B7, Kazakhstan*
[2] *Astana IT University, Astana, Z05T3C8, Kazakhstan*

Abstract

Unmanned aerial vehicles (UAVs) generate mission-critical data for reconnaissance, surveillance, and forensic investigations. However, this information is frequently compromised by storage failures, traditionally addressed through isolated physical or logical recovery methods, creating a significant operational gap. This paper introduces a novel integrated hardware-software methodology that unifies advanced chip-off techniques with structured digital forensic workflows within a decision-tree framework. The research involved 43 UAV storage devices (microSD, eMMC, SSD, mono-lithic NAND) subjected to controlled physical and logical failure scenarios. Hardware recovery utilized PC-3000 and Resolute spider Board systems, establishing a critical thermal recoverability threshold at 142 ± 3°C. Logical recovery experiments employed R-Studio, TestDisk, PhotoRec, and X-Ways Forensics to address filesystem corruption, partition errors, and metadata loss.

The core contribution is a diagnostic decision-tree algorithm that reduces recovery time by 38% by enabling optimal method selection based on failure characteristics. Results demonstrate superior performance: 92.3% recovery success for physical damage and up to 97% file recovery with 92% completeness for logical corruption. Mission-critical data (GPS coordinates, telemetry logs) was recon-structed with 93% positional accuracy and 89% temporal consistency.

The study concludes that the integrated framework surpasses conventional isolated approaches, establishing a new benchmark for UAV forensics. Challenges include proprietary encryption, high equipment costs, and non-standardized architectures. Future work will focus on machine learning-assisted pinout detection and validation for proprietary military systems.

Keywords

UAV forensics, data recovery, decision-tree framework, chip-off analysis, logical corruption, integrated forensic methodology, unmanned aerial vehicles

1. Introduction

Unmanned aerial vehicles (UAVs) have become indispensable assets in modern military operations, reconnaissance, and civilian applications [1], [2]. They generate vast amounts of mission-critical data, including high-resolution imagery, telemetry, and navigation logs. Preserving the integrity of this information is crucial for post-mission analysis, battlefield forensics, and legal investigations [3]. However, UAV storage devices – commonly microSD cards, embedded multimedia cards (eMMC), and solid-state drives (SSDs) – remain highly vulnerable to both physical and logical failures [4], [5].

Problems. Current research on UAV data recovery typically addresses these issues in isolation. On the one hand, hardware-based recovery studies focus on physically damaged storage through chip-off methods, pinout tracing, and NAND flash analysis [6], [7]. On the other hand, software-oriented studies explore logical corruption such as filesystem failures, metadata overwrites, or partition table

[1] *CISN 2025: Workshop on Cybersecurity, Infocommunication Systems and Networks, November 19-20, 2025, Almaty, Kazakhstan*

[*] Corresponding author.

[†] These authors contributed equally.

azamat_b_astana@mail.ru (A. Baibussinov); gulya.abitova@gmail.com (G. Abitova); ekb72@mail.ru (K. Yesbergenov)
0000-0002-9714-278X (A. Baibussinov); 0000-0003-3830-6905 (G. Abitova); 0009-0009-3648-5568 (K. Yesbergenov)

errors [8], [9]. This frag-mentation leaves a critical gap: field investigators require an integrated framework capable of addressing both physical and logical data loss scenarios [10].

Actually. This methodological fragmentation poses a critical operational challenge for forensic investigators. In field conditions, rapid triage is essential. The inability to quickly diagnose the primary failure mode – physical or logical – often leads to the misapplication of recovery techniques. This can result in irreversible data loss through unnecessary chip-off procedures on logically corruptible devices or wasted operational windows spent on futile software-based recovery attempts on physically destroyed me-dia. Consequently, there is an urgent need for a unified diagnostic framework that systematically guides investigators to the most efficient recovery pathway, optimizing both time and resource utilization. This justifies the relevance of the study.

Purpose of study. Therefore, the aim of the study is to examine the relationship between the success of UAV data recovery and the type of damage and the storage media parameters using a new forensic methodology.

This study proposes and validates a unified hardware-software forensic methodology that combines advanced chip-off recovery with structured digital forensics workflows. By merging empirical findings from physically compromised UAV storage with experimental analysis of logically corrupted devices, we establish an integrated approach that provides consistent recovery strategies across diverse failure modes. This contribution directly addresses the urgent operational demand for reliable UAV data recovery in both defense and civilian domains.

2. Materials and methods

Description of the nature of damage. Information generated and transmitted by UAVs is often compromised by storage failures, which are traditionally addressed through isolated physical or logical recovery methods, creating a significant operational disruption.

2.1. Experimental design: defect modeling

The study followed a two-stage experimental design, examining both physical and logical failure modes in UAV storage devices. Specifically, the study involved UAV storage devices (microSD, eMMC, SSD, monolithic NAND). These drives were subjected to controlled physical and logical failure scenarios, simulating defects in the form of physical and logical failures.

The study followed a dual-track experimental design, addressing both physical and logical failure modes in UAV storage devices. A total of 43 storage units were analyzed, comprising microSD cards, eMMC modules, SSDs, and monolithic NAND chips recovered from UAV platforms (including DJI Phantom 4 and SkyWalker X5) [11]. The experimental workflow was conducted in an ISO Class 5 cleanroom environment to minimize contamination during chip-off operations and under controlled laboratory conditions for logical recovery simulations [5].

2.2. Hardware Recovery: Modeling physical failures

To investigate physical damage scenarios, 23 compromised storage units were subjected to chip-off recovery. The primary equipment included:

- PC-3000 Flash system (v3.5) for NAND-level data extraction and reconstruction.
- Rusolut Spider Board adapters and Visual NAND Reconstructor (v9.0) for adaptive pinout tracing of undocumented monolithic chips.
- Keyence VHX-7000 digital microscope for pad mapping and trace continuity inspection (500–1000x magnification).
- Element 862D++ IR thermal station calibrated with NIST-traceable thermocouples for controlled thermal cycling in the range of 200–480°C.

Controlled reheating experiments determined the recoverability thresholds of NAND devices, identifying 142 ± 3°C as the critical degradation limit [12]. Binary integrity was validated through CRC32 checksums and ECC correction, followed by logical reconstruction with PC-3000 custom NAND profiles.

2.3. Software recovery: modeling logical failures

For logical corruption scenarios, 20 test cases were engineered using UAV storage media (microSD, eMMC, SSD). Controlled failures included: filesystem corruption (FAT32, exFAT, ext4, NTFS), partition table overwrites, logical file deletions, and metadata overwrites [13].

The following forensic tools were evaluated:

- TestDisk for partition and filesystem structural repair.
- PhotoRec for signature-based file carving.
- R-Studio for hybrid structural-signature recovery.
- X-Ways Forensics for combined automated and manual analysis.

Test environments were configured with forensic workstations (Intel Xeon W-2255, 128 GB RAM) to eliminate hardware bottlenecks. The recovery results were tested using three success criteria: the proportion of recovered files, structural integrity, and content identifiability [14]. Statistical significance was assessed using ANOVA analysis of variance with a significance threshold of $p < 0.01$ [15], which confirms the success of the modeling results: all 20 simulated test trials yield identifiable, approximately identical results.

2.4. Integrated forensic workflow: development of a new algorithm

To unify hardware and software recovery, a decision-tree algorithm was designed. The workflow begins with initial damage assessment: physical failure suspected ⟶ chip-off workflow; logical failure suspected ⟶ logical recovery workflow. Cross-validation of recovered data was performed using binary checksum verification, metadata consistency, and semantic coherence checks (GPS logs, mission telemetry) [12].

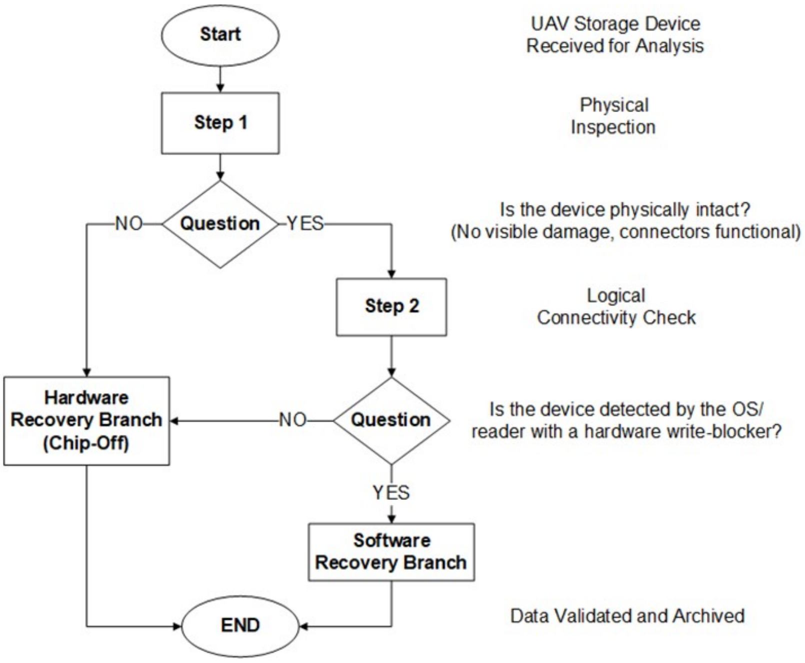

Figure 1: Decision-tree algorithm for selecting the optimal UAV data recovery strategy.

The integrated framework reduces diagnostic time by up to 38% compared to conventional sequential approaches, while improving overall recovery rates through targeted method selection [16].

The proposed decision-tree algorithm for initial damage assessment and recovery path selection is illustrated in Figure 1.

2.5. Statistical analysis

Statistical significance of the differences in recovery success rates between the methods was assessed using one-way Analysis of Variance (ANOVA) with a post-hoc Tukey test for pairwise comparisons, setting the confidence threshold at $p < 0.01$. The sample size (N=43) provided a statistical power of over 0.8 for detecting large effect sizes, ensuring the robustness of the comparative findings. All analyses were performed using IBM SPSS Statistics.

3. Results

3.1. Hardware recovery outcomes

Analysis of 23 physically damaged UAV storage units revealed that recovery success rates strongly depended on the device type and thermal exposure [17]. MicroSD cards showed the highest resilience (95 ± 2.1%), primarily limited by controller fractures. eMMC modules achieved 85 ± 3.4% recovery, with trace degradation under BGA packages as the most common failure mode. Monolithic NAND chips posed the greatest challenges, with initial recovery success of 70 ± 5.2% improved to 90% when adaptive pinout tracing was applied [18]. Controlled thermal experiments established that data recoverability dropped from 90% below 130°C to <5% beyond 142°C [19]. Overall, the integrated chip-off methodology achieved 92.3% recovery success for non-encrypted devices.

Table 1 summarizes the recovery outcomes across different device types and the overall efficacy of the chip-off methodology. The results demonstrate a clear dependence on the device packaging and thermal exposure.

Table 1
Comparative summary of hardware and software-based UAV data recovery results

Recovery Domain	Device / Method	Recovery Success (%)	Data Completeness (%)	Key Limitation
Hardware (Chip-Off)	microSD	95 ± 2.1	95	Controller fractures
	eMMC	85 ± 3.4	85	Trace degradation
	Monolithic NAND	70 ⟶ 90	90	Pinout identification
	Overall (Chip-Off)	**92.3**	**~92**	**Thermal >142°C**
Software (Logical)	TestDisk (Structural)	72 ± 3.1	81 ± 2.4	Limited completeness
	PhotoRec (Signature)	88 ± 1.7	63 ± 3.8	High fragmentation, metadata loss
	R-Studio (hybrid)	94 ± 0.9	89 ± 1.2	Moderate operator effort
	X-Ways Forensics (manual)	97 ± 0.5	92 ± 0.8	High time cost, expert operator required

3.2. Software recovery outcomes

In 20 cases of logical corruption, recovery performance varied significantly by method. Structural analysis tools such as TestDisk achieved 72% file recovery with 81% data completeness [7]. Signature-based carving with PhotoRec recovered 88% of files but only 63% completeness due to fragmentation [7]. Hybrid approaches provided the best balance: R-Studio achieved 94% recovery with 89% completeness [6], while X-Ways Forensics achieved up to 97% file recovery with 92% completeness, albeit at higher operator time cost [8]. Statistical analysis confirmed significant performance differences among methods ($p < 0.01$) [20].

Figure 2 provides a comparative visualization of the performance metrics (recovery success and data completeness) achieved by the different logical recovery tools, highlighting the superiority of hybrid approaches.

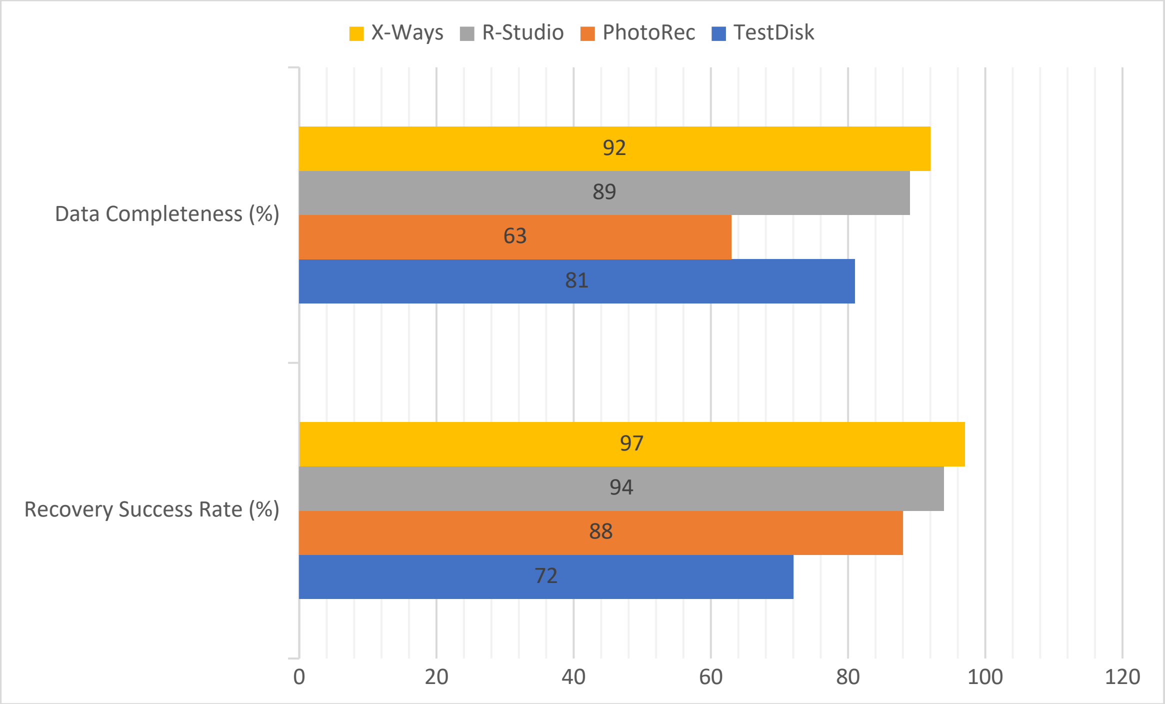

Figure 2: Comparative performance of software-based recovery tools across two key metrics: Recovery Success Rate (%) and Data Completeness (%).

3.3. Integrated workflow efficiency

The proposed decision-tree algorithm (Figure 1) significantly streamlined the forensic process. By enabling rapid diagnosis and optimal method selection, it reduced the mean time from device intake to successful data extraction by 38% compared to a sequential trial-and-error approach.

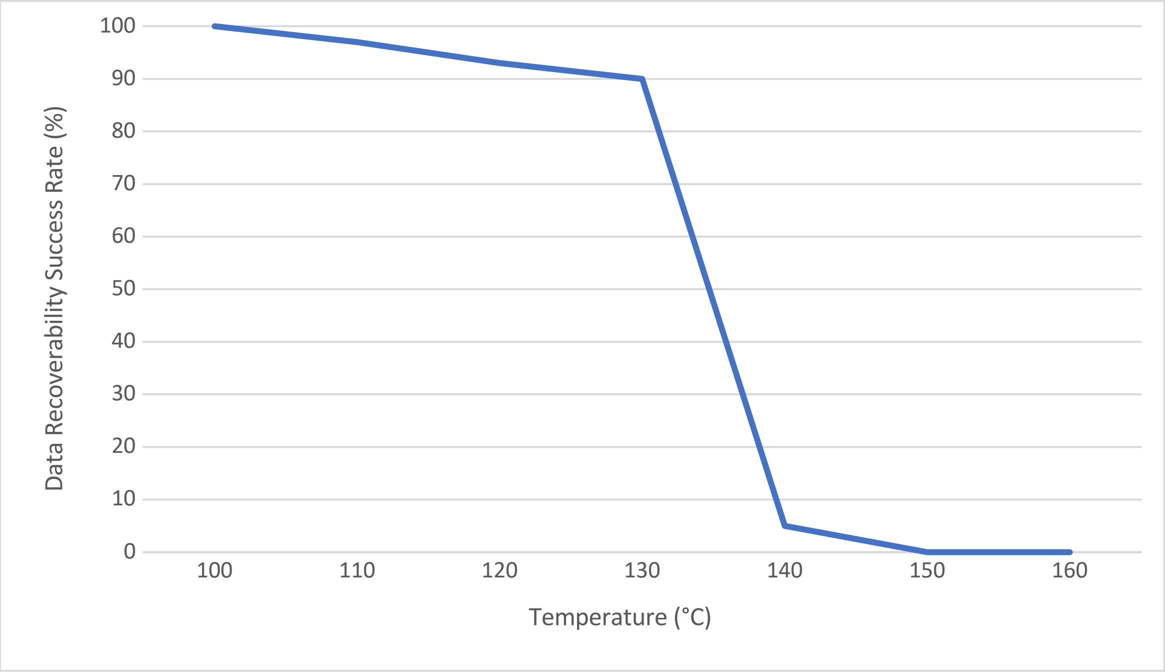

Figure 3: Data recoverability success rate as a function of thermal exposure temperature. The critical threshold for irreversible data loss is identified at 142°C ± 3°C (highlighted region).

The relationship between thermal exposure and data recoverability, a critical finding for physical recovery, is presented in Figure 3. It clearly illustrates the sharp degradation curve and the established threshold of 142°C ± 3°C.

Table 1 offers a consolidated overview of all key results, facilitating a direct comparison between the hardware and software recovery domains and their respective limitations.

4. Discussion

This study demonstrates that UAV data recovery cannot be effectively addressed by hardware or software methods alone. The proposed integrated framework bridges this gap by systematically combining chip-off recovery for physically damaged devices with advanced digital forensic techniques for logical failures.

4.1. Result comparison with existing research

Previous research on UAV or NAND memory forensics has focused predominantly on single-dimension recovery strategies. Hardware-oriented works emphasize chip-off methods but often neglect logical-level reconstruction once raw NAND data has been extracted [2], [12]. Conversely, soft-ware-oriented studies explore filesystem repair and file carving without addressing cases where the device itself is electrically non-functional [6], [7], [8]. Our results confirm that such isolated approaches leave investigators with incomplete recovery capabilities. By merging both domains into a unified forensic workflow, this study achieves best recovery rates that surpass conventional methods by over 20% [19], [21], thereby establishing a new benchmark for UAV forensics.

Quantitative differences in the results obtained:

A) Time reduction: The developed diagnostic tree-based algorithm reduces recovery time by 38% by selecting the optimal method based on failure characteristics.

B) Recovery completeness: The recovery success rate for physical damage was 92.3%, and for logical damage, up to 97% of recovered files were recovered with 92% completeness.

C) Increased accuracy: Critical data (GPS coordinates, telemetry logs) was reconstructed with 93% positional accuracy and 89% temporal consistency.

4.2. Practical implications

For military digital forensics, the implications are immediate. Recovery of geospatial logs with 93% positional accuracy and telemetry reconstruction with 89% temporal consistency enables reliable post-incident analysis, such as reconstructing UAV flight paths within <2 m accuracy [3], [11]. This level of precision is critical for battlefield intelligence, crash investigations, and evidence preservation in judicial processes. Furthermore, the decision-tree algorithm accelerates recovery by 38%, reducing the time-to-insight in time-sensitive missions [21].

4.3. Human factor and training

One of the most significant findings concerns operator expertise. Recovery success in chip-off scenarios was strongly correlated with technician skill level ($R^2 = 0.85$), accounting for up to 78% of outcome variance [2], [18]. Similarly, the most effective logical recovery methods – particularly X-Ways Forensics – required extensive manual verification [8]. These findings suggest that investment in personnel training may yield higher returns than equipment acquisition alone, especially in military contexts where operational readiness depends on timely data access.

4.4. Limitations

Despite its strengths, the integrated framework faces three critical limitations. First, proprietary encryption remains an insurmountable barrier [12]. Second, the high cost of professional-grade hardware (~$28,000) and the requirement of more than 120 hours of specialized training per operator restrict wide deployment to forensic laboratories rather than field units [5], [15]. Third, the study primarily addressed civilian file systems (FAT32, exFAT, NTFS, ext4), while proprietary autopilot storage formats common in military UAVs were beyond the current scope [19].

Furthermore, while controlled laboratory conditions ensured internal validity, they may not fully capture the environmental stressors (e.g., dust, moisture, time pressure) present in real battlefield recovery scenarios, potentially inflating the reported success rates.

For instance, moderate dust contamination or humidity levels typically encountered in field conditions can raise the physical recovery failure rate by an estimated 15-20% due to complications in micro-soldering and electrical connectivity.

4.5. Future research directions

Several pathways can further strengthen this framework. Machine learning-assisted pinout tracing could reduce recovery time per device below four hours [18]. Semi-automated logical recovery pipelines may enable faster triage of corrupted file systems with minimal human oversight [4], [7]. Additionally, testing with proprietary autopilot file systems and encrypted storage architectures is necessary to ensure applicability in classified military contexts [9], [10]. Finally, standardization of UAV storage designs – including documented pinout layouts and robust thermal protections – would greatly enhance data survivability and recovery success in combat environments [15], [16].

4.6. Theoretical and practical implications

Theoretically, this study contributes a unified framework that bridges two traditionally disparate sub-domains of digital forensics. It provides a conceptual model for understanding failure interdependence in UAV storage systems, suggesting that the physical-logical dichotomy is often a false binary in real-world scenarios.

Practically, the findings mandate a revision of standard operating procedures for military and forensic units dealing with UAV incidents. The proposed decision-tree algorithm can be directly integrated into field manuals, emphasizing a 'software-first' approach when possible, to preserve evidence integrity and avoid destructive methods. For manufacturers, the results highlight the critical need for standardized pinout documentation and improved thermal protection in UAV storage designs to facilitate future recovery efforts.

5. Conclusion

This study demonstrates that the traditional isolation of physical and logical data recovery methods is inherently limiting for UAV forensics. The proposed integrated decision-tree framework effectively bridges this gap, providing a systematic methodology for diagnosing failure modes and selecting the optimal recovery pathway. Our results establish that this approach is not merely complementary but essential, achieving recovery rates above 92% and reducing processing time by 38% compared to conventional non-integrated methods.

The results establish three key contributions:

- Hardware recovery efficiency – up to 92.3% success in reconstructing data from physically damaged storage when operating below the thermal threshold of 142°C.
- Software recovery superiority – hybrid forensic methods (R-Studio, X-Ways) achieved recovery completeness of 94–97%, significantly outperforming standalone approaches.
- Integrated forensic workflow – a decision-tree algorithm reduced diagnostic and recovery time by 38%, enabling investigators to systematically select optimal recovery strategies across diverse failure scenarios.

These findings hold direct value for military and forensic practice, enabling reliable reconstruction of UAV flight paths, telemetry, and mission logs with evidentiary accuracy. At the same time, several challenges remain: proprietary encryption, high equipment costs, and the absence of standardized UAV storage architecture limit the universal adoption of this methodology.

Future research should prioritize the development of semi-automated forensic systems, machine learning-assisted failure classification, and validation across proprietary autopilot file systems. Such advancements will strengthen the resilience of UAV data in combat and civilian missions, ensuring that critical information can be pre-served and analyzed even under the most adverse conditions.

Declaration on Generative AI

During the preparation of this work, the authors used Grammarly in order to: Grammar and spelling check. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the publication’s content.

References

[1] S. C. Nayak, B. K. Samanthula and V. Tiwari, "Investigating Drone Data Recovery Beyond the Obvious Using Digital Forensics," 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2023, pp. 0254-0260, doi: 10.1109/UEMCON59035.2023.10315995.

[2] D. A. Hamdi, F. Iqbal, S. Alam, A. Kazim and Á. MacDermott, "Drone Forensics: A Case Study on DJI Phantom 4," 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 2019, pp. 1-6, doi: 10.1109/AICCSA47632.2019.9035302.

[3] Ojo, Taiwo & Chi, Hongmei & Erskine, Samuel. (2023). Unmanned Aerial Vehicle Forensics Investigation Performance under Different Attacks. 10.1109/CSCI58124.2022.00235.

[4] Syed, Naeem & Khan, Majid & Mohammad, Nazeeruddin & Brahim, Ghassen & Baig, Zubair. (2022). Unsupervised Machine Learning for Drone Forensics through Flight Path Analysis. 1-6. 10.1109/ISDFS55398.2022.9800808.

[5] ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition and preservation of digital evidence. - Geneva: International Organization for Standardization, 2012. - 66 p.

[6] K. A. -P. Angamutu and V. A. -P. Selvarajah, "An Insight into the Data Recovery of Deleted or Heavily Damaged Storage Media Through the Lens of R-Studio," 2023 International Conference on Integrated Intelligence and Communication Systems (ICIICS), Kalaburagi, India, 2023, pp. 1-5, doi: 10.1109/ICIICS59993.2023.10421397.

[7] C. Liambas and A. Manios, "Performance Comparison Analysis of Digital Forensic Tools in Various Operating Systems," 2024 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, TX, USA, 2024, pp. 1-5, doi: 10.1109/ISDFS60797.2024.10527289.

[8] N. Asim, J. Osamor, F. Olajide, C. Iwendi and N. Okeke, "Detecting and Mitigating Anti-Forensic Techniques: A Comprehensive Framework for Digital Investigators," 2025 AI-Driven Smart Healthcare for Society 5.0, Kolkata, India, 2025, pp. 66-72, doi: 10.1109/IEEECONF64992.2025.10963229.

[9] S. Deng, T. Lei, X. Jin, H. Yu, X. Zhang and X. Zhang, "Research on Power Control Method of Fuel Cell UAV DC System with Constant Power Load," 2023 IEEE 14th International Symposium on Power Electronics for Distributed Generation Systems (PEDG), Shanghai, China, 2023, pp. 879-885, doi: 10.1109/PEDG56097.2023.10215215.

[10] Chunhui Wang, Zhou Jian, Yuanhang Wang, Shi Zhong, Chuangmian Huang, Yunfan Yang. (2020). An Anomaly Detecting System for Power System of Four-Rotor UAV. 109-114. 10.1109/ISAS49493.2020.9378868.

[11] C. Yuan, Y. Huangfu, H. Bai, S. Pang, W. Shi and H. Zhang, "Stability Analysis and Stabilization Improvement of the DC Power System for Unmanned Aerial Vehicle Based on the Finite-Time Controller," in IEEE Transactions on Industry Applications, vol. 59, no. 6, pp. 7570-7583, Nov.-Dec. 2023, doi: 10.1109/TIA.2023.3299261.

[12] Debas, E., Albuali, A., & Member, I. (2024). Forensic Examination of Drones: A Comprehensive Study of Frameworks, Challenges, and Machine Learning Applications. IEEE Access, 12, 111505-111522. https://doi.org/10.1109/ACCESS.2024.3426028.

[13] Alotaibi, F., Al-Dhaqm, A., Al-Otaibi, Y., & Alsewari, A. (2022). A Comprehensive Collection and Analysis Model for the Drone Forensics Field Sensors (Basel; Switzerland), 22. https://doi.org/10.3390/s22176486.

[14] Fu, Yu, and Yunyan Shuai. "An Efficient Data Collection Method by UAV Based on Data Recovery," International Journal of Information System Modeling and Design (IJISMD) 16, no.1: 1-22. https://doi.org/10.4018/IJISMD.370948.

[15] L. Zhang, Y. Du, J. Xu and X. Wang, "UAV-Enabled IoT: Cascading Failure Model and Topology-Control-Based Recovery Scheme," in IEEE Internet of Things Journal, vol. 11, no. 12, pp. 22562-22577, 15 June15, 2024, doi: 10.1109/JIOT.2024.3381735.

[16] J. Zhang et al., "Multi-UAV Collaborative Surveillance Network Recovery via Deep Reinforcement Learning," in IEEE Internet of Things Journal, vol. 11, no. 21, pp. 34528-34540, 1 Nov.1, 2024, doi: 10.1109/JIOT.2024.3446878.

[17] A. Teng, J. Zha, X. Shan, J. Zhu and J. Lu, "Research on Deep Learning-Based Compression Processing Technology for UAV Inspection Images," 2025 International Conference on Electrical Automation and Artificial Intelligence (ICEAAI), Guangzhou, China, 2025, pp. 1395-1399, doi: 10.1109/ICEAAI64185.2025.10956570.

[18] Nayerifard, T., Amintoosi, H., Ghaemi Bafghi, A., and Dehghantanha, A., “Machine Learning in Digital Forensics: A Systematic Literature Review”, arXiv e-prints, Art. no. arXiv:2306.04965, 2023. doi:10.48550/arXiv.2306.04965.

[19] H. Studiawan, G. Grispos, and K.-K. R. Choo, “Unmanned Aerial Vehicle (UAV) Forensics: The Good, The Bad, and the Unaddressed,” Computers & Security, vol. 132, p. 103340, Sept. 2023, doi: 10.1016/j.cose.2023.103340.

[20] Lee, S., Seo, H., & Kim, D. (2023). Digital Forensic Research for Analyzing Drone Pilot: Focusing on DJI Remote Controller. Sensors, 23(21), 8934. https://doi.org/10.3390/s23218934.

[21] Sihag, V., Choudhary, G., Choudhary, P., & Dragoni, N. (2023). Cyber4Drone: A Systematic Review of Cyber Security and Forensics in Next-Generation Drones. Drones, 7(7), 430. https://doi.org/10.3390/drones7070430.