A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field

Fahad Alotaibi
Faculty of Computing and Information Technology (FCIT), King Abdulaziz University, Saudi Arabia
fmmalotaibi@kau.edu.sa

Arafat Al-Dhaqm
Computer & Information Sciences Department, Universiti Teknologi PETRONAS, Malaysia
arafataldoqm@gmail.com (corresponding author)

Yasser D. Al-Otaibi
Department of Information Systems, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Saudi Arabia
yalotaibi@kau.edu.sa

Received: 13 July 2023 | Revised: 7 August 2023 | Accepted: 5 October 2023

 DOI: https://doi.org/10.48084/etasr.6195

ABSTRACT

Although there is a considerable amount of studies in drone forensics that describe numerous practical and technical perspectives, there is a lack of a comprehensive investigation framework. This study used design science research methodology to design a conceptual model for the comprehensive investigation of Unmanned Aerial Vehicles (UAVs) under forensic conditions. This model can identify, capture, preserve, analyze, and document UAV incidents. The proposed model consists of four stages: preparation, data collection, analysis, and documentation. In the preparation stage, data are collected and analyzed about UAV-related resources, including the origin and model of the aircraft, any software or hardware installed onboard, and the legal framework and regulations in place. The data collection stage involves the completion of the collection process, where participants gather parts of the UAV and the data needed, such as the flight controller, flight log, and memory cards. The analysis stage involves analyzing the collected evidence. Lastly, the documentation stage involves documenting relevant evidence, analysis results, and any conclusions derived. This model provides a comprehensive process to forensically investigate UAV incidents and provides an efficient and effective approach to the analysis of UAV evidence, ensuring that evidence was collected and analyzed according to accepted forensic techniques. The proposed model can be applied to any UAV type and legal framework.

Keywords-drone forensics; digital forensics; design science research; unmanned aerial vehicles

I. INTRODUCTION

Digital forensics essentially focuses on capturing and analyzing cybercrimes and is divided into many subfields, such as database, Internet of Things (IoT), malware, network, drone, cloud, wireless, data, and mobile forensics [1]. These branches vary in terms of models, approaches, frameworks, policies, procedures, and activities. Therefore, digital forensics lacks a standardized framework that could unify these branches [2]. This field consists of two main stages, proactive and reactive forensics, both designed to resolve cybercrimes [3-4]. Proactive forensics refers to forensic readiness before a crime occurs. During this stage, digital evidence is collected to reduce future risks and disasters. On the other hand, reactive forensics focuses on the necessary procedures after the crime is committed. The primary objective of this stage is to locate, seize, preserve, analyze, and record cybercrime data. Essentially, both stages are used in digital forensics, and the ISO/IEC 27043:2015 standard serves as the primary context for studies on proactive forensic approaches [5-14]. Drone forensics (DRF) aims to provide the tools and techniques necessary to identify and investigate potential drone-related incidents [15-17]. The primary focus of DRF is to identify the drone's owner, the activities that occurred during a drone-related incident, the nature of the data stored on the drone, and any evidence the drone may have left behind. A drone forensic process involves four steps. The drone must first be identified, which is performed using a combination of visual and electronic identification techniques. The drone must then be secured for forensic analysis. This involves stopping any moving parts, turning off the device, and taking precautions to avoid data manipulation [18-19]. Specialized software and hardware can be used to analyze drone data after they have been secured. Lastly, it is imperative to examine and document

the data gathered to determine if they contain any relevant evidence. In addition to data analysis, DRF researchers need a thorough understanding of the legal implications of drone use. Therefore, a solid understanding of drone laws and regulations and their consequences based on acquired evidence is fundamental. Investigating a drone incident is an essential task for law enforcement, government, and security personnel [20-23]. Through the integration of cutting-edge technology and in-depth legal knowledge, DRF can help investigators discover, investigate, and prosecute drone-related incidents.

This study used Design Science Research (DSR) methodology to design a conceptual forensic model for DRF. DSR was used in the construction of the representation component, and semantic analysis was applied to determine its structure and constituent elements. The proposed model consisted of four stages: preparation, collection, analysis, and documentation. In the preparation stage, it is necessary to determine the type of drone, define the investigation objective, and select the appropriate equipment. The collection stage involves collecting all the components related to the device, such as its controller, camera, etc. The subsequent analysis stage is used to identify the data sources and extract the necessary evidence. Finally, the necessary reports are compiled, documenting the evidence, the results of the analysis, and any conclusions derived. The proposed model can be used in any DRF investigation.

II. RELATED WORKS

Various models and frameworks have been proposed in DRF, based on the following four aspects: forensic, non-forensic, forensic framework, and forensic analysis applications [24-26]. In [8-9], the ways to ensure the best recovery of evidence related to drone incidents were discussed. Most studies emphasized the advantages of using Linux-based operating systems to collect information about the Linux filesystem. In [27], the Parrot A.R Drone 2.0 was used for digital forensic analysis, covering a variety of general data points and file types and using Google Earth to fully visualize the flight path. In [28], DRF was reviewed using DJI Phantom 2, initiating a detailed analysis of the hardware and software components of the drone and discussing their applicability to DRF. In [29], a specific tool was developed using Java-FX to efficiently visualize real-time flight control. Although this tool was not designed to work directly with forensics, it can build a strong integration between the controller and the drone, which could facilitate data transfer procedures and allow pilots to monitor sensor parameters such as IMU, GPS, and altitude. In [30], the DJI Phantom 2 Vision Plus was used to reconstruct the flight path of a UAV based on positional data. In [31], a preliminary forensic examination was described using Parrot AR Drone 2.0 and Parrot Bebop.

In [14], the main difficulties in UAV forensics were discussed before studying the UAV and flight controller individually. All flight-related data from the investigated device were retrieved in .pud file format, which was examined during the investigation process to extract a set of metadata such as the serial number of the UAV, the flight controller model, the flight controller application, and the date- and time-related flight data. Additionally, an identification stage was followed to retrieve videos and images captured by the UAV onboard camera. Furthermore, the latitude/longitude coordinates of the locations of the captured images were preserved in the EXIF data. In this part, ownership can only be established when the UAV and controller are seized and the serial number of the device is identified. In [32], a non-forensic approach was integrated with data visualization using Parrot AR Drone 2.0. In [33], drone vulnerabilities and applications were investigated, along with their connections and cybersecurity-related problems. The results confirmed that there could be serious risks or consequences in circumstances where drones are hacked and misused by adversaries. In [34], a novel approach was proposed to comprehensively investigate UAVs using a 12-phase forensic framework. The suggested framework was experimentally validated on five commercial UAVs. Some of the components of each UAV tested were altered and some were added (if applicable). The major goal of these tests was to see if the framework applies to a thorough UAV analysis and if it covers all the different parts of any typical commercial UAV. The results showed that one major obstacle is the lack of law enforcement training procedures in UAVs. In [35], the DJI Phantom 3 standard was analyzed and the Drone Open Source Parser (DROP) tool was developed. The collected data were then classified into three groups: controller, drone, and phone/tablet. Finally, the .dat files generated by the UAV and the .txt files generated by the DJI GO application were examined. The files were encrypted first, then decoded, and flight information, including flight status, remote controls, Wi-Fi connections, motors, and GPS locations, was extracted. The collected data were analyzed and the DROP tool was used to examine the evidence files. In [36], the use of GPS coordinates was discussed as location evidence when investigating crimes committed using drones, extracting system logs, and using a third-party web-based platform to plot the flight path and visualize GPS coordinates on maps. In [37], a correlation investigation was performed on the flight data collected from the drone's SD card and mobile phone. The results showed that it was possible to establish a connection between the drone and the suspect to aid in a criminal investigation underway. In addition, by installing specialized software on personal UAV devices, a variety of digital artifacts can be obtained, such as GPS timestamps, videos, and images. In [38], the key log parameters of autonomous drones were examined and a comprehensive software architecture for DRFs was proposed, offering a user-friendly graphical user interface to extract and examine on-board flight data.

Several studies have used mobile forensic methods to extract data from drone mobile applications using open-source tools such as CSV View and ExifTool. In [39], forensic workstations running Windows and Kali Linux were used to perform the necessary forensic analyses on two drones, the DJI Phantom 3 and A.R Drone. The flight path data were primarily visualized using open-source tools like Geo-Player. This option requires a significant amount of data modification, as UAV systems lack a compatible built environment consisting of configuration tools, a package manager, and a compiler. In [40], the challenges associated with the forensic analysis of a UAV/drone were investigated. This study reviewed and analyzed the effectiveness of existing DRF guidelines and

provided a set of recommendations. The main drawback of UAV forensics is the lack of previously validated forensic sound tools. The next logical step would be to create various parsing tools that can analyze the original data and provide accurate and trustworthy information. UAVs should also be able to integrate radio communication services.

In [41], a framework was suggested to secure authentication and preserve privacy using id-based signcryption. RFID tags were used to track the drones and their temporary identity to maintain privacy. The average renewal of temporary identity was calculated using a simulation in which the speed and duration of the drones changed. In [42], a scenario was described in which security forces can use a shotgun or any other appropriate tool to bring down a suspected UAV. The study emphasized the necessity of identifying the software and hardware modules of the UAV before subjecting it to forensic investigation. The next step was to gather all available evidence, demonstrate the chain of custody, and examine the media or data loaded onto the device. The increasing illegal use of UAVs demonstrates a legal weakness in current aviation regulations. Therefore, there is a lack of knowledge and accepted practices regarding how to investigate UAV incidents. A comprehensive framework for drone forensic investigations was presented, taking into account both physical and digital forensics. A physical forensics model was created, capable of recognizing drone parts right at the crime scene. The framework proved to be effective enough to be implemented in post-flight analyses of the drone's performance. Furthermore, a powerful application was created to mainly concentrate on the analysis of critical log parameters using JavaFX 8.0. In [43], potential cyber-physical security risks were investigated to address any issues related to UAV security. This study provided a method to examine large-scale cyber-security attack vectors of such systems, based on four essential categories for UAV operations, and effective countermeasures to such attacks. In [44], software was developed to gain access to the sensors and logs inside the device under investigation, to estimate the effectiveness of using neutralization and strengthening processes.

In [45], the Distributed Agent-based Secure Mechanism (DASMIS) was proposed to monitor IoD and smart grid sensors using a hybrid peer-to-peer and client-server network architecture with little protocol overhead for fast and bandwidth-efficient communication. Each node in this system had a Python-based agent capable of scanning and detecting modifications, system calls, installed applications, and all currently running system programs, and burned-in read-only node IDs, IP, and MAC addresses. This mechanism also hashes and encrypts data, reports changes to the server located in the C&C center, and communicates with other peer nodes. The agent encrypts communication and securely authenticates and grants access between nodes, while attacks such as masquerading, modification, and denial of service are detected and prevented. In [46], a study was presented to help those responsible for data generation, analysis, validation, and/or optimization to recover trace evidence. In [47], the implementation of digital forensic analysis to enhance the Drone Forensic and Incident Response Plan (DFIR) was investigated. The results demonstrated that the Federal Aviation Administration (FAA) can update the specifications of Unmanned Aerial Systems (UAS) based on two classifications. Furthermore, an in-depth literature review was conducted, concluding that there were limited studies related to incident responses and forensic analysis frameworks for remotely piloted aerial systems.

III. METHODOLOGY

This study designed a conceptual digital forensic model for UAVs based on DSR. This method produces unique and persistent objects for a specific problem space, which enables the exploration of analytics [48]. According to [49], the development process consists of two main stages: problem identification and the development stage, as shown in Figure 1.

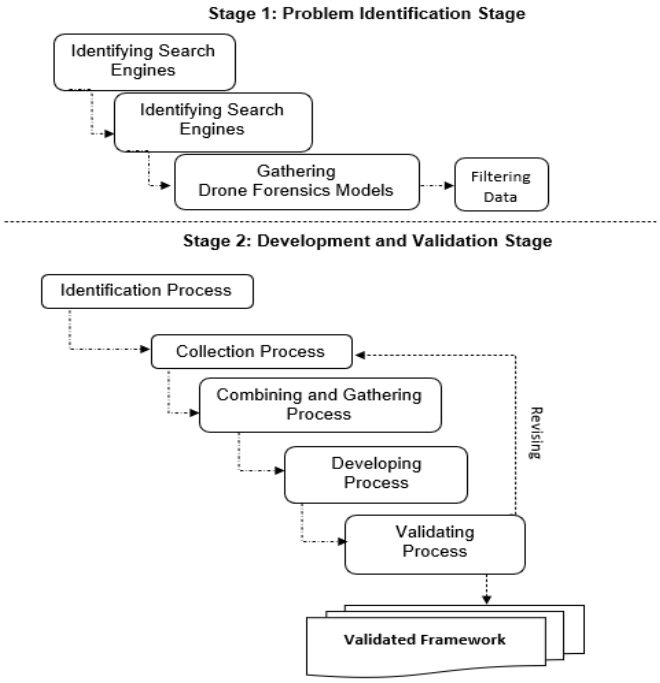

Fig. 1. Developed approach.

A. Stage 1: Problem Identification

The existing literature was reviewed and relevant data were collected. This stage involved three major steps:

- Identifying search engines: Seven widely used search engines were used to gather data: Web of Science, Scopus, IEEE, Springer, Google Scholar, ACM, and Science Direct.
- Gathering drone forensics models: The keywords "Drones Forensics" and "Drone Forensics + Model" were used to gather data. This resulted in a total of 132 publications.
- Filtering data: The search was limited to publications between January 2000 and January 2021 from research journals, conferences, dissertations, and books, while all other document types were ignored. Table I shows the findings per search engine. This step left 25 articles that focused on DRF processes and technological perspectives, to be considered for further analysis.

TABLE I. FINDINGS FROM SEARCH-ENGINES

Database search engines	Number of DRF-related articles
Scopus	97
Web of Science	54
IEEE	15
Google Scholar	70
Springer	120
Science Direct	2
ACM	20

B. Stage 2: Development

This stage involved the development and validation of a drone forensic model. The steps involved in this stage were:

- Identification Process: This step identified the development and validation models as shown in Table II.
- Collection process: It is difficult to collect common concepts and processes from DRF models because it is a relatively new field and, consequently, the literature consists of only a limited number of such models. However, some general concepts and processes that could be extracted from these models included data collection, analysis and interpretation, legal and ethical considerations, data storage and preservation, digital evidence examination, and digital forensic examination. Additionally, some models may include specific concepts and processes such as drone surveillance, image analysis, and GPS tracking. The 25 identified models were used to extract common processes based on the extraction criteria outlined in [50].
- Combining extracted processes: Common processes with similar meanings or modes of operation were grouped into the same category. Each group shared similar ideas and procedures in their semantic or practical applications [57].

TABLE II. DEVELOPMENT AND VALIDATION MODELS

ID	Model Reference	Year
1	[29]	2015
2	[33]	2016
3	[28]	2016
4	[32]	2016
5	[36]	2017
6	[34]	2017
7	[35]	2017
8	[37]	2017
9	[39]	2017
10	[40]	2018
11	[41]	2018
12	[43]	2018
13	[44]	2018
14	[42]	2019
15	[45]	2019
16	[46]	2019
17	[47]	2019
18	[51]	2019
19	[52]	2019
20	[53]	2019
21	[54]	2020
22	[55]	2021
23	[18]	2022
24	[15]	2022
25	[56]	2023

- Developing process: The conceptual model presented in this step was based on the common processes proposed in the previous step. The proposed model consists of four investigation stages: preparation, collection, analysis, and documentation, as shown in Figure 2.

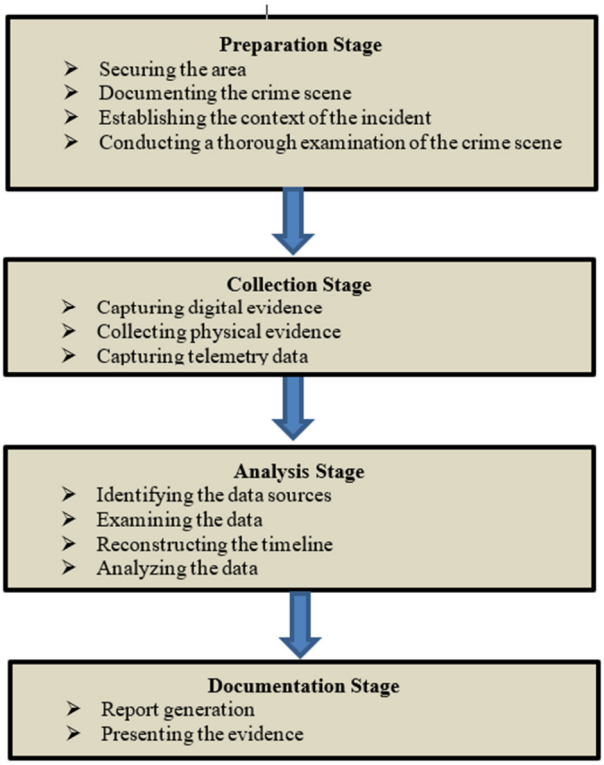

Fig. 2. Conceptual digital forensics model for the DRF field.

1) Stage 1: Preparation

This stage aims at observing and securing the patterns of the drone flight path as well as capturing the complete streaming activities (e.g. photos, GPS data, and records). The monitoring component employs a firewall to filter incoming and outgoing wireless traffic for security reasons. The term filtering refers to the process of restricting access by looking at each packet's header information. Although certain laptops and mobile devices can counterfeit their identity to look like authorized network users, a firewall cannot catch all the misbehavior data. This stage involves four steps:

- Securing the area: The area around the suspected drone is secured by cordoning the area and notifying local authorities. It is important to ensure that all personnel entering the area wear protective clothing and gloves. Cordoning off the area can be done by installing a physical barrier or using warning signs to prevent unauthorized personnel or laypeople from entering. After the area has been sealed off, the incident should be reported to the local authorities so that appropriate measures could be taken to effectively secure the area. Additionally, local authorities can advise on how to safely dispose of any hazardous materials that may be present.

- Documenting the crime scene: Before accessing the drone, it must be ensured that there is a record of the incident in the form of photos and videos to provide a visual reference for the drone's location. Furthermore, any available evidence to support the claim that the drone had operated in that area must also be provided. To document a scene with a drone, the first step is to take pictures or videos of the area where the drone is stationed. Landmarks, buildings, or topographical characteristics relevant to the location of the drone should be included.
- Establishing the context of the incident: Drone types, suspects, and any pertinent information that can help in the investigation of the case should be analyzed. It is important to identify the type of drone used since drones of different manufacturers and models often have different capabilities, ranges, purposes, and applications. Additionally, the manufacturer and model of the drone could provide clues about the responsibility for the crime.
- Conducting a thorough examination of the crime scene: To facilitate the assessment of the event, it is crucial to conduct an extensive inspection of the crime scene to locate and gather any evidence that could facilitate the investigation. The first step in responding to a drone incident should be a thorough investigation of the site in question.

2) Stage 2: Data Collection

This is an important stage in any investigation, as it allows data to be collected and then analyzed to identify any indications of criminal activity. Data can be collected from the drone itself or external sources, such as telecommunication towers or cellular networks, depending on the type of drone. A drone may be equipped with onboard recording equipment, such as cameras, which can be analyzed for evidence of suspicious conduct. The collection process should be carried out following established procedures and protocols, regardless of the type of drone used, to ensure that any evidence acquired is admissible in court. The collection process may include obtaining a search warrant to gain access to the drone or its data. It might include downloading any records or data onboard, such as GPS coordinates, altitude, speed, and direction. In some circumstances, gathering data from a drone may require the assistance of other agencies or individuals to acquire access to the drone or its data. It is critical to maintain respect and diplomacy in such situations because it could be a sensitive topic for everyone involved. Finally, to obtain any evidence related to the suspected drone, the collection stage of a drone investigation is critical for investigators to stay up-to-date with the newest drone laws and procedures to ensure that any evidence acquired is legally admissible in court. This stage consists of three major steps:

- Capturing digital evidence: Obtaining digital data such as pictures, videos, and audio recordings from the drone's onboard cameras or other recording systems may be part of capturing digital evidence. Furthermore, metadata connected with the files saved on the drone's onboard storage device may be included in digital evidence. The onboard storage system may include a memory card, hard drive, or other types of digital storage medium. To gather digital evidence from a drone, the drone must be seized and secured so that the digital evidence could be well protected. Once the drone has been secured, digital data can be recovered using forensic tools and techniques. Digital evidence should be extracted preserving their integrity and authenticity. Documenting the actions used to obtain the evidence is critical, as well as the environment in which it is obtained. Any tools used to extract evidence should also be examined and validated to ensure that the digital evidence is not corrupted or manipulated in any way. After extracting digital evidence, it should be analyzed to determine its relevance and accuracy. This could include inspecting the metadata associated with each file to discover where it came from and when it was generated or modified.
- Collecting physical evidence: To analyze a suspected drone, its outer shell or other components can be collected. Additionally, the drone's memory card or storage system must be properly removed and saved. Moreover, residue and other components left at the scene should be collected and preserved. Gathering evidence safely and effectively requires proper equipment and personnel.
- Capturing telemetry data: Flight logs, GPS locations, and other telemetry data may provide information on a drone's flight path. During an investigation involving drones, telemetry data must be collected to be delivered to law enforcement officers and other organizations that monitor and analyze drone activities.

3) Stage 3: Analysis

In this stage, patterns and trends are identified that can be applied to identify drone crimes, the locations they were committed, and the patterns associated with them. As part of this process, the data obtained are analyzed for possible links to potential crimes. These data include the types of drones used, locations, and other factors that could contribute to the crime. This stage involves four steps:

- Identifying data sources: An investigation cannot be successful without identifying the data sources, which is the first step in analyzing and interpreting the data. When identifying data sources, several factors should be considered. It is important to first determine what type of data was acquired to identify the data sources. A drone's movement, altitude, payload, or anything else useful could be included in this data category. Considering the data source can also provide insight into the dependability and accuracy of the data.
- Examining the data: Data must be thoroughly checked for any trends or anomalies that could indicate the presence of drones. First, it should be determined where the data came from. There is a necessity to differentiate between data collected from common or private resources, for example, data gained from surveillance or safety cameras.
- Reconstructing the timeline: To establish a timeline, it is vital to take great care of all alleged drone actions. If an investigator can identify the way the drone worked in the past, then it may be possible to rebuild a timeline of its actions in the future. All available data should be used to

recreate the timeline using all available information. Among the drone data that can be collected are altitude, speed, and GPS coordinates. Recording a drone flight, in addition to providing video and audio, can provide additional clarity to the sequence of events. Drone debris, observations, and eyewitnesses can also contribute to the gathering of more information. To construct the timeline, all data need to be collected first. Data points need to be arranged in the right sequence to be able to develop the timeline. To compare the data with the timeframe, it is necessary to examine the data over time. Based on information such as the time the drone took off and landed, investigators can use that information to create a timeline for the investigation. The investigator can also check for inconsistencies in the timeline. If data points contradict each other, the investigator can look for additional evidence that favors one over the other and, therefore, can be used to rebuild and verify the timeline. Understanding what occurred during a suspected drone operation necessitates reconstructing the timeline of the drone's operations, which assists the investigator in gaining knowledge of the sequence of events that occurred by collecting important data points and piecing them together in the correct order.

- Determining the prevalence of drone crime: Drone crimes can be analyzed for types, trends, and potential solutions to reduce or eradicate them. This can be done by analyzing the data collected. As a starting point, it is vital to recognize that many types of drone crimes are increasingly occurring across the globe.

4) Stage 4: Documentation

Each stage of the drone investigation should be recognized properly. This stage covers various actions such as classifying the drone, its worker, and its site, conducting meetings with the worker, and assembling photos, videos, and other available evidence. Additionally, any results during the examination must be recognized, such as laws or principles, consequences delivered, or other consequences arising. A detailed examination description will be given lastly based on this documentation, which will guide future investigations. This stage includes several steps: generating reports and presenting the evidence.

IV. RESULTS AND DISCUSSION

UAVs can serve a variety of different purposes, including surveillance, inspection, data collection, and delivery. A growing number of these devices are used by individuals for malicious purposes, which requires the development of robust forensic frameworks to investigate and manage them. This study developed a forensic framework for drones and UAVs. At first, the history and existing forensic work on UAVs was discussed. In addition, this study discussed the current obstacles and problems associated with the use of drones and UAVs in the field of investigative research. The lack of standardization and the complexity of the hardware and software components of UAVs and drones, which are associated with their application in forensics, were also examined.

The proposed model consists of four main stages: preparation, collection, analysis, and documentation. During the preparation stage, the investigation requirements are identified, the necessary equipment is collected, and key personnel who can assist with the investigation are employed. This collection stage is an essential part of the process to obtain all crucial information on the drone and any external systems that may be involved. Furthermore, it involves the establishment of essential safety protocols that protect the safety of all staff and minimize the risk of poisoning evidence. During this stage, the drone and any components associated with it are physically obtained. The drone and its components should be secured to prevent contamination or destruction of any evidence. After analyzing the evidence, a determination is made as to whether criminal activity has occurred. To accomplish this, the drone and any components connected to it must be inspected for potential signs of criminal activity. It might be necessary to examine the flight logs of the drone and/or analyze photographs and videos that the drone has taken. The documentation stage is the last step in the investigation process, during which all evidence and information related to the investigation is recorded. At this stage, it is important to document the results of the analysis and any other information that may be valuable for future inquiries. This information should be stored in a secure and tamperproof manner to be used as evidence in a criminal case if necessary. The proposed DRF model is a consistent approach to investigating drone-related crimes. It is possible to verify that the evidence was acquired and examined appropriately if the investigators follow this model and adhere to it. A successful criminal prosecution depends on secure and documented evidence, which is one of the most important factors. Additionally, this framework can help investigators ensure that any criminal activity involving drones is thoroughly investigated and prosecuted.

V. CONCLUSION

UAVs play a critical role in forensic investigations. In this paper, a four-stage forensic investigation model was presented, which can be used to recognize, assemble, examine, and document incidents involving drones. Based on this model, law enforcement agencies will be able to improve their examination procedures for such crimes. Future work must explore the efficacy of the suggested model in a real-world setting. Additionally, further research should be carried out to investigate the potential of UAVs to be used in a broader range of forensic applications. Finally, this model should be subjected to further research due to its potential to be tailored to meet the demands of law enforcement agencies.

ACKNOWLEDGEMENT

This research work was funded by the Institutional Fund Projects under grant no (IFPRC-062-611-2020). Therefore, the authors gratefully acknowledge the technical and financial support from the Ministry of Education and King Abdulaziz University, Jeddah, Saudi Arabia.

REFERENCES

[1] V. R. Kebande and I. Ray, "A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)," in *2016 IEEE 4th International*

Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, Dec. 2016, pp. 356–362, https://doi.org/10.1109/FiCloud.2016.57.

[2] V. R. Kebande, "Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0," *Forensic Science International: Reports*, vol. 5, Jul. 2022, Art. no. 100257, https://doi.org/10.1016/j.fsir.2022.100257.

[3] S. M. Makura, H. S. Venter, R. A. Ikuesan, V. R. Kebande, and N. M. Karie, "Proactive Forensics: Keystroke Logging from the Cloud as Potential Digital Evidence for Forensic Readiness Purposes," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, Doha, Qatar, Oct. 2020, pp. 200–205, https://doi.org/10.1109/ICIoT48696.2020.9089494.

[4] V. R. Kebande and H. S. Venter, "Requirements for Achieving Digital Forensic Readiness in the Cloud Environment using an NMB Solution," presented at the 11th International Conference on Cyber Warfare and Security ICCWS, Boston, MA, USA, Mar. 2016.

[5] V. R. Kebande, N. M. Karie, R. A. Ikuesan, and H. S. Venter, "Ontology-driven perspective of CFRaaS," *WIREs Forensic Science*, vol. 2, no. 5, 2020, Art. no. e1372, https://doi.org/10.1002/wfs2.1372.

[6] V. R. Kebande and H. S. Venter, "A comparative analysis of digital forensic readiness models using CFRaaS as a baseline," *WIREs Forensic Science*, vol. 1, no. 6, 2019, Art. no. e1350, https://doi.org/10.1002/wfs2.1350.

[7] A. Valjarevic and H. S. Venter, "Harmonised digital forensic investigation process model," in *2012 Information Security for South Africa*, Johannesberg, South Africa, Dec. 2012, pp. 1–10, https://doi.org/10.1109/ISSA.2012.6320441.

[8] V. R. Kebande, N. M. Karie, and H. S. Venter, "Adding digital forensic readiness as a security component to the IoT domain," *International Journal on Advanced Science Engineering Information Technology*, vol. 8, no. 1, 2018, https://doi.org/10.18517/ijaseit.8.1.2115.

[9] H. Munkhondya, A. Ikuesan, and H. Venter, "Digital Forensic Readiness Approach for Potential Evidence Preservation in Software-Defined Networks," in *Proceedings of the 14th International Conference on Cyber Warfare and Security*, Stellenbosch, South Africa, Feb. 2019, pp. 268–276.

[10] A. R. Ikuesan, S. Abd Razak, M. Salleh, and H. S. Venter, "Leveraging Human Thinking Style for User Attribution in Digital Forensic Process," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 7, no. 1, pp. 198–206, 2017.

[11] A. Singh, A. R. Ikuesan, and H. S. Venter, "Digital Forensic Readiness Framework for Ransomware Investigation," in *Digital Forensics and Cyber Crime*, New Orleans, LA, USA, 2019, pp. 91–105, https://doi.org/10.1007/978-3-030-05487-8_5.

[12] S. Makura, H. S. Venter, V. R. Kebande, N. M. Karie, R. A. Ikuesan, and S. Alawadi, "Digital forensic readiness in operational cloud leveraging ISO/IEC 27043 guidelines on security monitoring," *Security and Privacy*, vol. 4, no. 3, 2021, Art. no. e149, https://doi.org/10.1002/spy2.149.

[13] V. R. Kebande, N. M. Karie, K.-K. R. Choo, and S. Alawadi, "Digital forensic readiness intelligence crime repository," *Security and Privacy*, vol. 4, no. 3, 2021, Art. no. e151, https://doi.org/10.1002/spy2.151.

[14] A. Ali, S. A. Razak, S. H. Othman, and A. Mohammed, "Extraction of Common Concepts for the Mobile Forensics Domain," in *Recent Trends in Information and Communication Technology*, 2018, pp. 141–154, https://doi.org/10.1007/978-3-319-59427-9_16.

[15] F. M. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field," *Computational Intelligence and Neuroscience*, vol. 2022, Feb. 2022, Art. no. e8002963, https://doi.org/10.1155/2022/8002963.

[16] S. O. Baror, H. S. Venter, and V. R. Kebande, "Conceptual Model for Crowd-Sourcing Digital Forensic Evidence," in *Innovations in Smart Cities Applications Volume 5*, 2022, pp. 1085–1099, https://doi.org/10.1007/978-3-030-94191-8_88.

[17] T. Hungwe, Hein. S. Venter, and V. R. Kebande, "Scenario-Based Digital Forensic Investigation of Compromised MySQL Database," in *2019 IST-Africa Week Conference (IST-Africa)*, Nairobi, Kenya, Feb. 2019, pp. 1–11, https://doi.org/10.23919/ISTAFRICA.2019.8764819.

[18] A. A. Alhussan, A. Al-Dhaqm, W. M. S. Yafooz, S. B. A. Razak, A.-H. M. Emara, and D. S. Khafaga, "Towards Development of a High Abstract Model for Drone Forensic Domain," *Electronics*, vol. 11, no. 8, Jan. 2022, Art. no. 1168, https://doi.org/10.3390/electronics11081168.

[19] V. R. Kebande and H. S. Venter, "CFRaaS : architectural design of a Cloud Forensic Readiness as-a-Service Model using NMB solution as a forensic agent," *African Journal of Science, Technology, Innovation and Development*, vol. 11, no. 6, pp. 749–769, Oct. 2019, https://doi.org/10.1080/20421338.2019.1585675.

[20] F. M. Alotaibi, A. Al-Dhaqm, Y. D. Al-Otaibi, and A. A. Alsewari, "A Comprehensive Collection and Analysis Model for the Drone Forensics Field," *Sensors*, vol. 22, no. 17, Jan. 2022, Art. no. 6486, https://doi.org/10.3390/s22176486.

[21] V. R. Kebande and R. A. Ikuesan, "Virtual sensor forensics," in *Proceedings of the 2nd International Conference on Intelligent and Innovative Computing Applications*, Jun. 2020, pp. 1–6, https://doi.org/10.1145/3415088.3415117.

[22] V. R. Kebande, H. S. Ntsamo, and H. S. Venter, "Towards a prototype for Achieving Digital Forensic Readiness in the Cloud using a Distributed NMB Solution," presented at the 15th European Conference on Cyber Warfare and Security, Munich, Germany, 2016.

[23] A. Ali *et al.*, "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," *Applied Sciences*, vol. 12, no. 19, Jan. 2022, Art. no. 9637, https://doi.org/10.3390/app12199637.

[24] N. M. Karie and V. R. Kebande, "Knowledge Management as a Strategic Asset in Digital Forensic Investigations," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 1, pp. 10–21, Jan. 2018.

[25] A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Razak, and F. M. Ghabban, "Research Challenges and Opportunities in Drone Forensics Models," *Electronics*, vol. 10, no. 13, Jan. 2021, Art. no. 1519, https://doi.org/10.3390/electronics10131519.

[26] S. O. Baror, H. S. Venter, and V. R. Kebande, "A Framework for Concurrent Contact-Tracing and Digital Evidence Analysis in Heterogeneous Environments," in *Innovations in Smart Cities Applications Volume 4*, 2021, pp. 1183–1196, https://doi.org/10.1007/978-3-030-66840-2_90.

[27] H. Bouafif, F. Kamoun, F. Iqbal, and A. Marrington, "Drone Forensics: Challenges and New Insights," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, Oct. 2018, pp. 1–6, https://doi.org/10.1109/NTMS.2018.8328747.

[28] David Kovar, Greg Dominguez, and Cindy Murphy, "UAV (aka drone) Forensics," presented at the SANS DFIR Summit, Austin, TX, USA, Jun. 2016.

[29] V. Mhatre, S. Chavan, A. Samuel, A. Patil, A. Chittimilla, and N. Kumar, "Embedded video processing and data acquisition for unmanned aerial vehicle," in *2015 International Conference on Computers, Communications, and Systems (ICCCS)*, Kanyakumari, India, Aug. 2015, pp. 141–145, https://doi.org/10.1109/CCOMS.2015.7562889.

[30] A. Roder, K.-K. R. Choo, and N.-A. Le-Khac, "Unmanned Aerial Vehicle Forensic Investigation Process: Dji Phantom 3 Drone As A Case Study." arXiv, Apr. 23, 2018, https://doi.org/10.48550/arXiv.1804.08649.

[31] G. Horsman, "Unmanned aerial vehicles: A preliminary analysis of forensic challenges," *Digital Investigation*, vol. 16, pp. 1–11, Mar. 2016, https://doi.org/10.1016/j.diin.2015.11.002.

[32] T. Procházka, "Capturing, Visualizing, and Analyzing Data from Drones," BSc Thesis, Charles University, Prague, Czech Republic, 2016.

[33] M. Mohan, "Cybersecurity in drones," MSc Thesis, Utica College, New York, NY, USA, 2016.

[34] U. Jain, M. Rogers, and E. T. Matson, "Drone forensic framework: Sensor and data identification and verification," in *2017 IEEE Sensors Applications Symposium (SAS)*, Glassboro, NJ, USA, Mar. 2017, pp. 1–6, https://doi.org/10.1109/SAS.2017.7894059.

[35] D. R. Clark, C. Meffert, I. Baggili, and F. Breitinger, "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III," *Digital Investigation*, vol. 22, pp. S3–S14, Aug. 2017, https://doi.org/10.1016/j.diin.2017.06.013.

[36] S. E. Prastya, I. Riadi, and A. Luthfi, "Forensic Analysis of Unmanned Aerial Vehicle to Obtain GPS Log Data as Digital Evidence," *International Journal of Computer Science and Information Security*, vol. 15, no. 3, pp. 280–285, Mar. 2017.

[37] M. Llewellyn, "DJI Phantom 3 – Drone Forensic data exploration.," Edith Cowan University, Perth, Australia, 2017.

[38] A. L. P. S. Renduchintala, A. Albehadili, and A. Y. Javaid, "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, Sep. 2017, pp. 91–96, https://doi.org/10.1109/CSCI.2017.15.

[39] T. E. A. Barton and M. A. Hannan Bin Azhar, "Forensic analysis of popular UAV systems," in *2017 Seventh International Conference on Emerging Security Technologies (EST)*, Canterbury, UK, Sep. 2017, pp. 91–96, https://doi.org/10.1109/EST.2017.8090405.

[40] R. L. Fairbrother, "A project completed as part of the requirements for the BSc (Hons) Computer Forensics and Security," University of Derby, Derby, UK, 2018.

[41] S. Benzarti, B. Triki, and O. Korbaa, "Privacy Preservation and Drone Authentication Using ID-Based Signcryption," in New Trends in Intelligent Software Methodologies, Tools and Techniques - Proceedings of the 17th International Conference SoMeT_18, 2018, pp. 226–239, https://doi.org/10.3233/978-1-61499-900-3-226.

[42] A. Renduchintala, F. Jahan, R. Khanna, and A. Y. Javaid, "A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework," *Digital Investigation*, vol. 30, pp. 52–72, Sep. 2019, https://doi.org/10.1016/j.diin.2019.07.002.

[43] E. S. Dawam, X. Feng, and D. Li, "Autonomous Arial Vehicles in Smart Cities: Potential Cyber-Physical Threats," in 2018 IEEE 20th International Conference on High Performance Computing and Communications, Exeter, UK, Jun. 2018, pp. 1497–1505, https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00247.

[44] J. L. Esteves, E. Cottais, and C. Kasmi, "Unlocking the Access to the Effects Induced by IEMI on a Civilian UAV," in *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*, Amsterdam, Netherlands, Dec. 2018, pp. 48–52, https://doi.org/10.1109/EMCEurope.2018.8484990.

[45] A. Fitwi, Y. Chen, and N. Zhou, "An agent-administrator-based security mechanism for distributed sensors and drones for smart grid monitoring," in *Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII*, May 2019, vol. 11018, pp. 173–188, https://doi.org/10.1117/12.2519006.

[46] Z. V. Jones, C. Gwinnett, and A. R. W. Jackson, "The effect of tape type, taping method and tape storage temperature on the retrieval rate of fibres from various surfaces: An example of data generation and analysis to facilitate trace evidence recovery validation and optimisation," *Science & Justice*, vol. 59, no. 3, pp. 268–291, May 2019, https://doi.org/10.1016/j.scijus.2018.12.003.

[47] F. E. Salamh, U. Karabiyik, M. Rogers, and F. Al-Hazemi, "Drone Disrupted Denial of Service Attack (3DOS): Towards an Incident Response and Forensic Analysis of Remotely Piloted Aerial Systems (RPASs)," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Tangier, Morocco, Jun. 2019, pp. 704–710, https://doi.org/10.1109/IWCMC.2019.8766538.

[48] S. T. March and G. F. Smith, "Design and natural science research on information technology," *Decision Support Systems*, vol. 15, no. 4, pp. 251–266, Dec. 1995, https://doi.org/10.1016/0167-9236(94)00041-2.

[49] A. Al-dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. A. Mohammed, "Development and validation of a Database Forensic Metamodel (DBFM)," *PLOS ONE*, vol. 12, no. 2, 2017, Art. no. e0170793, https://doi.org/10.1371/journal.pone.0170793.

[50] A. Al-Dhaqm *et al.*, "CDBFIP: Common Database Forensic Investigation Processes for Internet of Things," *IEEE Access*, vol. 5, pp. 24401–24416, 2017, https://doi.org/10.1109/ACCESS.2017.2762693.

[51] N. Mei, "An Approach to Unmanned Aircraft Systems Forensics Framework," Ph.D. dissertation, Capitol Technology University, South Laurel, MD, USA, 2019.

[52] F. Le Roy, C. Roland, D. Le Jeune, and J.-P. Diguet, "Risk assessment of SDR-based attacks with UAVs," in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, Oulu, Finland, Dec. 2019, pp. 222–226, https://doi.org/10.1109/ISWCS.2019.8877144.

[53] S. Sciancalepore, O. A. Ibrahim, G. Oligeri, and R. Di Pietro, "Detecting Drones Status via Encrypted Traffic Analysis," in *Proceedings of the ACM Workshop on Wireless Security and Machine Learning*, Feb. 2019, pp. 67–72, https://doi.org/10.1145/3324921.3328791.

[54] F. Lakew Yihunie, A. K. Singh, and S. Bhatia, "Assessing and Exploiting Security Vulnerabilities of Unmanned Aerial Vehicles," in *Smart Systems and IoT: Innovations in Computing*, Singapore, 2020, pp. 701–710, https://doi.org/10.1007/978-981-13-8406-6_66.

[55] C. C. Yang, H. Chuang, and D. Y. Kao, "Drone Forensic Analysis Using Relational Flight Data: A Case Study of DJI Spark and Mavic Air," *Procedia Computer Science*, vol. 192, pp. 1359–1368, Jan. 2021, https://doi.org/10.1016/j.procs.2021.08.139.

[56] S. Silalahi, T. Ahmad, and H. Studiawan, "Transformer-Based Named Entity Recognition on Drone Flight Logs to Support Forensic Investigation," *IEEE Access*, vol. 11, pp. 3257–3274, 2023, https://doi.org/10.1109/ACCESS.2023.3234605.

[57] A. Al-Dhaqm, S. A. Razak, K. Siddique, R. A. Ikuesan, and V. R. Kebande, "Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field," *IEEE Access*, vol. 8, pp. 145018–145032, 2020, https://doi.org/10.1109/ACCESS.2020.3008696.