technologies

MDPI

Article

Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology

Asma Almusayli, Tanveer Zia and Emad-ul-Haq Qazi *

Center of Excellence in Cybercrimes and Digital Forensics (CoECDF), Naif Arab University for Security Sciences (NAUSS), Riyadh 11452, Saudi Arabia; 443000016@student.nauss.edu.sa (A.A.); tzia@nauss.edu.sa (T.Z.)
* Correspondence: qabdulrab@nauss.edu.sa

Abstract: In recent years, drones have become increasingly popular tools in criminal investigations, either as means of committing crimes or as tools to assist in investigations due to their capability to gather evidence and conduct surveillance, which has been effective. However, the increasing use of drones has also brought about new difficulties in the field of digital forensic investigation. This paper aims to contribute to the growing body of research on digital forensic investigations of drone accidents by proposing an innovative approach based on the use of digital twin technology to investigate drone accidents. The simulation is implemented as part of the digital twin solution using Robot Operating System (ROS version 2) and simulated environments such as Gazebo and Rviz, demonstrating the potential of this technology to improve investigation accuracy and efficiency. This research work can contribute to the development of new and innovative investigation techniques.

Keywords: drone forensics; digital forensic investigation; digital twin technology; simulation environment

check for updates

Citation: Almusayli, A.; Zia, T.; Qazi, E.-u.-H. Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology. *Technologies* **2024**, *12*, 11. https://doi.org/10.3390/technologies12010011

Academic Editor: Juan Gabriel Avina-Cervantes

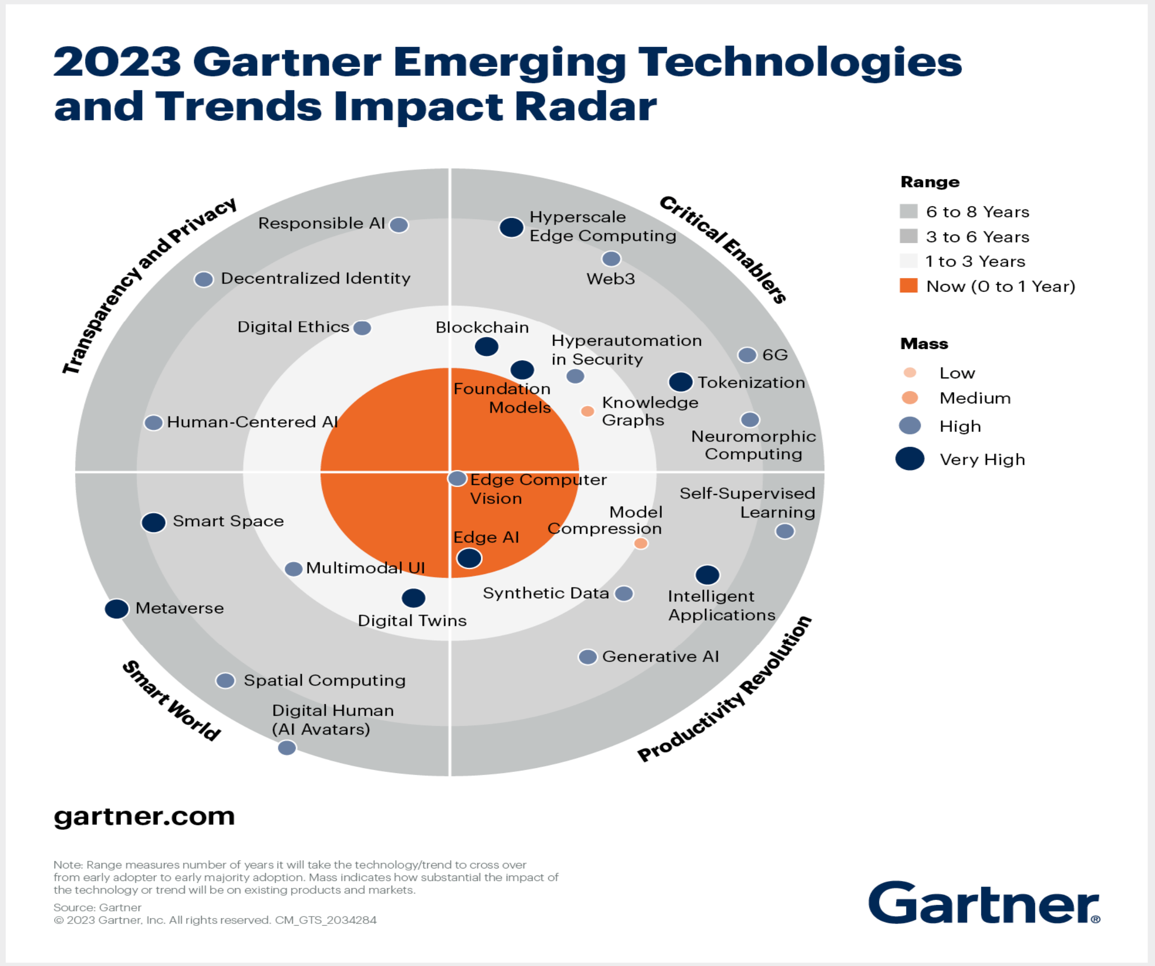
Received: 26 October 2023
Revised: 3 January 2024
Accepted: 8 January 2024
Published: 19 January 2024

1. Introduction

In recent years, the use of drones has been increasing in various fields. According to the official website of the Federal Aviation Administration (FAA) Unmanned Aircraft Systems (UAS) Division [1], there are more than 1.7 million drones registered in the United States, and that number is expected to double in the next few years. This growth is due to the increasing affordability of drones and their various uses such as aerial photography, search and rescue operations, and delivery services. This leads to an increase in drone accidents, which pose significant challenges for digital forensics investigators who must reconstruct accident scenes, collect and analyze data, and determine the cause of accidents. Traditional investigation methods are time-consuming, expensive, and can pose security risks to investigators. Furthermore, this has increased drone-related digital forensics. Digital forensics (DF) is the process of collecting, analyzing, and storing digital evidence, such as flight logs and video recordings, for use in criminal investigations to determine whether criminal activity has taken place. As drones become more popular, they are increasingly being used as digital sources of evidence for criminal investigations. For example, drone footage can be used to identify suspects or provide crime scene evidence.

The use of drones to fight crime has gained a lot of attention in recent years as they can obtain a bird's-eye view of areas that are difficult or impossible for humans to access. A study published in the Journal of Unmanned Vehicle Systems in 2019 examined the use of drones by U.S. law enforcement agencies and found that drones were most commonly used for surveillance, search and rescue operations, and crime scene documentation [2]. Another study [3] published in the Journal of Forensic Sciences in 2022 examined the use of drones in forensic investigations and found that drones were effective in documenting crime scenes and collecting evidence in hard-to-reach places.

Despite the many potential benefits of using drones for crime-fighting purposes, unfortunately, there are some associated challenges and limitations that limit these benefits. These challenges include but are not limited to identifying flight paths, collision information, possible malfunctions, and forensically retrieving imagery and audio and visual data from storage in drones or drone controllers. In extreme circumstances, there is also a possibility that a drone might be carrying explosives, and the drone controller may remotely trigger an explosion to wipe evidence and cause more damage. These issues must be addressed so that drone digital forensics can continue to play an important role in helping investigate crimes more effectively. There are potential solutions available based on technologies that could help address these issues to ensure successful investigations into drone incidents. Digital twin technology has emerged as a promising solution to address challenges in the forensic investigation of drone accidents. Digital twin technology involves creating a virtual replica or simulation of a physical object or system by using real-time data and other information sources. According to Gartner's Emerging Technologies and Trends Impact Radar 2023 publication on technologies, digital twin technology will have a significant impact on current markets and products within the next 1–3 years, as shown in Figure 1, in the 2023 Gartner Emerging Technologies and Trends Impact Radar publication (GartnerInsights) [4].



Note: Range measures number of years it will take the technology/trend to cross over from early adopter to early majority adoption. Mass indicates how substantial the impact of the technology or trend will be on existing products and markets.

Source: Gartner
© 2023 Gartner, Inc. All rights reserved. CM_GTS_2034284

Figure 1. 2023 Gartner Emerging Technologies and Trends Impact Radar [4].

This study aimed to discuss the challenges and limitations associated with the digital forensic investigation of drones and to demonstrate the effectiveness of using digital twin technology in investigating drone accidents, collecting and analyzing data, and determining the cause of an accident. By simulating this technology using a specific accident scenario, the potential benefits of using this technology in the forensic investigation of drone accidents are also highlighted.

The main contributions of this study are as follows:

1. We discuss the current challenges and limitations associated with drone forensic investigations.
2. We provide an overview of the key aspects of digital twin technology as a proposed solution.
3. We showcase how the proposed solution can be used to investigate the cause of an accident in a specific drone accident scenario and its impact on the drone through a simulation.

The remainder of this paper is organized as follows: Section 2 presents a literature review that examines the challenges of digital forensic investigations of drone accidents, including physical, legal, and technical challenges, and the methods used in investigating drone accidents. Section 3 focuses on digital twin technology and examines the concept, architecture, and characteristics of digital twins. This section also explores how this technology works and highlights potential vulnerabilities. Section 4 provides the rationale behind choosing digital twin technology as a solution to the challenges posed by the digital forensic investigation of drone accidents. This section also discusses the potential benefits of using digital twin technology in this context. Section 5 presents a simulation scenario for a drone accident and the implementation of a simulation. This section describes the hardware and software components used in the simulation, as well as the simulation experience. Section 6 presents the primary research results, including the effectiveness of using digital twin technology in investigating drone accidents, the accuracy of the data collected, and the potential benefits of using this technology in the future. Finally, Section 7 provides a conclusion and directions for future work.

2. Literature Review

This section outlines some advances in the field of drone forensics and provides a brief review of some relevant drone forensic research that could be useful to digital forensics. Additionally, this literature review examines the challenges of digital forensic investigations of drone accidents, including physical, legal, and technical challenges, and the methods used in investigating drone accidents.

2.1. Related Work and Comparative Analysis

Our understanding of drone forensics was enhanced by the study conducted by Bouafif et al. [5], which addresses both technical and non-technical aspects of this field through a comprehensive case study involving the Parrot AR Drone 2.0 model specifically and provides valuable insights into how best to approach investigations of drones. Technical limitations in collecting evidence from drones are also discussed in the context of drone forensics, including privacy concerns and legal implications [6]. These challenges further demonstrate the complexity of implementing a digital forensic investigation framework for unmanned aerial vehicles (UAVs). The connection of mobile devices within the realm of the Internet of Things (IoT) introduces a complex landscape, particularly in cases involving international crimes. The absence of standardized legal processing systems creates challenges, potentially leading to conflicts among different countries. As mobile devices transcend national borders, diverse legal frameworks and security measures across jurisdictions can impede seamless cooperation and collaboration between involved parties. In this paper, the authors investigate critical aspects of drone security, emphasizing the necessity for anticipatory measures and architectural modifications to ensure the efficacy of upcoming drone applications. The review focuses on security-critical drone applications, highlighting challenges in drone communication, including DoS attacks, man-in-the-middle attacks, and de-authentication attacks. The proposed solution architectures incorporate cutting-edge technologies such as blockchain, software-defined networks (SDNs), machine learning, and edge computing, addressing the resource constraints of drones [7].

In an overview of existing research related to drone forensics, the potential benefits of using AI and UAVs in forensic investigations are highlighted [8]. These technologies offer significant advantages over traditional investigative methods, but more research is needed to fully understand their applications and effects. Kao et al. [9] presented a case study in which data from a DJI Spark drone were acquired using physical extraction techniques and analyzed using forensic tools such as EnCase Forensic Suite and Autopsy Forensic Browser. The researchers were able to identify the user of the drone by analyzing metadata from photographs taken with its camera. Additionally, Bouafif et al. [10] provided the findings of a Parrot AR drone 2.0 digital forensic investigation and highlighted several challenges associated with drone forensics, as well as new insights into this field provided by recent advances in research.

Al-Room et al. [11] highlighted key challenges associated with conducting digital forensic investigations on common drone models. The researchers examined six drone brands that are frequently utilized in criminal activity and extracted forensically important data, including location details, photographs and videos that were obtained, the flight patterns used by the drones, and information about the drones' owners. In addition, a proactive approach is crucial for digital forensic investigations involving drones. Al-Dhaqm et al. [12] proposed an investigation model to establish a digital forensic preparedness system that can improve proactive techniques for drone-related investigations. They presented a detailed analysis of the current drone forensics framework in place.

The flight log is considered the most significant piece of digital evidence in drone forensics, but the lack of standardization among different types of UAVs makes it challenging to accurately identify and track their sources. Salamh et al. [13] demonstrated the potential challenges of tracking it using purple team techniques and suggested new technologies for engineering UAVs that can simplify the process of evidence identification.

Stanković et al. [14] presented a valuable case study involving a DJI Mini 2 device that simulated criminal-like situations. This paper contributes to the field of drone forensics by highlighting the challenges associated with drone investigations and providing potential solutions for overcoming these obstacles to facilitate successful drone forensic investigations. The case study emphasizes the importance of examining all available forensic data, such as flight logs and images, to reconstruct the events leading up to an incident. However, the use of UAVs poses numerous security and privacy issues that must be addressed to ensure their safe and responsible use in both civilian and military contexts, as demonstrated by Mekdad et al. [15]. Further research is needed to develop effective countermeasures against potential threats and comprehensive legal frameworks.

DJI Phantom 4 and Matrice 210 drone models have been proven to deliver high-quality imagery and data, making them well-suited for forensic analysis [16]. To further enhance their forensic capabilities, researchers have developed software tools designed specifically for these models. These tools can be used to assess system performance in real time or analyze flight logs after a mission has been completed.

To facilitate successful drone forensic investigations, recent research has focused on developing digital forensic methodologies for detecting abnormal flight patterns in drones [17]. One promising approach involves using a drone's motor current and controller direction values to identify abnormal patterns. These methods have shown high levels of accuracy and reliability when tested on real-world datasets involving both normal and abnormal patterns. By combining high-quality imagery and data obtained from drones with advanced digital forensic techniques for analyzing flight patterns, investigators can improve their ability to reconstruct events leading up to incidents and identify potential sources of evidence.

In contrast, Atkinson et al. [18] provided an overview of the current state of drone forensics, its impact on law enforcement, and the challenges associated with drone investigations, as well as the lack of standardized procedures and tools. To address the challenges related to drone forensics, researchers have proposed various solutions. For example, Alotaibi et al. [19] proposed a new framework called the Drone Forensics Readiness Framework and provided a comparison with different models previously existing in the DRF field to validate its use to precede, prepare for, and prevent drone incidents. Similarly, Alhussan et al. [20] suggested a DRFM strategy to standardize DRF protocols and make it easier to store, share, and reuse information. Liang et al. [21] proposed a forensic structure for the Internet of Things based on blockchain technology. Alotaibi et al. [22] provided a comprehensive collection and analysis model for drone forensics which enables the collection of evidence from multiple sources and analysis using automated tools such as machine learning algorithms, while Studiawan et al. [23] presented an innovative approach to forensic timeline analyses for drones. These proposed solutions have the potential to improve the efficiency, reliability, and accuracy of drone forensics, as well as to facilitate communication and collaboration among investigators and agencies.

Overall, the use of UAVs has become increasingly popular in recent years. However, as the use of UAVs has grown, so has the potential for security threats and attacks. Recently, Siddiqi et al. [24] highlighted the various types of attacks that can be used against UAVs as well as the limitations associated with current security measures, such as authentication protocols and encryption, and the need for more advanced security solutions to protect UAVs from potential attacks. A study by Muthanna et al. [25] focuses on addressing these concerns through countermeasures such as blockchain technology, machine learning, fog computing, and software-defined networks.

To address the security threats posed by UAVs, researchers have proposed various detection methods, security measures, and communication advancements. For example, Abro et al. [26] provided an extensive overview of current detection methods, security measures, and communication advancements to improve the security of UAVs and their communication networks. Ko et al. [27] has discussed UAVs, which are integral across diverse sectors and face increasing security vulnerabilities, necessitating robust protocols. Addressing research gaps, our paper proposes a military-focused UAV communication protocol, emphasizing UAV-to-UAV secure communication with features like perfect forward secrecy and non-repudiation. The security position of drone communications is multifaceted, encompassing various challenges that demand thorough consideration. Authentication stands as a critical aspect, ensuring that drones can verify the legitimacy of communication partners. Weak authentication mechanisms may lead to unauthorized access and potential misuse. Encryption is a dominant approach to safeguarding the confidentiality of transmitted data. Without robust encryption protocols, sensitive information, such as surveillance data or control signals, becomes vulnerable to interception by malicious actors. Integrity protection is equally crucial to prevent tampering with communication packets, guaranteeing that received information accurately reflects the sender's intent. Furthermore, the discussion extends to safeguarding against cyber–physical attacks in which not only digital data but also the physical movements and operations of the drone are commandeered. Additionally, the inclusion of perspectives from "Cybersecurity for Industry 4.0 and Cyber-Physical Systems" provides a broader context for understanding cybersecurity challenges in the broader domain of cyber–physical systems, as discussed in [28]. Collectively, addressing these security challenges is imperative to ensuring the safe and reliable operation of drones in various applications from surveillance to delivery services.

A comparative analysis of 20 previously discussed scientific papers, including the aims of the papers, the methodologies used, results, future work, challenges, and weaknesses, is presented in Table 1.

Table 1. Comparative analysis of reviewed studies.

R.P	Subject Matter	Methodologies Used	Results And Future Work	Challenges and Weaknesses
[5]	Drone forensics methods, access to a drone's digital storage, and the retrieval of important data	Inspired by the general instructions from "NIST Special Publication 800-86" for examining artifacts forensically.	Increases knowledge in the field of drone forensics: access to the file system and retrieval of the Android ID of the controller. In future work, carry out more forensic examinations on the Parrot AR and its controller, in addition to other UAVs.	The ability to image a UAV camera forensically without compromising its integrity. There are more than five different file system types on a single UAV aircraft. The software and hardware for the drone have not yet been standardized.
[6]	An increasing need for reliable digital forensic investigation frameworks for UAV	Created a framework for UAV DF investigation and applied it to the DJI Phantom III UAV.	A reliable framework for drone forensic investigation assists in conducting the forensic investigation methodically.	A lack of standards and sufficient details on the forensic investigation of drone incidents.
[8]	The implications of using AI-enabled UAVs for forensic investigations	UAV and AI comparison and implications for forensic investigations.	AI-enabled UAVs can provide more accurate information than traditional methods, reduce the amount of time needed for an investigation by providing real-time data about a crime scene or location, and reduce costs. In the future, further explore these technologies as a means of improving the efficiency and accuracy of forensic investigations.	Preparing UAV investigators to handle UAVs securely throughout operations. The guidelines that drone operators follow differ according to different countries' aviation rules.
[9]	Gathering, fixing, and analyzing significant artifacts from flight data; investigating and assess the relationship between a drone, a mobile phone, and an SD card	Drone flight experiments to simulate a drone's criminal behavior.	According to flight data logs, there is no proof linking a drone, SD card, and smartphone. Identified relational artifacts and temporal analysis rules. Future work will include additional drone-related experiments.	Limited access to certain components due to their small size and lack of standardization among different manufacturers' drones.

Table 1. *Cont.*

R.P	Subject Matter	Methodologies Used	Results And Future Work	Challenges and Weaknesses
[10]	The current state of drone forensics, focusing on challenges and insights	The theory that file carving and a forensic examination of the important discrete digital containers of a drone can be combined into one logical process known as "drone forensics".	The analysis added new perspectives to the knowledge already available on drone forensics and brought forth several characteristics and special difficulties. A futile analysis of the Parrot AR and its controller.	Lack of standardization and understanding about how drones store their data.
[11]	Developing a new method for the digital forensic examination of drones	Examines six drone brands that are frequently utilized for illicit activity and gathers information that might be used in court.	Drone forensics might help law enforcement gather important data required for criminal investigations. Developed a detailed process model for conducting investigations in future work.	Lack of digital forensic tools that are already designed and cover all types of drones and how to handle the data gathered.
[12]	Obtaining a digital forensic preparedness system and improve a proactive technique for DRFs	A comprehensive review of the existing drone forensic framework.	Proposed a model to investigate which obtains a digital forensic preparedness system and can be used to improve a proactive technique for DRFs.	DF tools are insufficient for investigations, even whenexist to extract data from drones. DF software, tools, and methodologies must be updated to consider continuous developments in drones.
[13]	Tracking digital evidence, both live and static, in drones is forensic and makes the evidence identification process easier	The purple team technique was used, technical difficulties relating to digital evidence traceability were investigated, the integrity of recent digital forensic tools when conducting forensic analyses for drones was evaluated.	The suggested UAV Kill Chain can assist in resolving significant issues with UAV security and forensics. Plans call for the use of unencrypted links to expand this research.	Due to drones' architectures and data flow, anti-drone detection and counter-forensics systems are complicated subjects. To perform additional research on different types of drones, it will be necessary to acquire more tools, equipment, and laboratory space, as well as a flight permit.

Table 1. *Cont.*

R.P	Subject Matter	Methodologies Used	Results And Future Work	Challenges and Weaknesses
[14]	Building several criminal-like drone scenarios and investigating them	Examined which approaches and standards work best when conducting investigations using DJI drones.	The DJI Mini2 has a maximum capacity greater than its weight, which could be exploited by bad actors in a variety of situations. Future work will focus on chip-off data extraction and analysis, how carrying different weights affects battery life, and OcuSync 2.0 transmission technologies.	Physical damage to the device, encryption, and limited access to internal components.
[15]	Analyzing the current state of security and privacy issues related to UAVs	Discussed the security risks posed by UAVs and the privacy implications of UAVs.	Proposed various countermeasures against security risks and various measures to preserve privacy. Future work will develop effective countermeasures against potential threats as well as comprehensive legal frameworks.	Current laws are inadequate for addressing the security and privacy risks posed by UAVs. The need to develop more effective countermeasures against several potential threats.
[16]	The potential for UAVs to provide detailed imagery and data that can be used to reconstruct events or identify suspects	Evaluated forensic tool products' capabilities in depth, showed how to analyze recovered evidence, and examined the validity and dependability of retrieved digital evidence.	The DJI Phantom 4 and Matrice 210 UAVs are capable of providing high-quality imagery and data for forensic analysis purposes. Future work will examine the accuracy and dependability of additional artifacts extracted from UAVs.	No widely available instrument can perform a thorough forensic investigation of drones. Different drone processes and data structures, as well as a large amount of diverse data.
[17]	Enhanced digital forensic techniques to identify drones flying unusually	Used a drone's motor current and controller direction values.	The values of the two motors on the right side significantly rose during an unusual flight when the drone moved to the right owing to an outside force. In the future, these values will be used to figure out why this is happening.	Due to the limited number of DJI Phantom 4 Pro trials that were carried out, this conclusion cannot be generalized. The measurement data could be wrong.

Table 1. *Cont.*

R.P	Subject Matter	Methodologies Used	Results And Future Work	Challenges and Weaknesses
[18]	Investigating the present state of drone forensics and how it affects law enforcement and other stakeholders	Explored the various types of drones and their associated forensic challenges.	It is important to understand how drones can be used to commit crimes and how they can be tracked and identified to facilitate investigations.	Due to their small size and limited battery life, drones pose technical challenges when collecting evidence, a lack of clarity regarding how laws should be applied, and ethical considerations and privacy concerns.
[19]	Development of a viable comprehensive framework preparedness for drone forensics	Used a design science research method.	The proposed DRFR framework consists of two levels: a proactive level and a reactive level to deal with drone crime from some pre- and post-incident perspectives. Future work will center on the implementation of the DRFRF in an actual case.	Due to a lack of specific rules or standards that handle incident response, the ISO/IEC 27043 investigative process classes are used as a general framework for incident response.
[20]	Solving the DRF domain's heterogeneity, interoperability, and difficulty problems	The design-science methodology was used to research "metamodeling".	The DRFM model integrates the DRF models, processes, activities, and tasks and comprises three primary levels: the M2-Metamodel Level, the M1-DRF Model Level, and the M0-DRF User Data Model Level. In the future, work will focus on establishing a repository for the DRFM to store all relevant information related to the DRF field.	The lack of standardization in drone forensics models and the diversity of drone infrastructure are challenges.
[21]	The security and privacy of IoT devices and networks	Reviewed IoT forensic systems using blockchain technology.	Ensuring the security of IOT devices by using distributed ledgers to trace transactions and smart contracts to store evidence. Future work will develop more effective solutions for privacy issues.	Scalability, privacy protection, interoperability between different blockchains, and legal considerations are challenges.

Table 1. *Cont.*

R.P	Subject Matter	Methodologies Used	Results And Future Work	Challenges and Weaknesses
[22]	A complete model for data gathering and processing in drone forensics	Adapted systematic methods of design science research.	Presented a CCAFM model which consists of 4 components: data acquisition, data extraction, data analysis, and reporting. Future work will examine the CCAFM model in practice.	Current methods are limited in their ability to collect evidence from drones.
[23]	Examining the timeline of events related to drone operations	Described the architecture of DroneTimeline and the advantages of using it over existing methods, then presented a case study.	Proposed a new tool, "DroneTimeline." Future work includes potential improvements in accuracy and scalability	Open-source forensic software ignores the timeline that might be gleaned from drone device file metadata.
[26]	Complete knowledge of the recent developments that have brought about problems with UAVs	Discussed security risks, privacy concerns, and constraints with UAVs.	Provided potential solutions for security and privacy issues.	Constraints associated with security and privacy and safety are challenges.

2.2. Challenges of Digital Forensics for Drones

The use of drones has increased in recent years, and there has been an increase in drone accidents, causing the need for digital forensic investigations of drones. However, when using drone digital forensics, law enforcement and other investigative agencies must overcome a unique set of challenges. Additionally, there are additional ethical and legal considerations when using drones in criminal investigations. Digital forensic investigations of drone accidents are fraught with intricate challenges spanning technical, legal, and practical domains. The acquisition of crucial flight data stored on manufacturer servers is often hindered by legal restrictions and manufacturers' reluctance to share proprietary information. Ensuring the integrity of flight data proves difficult, with malicious alterations or deletions complicating the accurate reconstruction of accident sequences. Signal interference or communication loss during accidents further delay real-time data capture, creating challenges in reconstructing events. The absence of standardized tools and methodologies in drone forensics leaves investigators grappling with diverse systems and file formats. The complexity of drone software ecosystems, spanning flight control software, firmware, and third-party applications, demands deep expertise in various programming languages. Balancing the need for thorough investigations with privacy concerns becomes delicate, especially when accidents involve sensitive or private areas. Rapid advancements in drone technology require forensic experts to adapt continually. Physical damage, environmental factors, and the global variability of regulatory frameworks add further layers of complexity. Finally, remote or inaccessible accident locations pose logistical challenges in retrieving evidence. Addressing these multifaceted challenges necessitates a collaborative, multidisciplinary approach encompassing forensic experts, legal professionals, drone manufacturers, and regulatory bodies, emphasizing ongoing research and development in drone forensics to keep pace with technology. Three major categories of criminal investigations are discussed below.

2.2.1. Physical Challenges

The physical obstacles that must be overcome in drone forensics investigations are referred to as "physical challenges" and include the following:

- Hardware component fragility: Drones are typically made of lightweight materials that can be easily damaged or destroyed during the investigation process. The variety of the components, their interconnectedness, and their interactions with the environment all contribute to the drone forensic domain's complexity [20].
- Small size: Finding drones can be difficult because they are often small and can be easily destroyed or hidden by suspects [9].
- Environmental factors such as temperature, humidity, and dust may make it challenging for investigators to access actual evidence, such as parts of crashed drones or damage from an unusual flight occurrence [17].
- Power supply: Drones can be utilized in isolated areas where power sources may be hard to obtain or nonexistent. As a result, drones may not be able to stay in the air long enough for investigators to gather all the necessary evidence because of their short battery lives [6].
- Transportation: As drones are frequently used in remote areas, it is more difficult for investigators to reach them, locate them, or transport them to a lab for analysis for a forensic investigation [6]. This also presents issues for establishing a chain of custody.

2.2.2. Legal Challenges

The legal problems that arise when attempting to use drones in forensic investigations are referred to as "legal challenges" and include the following:

- Jurisdictional concerns: The recovery of evidence from drones can be made more difficult by the use of cloud-based storage systems because data may be kept in various locations [5].

- Privacy concerns, particularly when drones are used to collect data from individuals without their knowledge or consent or fly over restricted areas that may limit or restrict access to certain types of data or information during an investigation. In addition, drones can offer a more thorough view of a crime scene than conventional techniques, but they also pose special data security and privacy issues [8].
- Powers and permissions: Analyzing and storing these data securely may require specialized hardware and software and access to specialist tools and equipment, as well as specialized knowledge and expertise; these are requirements for drone forensics which not all investigators may have [8].
- Ethical considerations: There is a risk of unauthorized access to UAVs due to weak authentication protocols or a lack of encryption [15] which must be considered when conducting a drone forensic investigation, including ensuring that any data gathered are used only for the investigation and are not shared with third parties without consent, transparency about methods and findings, and compliance with laws.
- Lack of regulation: There are no laws or regulations governing the use of drones for this purpose in many countries, which can lead to potential legal issues if the drone is used improperly or without proper authorization [15]. Additionally, some countries have restrictions on where drones can be flown.
- Potential evidence contamination: Certain traces are extremely fragile and are quickly altered by environmental, animal, or human activities [8]. There is also a risk that using a drone could damage or destroy evidence at a crime scene if it is not operated properly.

2.2.3. Technical Challenges

“Technical challenges” are the issues associated with collecting, analyzing, and interpreting data from drones, including managing the several types of data saved on a drone, such as videos and photographs. Additionally, technical challenges encompass comprehension of the different protocols necessary for communication between a drone and its controller or other devices, as well as knowledge of the various drone sensor types and how they relate to one another. Technical challenges related to drone forensics include the following:

- Preservation: Due to the intricacy of the technology and the requirement for specialized training, the use of UAVs in forensic investigations has a unique set of difficulties [8] which include data that can be easily corrupted or lost due to hardware or software failures, malicious attacks, or other external reasons.
- Collection: A thorough investigation into a crime or incident using a drone may not be possible given its small size and limited storage capacity. In addition, the drone may not be able to stay in the air long enough for investigators to gather all necessary evidence because of its short battery life, making it difficult to collect a large amount of data in a short amount of time [6].
- Analysis: To understand what transpired during a certain flight or event, it is often necessary to examine the various sorts of data that drones frequently hold, including pictures, videos, and flight logs. In addition, it is challenging to collect and evaluate data from drones due to the complexity of the data contained there and the lack of standardized data formats [10].
- Storage: Data kept on remote servers or in on a cloud server can present additional difficulties because investigators require access to these services [19]. It may be possible for users to delete or modify data stored on drones, making it more difficult for investigators to gather evidence properly.
- Recovery: To properly recover deleted or corrupted data from a drone’s memory card or other storage device, specialist tools may be needed. The investigations are made more difficult by the lack of tools, particularly those intended for digital forensics on drones [8].

- Complexity: Drones use a variety of different software platforms that are constantly being updated and changed. This can make it difficult to accurately capture and analyze all relevant data from a drone's system during an investigation. In addition, finding evidence that can be utilized to recreate the events that took place during a drone's operation is the most difficult part of drone digital forensics [9].
- Encryption: Data encryption can make it difficult or even impossible for digital forensic investigators to access encrypted data stored on or transmitted by a drone, which poses a substantial barrier for them when working with drones [13]. So, either the drone maker or the user must provide investigators with the encryption key or password in the beginning.
- Lack of consistency: A significant problem occurs when the data collected from drones are inconsistent. This makes it difficult to create a uniform set of digital forensics tools and methodologies for UAVs [9]. This is brought on by several elements, such as the kind of drone and its operating system. Moreover, comparing data from various sources might be challenging because different drones may use different data formats.
- Lack of standardization: This makes it challenging to create a consistent set of digital forensics methods and procedures for UAVs [20]. So, there is currently no standard protocol for the use of drones in digital forensic investigations, making it difficult to ensure consistency and accuracy in the collection and analysis of data.
- Cost: Forensic investigators are faced with an additional obstacle due to the quick development of drone technology and related components [22]. Accordingly, drone forensic investigations can be costly due to the need for specialized equipment and personnel to keep pace with this development.
- Limited battery life: Drones may not be able to stay in the air long enough for investigators to gather all necessary evidence [6]. This means that drones have a limited operational time before requiring recharge.
- Connections: The majority of drones are connected to other devices through Wi-Fi or Bluetooth, so gathering evidence from these connections presents an additional challenge [8], making it vulnerable to interception by malicious attackers.
- Big data: Drones are frequently fitted with numerous sensors, cameras, and other devices that produce a significant amount of data, which further increases the complexity of the digital forensic procedure [17].
- Training: Skills and specialized knowledge are needed for drone forensics. To properly examine drones, forensic investigators need to have a good understanding of the system's architecture. Due to the complexity of drone hardware and software, they must be familiar with various drone types and their components [20].
- Open-source software: It may be challenging for forensic investigators to recognize the source code used on a specific drone. This also makes it difficult to identify any modifications that have been made, the origin of malicious payloads, and activity on drones [26].
- Limited computing power: Several drone models cannot save a significant amount of data because of their low computational capacity, which might make it challenging for digital forensics investigators to gather all pertinent information throughout an investigation [11].
- Quality of images: The challenge of obtaining high-quality images from drones is that the resolution of the camera and the distance from which it captures images can have a significant impact on the quality of photographs taken by drones [18].

2.3. Methods Used in Investigating Drone Accidents

Investigating drone accidents requires the use of different digital investigation methods to ensure accuracy. Each method has its advantages and disadvantages, and investigators must carefully evaluate and decide which methods to use based on the specific circumstances of each case. Table 2 illustrates the advantages and disadvantages of various methods used in digital investigations of drone accidents. Before creating the table, it was necessary to identify commonly used digital investigation methods for such investigations. Some of the frequently utilized methods include the following:

- Forensic imaging entails making a complete copy of a drone's storage media for further analysis.
- Network forensics involves analyzing network traffic to detect any suspicious activities associated with a drone.
- Memory analysis involves examining the volatile memory of a drone to uncover any relevant running processes or data.
- Mobile device forensics involves analyzing any mobile devices that may have been used to control or communicate with a drone.

Table 2. The advantages and disadvantages of various methods used in digital investigations of drone accidents.

Methods	Source	Advantages	Disadvantages
Forensic Imaging	[29]	Creates a comprehensive copy of all data, allowing for an accurate analysis. Can recover deleted data and examine essential metadata such as GPS coordinates and timestamps. Ensures that all evidence gathered during the investigation is admissible in court.	Demands specialized equipment and expertise and can be time-consuming. May not capture all relevant data. Requires physical access to the drone's storage device. It may not be possible to recover all data from a damaged or destroyed drone.
Network Forensics	[30]	Can detect suspicious network activity. Provides details about a drone's communication with other devices. Helps track down perpetrators without requiring physical access to the drone or its components.	Requires access to network logs or other data from third-party devices. May not be useful if the drone was not connected to a network during the accident. May not capture all relevant data and may be incomplete or corrupted due to issues with network connectivity. Requires specialized expertise.
Memory Analysis	[31]	Can provide information about running processes on the drone. Can recover deleted data from volatile memory. Can be used to identify malware or other malicious activity.	Requires specialized tools and expertise. Volatile memory is easily overwritten or lost if power is lost. May not be able to provide information about external factors that contributed to the accident.
Mobile Device Forensics	[32]	Can provide information about control or communication with a drone. May contain valuable evidence such as GPS location data or text messages related to the incident. Does not require physical access to the drone itself. Can provide valuable information about the drone's flight path, altitude, and speed.	Requires access to the mobile device. May require specialized tools and expertise. May require access to third-party data such as cloud backups or application usage logs. May be subject to tampering or hacking, which could compromise their integrity. The accuracy of the data obtained may be affected by factors such as signal strength and interference.

3. Digital Twin Technology

This section focuses on digital twin technology (DTT) and examines the concept, architecture, and characteristics of digital twins. The section also explores how this technology works and highlights its potential vulnerabilities.

3.1. Digital Twin Concept

The concept of digital twin technology is gaining traction in the fields of engineering and computer science. It uses real-time data and simulations to create a digital copy of a physical object, system, or process. This virtual model can be used to analyze, monitor, and tune performance, as shown in Figure 2. DTT is widely used in the engineering, manufacturing, and construction industries to improve efficiency and reduce costs by predicting potential problems before they occur. It can also be applied to other fields like transportation and healthcare to improve decision making and increase performance. DTT can be defined as a system that combines physical and virtual components to create a real-time digital copy of a physical asset or process and an advanced simulation tool that allows for the creation of a virtual model of a physical system that can be used to monitor and enhance its performance. It employs data analytics and machine learning algorithms to generate a dynamic, real-time model of a physical system that enables optimization and predictive maintenance [33–35]. It should be noted that there is not yet a unified definition of digital twin technology because DTT is an innovative approach and a rapidly growing field.

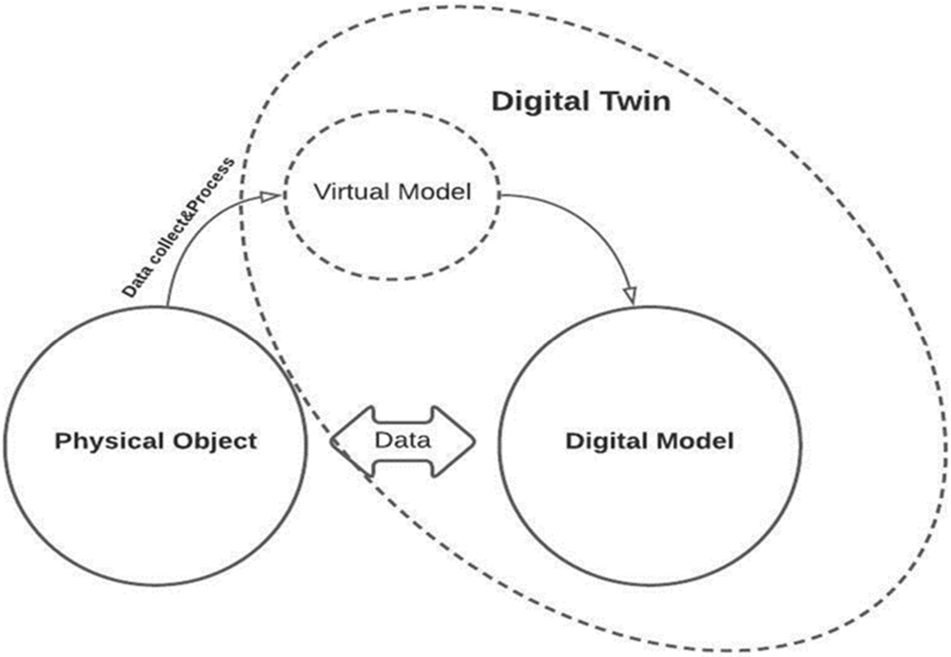


Figure 2. Bridging the physical and digital realms with the concept of digital twins.

3.2. Digital Twin Architecture

There are several different architectures for digital twin technology, depending on its specific application and requirements. However, all these architectures have similar characteristics, including the integration of sensors, capabilities for managing and analyzing data, tools for simulation and modeling, and end-user interfaces. Figure 3, illustrates the typical structure of a digital twin, which consists of three layers.

An example of a digital twin architecture is given in a recent research article by Redelinghuys et al. [36] in which a six-layer digital twin architecture is proposed. These layers include data acquisition, data processing, data analysis, decision making, communication, and application. The primary goal of this architecture is to enable real-time monitoring and control of manufacturing processes by creating a virtual replica of a physical system.

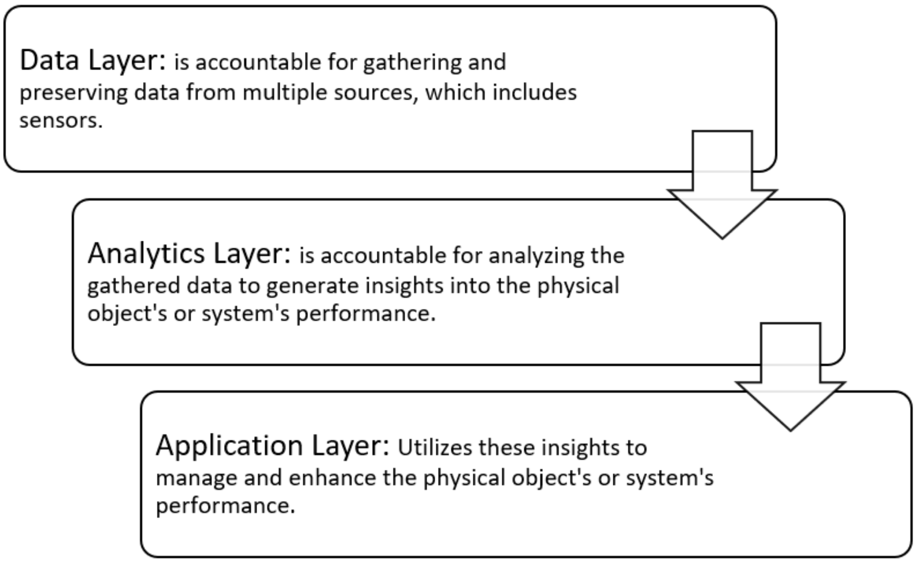

Data Layer: is accountable for gathering and preserving data from multiple sources, which includes sensors.
Analytics Layer: is accountable for analyzing the gathered data to generate insights into the physical object's or system's performance.
Application Layer: Utilizes these insights to manage and enhance the physical object's or system's performance.

Figure 3. Comprehensive digital twin structure.

In another example, according to [37], a digital twin architecture comprises three essential components: a physical system, a cyber system, and a cloud system. This architecture aims to facilitate more efficient management of complex cyber–physical systems across various domains.

Through the examples mentioned, we can conclude that the structure of a digital twin is not fixed and varies according to the purpose of its creation, but some basic layers must be present.

3.3. Characteristics of a Digital Twin

It is common knowledge that each technology has a distinct collection of characteristics that distinguish it and differ depending on the specific application and use case. Consequently, it is important to understand a technology's features and its potential applications before utilizing it. The key characteristics of digital twins are presented in this section. Table 3 presents an overview of these characteristics, including their descriptions, benefits, and examples.

Table 3. Characteristics of digital twins.

Characteristics	Description	Benefits	Examples
Real-Time Monitoring	This is achieved through the integration of various sources, such as sensors, cameras, and other IoT devices.	Allows for the early detection of potential issues or anomalies in a physical asset, enabling proactive maintenance and reducing downtime. Provides valuable insights into the performance and behavior of the asset, allowing for optimization and improvement.	In healthcare, digital twins can monitor patient vital signs or medical equipment to ensure timely interventions. For example, a DT of a cancer patient can continuously monitor their vital signs and alert healthcare providers if there are any abnormalities that require immediate attention [38].

Table 3. *Cont.*

Characteristics	Description	Benefits	Examples
Predictive Analytics	Includes the use of statistical algorithms and machine learning techniques to analyze data from sensors, IoT devices, historical data, and other sources and predict future outcomes.	Identifying potential problems before they occur, enabling proactive measures to prevent them from happening. Optimizing operations by identifying areas where improvements can be made. Reduces downtime by predicting when maintenance or repairs will be required.	In the energy sector, where DTs are used to monitor power plants and predict when maintenance will be required, energy companies can identify potential problems before they arise and take corrective action by examining historical data on equipment performance and environmental factors like temperature and humidity levels [39].
Simulation Capabilities	This is achieved through the use of advanced modeling and simulation techniques that allow digital twins to accurately replicate the behavior of physical systems.	Testing and refineing designs before they are implemented in the real world, reducing the risk of costly errors and delays. Optimizing performance by identifying areas for improvement and testing different scenarios to find the best solution.	Engineers can test new designs and improve existing ones using digital twins to simulate aircraft performance. For example, it has been discovered that the implementation of a UAV DT system can greatly enhance the safety performance of a UAV throughout its airspace flight [40].
Scalability	The capacity to handle an increasing system's complexity and data volume; because of this, digital twins can change and adapt to the changing requirements of the system they represent.	Enables organizations to grow without having to invest in additional physical assets. Enables better decision making by providing real-time insights into the system's performance. Facilitates collaboration between different stakeholders and teams by providing a common platform for data exchange.	DTs can simulate entire cities, including transportation systems, buildings, and energy grids, to improve sustainability and optimize resource usage. For example, the project Digital Twin Earth, which aims to create a virtual replica of the planet Earth to study climate change and its impact on various ecosystems [41].
Remote Control	This indicates that users are able to interact with and modify the digital twin even without physically being present at the site.	Facilitating a secure space for experimentation without potential harm, allowing remote control of physical systems globally in real time and enabling collaborative access and modification of the digital twin by multiple users Enables multiple users to access and modify the digital twin, regardless of their physical location.	DTs can be used to enable users to interact with and control a physical entity. For example, a human user and a robot can be connected through a DT system, which enables real-time remote control to monitor and adjust parameters [42,43].

3.4. How Does a Digital Twin Work?

The creation of a digital twin involves multiple steps. Initially, sensors installed on a physical object or system collect data regarding its position, temperature, pressure, vibration, and other relevant parameters. This data are then processed using machine learning algorithms to generate a virtual model of the physical object or system that includes all relevant parameters affecting its behavior and performance. Subsequently, a digital model of the physical object or system is created based on the processed data. The digital twin is utilized to simulate various scenarios and conditions that the physical object or system may encounter in the real world, enabling engineers and operators to test different strategies and optimize performance. As the physical object or system operates in reality, sensors continue to gather data that are fed back into the digital twin model for ongoing monitoring and analysis of its behavior.

3.5. Potential Vulnerabilities

As with any technology, digital twins also have potential vulnerabilities that need to be addressed. In this section, we discuss the potential vulnerabilities of digital twins.

- Cybersecurity: The data contained within digital twins can be compromised in terms of their confidentiality and integrity due to cyberattacks [44].
- Data privacy: If digital twins are accessed by unauthorized individuals, the sensitive information they contain could be exploited for harmful intentions [45].
- Interoperability: The usefulness of digital twins can be limited if they are unable to communicate with other systems or devices [46].
- Lack of standardization: At present, there is a lack of uniformity in the creation and utilization of digital twins, which may result in irregularities and weaknesses in their construction and execution [47].
- Ethical issues: The utilization of digital twins gives rise to ethical issues regarding confidentiality and privacy [48].
- Reliability: The dependability and precision of digital twins rely on the excellence of the information they hold, which may be jeopardized by inaccuracies or deliberate tampering [49].
- Integration with legacy systems: Incorporating digital twins into pre-existing legacy systems can prove to be a difficult task as there may be disparities in technology, standards, and protocols [50].

4. The Rational behind Choosing the Digital Twin Technology

In recent years, drones have gained increasing popularity as either means of committing crimes or as tools to assist in investigations, leading to an increase in accidents involving drones. Consequently, digital forensic investigations play a crucial role in drone accident investigations and implementing preventive measures to improve safety [51,52].

As discussed previously, unfortunately, drone accident investigation can be difficult, has many weaknesses, and faces many challenges. Also, traditional forensic investigation methods, such as physical examinations and analyses, can be time-consuming and could potentially exacerbate damage to the drone or its surroundings. Furthermore, the high heights, long distances, and remote locations that drones can cover make it challenging to accurately reconstruct accident sites and understand drone behavior before and during an incident.

As discussed, digital twin technology has emerged as a solution with great potential for addressing the complexities of forensic investigations of drone incidents. DT technology involves generating a virtual replica of an actual drone and its surroundings, enabling the simulation of different scenarios, and analyzing the details of accidents. This technology provides numerous advantages, including the following:

1. It provides a secure and controlled environment for drone incident investigation. Investigators can interact with and modify the digital twin without risking further damage to the physical drone or its surroundings. This can help preserve evidence and prevent contamination of the accident site, ensuring a thorough investigation.
2. It supports the real-time monitoring and analysis of drone behavior. The data transmitted from cameras and sensors on an actual drone allow investigators to monitor the drone's movements and behavior during and before the accident. This can aid in identifying the potential causes of an accident and implementing preventive measures to improve safety.
3. By creating a virtual replica of the drone and its surroundings, investigators can test hypotheses, simulate different scenarios, examine various theories regarding the causes of the crash and identify the most probable scenario. This can save time and resources compared to traditional methods.

As a result, digital twin technology is considered a promising solution to enhance the accuracy and effectiveness of forensic investigations related to drone accidents.

5. Simulation Scenario and Implementation

In this section, part of the digital twin technology solution is simulated using ROS (Robot Operating System, version 2), an open-source software framework for building robotics applications. It provides a variety of libraries and tools for developing and simulating robotic systems, including support for simulation environments such as Gazebo (3-D simulator) and Rviz (3-D visualization). Additionally, ROS (version 2) provides a wide range of tools for monitoring and controlling the system in a virtual environment, allowing developers to fine-tune and optimize the system in real time. This makes simulating the digital twin technology using ROS software (version 2), along with Gazebo and Rviz, a powerful tool.

The simulation scenario and the implementation of the simulation are described in this section.

5.1. Drone Accident Scenario

An autonomous drone navigating to the desired location is equipped with four brushless DC motors, a sonar sensor for the dynamic and accurate mapping of the accident site, and a camera that takes photographs directly in sequence [53–56]. The drone is sent to a desert environment to surveil an incident scene, but the drone is exposed to the wind, which causes it to become unbalanced. This leads to the drone deviating from its trajectory, colliding with an obstacle (a mountain), and then crashing, and the quality of the captured images is impacted. Figure 4 provides the sequence of the scenario that was simulated.

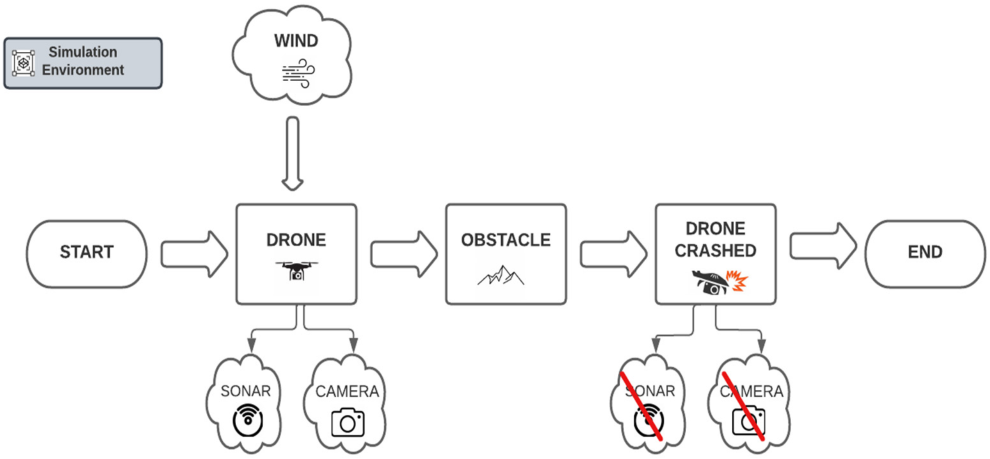


Figure 4. Sequential simulation scenarios unfolding to model dynamic processes and interactions.

5.2. Implementation of the Simulation

This section describes the hardware and software components required for implementing the simulation scenario. The key point is that after reading this section, it will be possible to set up a simulation environment and demonstrate the scenario.

5.2.1. Hardware Components

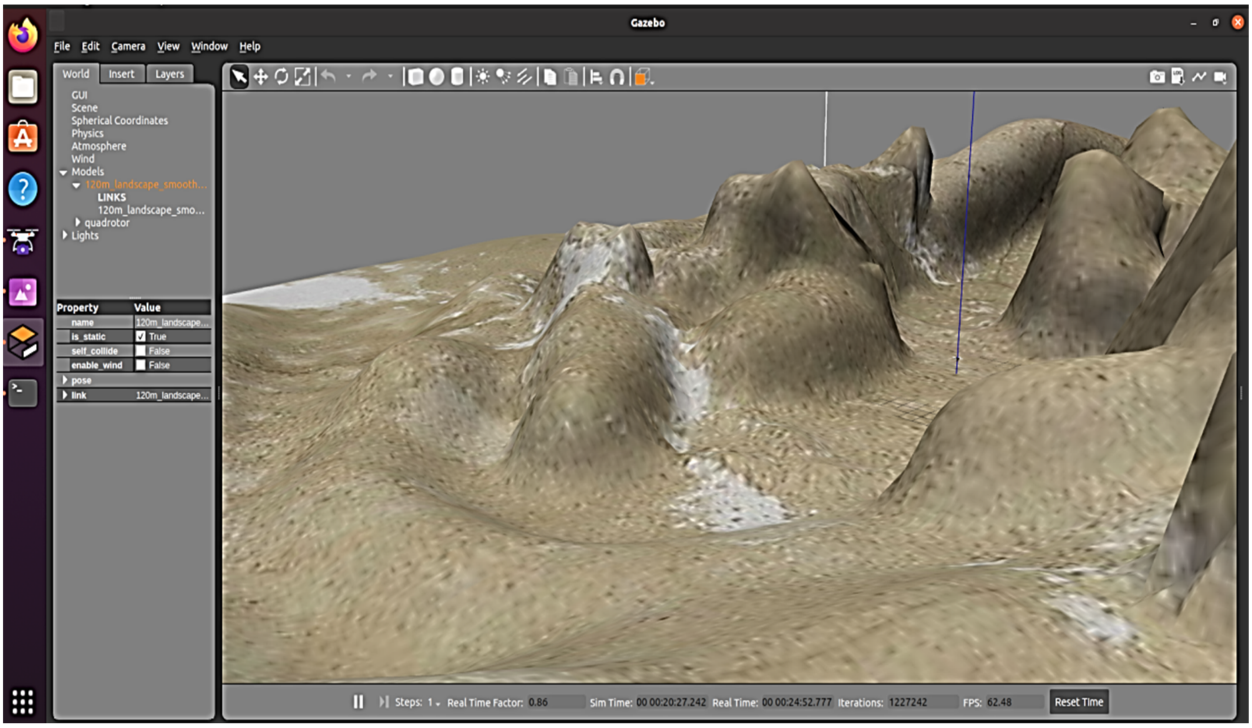
- The simulation environment was developed and tested on a Dell computer.
- The computer has a 2.20 GHz Intel Core 2.19 processor, 63.7 GB of memory, and the operating system Windows 10.

5.2.2. Software Components

The software components included Ubuntu 20.04 (Bionic), an open-source software operating system, and Robot Operating System (ROS version 2) noetic distribution, an open-source software framework for building and programming robots, including support for simulation environments Gazebo (3-D simulator) and Rviz (3-D visualization), all of which were executed on VMware Workstation version 16. ImageJ software (version 1.54f) was used to analyze and process digital images.

5.2.3. Simulation Experiment

The ROS software (version 2) was used to simulate a drone accident in a desert and in a controlled environment, as shown in Figure 5. A 3D model of a drone equipped with sonar and a camera was used, as shown in Figure 6. The data collected included the orientation of the drone in three dimensions (X, Y, and Z), as shown in Figure 7, as well as the time log data. It also included the simulation parameters, such as winds at a speed of 20 mph in the direction of the Y-axis, which were used to determine the effectiveness of the simulation in causing the drone's imbalance, deviation, and crash. Additionally, the study compared the quality of the images captured before and after the incident to assess the impact of the accident on image quality [57]. In addition, the ROS software (version 2) incorporated the Rviz tool to visualize camera and sonar data collected during the simulation, as shown in Figures 8 and 9.



Property	Value
name	120m_landscape...
is_static	☑ True
self_collide	□ False
enable_wind	□ False
pose	
link	120m_landscape...

Steps: 1 Real Time Factor: 0.86 Sim Time: 00 00:20:27.242 Real Time: 00 00:24:52.777 Iterations: 1227242 FPS: 62.48

Figure 5. High-fidelity simulation capturing the nuances of a desert environment.

This provided a comprehensive view of the drone's movements and helped identify any anomalies or deviations in its flight path. The simulation of the scenario was performed in a pre-programmed environment that emulates real-world conditions, using the Python programming language and the widely used Rospy library that is typically used for developing robotics applications.

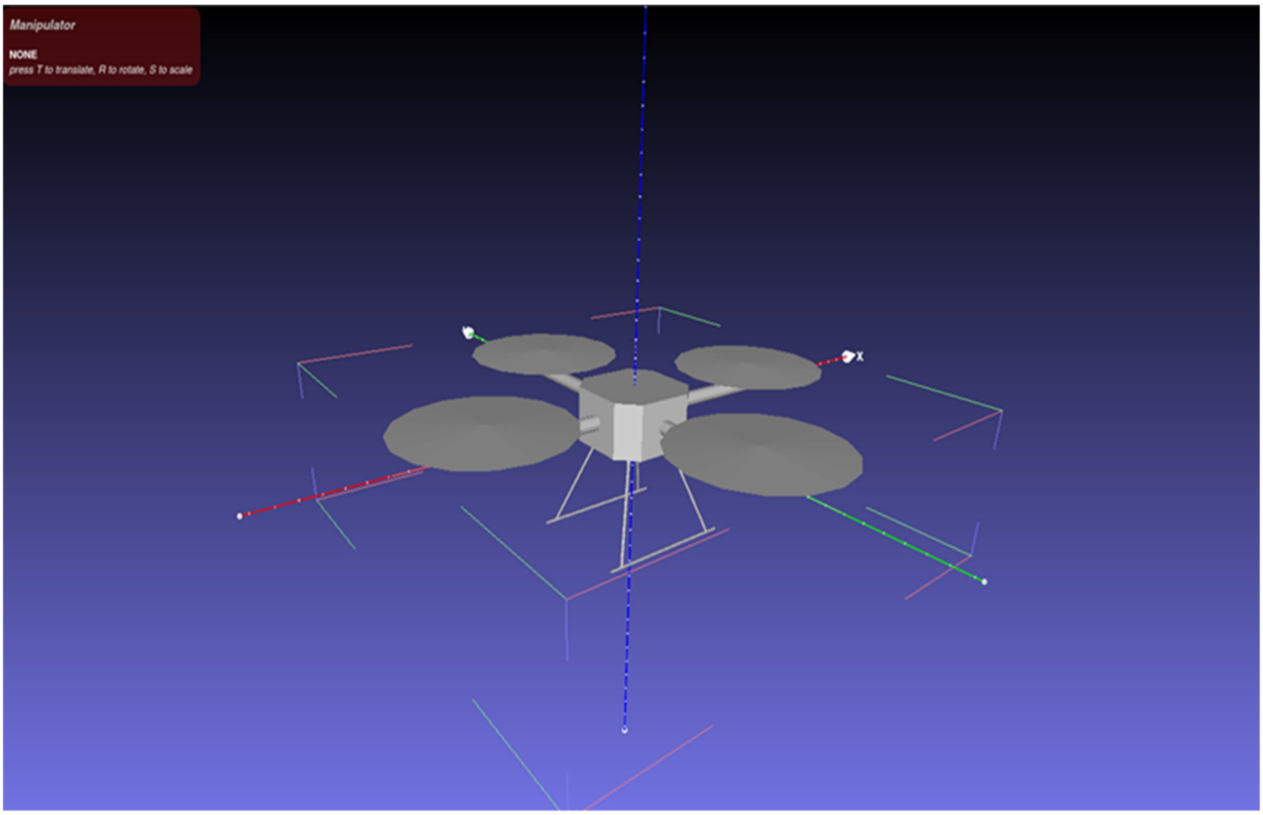
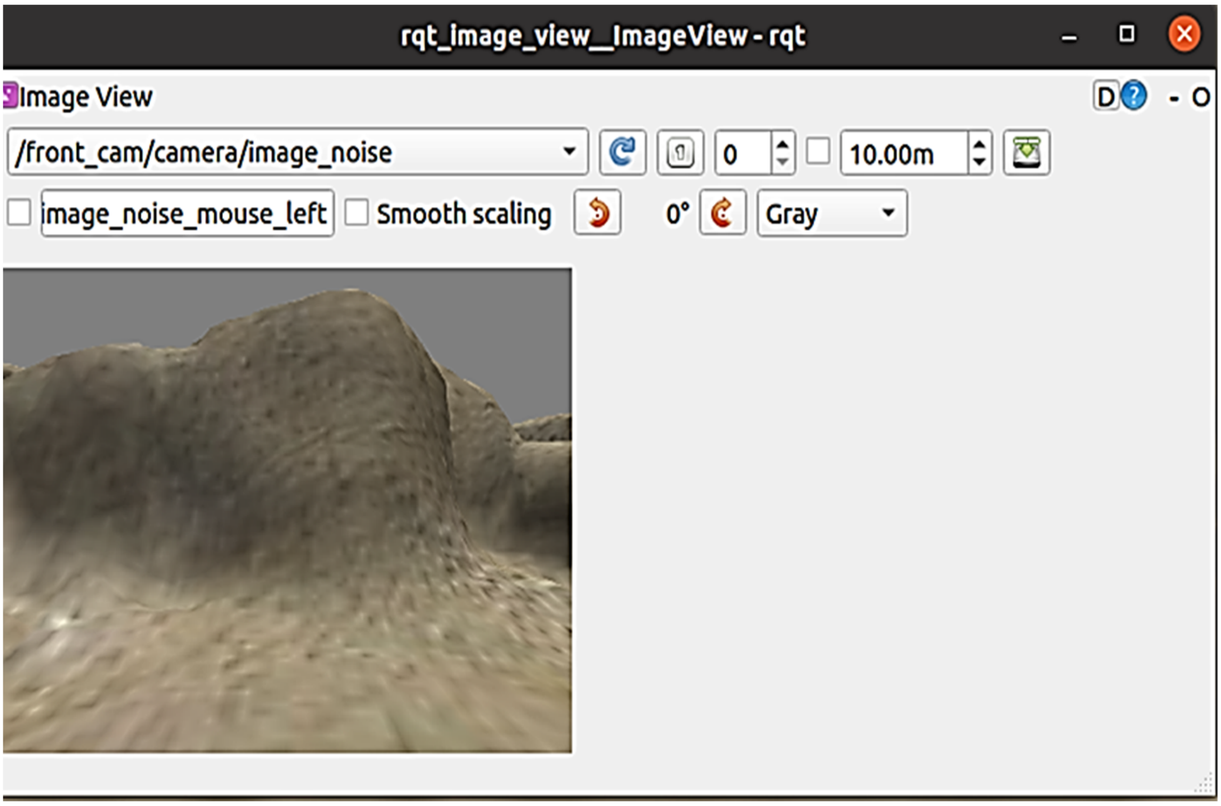


Figure 6. Detailed 3D model of a drone, showcasing design intricacies.



rqt_image_view__ImageView - rqt

Image View

/front_cam/camera/image_noise 0 □ 10.00m

□ image_noise_mouse_left □ Smooth scaling 0° Gray

Figure 7. Visual representation of various drone orientations.

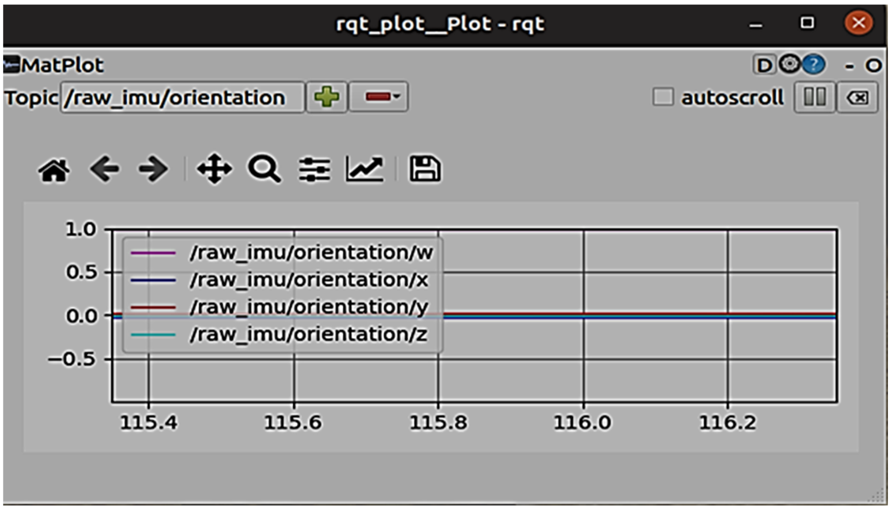
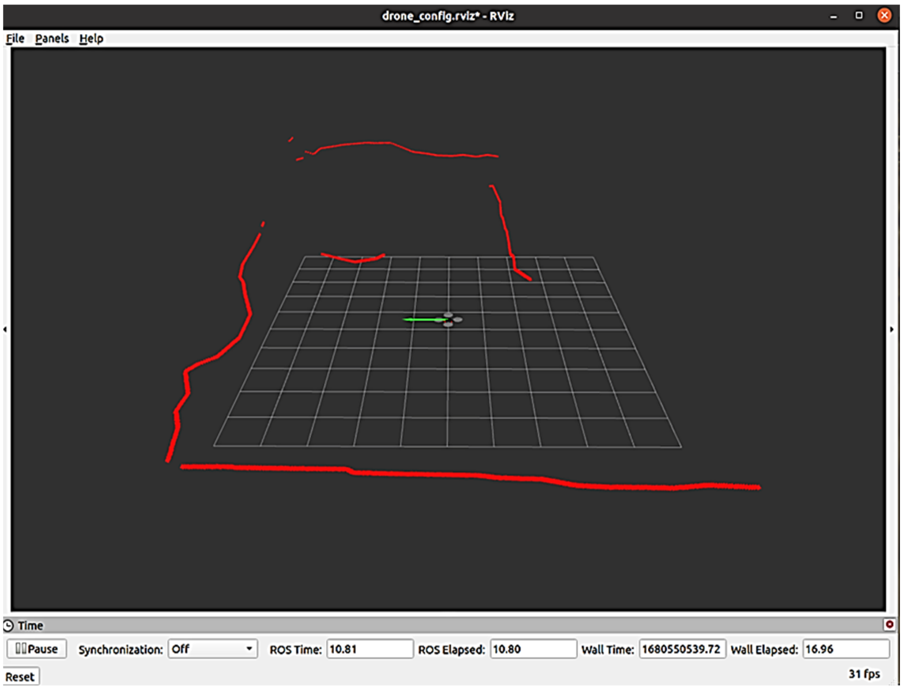


Figure 8. Drone camera.



Synchronization: Off ROS Time: 10.81 ROS Elapsed: 10.80 Wall Time: 1680550539.72 Wall Elapsed: 16.96

Figure 9. Utilization of drone-mounted sonar technology for precise mapping.

6. Results and Discussion

The results of the experiment highlighted the importance of simulation in investigating drone accidents and providing a safe and controlled environment to replicate real-world scenarios and gather valuable data without risking damage to the drone or other equipment or when the drone is not physically accessible. After conducting simulations for the aforementioned scenario and collecting and analyzing data, the results showed the following:

1. Orientation data: The graph in Figure 10, shows the orientation of the drone in the X, Y, and Z dimensions over time. The X, Y, and Z dimensions are represented by the blue, red and green lines, respectively. The time (in seconds) is represented by the x-axis. The graph shows that the drone's orientation remains relatively stable in the X, Z, and Y dimensions but then experiences significant variations, which could indicate the drone's response to a simulated wind of 20 mph in the y-axis direction, as

mentioned earlier. This indicates that the simulation is efficient and provides valuable data for analyzing the stability of the drone and the response to various simulation parameters [25,27].

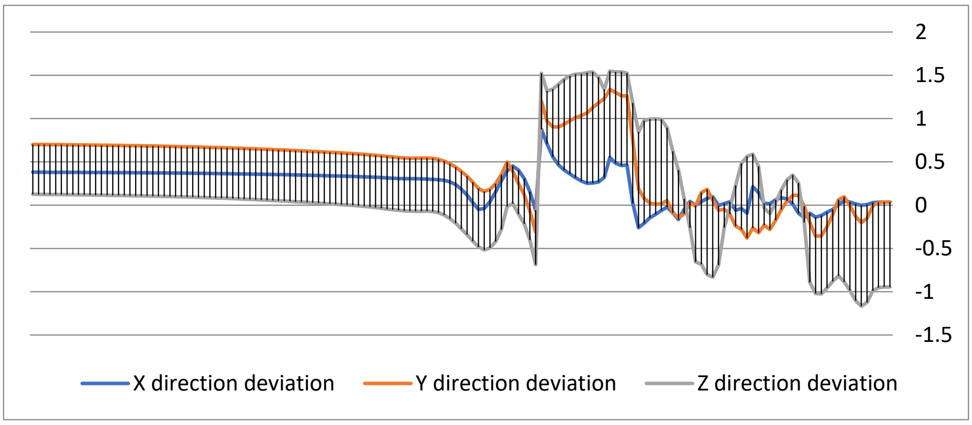


Figure 10. Visualization of drone orientation.

2. Image quality: The image quality analysis was conducted by visual inspection, which involved visually comparing the two images side by side and identifying any differences in image quality, such as differences in sharpness, color accuracy, and noise levels. As shown in Figure 11, a photograph was taken before the drone was exposed to the wind, while in Figure 12, a photograph was taken while the drone was exposed to the wind. In addition, ImageJ software (version 1.54f) was used for image analysis, which involved analyzing the image contrast factor, for which the contrast of image 1 (after) was 0.849, while the contrast of image 2 (before) was 1.160. This suggests that image 2 (before) has greater contrast than image 1 (after). As shown in Figure 13, this suggested that it was of higher quality in terms of image clarity and sharpness, demonstrating the impact of the accident on the camera system and the effectiveness of simulation in proving it [7,28].

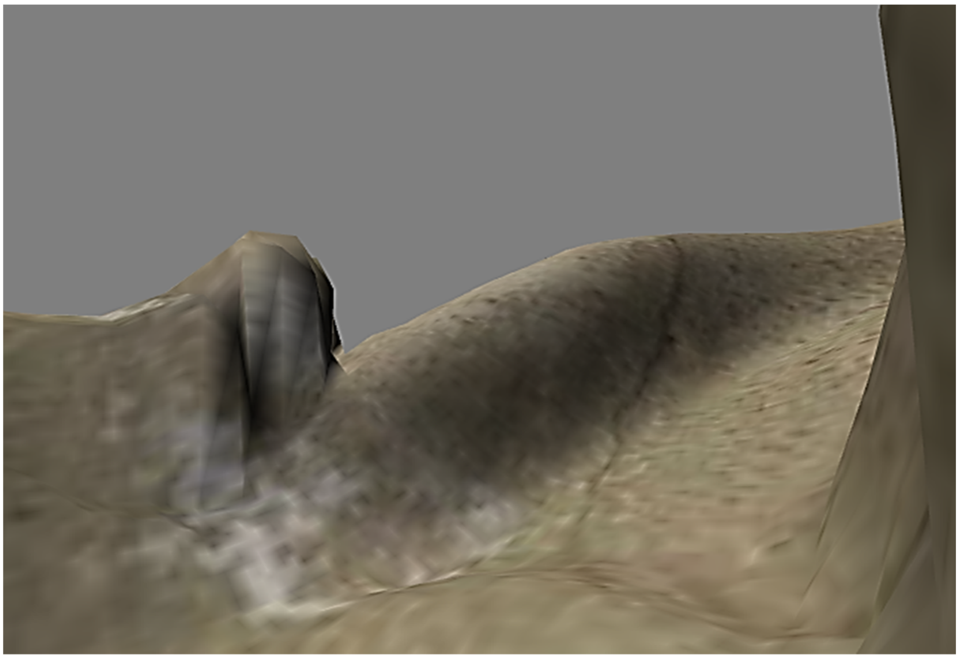
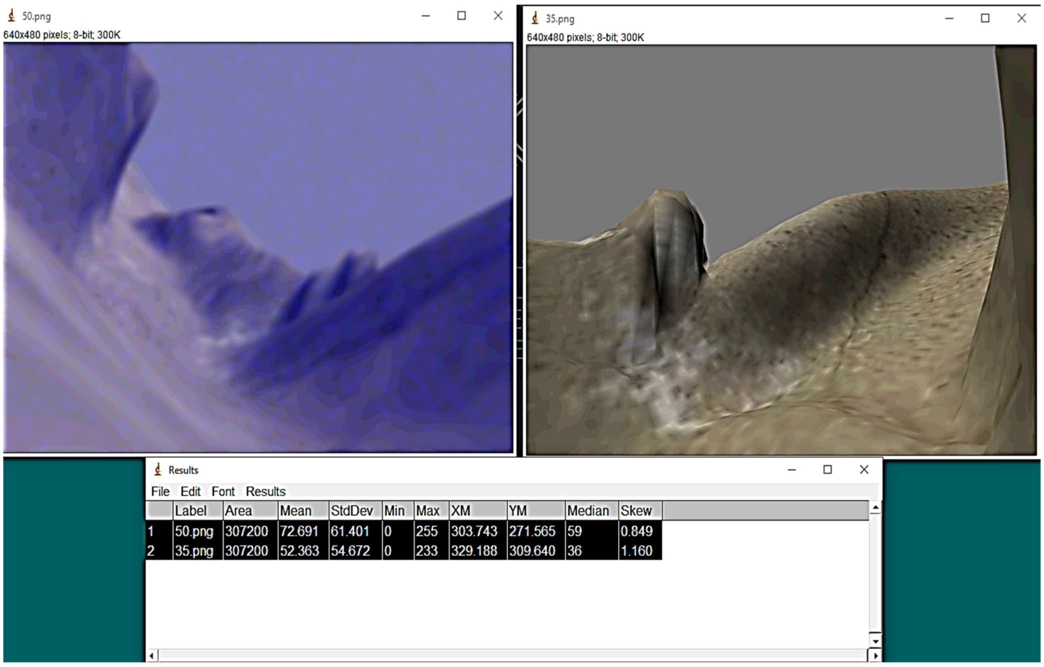


Figure 11. A Photograph taken before (image 1).

Figure 12. A photograph taken after (image 2).

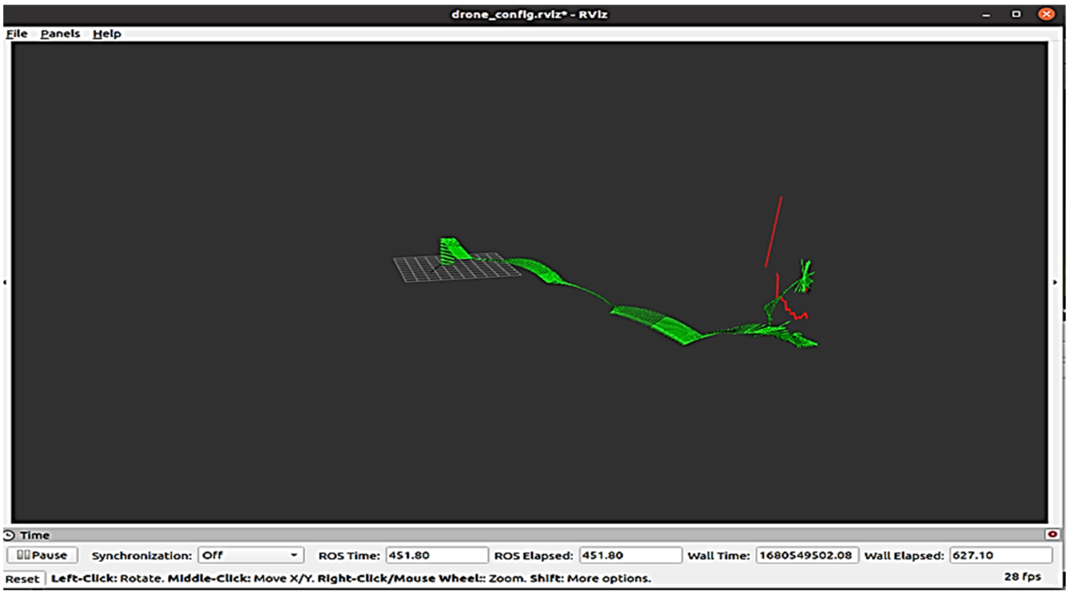


	Label	Area	Mean	StdDev	Min	Max	XM	YM	Median	Skew
1	50.png	307200	72.691	61.401	0	255	303.743	271.565	59	0.849
2	35.png	307200	52.363	54.672	0	233	329.188	309.640	36	1.160

Figure 13. A Comparison of the two images, analyzed using ImageJ (version 1.54f).

3. Sonar data: Sonar data collected during the experiment were used to identify potential hazards and obstacles in the environment that may have contributed to the accident, as well as to provide a detailed view to study the drone's flight path during the simulation process. From launch to collision and crash, the simulation of sonar data provides valuable insights into the drone's behavior and the factors that contributed

to the accident. Figure 14, shows sonar data in which the red color represents the obstacles surrounding the drone and the green color represents the drone's path.



Synchronization: Off
ROS Time: 451.80
ROS Elapsed: 451.80
Wall Time: 1680549502.08
Wall Elapsed: 627.10

Left-Click: Rotate. Middle-Click: Move X/Y. Right-Click/Mouse Wheel:: Zoom. Shift: More options.

28 fps

Figure 14. Sonar data.

The results of these experiments, which included analyzing both the deviation in the directions of the drone and therefore its instability and crash and the quality of the extracted images as well as the sonar maps, indicate that the simulation was effective as it became easy to visualize and analyze the behavior of the drone over time and in various conditions and to clarify the surrounding environment, which provided insights into their behavior and response to different simulation criteria, which led to a better understanding.

Thus, we can consider simulation a valuable tool that helps in digital forensic investigations of drone accidents. By recreating an accident scenario in a simulated environment, investigators can analyze the behavior of a drone and the surrounding environment gain insight into the causes of the accident and identify possible contributing factors. Simulations can also help investigators test different scenarios and hypotheses, which can lead to a better understanding of accidents and the development of effective countermeasures.

As a result, simulation technology can be a valuable asset in the field of digital forensics, particularly when it comes to drone incidents, demonstrating the potential of digital twin technology in this field.

As drones become vital first responders in law enforcement and emergency situations, the proposed forensic approach offers significant advantages by streamlining investigations. In critical scenarios like fire emergencies, drones can provide real-time situational awareness to teams before their engagement, ensuring their safety and the community's. Similarly, during hostage situations with armed perpetrators, continuous drone footage can inform optimal decision making as the situation evolves. Moreover, even if drones malfunction or are compromised, the proposed forensic approach allows for the recovery of digital evidence for further analysis and actionable insights.

7. Conclusions and Future Work

7.1. Conclusions

In this study, we conducted a thorough review of the literature on the challenges associated with drone digital forensic investigation and divided them into three different categories. Considering this, we proposed a promising solution to overcome the challenges of the digital forensic investigation of drones. The solution is based on digital twin technology, which is one of the technologies that is having a noticeable impact in various fields such as healthcare and industry. The simulation is implemented as part of the digital twin solution. Using ROS (version 2) and the simulation environments Gazebo and Rviz, a specific drone crash scenario was simulated, and real-time data were extracted and analyzed. As a result, the simulation proved effective in determining the behavior of a drone before and during the accident and its impact on the quality of images collected by the drone, which indicates the effectiveness of this technology in the future and what it offers in the context of drone digital forensic investigation.

7.2. Future Work

Although digital twin technology (DTT) is a technology that is currently being developed and is still in its infancy, since the aim of this paper was to demonstrate and test the effectiveness of using this technology for drone accident simulation and investigation, it paves the way for more work in the future by implementing DTT in a digital model for a real case. In addition, this paper provides a basis for other researchers to further investigate this field and its use in the digital forensic investigation of drones. As part of our future work, we intend to test DTT in a real case scenario to evaluate its effectiveness in a digital forensic investigation.

Author Contributions: Conceptualization, A.A. and T.Z.; data curation, A.A., T.Z. and E.-u.-H.Q.; formal analysis, A.A., T.Z. and E.-u.-H.Q.; funding acquisition, T.Z.; methodology. A.A., T.Z. and E.-u.-H.Q.; project administration, T.Z.; resources, T.Z.; software, A.A., T.Z. and E.-u.-H.Q.; supervision, T.Z. and E.-u.-H.Q.; validation, A.A., T.Z. and E.-u.-H.Q.; visualization, A.A., T.Z. and E.-u.-H.Q.; writing—original draft, A.A. and T.Z.; writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Security Research Center at Naif Arab University for Security Sciences (Project No. NAUSS-23-R10).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The author would like to express their deep thanks to the Vice Presidency for Scientific Research at Naif Arab University for Security Sciences for their kind encouragement of this work.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Unmanned Aircraft Systems (UAS). Unmanned Aircraft Systems (UAS) | Federal Aviation Administration. Available online: https://www.faa.gov/uas (accessed on 6 May 2023).
2. Milner, M.N.; Rice, S.; Winter, S.R.; Anania, E.C. The effect of political affiliation on support for police drone monitoring in the United States. *J. Unmanned Veh. Syst.* **2019**, *7*, 129–144. [CrossRef]
3. Georgiou, A.; Masters, P.; Johnson, S.; Feetham, L. UAV-assisted real-time evidence detection in outdoor crime scene investigations. *J. Forensic Sci.* **2022**, *67*, 1221–1232. [CrossRef] [PubMed]
4. Emerging Tech Impact Radar: 2023. Gartner. (n.d.). Available online: https://www.gartner.com/en/doc/emerging-technologies-and-trends-impact-radar-excerpt (accessed on 6 May 2023).
5. Bouafif, H.; Kamoun, F.; Iqbal, F.; Marrington, A. Drone forensics: Challenges and new insights. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; IEEE: Piscataway, NJ, USA; pp. 1–6.
6. Gülataş, İ.; Baktir, S. Unmanned aerial vehicle digital forensic investigation framework. *J. Nav. Sci. Eng.* **2018**, *14*, 32–53.
7. Hassija, V.; Chamola, V.; Agrawal, A.; Goyal, A.; Luong, N.C.; Niyato, D.; Yu, F.R.; Guizani, M. Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2802–2832. [CrossRef]
8. Sharma, B.K.; Chandra, G.; Mishra, V.P. Comparitive analysis and implication of UAV and AI in forensic investigations. In Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 4–6 February 2019; IEEE: Piscataway, NJ, USA; pp. 824–827.
9. Kao, D.Y.; Chen, M.C.; Wu, W.Y.; Lin, J.S.; Chen, C.H.; Tsai, F. Drone forensic investigation: DJI spark drone as a case study. *Procedia Comput. Sci.* **2019**, *159*, 1890–1899. [CrossRef]

10. Bouafif, H.; Kamoun, F.; Iqbal, F. Towards a better understanding of drone forensics: A case study of parrot AR drone 2.0. *Int. J. Digit. Crime Forensics (IJDCF)* **2020**, *12*, 35–57. [CrossRef]
11. Al-Room, K.; Iqbal, F.; Baker, T.; Shah, B.; Yankson, B.; MacDermott, A.; Hung, P.C. Drone forensics: A case study of digital forensic investigations conducted on common drone models. *Int. J. Digit. Crime Forensics (IJDCF)* **2021**, *13*, 1–25. [CrossRef]
12. Al-Dhaqm, A.; Ikuesan, R.A.; Kebande, V.R.; Razak, S.; Ghabban, F.M. Research challenges and opportunities in drone forensics models. *Electronics* **2021**, *10*, 1519. [CrossRef]
13. Salamh, F.E.; Karabiyik, U.; Rogers, M.K.; Matson, E.T. A comparative UAV forensic analysis: Static and live digital evidence traceability challenges. *Drones* **2021**, *5*, 42. [CrossRef]
14. Stanković, M.; Mirza, M.M.; Karabiyik, U. UAV forensics: DJI mini 2 case study. *Drones* **2021**, *5*, 49. [CrossRef]
15. Mekdad, Y.; Aris, A.; Babun, L.; Fergougui, A.E.; Conti, M.; Lazzeretti, R.; Uluagac, A.S. A survey on security and privacy issues of UAVs. *arXiv* **2021**, arXiv:2109.14442. [CrossRef]
16. Salamh, F.E.; Mirza, M.M.; Karabiyik, U. UAV forensic analysis and software tools assessment: DJI Phantom 4 and Matrice 210 as case studies. *Electronics* **2021**, *10*, 733. [CrossRef]
17. Moon, H.; Jin, E.; Kwon, H.; Lee, S.; Gibum, K. Digital forensic methodology for detection of abnormal flight of drones. *J. Inf. Secur. Cybercrimes Res.* **2021**, *4*, 27–35. [CrossRef]
18. Atkinson, S.; Carr, G.; Shaw, C.; Zargari, S. Drone forensics: The impact and challenges. *Digit. Forensic Investig. Internet Things (IoT) Devices* **2021**, 65–124. [CrossRef]
19. Alotaibi, F.M.; Al-Dhaqm, A.; Al-Otaibi, Y.D. A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. *Comput. Intell. Neurosci.* **2022**, *2022*, 8002963. [CrossRef]
20. Alhussan, A.A.; Al-Dhaqm, A.; Yafooz, W.M.; Razak, S.B.A.; Emara, A.H.M.; Khafaga, D.S. Towards Development of a High Abstract Model for Drone Forensic Domain. *Electronics* **2022**, *11*, 1168. [CrossRef]
21. Liang, G.; Xin, J.; Wang, Q.; Ni, X.; Guo, X. Research on IoT Forensics System Based on Blockchain Technology. *Secur. Commun. Netw.* **2022**, *2022*, 4490757. [CrossRef]
22. Alotaibi, F.M.; Al-Dhaqm, A.; Al-Otaibi, Y.D.; Alsewari, A.A. A comprehensive collection and analysis model for the drone forensics field. *Sensors* **2022**, *22*, 6486. [CrossRef]
23. Studiawan, H.; Ahmad, T.; Santoso, B.J.; Shiddiqi, A.M.; Pratomo, B.A. DroneTimeline: Forensic timeline analysis for drones. *SoftwareX* **2022**, *20*, 101255. [CrossRef]
24. Siddiqi, M.A.; Iwendi, C.; Jaroslava, K.; Anumbe, N. Analysis on security-related concerns of unmanned aerial vehicle: Attacks, limitations, and recommendations. *Math. Biosci. Eng.* **2022**, *19*, 2641–2670. [CrossRef]
25. Muthanna, A.; AAteya, A.; Khakimov, A.; Gudkova, I.; Abuarqoub, A.; Samouylov, K.; Koucheryavy, A. Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. *J. Sens. Actuator Netw.* **2019**, *8*, 15. [CrossRef]
26. Abro, G.E.M.; Zulkifli, S.A.B.; Masood, R.J.; Asirvadam, V.S.; Laouti, A. Comprehensive review of UAV detection, security, and communication advancements to prevent threats. *Drones* **2022**, *6*, 284. [CrossRef]
27. Ko, Y.; Kim, J.; Duguma, D.G.; Astillo, P.V.; You, I.; Pau, G. Drone secure communication protocol for future sensitive applications in military zone. *Sensors* **2021**, *21*, 2057. [CrossRef] [PubMed]
28. Uhlenkamp, J.F.; Hribernik, K.; Wellsandt, S.; Thoben, K.D. Digital Twin Applications: A first systemization of their dimensions. In Proceedings of the 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Valbonne Sophia-Antipolis, France, 17–19 June 2019; IEEE: Piscataway, NJ, USA; pp. 1–8.
29. Akbal, E.; Dogan, S. Forensics image acquisition process of digital evidence. *Int. J. Comput. Netw. Inf. Secur.* **2018**, *10*, 1–8. [CrossRef]
30. Qureshi, S.; Tunio, S.; Akhtar, F.; Wajahat, A.; Nazir, A.; Ullah, F. Network Forensics: A Comprehensive Review of Tools and Techniques. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*. [CrossRef]
31. Azzery, Y.; Mulyanto, N.D.; Hidayat, T. Memory Forensic Development and Challenges in Identifying Digital Crime: A Review. *TEKNOKOM* **2022**, *5*, 96–102. [CrossRef]
32. Al-Dhaqm, A.; Abd Razak, S.; Ikuesan, R.A.; Kebande, V.R.; Siddique, K. A review of mobile forensic investigation process models. *IEEE Access* **2020**, *8*, 173359–173375. [CrossRef]
33. Glaessgen, E.H.; Stargel, D.S. The digital twin paradigm for future NASA and US Air Force vehicles. In Proceedings of the AIAA Modeling and Simulation Technologies Conference, Grapevine, TX, USA, 9–13 January 2017.
34. Tao, F.; Zhang, M.; Liu, X.; Nee, A.Y.C.; Li, X. Digital twin in industry: State-of-the-art. *IEEE Trans. Ind. Inform.* **2018**, *15*, 2405–2415. [CrossRef]
35. Wang, W.; Li, X.; Xie, L.; Lv, H.; Lv, Z. Unmanned aircraft system airspace structure and safety measures based on spatial digital twins. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 2809–2818. [CrossRef]
36. Redelinghuys AJ, H.; Basson, A.H.; Kruger, K. A six-layer architecture for the digital twin: A manufacturing case study implementation. *J. Intell. Manuf.* **2020**, *31*, 1383–1402. [CrossRef]
37. Alam, K.M.; El Saddik, A. C2PS: A digital twin architecture reference model for the cloud-based cyber-physical systems. *IEEE Access* **2017**, *5*, 2050–2062. [CrossRef]
38. Kaul, R.; Ossai, C.; Forkan, A.R.M.; Jayaraman, P.P.; Zelcer, J.; Vaughan, S.; Wickramasinghe, N. The role of AI for developing digital twins in healthcare: The case of cancer care. *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.* **2023**, *13*, e1480. [CrossRef]

39. Borowski, P.F. Digitization, digital twins, blockchain, and industry 4.0 as elements of management process in enterprises in the energy sector. *Energies* **2021**, *14*, 1885. [CrossRef]
40. Wang, Y.; Chen, X.; Liang, Y.; Zhang, J. Digital twin-driven predictive maintenance for industrial equipment: A review. *J. Manuf. Syst.* **2020**, *2020*, 6129995.
41. Nativi, S.; Mazzetti, P.; Craglia, M. Digital ecosystems for developing digital twins of the earth: The destination earth case. *Remote Sens.* **2021**, *13*, 2119. [CrossRef]
42. Wang, Q.; Jiao, W.; Wang, P.; Zhang, Y. Digital twin for human-robot interactive welding and welder behavior analysis. *IEEE/CAA J. Autom. Sin.* **2020**, *8*, 334–343. [CrossRef]
43. Wang, M.; Wang, C.; Hnydiuk-Stefan, A.; Feng, S.; Atilla, I.; Li, Z. Recent progress on reliability analysis of offshore wind turbine support structures considering digital twin solutions. *Ocean. Eng.* **2021**, *232*, 109168. [CrossRef]
44. Alshammari, K.; Beach, T.; Rezgui, Y. Cybersecurity for digital twins in the built environment: Current research and future directions. *J. Inf. Technol. Constr.* **2021**, *26*, 159–173. [CrossRef]
45. Son, S.; Kwon, D.; Lee, J.; Yu, S.; Jho, N.S.; Park, Y. On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain. *IEEE Access* **2022**, *10*, 75365–75375. [CrossRef]
46. Burns, T.; Cosgrove, J.; Doyle, F. A Review of Interoperability Standards for Industry 4.0. *Procedia Manuf.* **2019**, *38*, 646–653. [CrossRef]
47. Palensky, P.; Cvetkovic, M.; Gusain, D.; Joseph, A. Digital twins and their use in future power systems. *Digit. Twin* **2022**, *1*, 4. [CrossRef]
48. de Kerckhove, D. The personal digital twin, ethical considerations. *Philos. Trans. R. Soc. A* **2021**, *379*, 20200367. [CrossRef] [PubMed]
49. Suhail, S.; Hussain, R.; Jurdak, R.; Hong, C.S. Trustworthy digital twins in the industrial internet of things with blockchain. *IEEE Internet Comput.* **2021**, *26*, 58–67. [CrossRef]
50. da Silva Mendonça, R.; de Oliveira Lins, S.; de Bessa, I.V.; de Carvalho Ayres, F.A., Jr.; de Medeiros, R.L.P.; de Lucena, V.F., Jr. Digital twin applications: A survey of recent advances and challenges. *Processes* **2022**, *10*, 744. [CrossRef]
51. Lu, Y.; Liu, C.; Kevin, I.; Wang, K.; Huang, H.; Xu, X. Digital Twin-driven smart manufacturing: Connotation, reference model, applications and research issues. *Robot. Comput.-Integr. Manuf.* **2020**, *61*, 101837. [CrossRef]
52. Steindl, G.; Stagl, M.; Kasper, L.; Kastner, W.; Hofmann, R. Generic digital twin architecture for industrial energy systems. *Appl. Sci.* **2020**, *10*, 8903. [CrossRef]
53. Chaudhary, G.; Khari, M.; Elhoseny, M. (Eds.) *Digital Twin Technology*; CRC Press: Boca Raton, FL, USA, 2021.
54. Gill, P.; Kaur, M.; Singh, S. Drone Forensics: A Comprehensive Review on Digital Evidence Acquisition Techniques from Unmanned Aerial Vehicles (UAVs). *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 39–45.
55. Li, L.; Aslam, S.; Wileman, A.; Perinpanayagam, S. Digital twin in aerospace industry: A gentle introduction. *IEEE Access* **2021**, *10*, 9543–9562. [CrossRef]
56. Biesinger, F.; Weyrich, M. The facets of digital twins in production and the automotive industry. In Proceedings of the 2019 23rd International Conference on Mechatronics Technology (ICMT), Salerno, Italy, 23–26 October 2019; pp. 1–6.
57. Alazab, M.; Khan, L.U.; Koppu, S.; Ramu, S.P.; Iyapparaja, M.; Boobalan, P.; Baker, T.; Maddikunta, P.K.R.; Gadekallu, T.R.; Aljuhani, A. Digital twins for healthcare 4.0-recent advances, architecture, and open challenges. *IEEE Consum. Electron. Mag.* **2022**, *12*, 29–37. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.