International Journal of Safety and Security Engineering
Vol. 15, No. 1, January, 2025, pp. 1-12
Journal homepage: http://iieta.org/journals/ijsse

Metamodeling-Based Drone Forensics Investigation: A Systematic Literature Review

Senan A. M. Alhasan[1,2*], Siti Hajar Othman[1], Arafat Al-Dhaqm[3]

[1] Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Johor 81310, Malaysia
[2] Department of Computer Science, Collage of Education for Pure Science, University of Mosul, Mosul 42001, Iraq
[3] School of Computer Science, Taylor's University, Subang Jaya, Selangor 47500, Malaysia

Corresponding Author Email: senanadelmawlood@graduate.utm.my

https://doi.org/10.18280/ijsse.150101

Received: 7 November 2024
Revised: 28 December 2024
Accepted: 20 January 2025
Available online: 31 January 2025

Keywords:
drone forensics, UAV, healthcare, meta-model, SLR

ABSTRACT

The drone forensics field has received a great attention in recent years due to the important role it plays in the investigation of incidents as well as the identification and tracking of attacking entities and actions. In an era where technology intersects with nearly every aspect of human life, drone forensics has emerged as a transformative force in medicine, biomedical research, and healthcare. The present paper reviews the literature of drone forensics to improve the body of knowledge and identify the underlying challenges relevant to the studies conducted in this field. In addition, the paper discusses how to define and integrate models from many domains of drone forensics using the metamodeling technique. This technique is applicable to various fields, particularly for standardizing purposes. Moreover, the present study involves the systematic literature review (SLR) which is provided in a section alongside the research topics; it serves as the main source of inspiration in the current work. As the literature does not comprise any study focusing on this issue with the use of SLR, this paper can contribute to filling this gap effectively. The SLR was carried out in the current study by the categorization of the existing literature parametrically using bibliometric analysis. The findings of this paper showed that the use of metamodeling in the drone forensics can make this field more homogeneous and less complex.

1. INTRODUCTION

Recent years have witnessed a surge in people's curiosity about and awareness of the technology of unmanned aerial vehicles (UAV). These vehicles, also known as drones, act as pilotless aircrafts that could be controlled remotely and autonomously using pre-programmed flight routes. Numerous applications that these vehicles can have in public life (for instance aerial photography, surveying, inspection, and unarmed cargo) have caused this technology to go beyond its primary use, i.e., military applications [1]. The increasing congestion of airspace, on the other hand, has increased the risk of crashes. In addition, the implementation of security measures for drones is much more difficult compared to the case of conventional aircraft [2]. The necessity of forensic analysis for drones has become increasingly apparent with their growing application in various fields. In medicine and biomedical research, drones equipped with high-resolution cameras and sensors can collect extensive amounts of physiological data unattainable by conventional methods [3].

Consequently, the new field of drone forensics was developed as a branch of digital forensics to investigate scientifically the drone-related incidents in order to detect attacking entities and actions. This field of study inspects the evidence extracted from drones and the accompanied parts. The drone forensics filed encompasses two subfields: mobile forensics and wireless forensics [4]. The improper management and review of digital evidence will cause its brittleness, sensitiveness, and volatility. In addition, authorities and businesses can hardly keep up with the wide variety of drones universally used today and also their rapid evolution. Despite such difficulties and the relative infancy of the drone forensics field, there is still a lack of strong support for the development of investigative tools in this domain [5]. The digital forensics domain could be developed using the metamodeling technique that helps define and integrate models extracted from various domains [6].

2. THE RESEARCH PROBLEM

The lack of standardized techniques such as collecting and analyzing drone evidence is one of the research limitations in drone forensics that our research attempts to discuss and propose to address [7]. The present article is aimed at reviewing the literature on drone forensics to shed light on the path this field has come through and then make

recommendations for the future to support the strengths and minimize the weaknesses. Figure 1 illustrates the mapping of the research problem.

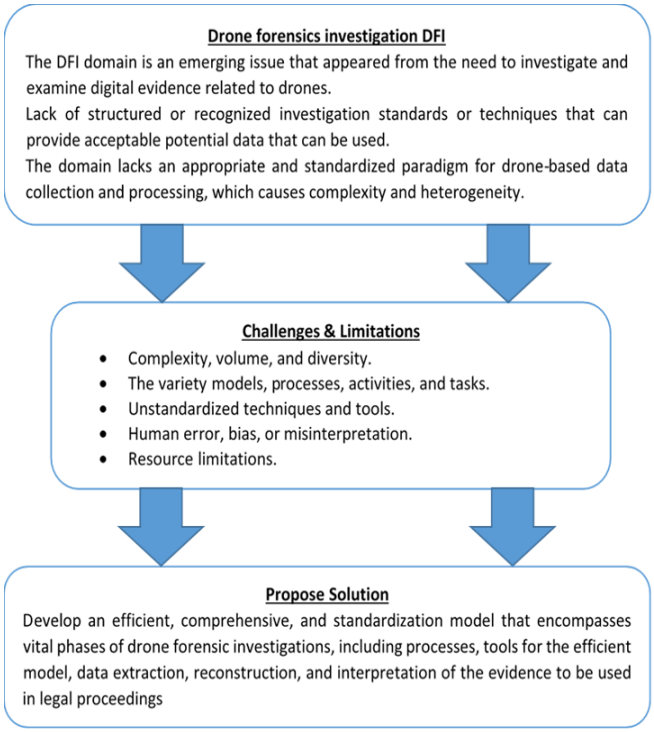

Figure 1. Mapping of the research problem

3. RESEARCH PLAN

This study aims to use systematic reviews and meta-analysis (PRISMA) and bibliometric analysis with the support of VOS viewer to respond to the following section's questions [8]. For the purposes of this study, the literature on drone forensics is reviewed in the search of findings that can support forensic investigations. To be more specific, the following questions were set to be answered in this study:

Q1: Which articles have studied "Drone forensics", "UAV, "Digital Forensic", and "Meta-model"?

Q2: What are the most cited articles, countries, and authors? And what are the most recent and popular subjects in "Drone forensics", "UAV, "Digital Forensic", and "Meta-model" among academics?

Q3: What are the research gaps, research findings, and future recommendations presented by previous articles in the same domain?

This research includes both a scientific review and a bibliometric analysis. The rest of the paper is organized as follows: Section 4 explains the methodology covering the review protocol and defining search terms. Then, Section 5 presents the results and discussion, including descriptive, bibliometric, and meta-analysis. Finally, Section 10 concludes the paper.

4. THE METHODOLOGY OF SEARCH STRATEGY

This study developed a search strategy to find pertinent literature in a systematic way. This study used four databases: Web of Science, IEEE, Google Scholar, and Scopus. The first trial searching included the following search terms: "drone forensics" OR "forensics investigation". Then, the second one included "Drone forensics", "UAV", "Digital Forensics", and "Meta-model". The search performed for the purposes of this paper encompassed all in the English language. The time range was set to begin from the database's creation date to the beginning of 2024. This study mapped all the literature created on drone forensics in five domains: information systems, computer science, engineering, economics, and business [7].

Then, the search was confined to topics in computer science, Internet of Things (IOT), artificial intelligence, and information security. The criteria considered in the selection process were set in accordance to the PRISMA model [9, 10].

The search covered the articles published in 2018 to 2024 by researchers from different countries without any limitation. At the end of the selection process, 316 articles were extracted and saved in the form of Microsoft Excel CSV files. Figure 2 illustrates the way articles were included/excluded at each level using the PRISMA model.

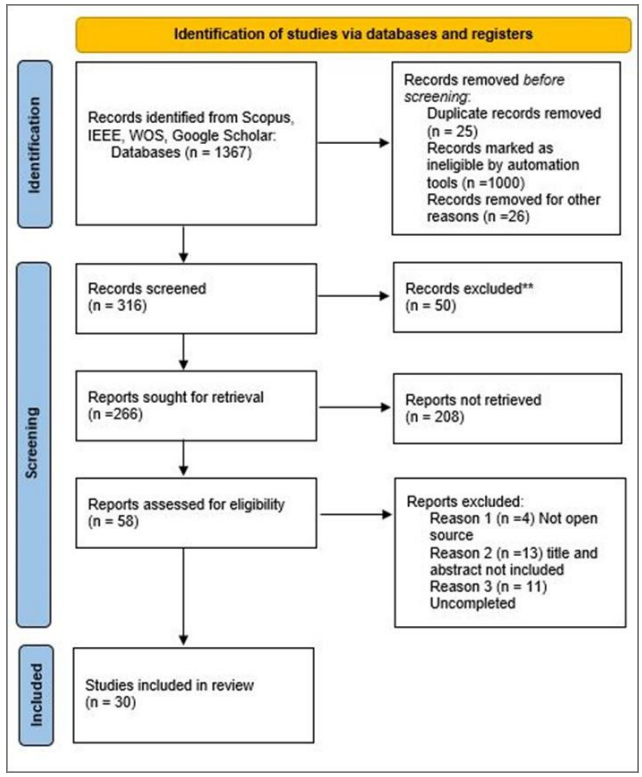

Figure 2. The (PRISMA) flowchart for including and excluding previous studies

The following details were collected from the 30 publications selected for the knowledge extraction phase:

(1) Research articles, reviews, and conference papers were included in the search for the present study.

(2) The search was limited to the articles written in the English language, on the interested domain in computer science, see Figure 3.

Several articles already published in the drone forensics domain have used the systematic literature review (SLR) as the method of their study [11]. These studies are not strictly laboratory-controlled; however, they can aid both researchers and practitioners in understanding the depth and breadth of the literature and also, they provide some useful facts in regard to the authors working in this domain, their findings, and the methodology they have used to achieve them. The present

research is specifically concentrated on the literature generated on the drone forensics and follows any military or civilian applications of drones. In recent years, many researchers, especially in the fields of law and ethics, computer science, and engineering have become interested in the topics related to drones. Since aerial vehicles are the most widely understood definition of drones, we will concentrate on them even though ground-based and maritime drones are also covered in the literature [12].

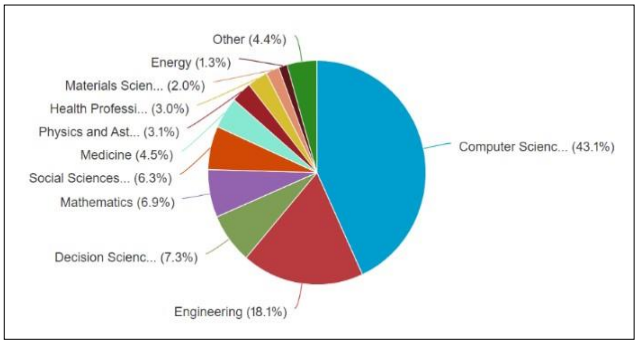

Figure 3. Document by subject area

5. RESULTS AND DISCUSSION

A wide range of results that reflected the variety of study focus contexts have been analyzed through bibliometric analysis. Many studies have provided evidence indicating that drone forensics continues to dominate the fields such as computer science and technical and engineering literature. Moreover, the results display the top ten (10) countries and regions and which countries that have high significant contribution, and the best articles contributed to the publication with highest citation of the related domain. Findings revealing differences in forensic processes may lead to initiatives to standardize methodologies. This would improve the interoperability of technologies and the reliability of forensic outcomes in legal contexts. Furthermore, drone forensics plays an important role in investigating illicit drone use. For example, forensic investigations were significant in the 2018 Gatwick Airport incident, in which drones halted hundreds of flights. The investigation produced tougher laws and enhanced drone-detecting technologies. In addition, results from forensic analysis can help terrorism prevention operations by revealing how drones are employed for illegal purposes.

5.1 Descriptive analysis

A descriptive analysis method utilizing a Microsoft excel pivot chart to identify high publications in related field reviews the findings. Figure 4 displays how drone forensics-related publications have evolved from 2018 to 2024. In this time period, the year 2024 has the lowest number of published articles, whereas 2021 demonstrates the largest number in this regard.

Table 1 gives specific information about the number of articles published in each year. Many of the articles on drone forensics have been resulted from a small number of sources. In addition, many of the analyzed articles indicated that drone forensics remains dominant in computer science and in both engineering and technical literature.

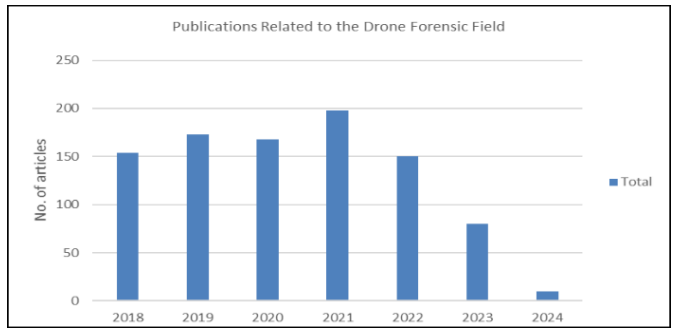

Figure 4. Publications related to the drone forensic field

Table 1. Number of articles published each year

Year	No. of Articles Per Year
2018	154
2019	173
2020	168
2021	198
2022	163
2023	80
2024	10
Grand Total	964

Figure 5 illustrates the contribution by country; it displays the top ten (10) countries and regions that contribute more. As can be seen, India has had more significant contribution, which is followed by the USA, UK, and Germany. From a continental perspective, regardless of the major contribution of India and USA, the varied efforts of Asian countries are also an obviously significant contribution.

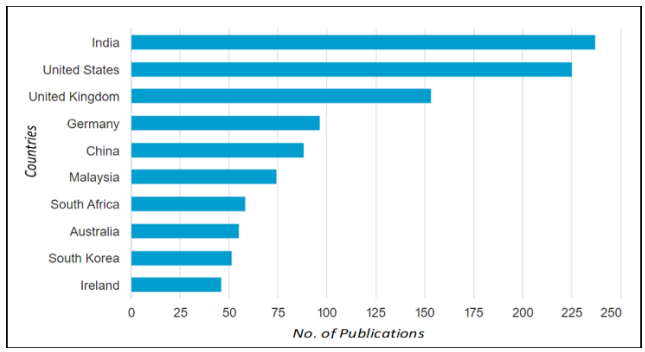

Figure 5. Countries contribution on relevant publications

Table 2 presents the key international journals that have shown interest in the publication of articles in regard to drones and drone forensics and also the number of articles already published by them.

Considering the frequency of being mentioned in others' studies can be an acceptable way to measure the significance of an article, an author, or a journal. Citation analysis is a method that could help in this case. The articles of highest citation frequency in a certain domain are typically written by the most proficient and well-known researchers of that domain. On the other hand, citation rates differ in different domains and older papers have had more chance of being cited than the articles published in more recent years. Therefore, these issues should be considered in the process of selecting most-cited articles. The initial step in the creation of distributions for each domain and year is to count the number of publications that have been cited at different levels of citation, see Table 3.

Table 2. The key international journals showing interest in publishing articles in the field of drone forensics

Resource Name	Sum of Publications
Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST	216
Procedia Computer Science	159
Digital Investigation	30
Sensors (Switzerland)	25
Electronics (Switzerland)	13
Internet of Things (Netherlands)	11

Table 3. Articles with highest citation

Title	Cited
Security analysis of drone's systems: Attacks, limitations, and recommendations [12]	145
The promising future of drones in prehospital medical care and its application to battlefield medicine [13]	45
Drone Forensics: Challenges and New Insights [14]	36
A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework [15]	36
Research challenges and opportunities in drone forensics models [16]	27
Drone forensic investigation: DJI spark drone as a case study [17]	24
Drone Forensics: A Detailed Analysis of Emerging DJI Models [18]	22
Design science research with focus groups – a pragmatic meta-model [19]	18
Drone Forensics: Digital Flight Log Examination Framework for Micro Drones [20]	12
Drone forensics: A case study on DJI phantom 4 [21]	12
GRYPHON: Drone Forensics in Data flash and Telemetry Logs [22]	12
Open-source forensics for a multi-platform drone system [4]	12
A comparative UAV forensic analysis: Static and live digital evidence traceability challenges [23]	10
Drone Forensics and Machine Learning: Sustaining the Investigation Process [24]	9
A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field [25]	9
Towards Development of a High Abstract Model for Drone Forensic Domain [26]	8
Towards a better understanding of drone forensics: A case study of parrot AR drone 2.0 [27]	8
Comprehensive Review of Drones Collision Avoidance Schemes: Challenges and Open Issues [28]	7
Transformer-Based Named Entity Recognition on Drone Flight Logs to Support Forensic Investigation [29]	7
Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models [30]	7
Drone Forensics: A Case Study on DJI Mavic Air 2 [31]	6
DFLER: Drone Flight Log Entity Recognizer to support forensic investigation on drone device [32]	6
Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology [33]	5
Digital Forensic Research for Analyzing Drone Pilot: Focusing on DJI Remote Controller [34]	4
Drone a technological leap in health care delivery in distant and remote inaccessible areas: A narrative review [35]	3
A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field [36]	2
Risks of Drone Use in Light of Literature Studies [37]	2

5.2 Bibliometric analysis

The 120 researchers of the evaluated papers represent a wide range of participants in terms of their contributions and potential for thought leadership. Top Authors in Related Research (Choo K.) have a high cited 673 citations [38], (Kebande V.) have 314 citations [39], while (Shalaginov A. and Iqbal F.) have low cited 104 and 106 citations [40]. Previous systematic reviews of other areas have demonstrated no apparent significant clustering of authors. There were four clusters, each represented by various colors, and were created by citation of the referenced authors. Table 4 illustrates the publications clearly related to each other from the same research activity, except for a few author pairs or group combinations.

The network visualization mapping process uses VOS viewer which is divided into 5 clusters: The yellow cluster is the largest, shows the work of one highest cited author (Choo K.), The purple cluster is the second largest cluster including two authors (Kebande V. and Venter H.), these are considered the most well-known authors in all clusters. The third largest cluster are represented in blue contains the lower citation under the author's name (Iqbal F.) as shown in Figure 6. Generally, these clusters are similar in research areas, although the publications focused on different issues.

Table 4. Top authors in related research areas

Authors	Citations
Choo K.	648
Kebande V.	285
Zawoad S.	270
Venter H.	200
Le-khac N.	184
Scanlon M.	180
Martini B.	155
Al-dhaqm A.	140
Li S.	116
Venter H.	111
Shalaginov A.	106
Iqbal F.	104

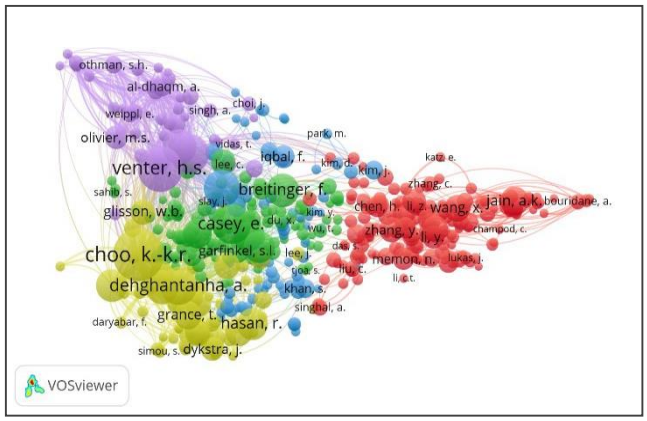

Figure 6. Network visualization of cited authors

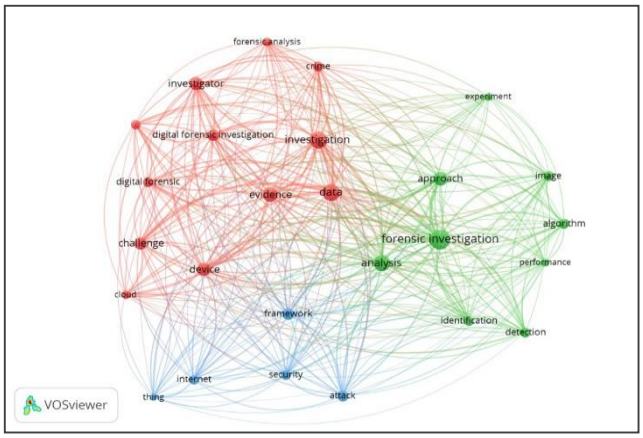

Figure 7. Map based on keyword analysis (title and abstract)

Figure 7 presents the analytic results of 163 keywords among which 30 keywords have been used only once and 138 non-essential terms or keywords didn't accurately describe the problem (e.g., "social informatics", "cloud environment", and "virtual machine"). Additionally, it produced equally wide-ranging and diverse results that reflected the variety of study focus contexts (e.g., Drone forensics, digital forensics, and forensics investigation).

6. ARTICLES QUALITY EVALUATION

In a study based on the systematic literature review (SLR), it is important to evaluate the quality of relevant primary studies. This procedure attempted to filter out studies that are conceptually irrelevant and evaluate the quality of the research studies [41]. The studies have been reviewed to provide answers to our research questions and to ascertain the validity of the research [42]. The following questions include criteria for quality evaluation of metamodeling-based drone forensic investigation research. Table 5 summarizes the conclusions of the analysis.

(1) Does the study provide a clear description of the research issue?

(2) Was the data analysis in the study sufficient for the researchers?

(3) Did the main goal of the research meet with achievement?

(4) Was there a comparison between the study's findings with the results of previous studies?

(5) Were the conclusions sufficient for the researchers

Therefore, if a primary study's mean score is below 4, it was disqualified. This stage was carried out by several authors, and any disagreements over the quality of the study were settled.

Table 5. Quality evaluation of primary studies

Articles	Q1	Q2	Q3	Q4	Q5	Score
[29]	√	√		√	√	4
[43]	√	√	√	√	√	5
[19]	√	√	√	√	√	5
[21]	√	√	√	√	√	5
[44]	√		√	√	√	4
[26]	√	√	√	√	√	5
[45]	√	√	√	√		4
[46]	√	√		√	√	4
[47]	√	√	√	√	√	5
[48]	√	√	√	√	√	5
[24]		√	√	√	√	4
[12]	√	√	√	√	√	5
[49]	√	√	√	√	√	5
[30]	√	√		√	√	4
[4]	√	√	√	√		4
[12]	√	√	√		√	4
[26]	√	√	√	√	√	5
[21]	√	√	√	√	√	5
[17]	√	√	√	√	√	5
[45]	√	√	√	√	√	5
[15]	√	√		√	√	4
[3]	√	√	√		√	4
[4]	√	√		√	√	4
[50]	√	√	√	√	√	5
[51]	√	√	√	√	√	5
[52]	√	√	√	√	√	5
[28]	√	√	√	√	√	5
[33]	√	√	√		√	4
[37]	√	√	√	√		4
[7]	√	√	√	√		4
[1]	√	√	√	√	√	5

(√) Fulfil questions for primary studies

7. DATA SYNTHESIS

This section delivers the data extracted in table form for synthesis and data visualization. Table 6 lists the publications for the chosen primary studies along with some vital information.

Table 6. Quality evaluation of primary studies

Name	No. of Studies	Published by	Impact Factor
Sensors (Switzerland)	3	MDPI	3.847
Forensic Science International: Digital Investigation	1	Elsevier	1.805
International Journal of Digital Crime and Forensics	2	IGI Global	0.921
Digital Investigation	2	Elsevier	2.192
Applied Sciences (Switzerland)	1	MDPI	2.679
Sustainability (Switzerland)	1	MDPI	4.17
Electronics (Switzerland)	3	MDPI	3.022
Internet of Things (Netherlands)	1	Elsevier	8.35
Procedia Computer Science	1	Elsevier	0.883
Safety Science	1	Elsevier	6.1

Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering	1	Springer	0.345
Journal of Information Science	1	ACM	3.282
Infrastructures (Switzerland)	1	MDPI	2.98
International Journal of Advanced Computer Science and Applications	1	SAI	1.30
PLoS ONE (USA)	1	PLoS ONE	0.852
The Journal of Digital Forensics, Security and Law	1	JDFSL	2.762
Journal of Information Science	1	ACM	2.4
Software Impacts	1	Elsevier	2.23
Journal of Computer Science	1	Elsevier	2.27
Drones (Switzerland)	1	MDPI	4.8
Engineering, Technology and Applied Science Research	1	Elsevier	1.5
Technologies (Switzerland)	1	MDPI	3.6
Production Engineering	1	Springer	1.7
Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies	1	ACM	4.96
International Journal of Managing Projects in Business	1	Emerald	3.91
IEE Access Journal	3	IEEE	3.9
10th International Symposium on Digital Forensics and Security	1	IEEE	N/A
11th Annual Computing and Communication Workshop and Conference	1	IEEE	N/A
11th International Conference on Information and Communication Systems	1	IEEE	N/A
International Conference on Computer Systems and Applications	1	IEEE	N/A
9th International Conference on New Technologies, Mobility and Security	1	IEEE	N/A

8. CURRENT CHALLENGES

In recent years, drones have emerged as revolutionary tools in military, civilian, medicine, biomedical research, and healthcare, building on these initial challenges, the intricacies of drone forensics in these fields are further compounded by multifaceted regulatory environments [43]. Standardization is essential for the incorporation of drone-collected data (such as photos, sensor data, or log files) into current electronic health record systems. Data formats, timestamps, and communication protocols need to be compatible with traditional medical systems. On the other hand, compatibility with conventional medical systems is required for data formats, timestamps, and communication protocols [44]. According to previous study [45], as the utilization of drones becomes more prevalent in these fields, there arises a critical need for sophisticated forensic analysis techniques. The lack of standardized protocols exacerbates this issue, making it difficult to ensure uniformity across various applications.

A forensic investigation may find that the tangible evidence for a UAV, e.g., a drone, radio controls, and server, could be found scattered in the scene. In addition, it is not easy to prove the ownership of a confiscated drone [46]. The vast variety of digital containers engaged in a certain UAV flight will cause difficulty in using one forensic tool for retrieving all the data required for a forensic examination. Sometimes, attaining a forensic image of the content of a drone camera without compromising its integrity is difficult, or even impossible [47].

As a result, in order to conduct a remote forensic imaging procedure, forensic investigators need to use wireless connectivity [48]. Numerous embedded data storage containers are available, some of which are hidden or have access controls, making it difficult for the investigator to obtain digital evidence and provide a source for forensic equipment for example, the flight controller microchip stores recorded flight data [49].

Additionally, as mentioned in possible access restrictions, it might not be able to include the content and files of operating system in the forensic image [50]. A UAV aircraft may have more than five different file system types on it, some of which are impossible for commercial forensic tools to identify at this time [51].

Forensic investigators and law enforcement agencies would probably not be able to access the remote controller, but in many cases, the on-board flight controller component needs specific owner's permission to access the flight data through the remote controller. Moreover, flight data extracted from the flight control system device is frequently encrypted.

Thus, forensic investigation becomes more complex when the remote controller is absent [52]. A big challenge is that drones have a considerable dependency on volatile memory, and the already-saved flight data is deleted when the device runs out of battery. Moreover, some sensing data are sharable on file-sharing websites or social media; these dates are typically transferred to a cloud-based platform that is based on a secure server [53]. Nevertheless, all commercial UAVs do not have data logging configured into their flight controls [54].

Considering the literature's generally low level of consideration, there is a great deal of potential for engaging research into drone control. However, the primary area of future study that we think is important is how the drone forensics investigation should be conducted generally [55]. There are still many issues that need to be resolved, including the potential for drone flight to become just as common as that of other vehicles and their potential use in forensic investigations.

9. RESEARCH GAP

Based on the results of analyzing the studies in this paper, the drone forensics field is still immature; must-be-resolved problems in this domain have not been well understood yet and also the relevant literature still lacks reliable techniques for investigating drones under forensic conditions [56]. Another problem in this field is that there is no a standardized forensic framework. Consequently, according to [57], there is no proactive forensic perspective. In addition, significant issues have still remained unsolved, for instance, the absence of

structured procedures and consistent automated methodologies in this domain [58].

The development of a weakness conceptual framework could have positive effects on the evidence's credibility and validity when a criminal issue occurs [59]. This article made an analysis on the currently used metamodeling development methods. The findings indicated that digital forensics still suffers from uncertain methods for the development of meta-models [60]. Table 7 illustrates the gap of research with the future recommendation and finding for thirty (30) articles in the domain of our study.

Table 7. Research gap, finding and future recommendation

Ref.	Research Gap	Finding	Future Recommendation
[13]	Drones' current and potential use in (civilian/military) medicine, as well as their acceptability and utility for prehospital patient care, are subject to several limitations, private data may be exposed by drones transporting patient samples or medical records.	Prehospital medicine and healthcare are definitely about to undergo a change because to drone technology. Its exceptional capabilities allow for the rapid delivery of vital, life-saving medical care to isolated outposts and locations where access is restricted due to hostile or natural disasters.	The worldwide scope of drone-based healthcare delivery demands highlights the necessity for international cooperation between the military and civilian medical sectors to use the resources that are now available as well as new and developing technology for greater lifesaving potential.
[29]	According of this study, no investigation of the evidence against the flight logs, specifically the human-readable message in the flight records, had been conducted.	An encrypted set of flight log files was utilized to produce a forensic report that included a timeline highlighting the locations of the entities mentioned in the log files.	Forensic investigators can identify important events on the created forensic timeline by using the researcher's strategy to add more data to make the tools more generic.
[19]	There is a need to support the various DSR stages, and this can be done by filling the research gap in practical applications by creating a DSR meta-model.	A unique meta-model for DSR that provides fresh perspectives and practical guidelines for professionals and academics carrying out and recording real-world research and development projects rooted in stakeholder participation.	A software platform that can assist a project team in better managing the entire DSR process, particularly about model retesting, will be beneficial to the artifact, improvement, and refinement, benefiting from its applicability to diverse contexts and circumstances.
[23]	Drone systems do not meet the baseline security standards, cheap development in an evolving technology leads to the formation of systems with lower secure.	This study emphasizes the value of protecting data while it is in use, in motion, and at rest. To strengthen the integrity of data, communication lines, another security risk, should be ciphered.	Analyzed several situations, including attack vectors connected to UAVs operating in untethered modes. Examined technical issues with data integrity and suggested a forensically valid method for conducting UAV forensic investigations.
[35]	The implementation of drone technology into medical systems faces the challenge of integrating and adapting data received and processed by drones with current standard medical systems, these are important issues that must be resolved.	The researchers emphasize how drones have the potential to completely transform the delivery of healthcare, especially in difficult and isolated locations. When road transportation is challenging or time-consuming, drones provide a practical and economical substitute for delivering medical supplies, vaccines, and other necessities.	Collaborate with drone operators and provide security standards, create regulatory frameworks, and encourage drone technology research and development, governments, academic institutions, healthcare providers.
[47]	From the perspective of completeness, the suggested model is validated by comparison with the methodology of another model.	Using reliable forensic techniques, the study's proposed method allows domain users to collect, store, reconstruct, and evaluate metadata about suspect drones that is volatile and non-volatile.	A practical CCAFM implementation is should be developed to examine the effectiveness of the developed model in the collection, preservation, and analysis of drone-related events.
[44]	It is not easy to find the data necessary for linking drone to a GCS. The majority of drones tend to preserve their logging functionality or configuration files in their internal memories in such a way that the user cannot modify them.	A high-level framework that provides recommendations for potential encounters and things to look for has been integrated with a few devices.	To improve drone device security, drone manufacturers should incorporate logging of user metadata into the drone's log files.
[23]	The lack of trustworthy drone forensics investigation methods and findings, as well as the incomplete knowledge of the issues that need to be resolved, show that drone forensics research is still in early stage.	Their analyses offer fresh insights into the field of drone forensics. They include the ability to retrieve the controller's	There is a need for forensically examining the components and controllers of a UAV and those of other UAVs to see the differences among damaged drones.
[45]	A technical challenge for the forensic investigation is the DAT file that contains the current encrypted flight data.	Their findings were obtained through examining the open File Transfer Protocol (FTP) channel and removing data from the storage card of a drone.	These DJI Mavic drone models may also be the subject of future forensic investigations.
[46]	It is difficult to find a drone's actual owner, particularly when it is left at the scene of crime.	UAVs are being increasingly popular, which could be accompanied by the increase of their illegal use, too. We have to wait to see the impacts UAVs will have upon digital forensics.	Data from numerous manufacturer devices will continue to be analyzed and presented in future work, for example, comparing drone forensics with mobile forensics and the challenges that may come to exist owing to the accessibility of so various devices.

[21]	The lack of a standardized forensic framework that can be applied effectively to each of the branches considered and the absence of a proactive forensic perspective.	The developed DRFRF framework was validated by comparing it with other models. preparedness. This study adopted the metamodeling approach and used the DSR methodology to provide a framework for drone forensic preparedness.	To show the efficacy of the suggested DRFRF in an actual scenario, the focus of this research's upcoming work will be on implementing the DRFRF.
[48]	The susceptibility of drones to cyberattacks is hazardous since when a drone gets compromised, its flight could be changed and also its collected data could be damaged.	Many observations were made during the flight, and these observations required automated and thoughtful analysis. GMM and K-Means algorithms were used to analyze drone data to find for unusual events and flight paths.	Machine learning could be applied to forensic data analysis, and such datasets could be created that can depict the cyberattacks launched against drones.
[49]	Data flow and design make UAV detection and forensics approaches challenging. The anti-detection and anti-forensic techniques developed for UAVs are affected by data flow and UAS architecture.	They investigated cyber risk issues in UAV forensics, defined different UAV assault scenarios, and presented several new UAS architecture-related methodologies to simplify the process of identifying the evidence.	Assessing the security threats related to different communication protocol types, and expanding the research by examining different control, data, and frequency channels and analyzing data that utilize an unencrypted channel.
[30]	Developing digital forensic analysis techniques in real-time with drones used for criminal activity is clearly necessary since the digital forensics field lacks reliable techniques for the identification of a UAV's owner.	The authors discover Certain UAVs might be able to save owner data in order to identify the devices that are used for controlling the drone and record flight data, However, some drones that are less expensive might not have this feature, in which case the media file is the only thing that can be extracted from the drone.	In the future, this data will be gathered, and explicit process models for investigative techniques and protocols will be created, taking into consideration the constraints discovered during research, including media ownership, encrypted data, and device state.
[4]	Drones' documentation and knowledge and the proprietary file systems are limited. And there is a lack of certain technologies for drone forensics analysis, which could assist the processes of forensic investigations.	Because of higher levels of security, most of the recently developed drone models can hardly be examined. And drones tend to operate with similar operating systems and file system standards, with a bit variation in data generated by each model.	There is a need for investigating more drone models developed by various manufacturers and used by various users. And different case studies are required to be examined in a way to involve the unlawful use of drones, considering the varied nature of forensic evidence attained using new techniques of forensic examination.
[12]	Mini drones could be simply piloted with smartphones, with no need for any remote control. This ease of use is for not only authorized parties, but also for unauthorized ones.	An entirely new era of autonomous UAV in both the military and civilian domains was brought about by the dramatic increase in the use of drones, outlined their use in different domains and for different purposes in detail.	Due to the worrying rise in the use of drones by terrorists, more study will be carried out on the best way to combat and prevent the UAV threats posed by terrorists.
[26]	The field is unclear and complicated because of the multiple infrastructure-based networks and operating systems and different standards. There is not a general paradigm applicable to managing, sharing, or reusing the activities and processes of the drone forensics field.	Drone forensics suffers from a number of issues making its understanding difficult for forensic specialists. To solve the heterogeneity and interoperability issues in the drone forensics domain, this research created the drone forensics meta model.	Future work may concentrate on creating a repository for the proposed DRFM for the purpose of storing all relevant data regarding the DRF field and confirm the suggested DRFM's completeness, effectiveness, and logicalness after the horizontal transformation.
[21]	In numerous cases of privacy invasion, data persistence may be a problem because it is less certain where the data originated from and is stored. It was found that a drone was flying across a military base.	It provided a complete forensic analysis for drones and also for the storage backup of phone devices through investigating the drone-related data.	Further research into the DAT and TXT file structures ought to be done in the future. Further research is also planned to design image processing tools capable of taking multimedia files as input and then producing reports using the processed data and metadata.
[33]	The challenges relate to gathering, analyzing, and preserving data from drones, particularly how to handle the different kinds of data that drones can store, like images and videos.	Digital twin technology, which is the foundation of the solution, is one of the technologies that is significantly influencing a number of industries and sectors, including industry and healthcare. The digital twin solution includes the simulation's implementation.	It provides a basis for research in this area and its application to drone digital forensic investigations. In the future, researchers plan to assess DTT's usefulness in a digital forensic investigation by applying it to the test in an actual case scenario.
[45]	There is still a need for developing proper methods for locating and producing proof of illegal drones. In addition, owing to the existence of varied types of drones, the process of extracting data from these devices is difficult.	Because of the weaknesses of the tools applied to the extraction and analysis of data, the authors failed to explore any TXT or DAT files in the internal memories experimented.	To locate the files or any other relevant information that could be helpful in a forensic investigation it would be beneficial to use established forensic techniques to investigate the remote controller and internal storage.
[15]	The surge in the use of UAVs has caused many security concerns. Drones,	This study maps the flight path with the use of Google Maps according to the author and	In the future, the application must be able to detect whether a flight is incomplete due to

	thank to their nature, are open to being used both inappropriately and unlawfully.	has multiple tabs to view various flight data at once. The API key required to use Google Maps is contained in the HTML file.	crashes, like crashing into an unanticipated wall or tree, to predict the entire flight path, a trajectory prediction model will be constructed using time series forecasting.
[28]	The challenges include limited environmental understanding, security concerns, expensive machine learning and automation costs, accurate detection of small and moving impediments, minimizing path deviations at min.	To effectively predict drone crashes, several crucial factors need to be considered. Using global algorithms for integration can aid in overcoming these difficulties.	To ensure efficacy and establish trust, it is imperative to develop more complex simulators that faithfully mimic real-world circumstances and to test and evaluate proposed algorithms in real test environments.
[57]	The literature was found to have gaps, and empirical research that may help optimize this crucial initial stage of the inquiry process was also needed.	It showed that the information gathering stage is mostly diverse, adhering to the particular circumstances of the incidents within the domain.	Future research is advised to retain the essential specifics of many sectors by concentrating on refining and strengthening information gathering for drone incident investigations inside particular domains.
[50]	There is a gap between domain-specific ontologies and heterogeneous data. And the majority of the currently used data extraction meta-models either are domain-specific or have inadequate information.	A significant amount of data and associated knowledge are irrelevant to the field of interest in the theoretical scenarios aiming to, for instance, gather all accessible web data.	It is recommended that prior to the use of data from the framework and extraction of pertinent sources of data, techniques such as keyword extraction and document clustering should be used.
[51]	The study performed a comparative analysis of different methodologies for metamodeling development, which are currently used.	The proposed approach outperformed the others in the modeling of any complicated knowledge domain.	It recommends that a semantic metamodeling language should be created for the digital forensics field for the purpose of enabling, organizing, unifying, and sharing it across domain users.
[49]	The literature lacks a face validity-based technique that can guarantee the applicability of produced DBFIM to the DBFI area.	The face validity approach can determine the rationality and compatibility of meta-models.	The use of DBFIM in real-life situations to make sure of its applicability to crimes.
[52]	The field of forensics investigation is currently afflicted by serious issues, such as a lack of organized processes, a lack of uniform automated methodologies, and an absence of conceptual organization.	The increasing use of smart technologies has led to an increase in the cybercrime crime rates and the development of anti-forensic methods.	They recommend the future authors that they validate Meta-model using two key processes in meta-model validation: techniques for frequency-based selection validation and comparison to other models.
[11]	The digital forensics field lacks knowledge management. Novice investigators have difficulties when doing an investigation. And the terms and concepts employed in this field are not of high clarity.	This study found out different challenges and difficulties that the field of digital forensics is still suffering from, for example, the absence of knowledge management.	It is necessary to develop a unified model on the basis of a meta-model for storing the knowledge generated in the digital forensics field and also to propose a methodology of high responsiveness and flexibility.

10. CONCLUSION

The present paper used the SLR method to investigate the drone forensics literature. An analysis was then performed on the findings on the basis of the application, collaboration, implementation, and maturity levels of the previously conducted research in this field. The findings showed the relative low number of publications on the applying UAVs to the field of digital forensics. Therefore, it is still necessary to re-analyze and develop drone forensics solutions that can open new doors to research in this domain. The paper also provided actionable suggestions considering the analytical results, which highlight the areas in need of further research. These suggestions were also based on the analysis of data compiled in the literature regarding various drones. The methodology offered in this study greatly improves the field of drone forensics by providing a unified and structured approach to data extraction, evidence analysis, and traceability. The contributions of this paper not only enhance the ability of investigators to uncover critical insights from drones but also establish a robust and unified framework for addressing emerging challenges in this rapidly evolving domain, also emphasizes the importance of interdisciplinary collaboration.

Furthermore, law enforcement, forensic investigators, technology developers, and academics must collaborate to address challenges. The practical applications improve public safety, increase accountability, and allow for the responsible development of drone technologies.

Accordingly, the present study was concentrated on practical use of an integrated drone forensic model. By using a software engineering strategy, i.e., a meta-model, this paper attempted to analyze the concepts and relationships that existed in each of the analyzed drone forensics. In this process, it also used systematic reviews and meta-analysis (PRISMA). The application of metamodeling causes a domain to become homogeneous, with less complexity. As a result, meta-models and models are needed to be defined precisely and organized appropriately.

11. RECOMMENDATIONS FOR FUTURE RESEARCH

As UAVs are increasingly applied to various civilian, military, medicine, and healthcare missions, the desire to collect and analyze more data for drone forensics from multiple perspectives and for different objectives is increasing, too. Moreover, interdisciplinary collaboration among

technologists, healthcare providers, forensics experts, and policymakers is crucial for developing innovative solutions that maximize the benefits of drone technology while mitigating risks. As the present research highlighted the challenges and the actions taken to overcome them, it could provide a proper guide for other researchers working in this field. The conclusion of every research provides chances to look further ahead of its time.

Additionally, this research recommends building a semantic metamodeling language for the drone forensics domain to simplify, coordinate, standardize, and encourage reuse across domain users, in parallel with AI-driven enhancements and ethical legislative structures to create a cohesive and adaptive framework for drone forensics. Only through such comprehensive efforts can this field not only keep pace with technological progress but also maintain public trust in its applications.

ACKNOWLEDGMENT

The authors would like to acknowledge the Ministry of Higher Education Malaysia and the Universiti Teknologi Malaysia (Vote: R.J130000.7851.5F566) for funding this research under the Fundamental Research Grant Scheme (Grant No.: FRGS/1/2022/ICT07/UTM/02/1).

REFERENCES

[1] Li, Z., Chen, B., Chen, X., Xu, C., Chen, Y., Lin, F., Li, C., Dantu, K., Ren, K., Xu, W. (2022). Reliable digital forensics in the air: Exploring an RF-based drone identification system. Proceedings of The ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 6(2): 1-25. https://doi.org/10.1145/3534598

[2] Alotaibi, F.M., Al-Dhaqm, A., Al-Otaibi, Y.D., Alsewari, A.A. (2022). A comprehensive collection and analysis model for the drone forensics field. Sensors, 22(17): 6486. https://doi.org/10.3390/s22176486

[3] Atkinson, S., Carr, G., Shaw, C., Zargari, S. (2021). Drone Forensics: The Impact and Challenges. In: Montasari, R., Jahankhani, H., Hill, R., Parkinson, S. (eds) Digital Forensic Investigation of Internet of Things (IoT) Devices. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-60425-7_4

[4] Barton, T.E.A., Azhar, M.H.B. (2018). Open source forensics for a multi-platform drone system. In Digital Forensics and Cyber Crime: 9th International Conference, ICDF2C 2017, Prague, Czech Republic, October 9-11, 2017, Proceedings. Springer International Publishing. Springer, Cham, 9: 83-96. https://doi.org/10.1007/978-3-319-73697-6_6

[5] Mantas, E., Patsakis, C. (2022). Who watches the new watchmen? The challenges for drone digital forensics investigations. Array, 14: 100135. https://doi.org/10.1016/j.array.2022.100135

[6] Candel, C.J.F., Ruiz, D.S., García-Molina, J.J. (2022). A unified metamodel for NoSQL and relational databases. Information Systems, 104: 101898. https://doi.org/10.1016/j.is.2021.101898

[7] Sinnemann, J., Boshoff, M., Dyrska, R., Leonow, S., Mönnigmann, M., Kuhlenkötter, B. (2022). Systematic literature review of applications and usage potentials for the combination of unmanned aerial vehicles and mobile robot manipulators in production systems. Production Engineering, 16(5): 579-596. https://doi.org/10.1007/s11740-022-01109-y

[8] Alquwayzani, A.A., Albuali, A.A. (2024). A systematic literature review of zero trust architecture for UAV security systems in IoBT. Computer Scient and Mathematics, 1(1): 1-33. https://doi.org/10.20944/preprints202403.0349.v1

[9] Merkert, R., Bushell, J. (2020). Managing the drone revolution: A systematic literature review into the current use of airborne drones and future strategic directions for their effective control. Journal of Air Transport Management, 89: 101929. https://doi.org/10.1016/j.jairtraman.2020.101929

[10] Yang, L., Zhang, H., Shen, H., Huang, X., Zhou, X., Rong, G., Shao, D. (2021). Quality assessment in systematic literature reviews: A software engineering perspective. Information and Software Technology, 130: 106397. https://doi.org/10.1016/j.infsof.2020.106397

[11] Othman, S.H., Al-Dhaqm, A. (2024). An improved machine learning method by applying cloud forensic meta-model to enhance the data collection process in cloud environments. Engineering, Technology & Applied Science Research, 14(1): 13017-13025. https://doi.org/10.48084/etasr.6609

[12] Yaacoub, J.P., Noura, H., Salman, O., Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, 11: 100218. https://doi.org/10.1016/j.iot.2020.100218

[13] Braun, J., Gertz, S.D., Furer, A., Bader, T., Frenkel, H., Chen, J., Glassberg, E., Nachman, D. (2019). The promising future of drones in prehospital medical care and its application to battlefield medicine. Journal of Trauma and Acute Care Surgery, 87(1S): S28-S34. https://doi.org/10.1097/TA.0000000000002221

[14] Bouafif, H., Kamoun, F., Iqbal, F., Marrington, A. (2018). Drone forensics: Challenges and new insights. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, IEEE, pp. 1-6. https://doi.org/10.1109/NTMS.2018.8328747

[15] Renduchintala, A., Jahan, F., Khanna, R., Javaid, A.Y. (2019). A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework. Digital Investigation, 30: 52-72. https://doi.org/10.1016/j.diin.2019.07.002

[16] Al-Dhaqm, A., Ikuesan, R.A., Kebande, V.R., Razak, S., Ghabban, F.M. (2021). Research challenges and opportunities in drone forensics models. Electronics, 10(13): 1519. https://doi.org/10.3390/electronics10131519

[17] Kao, D.Y., Chen, M.C., Wu, W.Y., Lin, J.S., Chen, C.H., Tsai, F. (2019). Drone forensic investigation: DJI spark drone as a case study. Procedia Computer Science, 159: 1890-1899. https://doi.org/10.1016/j.procs.2019.09.361

[18] Yousef, M., Iqbal, F., Hussain, M. (2020). Drone forensics: A detailed analysis of emerging DJI models. In 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, IEEE, pp. 66-71. https://doi.org/10.1109/ICICS49469.2020.239530

[19] Henriques, T.A., O'Neill, H. (2023). Design science research with focus groups–a pragmatic meta-model.

International Journal of Managing Projects in Business, 16(1): 119-140. https://doi.org/10.1108/IJMPB-01-2020-0015

[20] Renduchintala, A.L.S., Albehadili, A., Javaid, A.Y. (2017). Drone forensics: Digital flight log examination framework for micro drones. In 2017 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, IEEE, pp. 91-96. https://doi.org/10.1109/CSCI.2017.15

[21] Iqbal, F., Alam, S., Kazim, A., MacDermott, Á. (2019). Drone forensics: A case study on DJI phantom 4. In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, pp. 1-6. https://doi.org/10.1109/AICCSA47632.2019.9035302

[22] Mantas, E., Patsakis, C. (2019). GRYPHON: Drone forensics in dataflash and telemetry logs. In Advances in Information and Computer Security: 14th International Workshop on Security, IWSEC 2019, Tokyo, Japan, Proceedings. Springer International Publishing. Springer, Cham, 14: 377-390. https://doi.org/10.1007/978-3-030-26834-3_22

[23] Salamh, F.E., Karabiyik, U., Rogers, M.K., Matson, E.T. (2021). A comparative UAV forensic analysis: Static and live digital evidence traceability challenges. Drones, 5(2): 42. https://doi.org/10.3390/drones5020042

[24] Baig, Z., Khan, M.A., Mohammad, N., Brahim, G.B. (2022). Drone forensics and machine learning: Sustaining the investigation process. Sustainability, 14(8): 4861. https://doi.org/10.3390/su14084861

[25] Alotaibi, F.M., Al-Dhaqm, A., Al-Otaibi, Y.D. (2022). A novel forensic readiness framework applicable to the drone forensics field. Computational Intelligence and Neuroscience, 2022(1): 8002963. https://doi.org/10.1155/2022/8002963

[26] Alhussan, A.A., Al-Dhaqm, A., Yafooz, W.M., Razak, S.B.A., Emara, A.H.M., Khafaga, D.S. (2022). Towards development of a high abstract model for drone forensic domain. Electronics, 11(8): 1168. https://doi.org/10.3390/electronics11081168

[27] Bouafif, H., Kamoun, F., Iqbal, F. (2020). Towards a better understanding of drone forensics: A case study of parrot AR drone 2.0. International Journal of Digital Crime and Forensics (IJDCF), 12(1): 35-57. https://doi.org/10.4018/IJDCF.2020010103

[28] Rezaee, M.R., Hamid, N.A.W.A., Hussin, M., Zukarnain, Z.A. (2024). Comprehensive review of drones collision avoidance schemes: Challenges and open issues. IEEE Transactions on Intelligent Transportation Systems, 25(7): 6397-6426. https://doi.org/10.1109/TITS.2024.3375893

[29] Silalahi, S., Ahmad, T., Studiawan, H. (2023). Transformer-based named entity recognition on drone flight logs to support forensic investigation. IEEE Access, 11: 3257-3274. https://doi.org/10.1109/ACCESS.2023.3234605

[30] Al-Room, K., Iqbal, F., Baker, T., Shah, B., Yankson, B., MacDermott, A., Hung, P.C. (2021). Drone forensics: A case study of digital forensic investigations conducted on common drone models. International Journal of Digital Crime and Forensics (IJDCF), 13(1): 1-25. https://doi.org/10.4018/IJDCF.2021010101

[31] Lan, J.K.W., Lee, F.K.W. (2022). Drone forensics: A case study on DJI Mavic air 2. In 2022 24th International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea, Republic of, IEEE, pp. 291-296. https://doi.org/10.23919/ICACT53585.2022.9728844

[32] Silalahi, S., Ahmad, T., Studiawan, H. (2023). DFLER: Drone flight log entity recognizer to support forensic investigation on drone device. Software Impacts, 15: 100457. https://doi.org/10.1016/j.simpa.2022.100457

[33] Almusayli, A., Zia, T., Qazi, E.U.H. (2024). Drone forensics: An innovative approach to the forensic investigation of drone accidents based on digital twin technology. Technologies, 12(1): 11. https://doi.org/10.3390/technologies12010011

[34] 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

[35] Sharma, S., Sharma, H. (2024). Drone a technological leap in health care delivery in distant and remote inaccessible areas: A narrative review. Saudi Journal of Anaesthesia, 18(1): 95-99. https://doi.org/10.4103/sja.sja_506_23

[36] Alotaibi, F., Al-Dhaqm, A., Al-Otaibi, Y.D. (2023). A conceptual digital forensic investigation model applicable to the drone forensics field. Engineering, Technology & Applied Science Research, 13(5): 11608-11615. https://doi.org/10.48084/etasr.6195

[37] Tubis, A.A., Poturaj, H., Dereń, K., Żurek, A. (2024). Risks of drone use in light of literature studies. Sensors, 24(4): 1205. https://doi.org/10.3390/s24041205

[38] Zhang, X., Liu, C.Z., Choo, K.K.R., Alvarado, J.A. (2021). A design science approach to developing an integrated mobile app forensic framework. Computers & Security, 105: 102226. https://doi.org/10.1016/j.cose.2021.102226

[39] Karie, N.M., Kebande, V.R., Venter, H.S., Choo, K.K.R. (2019). On the importance of standardising the process of generating digital forensic reports. Forensic Science International: Reports, 1: 100008. https://doi.org/10.1016/j.fsir.2019.100008

[40] Shalaginov, A., Kotsiuba, I., Iqbal, A. (2019). Cybercrime investigations in the era of smart applications: Way forward through big data. In 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, pp. 4309-4314. https://doi.org/10.1109/BigData47090.2019.9006596

[41] Gordienko, Y., Rokovyi, O., Alienin, O., Stirenko, S. (2022). Context-Aware data augmentation for efficient object detection by UAV surveillance. In 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, IEEE, pp. 1-6. https://doi.org/10.1109/ISDFS55398.2022.9800798

[42] Yan, L., Mir, M., Sanchez, P., Beg, M., Peters, J., Enriquez, O., Gilbert, A. (2020). COVID-19 in a hispanic woman: Autopsy report with clinical-pathologic correlation. Archives of Pathology & Laboratory Medicine, 144(9): 1041-1047. https://doi.org/10.5858/arpa.2020-0217-SA

[43] Ameerbakhsh, O. (2023). Semantic forensic investigation framework for drone field. Journal of Computer Science, 19(2): 212-228. https://doi.org/10.3844/jcssp.2023.212.228

[44] Thornton, G., Zadeh, P.B. (2022). An investigation into unmanned aerial system (UAS) forensics: Data extraction and analysis. Forensic Science International: Digital Investigation, 41: 301379. https://doi.org/10.1016/j.fsidi.2022.301379

[45] Yousef, M., Iqbal, F. (2019). Drone forensics: A case study on a DJI Mavic Air. In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1-3. https://doi.org/10.1109/AICCSA47632.2019.9035365

[46] Horsman, G. (2016). Unmanned aerial vehicles: A preliminary analysis of forensic challenges. Digital Investigation, 16: 1-11. https://doi.org/10.1016/j.diin.2015.11.002

[47] Adorni, E., Rozhok, A., Revetria, R., Ivanov, M. (2021). Literature review on drones used in the surveillance field. In Lecture Notes in Engineering and Computer Science: Proceedings of the International Multi Conference of Engineers and Computer Scientists, pp. 20-22.

[48] Syed, N., Khan, M.A., Mohammad, N., Brahim, G.B., Baig, Z. (2022). Unsupervised machine learning for drone forensics through flight path analysis. In 2022 10th International Symposium on Digital Forensics and Security (ISDFS), Istanbul, Turkey, IEEE, pp. 1-6. https://doi.org/10.1109/ISDFS55398.2022.9800808

[49] Salamh, F.E., Karabiyik, U., Rogers, M.K., Matson, E.T. (2021). Unmanned aerial vehicle kill chain: Purple teaming tactics. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), NV, USA, pp. 1081-1087. https://doi.org/10.1109/CCWC51732.2021.9376090

[50] Chasseray, Y., Barthe-Delanoë, A.M., Négny, S., Le Lann, J.M. (2022). A generic metamodel for data extraction and generic ontology population. Journal of Information Science, 48(6): 838-856. https://doi.org/10.1177/0165551521989641

[51] Ameerbakhsh, O., Ghabban, F.M., Alfadli, I.M., AbuAli, A.N., Al-Dhaqm, A., Al-Khasawneh, M.A. (2021). Digital forensics domain and metamodeling development approaches. In 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Cameron Highlands, Malaysia, IEEE, pp. 67-71. https://doi.org/10.1109/ICSCEE50312.2021.9497935

[52] Bade, A.M., Othman, S.H. (2022). Towards adapting metamodelling technique for an online social networks forensic investigation (OSNFI) domain. International Journal of Advanced Computer Science and Applications, 13(7): 166-173. https://doi.org/10.14569/IJACSA.2022.0130722

[53] Georgiou, A., Masters, P., Johnson, S., Feetham, L. (2022). UAV-Assisted real-time evidence detection in outdoor crime scene investigations. Journal of Forensic Sciences, 67(3): 1221-1232. https://doi.org/10.1111/1556-4029.15009

[54] Menahil, A., Iqbal, W., Iftikhar, M., Shahid, W.B., Mansoor, K., Rubab, S. (2021). Forensic analysis of social networking applications on an android smartphone. Wireless Communications and Mobile Computing, 2021(1): 5567592. https://doi.org/10.1155/2021/5567592

[55] Zhou, Z., Irizarry, J., Lu, Y. (2018). A multidimensional framework for unmanned aerial system applications in construction project management. Journal of Management in Engineering, 34(3): 04018004. https://doi.org/10.1061/(ASCE)ME.1943-5479.0000597

[56] Sibe, R.T., Bekom, D. (2025). Digital forensic investigation of an unmanned aerial vehicle (UAV): A technical case study of a DJI phantom III professional drone. Journal of Cybersecurity & Information Management, 15(1): 197-210. https://doi.org/10.54216/JCIM.150115

[57] Thallapureddy, S., Sherratt, F., Hallowell, M., Bhandari, S. (2024). Effective information collection in incident investigations: A systematic review and narrative synthesis. Safety Science, 171: 106404. https://doi.org/10.1016/j.ssci.2023.106404

[58] Kerr, O.S. (2005). Digital evidence and the new criminal procedure. Columbia Law Review, 105: 279. https://doi.org/10.18574/nyu/9780814739334.003.0013

[59] Studiawan, H., Ahmad, T., Shiddiqi, A.M., Santoso, B.J., Pratomo, B.A. (2021). Forensic event reconstruction for drones. In 2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, IEEE, pp. 41-45. https://doi.org/10.1109/ISRITI54043.2021.9702864

[60] Saleh, M., Othman, S.H., Driss, M., Al-dhaqm, A., Ali, A., Yafooz, W.M., Emara, A.H.M. (2023). A metamodeling approach for IoT forensic investigation. Electronics, 12(3): 524. https://doi.org/10.3390/electronics12030524