



International Journal of Research Publication and Reviews

Journal Homepage: www.ijrpr.com ISSN 2582-7421

AI-Powered Aerial Automated Threat Detection and Secure Evidence Verification System: *Literature Review*

Dr. Snehal S. Golait, Moreshwar Pachbhai, Anshul Umbarkar, Tanvi Honade, Kapil Hokarne

Priyadarshini College of Engineering, Nagpur, India

Email: [snehal.golait@gmail.com] [moreshwarpachbhai490@gmail.com] [anshulumbarkar9@gmail.com] [tanvi47honade@gmail.com]

[kapilhokarne1@gmail.com]

ABSTRACT

This paper gives a short review on AI-powered aerial threat detection and secure evidence verification using unmanned aerial vehicles (UAVs). With the increasing use of drones for surveillance, monitoring, and security applications, aerial images are becoming an important source of information and evidence. However, these images can be modified after capture, while AI-based detection models can also be affected by adversarial attacks. Therefore, simply detecting objects in a drone image is not enough to ensure that the obtained information is reliable and trustworthy. This review discusses different approaches for improving the reliability of UAV-based evidence, including SHA-256 image integrity verification, image tampering detection, adversarial attack detection, YOLO-based object detection, confidence verification, and pattern recognition. It also examines the importance of secure evidence logging and maintaining the traceability of image-processing operations. Recent research shows that image-forensic methods can help identify manipulated content, while lightweight and multi-scale deep-learning models can improve object detection in challenging aerial environments. Based on these findings, an integrated approach combining image security, AI-based detection, and secure evidence management can provide a more reliable foundation for UAV surveillance systems. The review also highlights challenges such as small objects in aerial images, changing environmental conditions, limited computational resources, evolving adversarial attacks, and the need for better datasets and real-world evaluation.

1. Introduction

Unmanned Aerial Vehicles (UAVs), commonly known as drones, are increasingly being used for surveillance, monitoring, security, inspection, and other applications where collecting information from the air is useful. The images and data captured by these systems can provide important information about objects, locations, and activities. In security and forensic applications, however, the reliability of this information is just as important as the ability to collect it. A drone image may be modified after it has been captured, and such changes can affect the interpretation of the evidence. The reviewed project material therefore identifies image authenticity, tampering detection, and secure evidence handling as important requirements for a trustworthy UAV-based system.

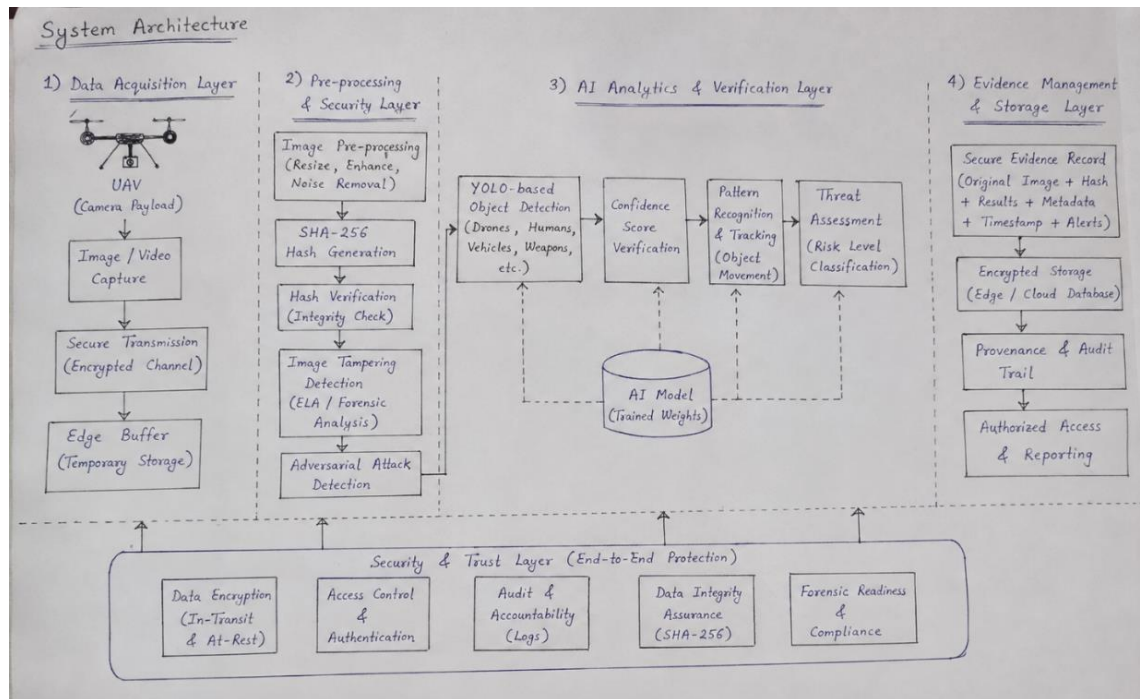
The problem becomes more challenging when artificial intelligence is used for analysing aerial images. Object detection models can identify relevant objects automatically, but their predictions may be affected by adversarial inputs and difficult environmental conditions. As a result, object detection alone cannot guarantee that the information produced by a UAV system is trustworthy. The proposed system materials emphasize the need to combine object detection with image integrity verification, tampering analysis, adversarial detection, and secure evidence management.

Image manipulation detection has also become an important research area because modern editing and generative technologies can produce increasingly difficult-to-detect modifications. Existing research broadly discusses **passive** and **active** approaches. Passive techniques examine the image itself to identify inconsistencies, while active techniques use additional information such as digital watermarks or embedded markers. Deep-learning methods have become increasingly important because they can detect and, in some cases, localize manipulated regions in complex images.

Another important aspect is the security and traceability of UAV-generated evidence. Digital forensic studies indicate that UAV systems can contain different types of flight logs, sensor events, software information, and other digital traces. Problems such as insecure communication, data tampering, encryption issues, and differences in UAV data structures can make evidence collection and verification more difficult. Therefore, maintaining a clear record of how an image is captured, processed, analysed, and stored is important for improving its forensic reliability.

To address these challenges, an integrated AI-based approach can combine **SHA-256 integrity verification, image tampering detection, adversarial analysis, YOLO-based object detection, confidence verification, pattern recognition, and secure evidence logging**. The project architecture identifies these components as key modules for creating a secure image-processing pipeline. Such a combination moves beyond simple object detection and focuses on whether the detected information can also be considered reliable and traceable.

This review therefore examines the major techniques and research trends related to **UAV-based object detection, digital image tampering detection, adversarial robustness, image integrity, and secure evidence management**. It discusses the strengths and limitations of existing approaches and identifies challenges that need further attention, particularly in real-world aerial environments where computational resources, changing conditions, evolving attacks, and the reliability of digital evidence must all be considered.



2. Literature Review

2.1 UAV Object Detection

[5] proposed an improved YOLOv8-based method, called SS-YOLOv8, for detecting small objects in UAV images. Their research focused on the difficulty of detecting small targets because UAV images often contain objects with very few pixels, which can result in missed detections and a large computational requirement. The authors improved the YOLOv8 architecture to increase its ability to detect small objects while reducing unnecessary model complexity. Their work shows that improving feature extraction and detection capabilities can make YOLO-based models more suitable for UAV applications. However, further improvement is still required for real-time operation on resource-limited UAV or edge devices and for handling changes in object scale, background, and environmental conditions.

2.2 YOLO and Real-Time Detection

[6] proposed BDMA-YOLO, an improved YOLO-based framework for detecting small objects in UAV aerial images. Their study addressed the difficulty of detecting small targets because UAV images often contain objects with limited pixel information and complex backgrounds. The authors used YOLOv8-S as the baseline and introduced dynamic multi-scale feature fusion and attention-based modules to improve the detection of small objects while keeping the model computationally efficient. Their experiments showed that BDMA-YOLO improved detection performance over YOLOv8-S and maintained real-time performance at 156 FPS on an RTX 4060 GPU. However, the authors noted that this performance was measured on a desktop GPU and that further testing is required on resource-constrained UAV edge devices such as Jetson platforms. Therefore, for our project, YOLO can be further implemented with real-time inference, confidence verification, lightweight architecture, and object tracking so that detected threats can be analysed continuously from UAV video streams.

2.3 Threat and Safety Detection

[4] conducted a systematic review of deep-learning techniques used for UAV cybersecurity and threat detection. Their study examined threats such as spoofing, jamming, intrusion, malware, and attacks on UAV communication and control systems. The review found that deep-learning models, particularly CNN- and RNN-based approaches, can identify abnormal UAV behaviour and support real-time threat detection. It also highlighted the increasing use of lightweight techniques such as pruning, quantization, and knowledge distillation to make AI-based security systems suitable for resource-limited UAV platforms. However, the authors identified important gaps in shared datasets, adversarial testing, explainability, and real-world deployment. Therefore, our project can further implement an integrated threat and safety detection module that combines adversarial-attack detection

with object detection, confidence verification, and alert generation, allowing suspicious objects or unsafe conditions detected from UAV imagery to be identified and reported in real time.

2.4 Image Integrity and Tampering

Image integrity can be understood through two complementary levels: file-level integrity and content-level integrity. File-level integrity can be checked using cryptographic hashing such as SHA-256, which helps determine whether the digital image file has been changed after its original hash was generated. Content-level integrity focuses on whether the actual visual information in the image has been manipulated. Research on image forensics commonly divides these techniques into passive and active methods. Passive methods examine clues already present in an image, such as statistical inconsistencies, noise patterns, compression artifacts, and other traces left by manipulation, while active methods use additional information such as digital signatures or watermarks during image creation to support later verification. Recent research has increasingly used deep-learning models to improve the detection and localization of manipulated regions. However, these techniques generally determine whether the digital image or its content shows evidence of modification; they do not, by themselves, prove that the physical scene was genuine at the moment the UAV captured it. Therefore, for our project, SHA-256 verification should be combined with image-forensic tampering detection, metadata, and secure evidence logging to provide stronger image authenticity and traceability. [3]

2.5 Adversarial Attacks and Defense

[4] reviewed the growing problem of adversarial attacks against UAV systems, where attackers can manipulate inputs, communication, navigation signals, or other system components to affect UAV decisions. Their review found that deep-learning models can be useful for identifying abnormal behaviour and detecting different cyber threats, but these models themselves can also be vulnerable to carefully manipulated inputs.

For our project, adversarial defense can be added before the object-detection stage to identify suspicious or manipulated inputs. A practical implementation could combine **adversarial-input detection, confidence verification, and alert generation** with the YOLO detection module. This would help the system distinguish between a normal UAV image and an image that may cause incorrect AI predictions.

2.6 Secure Digital Evidence

[2] studied the challenges involved in maintaining and tracing digital evidence generated by UAV systems. Their research focused on both static and live digital evidence and showed that issues related to data integrity, evidence preservation, repeatability, and forensic traceability can make UAV evidence difficult to verify during an investigation. The authors emphasized the need for proper evidence handling and documentation so that collected UAV data can be trusted during forensic analysis.

For our project, secure digital evidence can be implemented by storing the **original image, SHA-256 hash, detection results, timestamps, metadata, tampering analysis, and threat alerts** together in a secure evidence record. This creates an audit trail that can help demonstrate whether the evidence has remained unchanged after collection. The approach can therefore combine AI analysis with forensic traceability rather than treating object detection alone as proof of trustworthy evidence. This is consistent with the project's proposed **SHA-256 integrity verification, secure evidence logging, and secure database** modules.

3. Comparative Analysis

Sr. No.	Authors / Research Paper	Year	Main Focus	Method / Approach	Key Findings	Research Gap / Limitation	Relevance to Proposed System
1	Shakhathreh et al. – <i>Unmanned Aerial Vehicles: A Survey on Civil Applications and Key Research Challenges</i>	2019	UAV applications and challenges	Survey of UAV applications such as monitoring, surveillance, search and rescue, remote sensing and security	Identified the growing use of UAVs for real-time monitoring and surveillance and discussed challenges related to security, networking and deployment.	Does not provide an integrated AI-based evidence verification system	Provides the basic foundation for UAV surveillance and real-time monitoring.

Sr. No.	Authors / Research Paper	Year	Main Focus	Method / Approach	Key Findings	Research Gap / Limitation	Relevance to Proposed System
2	Salamh et al. – <i>A Comparative UAV Forensic Analysis: Static and Live Digital Evidence Traceability Challenges</i>	2021	UAV digital forensics and evidence traceability	Analysis of static and live UAV evidence using forensic and purple-teaming approaches	Identified challenges related to data integrity, repeatability, attack vectors, anti-forensics, encryption and flight-log traceability.	Different UAV systems have different file structures and security mechanisms, making forensic analysis difficult.	Supports secure evidence logging, integrity verification and forensic traceability.
3	Duszejko, Walczyna & Piotrowski – <i>Detection of Manipulations in Digital Images: A Review of Passive and Active Methods Utilizing Deep Learning</i>	2025	Image integrity and tampering detection	Review of passive image-forensic and active watermark-based methods	Passive methods analyse image characteristics, while active methods use embedded information for manipulation detection and localization.	Passive methods can struggle with advanced manipulation, while active methods require control over image creation and distribution.	Supports the image tampering detection and authenticity verification module.
4	Tariq, Ahanger & Ahmed – <i>Systematic Review of Trends in Deep Learning for UAV Cybersecurity</i>	2026	UAV cybersecurity and threat detection	Review of deep-learning techniques for UAV cyber-threat detection	Discussed AI-based detection of threats such as GPS spoofing, malware, DoS attacks and network intrusions.	Better datasets, explainable AI, stronger security and real-world validation are still required.	Supports threat detection, adversarial detection and alert generation.
5	Wang, Lin, Han & Pang – <i>Enhancing UAV Aerial Small Target Detection with Bidirectional Dynamic Multi-Scale Attention YOLO</i>	2026	UAV small-object and real-time detection	BDMA-YOLO with dynamic multi-scale feature fusion and spatial attention	Improved small-object detection compared with YOLOv8-S, reduced parameters by 7.2% and achieved 156 FPS in the reported experiments.	Mainly evaluated daytime scenarios; deployment on resource-constrained UAV edge devices requires further validation.	Supports YOLO object detection, real-time processing, confidence verification and pattern recognition.

4. Research Gaps

- 1. Lack of an Integrated Security Framework:** Existing studies generally focus on a single area such as UAV object detection, image manipulation detection, cybersecurity, or digital forensics. There is a need for an integrated framework that combines these components into a single secure UAV evidence-processing pipeline.
- 2. Limited Evidence Integrity Verification:** UAV forensic research highlights challenges related to data integrity and evidence traceability. However, object-detection systems generally focus on identifying objects rather than ensuring that the processed image has remained unchanged. A combination of **SHA-256 hashing, metadata preservation, and tampering analysis** can provide stronger evidence integrity.
- 3. Difficulty in Detecting Advanced Image Manipulations:** Image-forensic methods have improved through deep learning, but advanced manipulations and AI-generated images remain challenging to detect. Passive methods can be affected by sophisticated modifications, while active methods require control over the image-generation process.

4. Adversarial Vulnerability of AI Models: Deep-learning-based UAV systems can face adversarial and cybersecurity threats. Existing research highlights the need for stronger defensive mechanisms, better datasets, explainable AI, and realistic security testing before deployment in practical UAV environments.

5. Real-Time Detection on Resource-Constrained Devices: Recent YOLO-based research has achieved improved accuracy and real-time performance, but high-performance results are often obtained on powerful GPUs. Further testing is required on resource-constrained UAV edge devices with limited processing power, memory, and energy.

6. Limited Testing Under Diverse Conditions: UAV detection research has mainly evaluated models using available aerial datasets and, in some cases, favourable daytime conditions. More testing is required under **night-time conditions, adverse weather, different sensors, changing altitudes, and diverse environments.**

7. Insufficient Connection Between AI Results and Forensic Evidence: Existing object-detection methods primarily provide detection results, while forensic studies focus on evidence traceability. A major gap is connecting AI outputs such as detected objects, confidence scores, and threat alerts with **secure evidence records and audit trails.**

5. Proposed Integrated Research Direction

Motivated by the identified gaps, the proposed research direction is an end-to-end pipeline rather than a claim of experimentally superior performance:

Drone Camera → Image Acquisition → Input Validation → SHA-256 Image Integrity Verification → Tampering Detection → Adversarial Attack Detection → Image Enhancement → YOLO/Object Detection → Confidence Verification → Threat/Risk Assessment → Secure Evidence Storage → Automated Incident Report Module rationale.

Input validation rejects malformed frames. SHA-256 records a cryptographic fingerprint at capture, with timestamp and processing metadata. A passive tampering detector screens for splicing, copy-move, or inpainting artifacts. Adversarial screening flags suspicious perturbations before detection. Enhancement can improve small-object visibility after the original hash is recorded. A lightweight YOLO model performs real-time detection, while confidence calibration routes uncertain detections to human review. Hashes, detections, and metadata are stored with access logging, and each processing step is recorded to create an auditable chain of custody. Critical distinction. SHA-256 verifies file-level integrity, not scene authenticity. Tampering refers to post-capture modification of image content, whereas adversarial perturbation is designed to fool an AI model and may be imperceptible to humans. Accidental corruption produces a hash mismatch but is not itself a malicious attack. 7. Future Research Directions

6. Future Research Directions

Future work should prioritize (1) lightweight YOLO and edge deployment with power, thermal, and latency benchmarks; (2) efficient transformer-based aerial detection; (3) multimodal RGB-thermal/LiDAR sensing for adverse conditions; (4) adversarially robust training and evaluation using physically realizable attacks; (5) explainable AI for operator auditing; and (6) standardized evidence provenance that binds hashes, tampering scores, adversarial flags, detection confidence, and geospatial metadata into a signed evidence record. Standardized datasets combining object annotations, tampering labels, adversarial examples, and forensic metadata are particularly important for fair evaluation.

7. Conclusion

This review examined research in aerial object detection, UAV cybersecurity, image tampering detection, adversarial robustness, and digital evidence integrity. YOLO-family detectors currently provide a strong speed-accuracy balance for real-time UAV applications, while transformer-based detectors show promise for small-object detection at higher computational cost. Image manipulation and adversarial robustness are established research areas individually, but their integration into aerial threat-detection pipelines remains limited. SHA-256 provides essential file-level integrity verification but cannot establish that an image was authentic at capture or that its scene was not manipulated before hashing. The principal research opportunity is therefore an integrated framework that combines automated aerial threat detection, integrity verification, tampering and adversarial analysis, confidence-based risk assessment, and secure evidence preservation. Future work should evaluate such systems end-to-end on realistic UAV data and report both AI performance and forensic trustworthiness.

8. References

- [1] H. Shakhathreh, A. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned Aerial Vehicles: A Survey on Civil Applications and Key Research Challenges," *IEEE Access*, vol. 7, pp. 48572–48634, 2019.
- [2] F. E. Salamh, U. Karabiyik, M. K. Rogers, and E. T. Matson, "A Comparative UAV Forensic Analysis: Static and Live Digital Evidence Traceability Challenges," *Drones*, vol. 5, no. 2, p. 42, 2021, doi: 10.3390/drones5020042.
- [3] P. Duszejko, T. Walczyna, and Z. Piotrowski, "Detection of Manipulations in Digital Images: A Review of Passive and Active Methods Utilizing Deep Learning," *Applied Sciences*, vol. 15, no. 2, p. 881, 2025, doi: 10.3390/app15020881.

-
- [4] U. Tariq, T. A. Ahanger, and I. Ahmed, "Systematic Review of Trends in Deep Learning for UAV Cybersecurity," *Frontiers in Artificial Intelligence*, vol. 9, Art. 1752124, 2026, doi: 10.3389/frai.2026.1752124.
- [5] J. Qu, Q. Li, J. Pan, M. Sun, X. Lu, Y. Zhou, *et al.*, "SS-YOLOv8: Small-size object detection algorithm based on improved YOLOv8 for UAV imagery," *Multimedia Systems*, vol. 31, p. 42, 2025, doi: 10.1007/s00530-024-01622-3.
- [6] Z. Wang, J. Lin, Y. Han, and Y. Pang, "Enhancing UAV aerial small target detection with bidirectional dynamic multi-scale attention YOLO," *The Visual Computer*, vol. 42, p. 227, 2026, doi: 10.1007/s00371-026-04404-2.
- [7] J. Qiu, F. Cai, N. Fu, and Y. Yao, "YOLO-Air: An Efficient Deep Learning Network for Small Object Detection in Drone-Based Imagery," *IEEE Access*, vol. 13, pp. 79718–79735, 2025, doi: 10.1109/ACCESS.2025.3565560.
- [8] J. Ge, H. Lv, Y. Guo, Y. Chen, Y. Xu, and X. Yang, "MFR-YOLO: advancing UAV object detection with multi-scale feature refinement via deformable convolution and global attention," *Scientific Reports*, vol. 16, Art. no. 15587, 2026, doi: 10.1038/s41598-026-45641-8.
- [9] M. Li, H. Li, J. Zhu, and X. Zhang, "Visual Detection Algorithms for Counter-UAV in Low-Altitude Air Defense," *Computers, Materials & Continua*, vol. 86, no. 3, p. 32, 2026, doi: 10.32604/cmc.2025.072406.
- [10] D. R. Clark, C. Meffert, I. Baggili, and F. Breitingner, "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III," *Digital Investigation*, vol. 22, pp. S3–S14, 2017, doi: 10.1016/j.diin.2017.06.013.