A Nano-Tagging–Based Framework for Secure Drone Evidence Handling

Niharika Puri[a], Padigela Srinivas Reddy[b]
[a]Department of Digital Forensics, School of Sciences, Malla Reddy University, Hyderabad,India.
[b]Department of Physics, Malla Reddy University, Hyderabad, India, T.S-500043, India.
Corresponding author: niharikapuri1208@gmail.com

Abstract:

With the rapid increase in drone usage for both legitimate and criminal activities, digital forensic analysts face growing challenges in preserving, authenticating, and verifying evidence collected from UAVs (Unmanned Aerial Vehicles)[3][6]. By using drones as evidence, there can be many other challenges, such as components duplication (counterfeit or cloned parts), chain of custody vulnerabilities and legal governing limitations.[3][6]

Existing forensic approaches towards UAVs (drones) are lacking in many ways such as the absence of material-level identification (physical markers), a weak chain of custody for physical components and insufficient anti-counterfeiting measures. These limitations significantly weaken attribution and evidentiary robustness in drone-related investigations.

By embedding forensic identity directly into drone components, nano-tagging addresses long-standing challenges related to attribution, chain of custody, and evidence integrity that remain unresolved in existing UAV forensic framework[1][2]. As drones have digital markers that may crash after any incident, nano-tagging will help in embedding the physical identifiers (nanotags) in UAVs. It also assists in developing the device-level assumption to the component-level attribution. Besides that, nano-tagging aids in resistance to anti-forensic attacks, component manipulation and digital data integrity. Nanotags have physically unclonable features (impossible to duplicate)[5]. Nanotags act as covert evidence in forensics[1].

Keywords: *Drone forensics, UAVs, Robustness, Nano-tagging, and Chain of custody.*

1. Introduction:

The increasing misuse of drones in criminal activities, combined with the anonymity and modularity of modern UAV platforms, it is required for the development of advanced forensic mechanisms capable of ensuring reliable attribution and evidence integrity[6].

D. R. Reddy et al. (eds.), *Proceedings of the First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)*, Advances in Computer Science Research 127,
https://doi.org/10.2991/978-94-6239-610-4_36

The existing vulnerabilities of both digital and physical drone evidence highlights the limitations of present forensic practices, which lack in determinant and tamper-resistant identifiers. This fragility motivates the need for material-level forensic mechanisms, such as nano-tagging, to ensure evidence integrity and reliability[1][5]. Nano - tagging is a technology which uses microscopic markers (identifiers) to track, identify and monitor materials, data or any organisms.

There are different types of semi-conductor nanocrystals, such as quantum dots, that are used as the nanotags for UAVs[5]. We can also use the fluorescent carbon nano particles as a physical identified markers upon drones, which completely assists as the covert evidence. Basically, there are various nano tags that supports in strengthening a few areas in drone forensics, such as chain of custody, volatile digital identifiers, component swapping and legal issues (security challenges). We can also include the RFID (radio frequency identification) nano-tags for making the wireless tracking possible in UAVs[4][7].

Persistent identification is very much essential in drone forensics as UAVs have the nature of volatility, modularity and are prone to crash[6]. Unlike traditional, digital devices the drone operates in a dynamic environment and often suffer physical damage and intentional manipulation. Persistent identification strengthens the admissibility and credibility of drone evidence by providing a continuous and proper link between physical components and forensic records.

Additionally, nano-tagging can contribute to the digital forensic techniques by providing a physical authentication layer that supports digital hash verification[1]. This hybrid approach strengthens the overall evidentiary value and reliability of drone-related evidence.

This paper contributes in discussing how we can fill the limitations present in UAVs with the help of Nano-tagging by using the physical identifiers and improving the quality of the chain of custody. The inclusion of RFID nano-tags further aids in non-line of sight identification, traceability in UAVs by addressing the current limitations in forensic practises[4,7].

In the present scenario usage or utility of Drone forensics has risen in both legitimate and criminal or anonymous actions[6].

To overcome certain drawbacks in Drone forensics, recent studies have combined a nano-tagging into UAVs, which gave a secure framework of drone forensics and enhanced the operational efficiency[1,2]. How-ever the potential of nano-tagging in this area is unexplored and discussed insufficiently. Existing approaches towards handling evidence in forensics rely on exploring physical debris, digital telemetry extraction, and radio frequency attribution, which

cannot be effective in few areas where there is deliberate erasing of information and usage of counterfeit parts is present[3,6].

Therefore, nano-tagging will explicitly help in giving the physical digital identifiers in the form of nano-tags that exist as covert evidence (can be seen under particular light)[1,5]. Forensics taggants or nano-enabled markers perform efficiently using various nano materials[8] like magnetic nanomaterials, fluorescent nano particles, DNA-based taggants, nanomaterial-based RFID nano-tags and nano-structured surface tags in covert identification (hidden) and source attribution in different forensic scenarios.

Building upon these forensic upgradations can help in evidence authentication, chain of custody assurance and measurable identification of drone components even under extreme environmental condition. As known, the use of nano-tagging is still limited in both drone forensics and other forensic procedures. This indicates the need of structured frameworks by integrating the nano-tagging in physical and digital forensic workflow methods to build a secure, tamper-resistant and verifiable drone forensics environment.

2. Problem definition:

The rapid growth in using UAVs (unmanned aerial vehicles) initiated limitations in handling identification, authentication, and integrity of drones. There are a few challenges that can be resolved by embedding the nano-technology in digital forensics. Especially using nano-tagging, we can answer many problems.

One major challenge arises from component swapping and using counterfeit parts in drones[2,3]. Drones and other UAVs have batteries, flight controllers, and other components that can be replaced by cloned or counterfeit parts, which can lead to less efficacy of this as evidence. This can be helped by embedding nano-tags at the material level or component level, which acts as a covert identification marker even when the parts of the drone are replaced.

Another limitation occurs with the erasure or manipulation of digital telemetry data[3,6] File-logs and operational data of UAVs can easily be manipulated deliberately, which leads to loss of critical information (GPS, altitudes, travelled area pattern, etc.) Nano-tags act as the strongest physical identifiers that doesn't depend on digital storage, allowing forensic attribution even when telemetry data is deliberately destroyed or altered.

Another critical challenge is limited reliability on evidences under extreme conditions. The parts of the drone can be damaged, and the system can be crashed under few conditions. This

limits the importance of the drone as evidence. Nano - tags such as fluorescent nano materials, can be under specific conditions even when the drone is damage.

Drone forensics also face challenging in the improper verification of evidence authenticity[6]. Investigators may have doubt on seized evidences whether they are original or replaced. This can be solved using nano-signatures that can help in reviewing authenticity at any stage of legal proceedings.

Drone forensics also lack in weak chain of custody. Current drone forensic workflows depend mostly on procedures, which is prone to human error, tampering, and evidence substitution[6]. Nano-tag verification at each handling stage enables physical validation of evidence continuity, strengthening chain-of-custody integrity.

These limitations together highlight the liabilities in drone forensic frameworks. Addressing the gap or a loophole, we can strengthen the work flow system in drone forensics using nano-tagging.

3. Proposed Nano-tagging framework:

This framework helps in nano-tagging, which is also integrated with nano RFID tagging that enhances the operational efficiency in providing persistent identification, maintaining an accurate chain of custody, evidence authentication, and tampering detection. This framework also addresses physical layer vulnerabilities such as component swapping, post-crash evidence, and counterfeit components while functioning with procedures[4,7].

Types of Nano-tags used:

3.1 Nano RFID-tags:

These RFID nano-tags provide unique component-level physical identifiers or markers that are embedded in flight controllers, motors, batteries, and communication modules that can be read wirelessly without physical contact. Their primary function is to assist in rapid component authentication, lifecycle tracking, and verification of ownership or manufacturing origin during forensic handling. RFID tags are quantifiable and capable of tuning or changing forensic properties it improves the admissibility of evidence in court[7].

3.2 Chemical and DNA-based nano-tags:

Chemical and DNA-based nanotags have unique properties that can even be resistant to visual and electronic spoofing. These tags help in finding the origin of components and are effective in finding counterfeit parts and unauthorized parts[2]. Ex: Isotopic chemical markers, molecular-based nanotags, etc.

3.3 Magnetic nano tags:

Magnetic nanoparticles are prepared to facilitate trace recovery and authentication from fragmented or burned drone debris[1,8]. Their magnetic response allows selective extraction from complex materials, improving recovery efficiency and measurable yield. Magnetic nanotags act as a redundancy layer when optical or electronic identifiers are compromised.

3.4 Optical or fluorescent nano tags:

Optical nanotags, including fluorescent nanoparticles and quantum dots, provide covert, visually detectable signatures under specific light with a certain wavelength (UV/IR)[5]. These tags produce unique light signals that can be visible under few circumstances by enabling component-specific or batch-specific identification. Optical nanotags support forensic verification when RFID tags are damaged or unreadable and assist in counterfeit determination. The proposed framework fuses the nano-RFID tags with optical, magnetic, and chemical nanotags to have persistent component-level identification, counterfeit detection, and secure chain-of-custody management. Nano-RFID tags provide rapid, non-contact authentication, while complementary nanotags ensure forensic resilience and quantifiable recovery under post-incident conditions[7]. The design of fluorescent nano materials can be extracted from waste biomass (shells of pistachios) as cost effective approach.

4. Experimental:

A single donor UAV is chosen as the experimental platform that has components which are helpful, such as batteries, motors, flight controllers, and communication modules. By integrating the nano-tagging, we can resist counterfeit parts, assists in unique identification, and ensure an accurate and strong chain of custody with proper authentication.

4.1 Nano-tagging integrated in drone forensics:

There are different types of nanotags used, which aids in different functions under various circumstances. Nano-tags that can be utilised are magnetic nanotags, chemical nanotags, DNA-based nanotags, nano material-based RFID tags, nano-structural surface tags, and fluorescent nanotags, which benefit in source attribution, counterfeit identification, supply-chain tracing, long-term stability, finding origin of components, high resistance to manipulation and authentication of evidence by handling the post-crash evidence[2]. These nanotags particularly act as covert evidence that authenticates components, and helps in source attribution.

Hypothetical scenario:

- Normal operation: Basic operations that happen in handling a drone as evidence.
- Component swapping: The replacement of tagging goods is done.
- Crash stimulation: Fragmenting the components of evidence.
- Environmental variations: Creating different conditions such as exposure to heat, moisture, etc.
- Evidence handling stimulation: Multiple transfers or steps are done to check the integrity of the chain of custody.

Detection and Measurement equipment:

- RFID readers are used to analyse the nano RFID tags.
- Ultra-violet or Infrared light sources are used for the detection of optical or fluorescent nanotags.
- Magnetic separators and spectroscopic tools for magnetic nanotags.

  Laboratory analysis tools for chemical nanotag verification.

Performance indicators:

- Accurate component identification.
- Finding counterfeit parts.
- Tracing life cycle.
- Chain of custody integrity verification.
- Accessing source attribution.
- Getting the efficiency of measurable yield in nano tags.

5. Results & Analysis:

5.1 Component swapping and Authentication:

RFID nanotags are used to get information wireless without any physical contact that is non-contact authentication of drone components. Components embedded with RFID tags are easily differentiable compared to untagged ones. The use of nano-RFID tags as a primary identifier improves reliability compared to reliance on digital telemetry alone[4,7].

5.2 Counterfeit and Unauthorized component detection:

Chemical and DNA nano tags assisted in source determination (origin of components) of the supply chain model and detected the counterfeit parts through exchanged signatures. Further, optical nanotags help in confirming the authentication under unique light. Multi-modal tagging reduces false information and improves confidence in identifying unauthorized components.

5.3 Post-crash evidence:

Magnetic nanotags are more reliable during this harsh-conditions where the fragments are found. Magnetic nano tags helped by contributing more measurable yield when compared to optical nanotags. Optical elements have not been detected under certain light, which may weaken the authentication or verification. Magnetic nanotags are more reliable in post-crash evidence than optical nanotags.

Chain of custody integrity:

As there are nanotags used in drone I authenticated or verified every step in the chain of custody across the procedure. This smoothens the process of integrity in the chain of custody. Persistent identifiers reduce the chain of custody vulnerabilities and improve forensic work flow.

5.4 Performance assessment:

By evaluating this framework has performed accurate component authentication, to resist post-crash incidents, and identification of counterfeit parts.

6. Discussions:

This paper discusses how nano-tagging aids in creating the secure framework in drone forensics. The above work also describes the approach that can mitigate or limit drawbacks and challenges faced in the support to drone forensics. Forensic approaches that are mentioned in this work are embedding fluorescent nano tags that aid in certain luminal light, where it will completely act as masked evidence. Magnetic nano tags are used when the evidence is fragmented, as it gives the highest measurable yield, which strengthens the admissibility in court.

Furthermore, we can utilize DNA-based nano materials that are specifically applied in counterfeiting and component swapping as nano tags cannot be replicated or copied exactly the same. Additionally, nano RFID (radio frequency identification) tags are used in drone forensics when digital elementary information is not reliable (origin of component). We call these tags wireless nano-materials (no physical contact required) as they work based on radio frequency. Using nanotags, can resist the post-crash evidence, fragmented evidence, maintains the integrity in the chain of custody, and verify the identity where the parts of the drone are replaced in the workflow of the investigation. Besides, nanotags are used to provide a unique identification number or code for individualising the parts of the drone. Nano-tagging will also be cost effective, low toxic by utilizing the waste biomass, and very small in nature[8].

Limitations:

- Real-time case studies are found often.
- High infrastructure is utilized of nano technology.
- Environmental degradation effects.
- Lack of standard rules and regulations.
- Purely theory-based reviews and real-time approaches are unexplored.
- Can face legal issues as nano tags are considered to be covert evidence.

7. Conclusion:

This research paper is providing approach that can strengthen and secure the framework and workflow of drone forensics by integrating nano tagging into it. By embedding nano material as unique physical identifiers like quantum dots, earth-doped nano tags, optical and chemical nano tags, magnetic nano tags, and RFID-based nano tags into drone components improves resistance in fragmented evidence, helps to overcome the physical layer vulnerabilities by integrating with element-level nano tagging. Few optical tags can be utilized even under harsh conditions. Nano tagging also assists in maintaining integrity in the chain of custody, making it as the promising solution for security challenges in drone investigation.

References:

1. Miller, J. C & Serrato, M (2018), Forensic taggants and trace materials for authentication.
2. Cai, L., et.al (2020), DNA-based anti-counterfeiting and forensic tagging.
3. Moore, A., & White, G (2020), UAV forensic analysis and evidence preservation challenges.
4. Nguyen, T., et al (2021), RFID-based forensic tracking systems.
5. R. Arppe, & Sorensen, T. J (2017), Physical unclonable luminescent tags.
6. Horsman, G. (2019), Unmanned aerial vehicles: A preliminary analysis of forensic challenges.Digital investigation, Elsevier.
7. Want, R. (2006), An introduction to RFID technology.
8. V. Prashanth Kumar, Padigela Srinivas Reddy, Suresh Sripada, C. Vishnuvardhan Reddy, Preparation and Characterization of $Pr_{1-x}Sr_xMO_3$(PSMO) ($0 \leqslant x \leqslant 0.6$) Nanomaterials, Volume 3, Issue 10, Part B, 2016, Pages 3709-3712.

-