

Digital Forensic Investigation on Social Media Platforms: A Survey on Emerging Machine Learning Approaches

Abdullahi Aminu Kazaure* 

School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia
E-mail: aakazaure@student.usm.my

Aman Jantan 

School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia
E-mail: aman@usm.my

Mohd Najwadi Yusoff 

School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia
E-mail: najwadi@usm.my


ABSTRACT

An online social network is a platform that is continuously expanding, which enables groups of people to share their views and communicate with one another using the Internet. The social relations among members of the public are significantly improved because of this gesture. Despite these advantages and opportunities, criminals are continuing to broaden their attempts to exploit people by making use of techniques and approaches designed to undermine and exploit their victims for criminal activities. The field of digital forensics, on the other hand, has made significant progress in reducing the impact of this risk. Even though most of these digital forensic investigation techniques are carried out manually, most of these methods are not usually appropriate for use with online social networks due to their complexity, growth in data volumes, and technical issues that are present in these environments. In both civil and criminal cases, including sexual harassment, intellectual property theft, cyberstalking, online terrorism, and cyberbullying, forensic investigations on social media platforms have become more crucial. This study explores the use of machine learning techniques for addressing criminal incidents on social media platforms, particularly during forensic investigations. In addition, it outlines some of the difficulties encountered by forensic investigators while investigating crimes on social networking sites.

Keywords: machine learning, digital forensics, natural language processing, social media forensics

Received: November 30, 2022
Accepted: October 15, 2023

Revised: August 26, 2023
Published: March 30, 2024

***Corresponding Author:** Abdullahi Aminu Kazaure
 <https://orcid.org/0000-0002-8171-8609>
E-mail: aakazaure@student.usm.my



All JISTaP content is Open Access, meaning it is accessible online to everyone, without fee and authors' permission. All JISTaP content is published and distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>). Under this license, authors reserve the copyright for their content; however, they permit anyone to unrestrictedly use, distribute, and reproduce the content in any medium as far as the original authors and source are cited. For any reuse, redistribution, or reproduction of a work, users must clarify the license terms under which the work was produced.

1. INTRODUCTION

1.1. Research Background

Globally, billions of people use social media to interact with others, exchange information, and keep in contact with family and friends. It has become a key component of our daily socioeconomic activities for both individuals and commercial enterprises. The term “social media” refers to all communication platforms that are utilized for communication and social interaction among a group of people by exchanging their views and content sharing (Arshad et al., 2019). Facebook, WhatsApp, Messenger, Instagram, Twitter, Myspace, and other online gaming platforms are among the social media platforms available today for social interactions and networking (Ngejane et al., 2018). Due to recent advancements in computer science and modern technologies, social media networks have become a vital aspect of human life. These platforms are widely recognized for sharing information, news, and daily updates, and serve as the main channel for gathering and transmitting data (Shahbazi & Byun, 2021). Even though these platforms might be useful, it is important to remember that some of the information available to users is false and could mislead them wrongly. However, they also serve as a tool for fostering interaction and content dissemination among a group of users or a specific set of people. As a result of its scalability and adaptability, social media has quickly surpassed traditional forms of communication in both personal and professional settings. However, it is also used regularly by several businesses to increase efficiency on the job (Sun et al., 2021). Despite the many positive effects of social media, criminals are still finding new methods to use it for their interests. This social media exploitation has serious political, cultural, and sociological repercussions, in addition to the obvious economic costs of lost productivity, compromised systems, and stolen identities.

Social media and other types of cutting-edge communication technologies are being used by criminals in their operations. When these platforms are monitored, law enforcement authorities may be able to apply new methods for reporting crimes directly to the investigative authorities, allowing for a faster reaction time during the occurrence itself (Flores et al., 2021). Because of this, it is feasible to effectively adapt techniques across types of crime that need data or an established detection method (Fazil & Abulaish, 2018). Because of the advent and widespread use of the Internet, cybercriminals may now reach those who were previously out of their reach (Drury et al.,

2022). These drawbacks, however, raise the possibility that criminals may use social media to target several people in multiple locations. Data misuse, money laundering, e-terrorism, illegal access to computer systems, and theft of intellectual property are just a few examples of the types of computer-related crimes that digital forensics is often employed to investigate (Mohammad & Alqahtani, 2019). As a result, digital forensics investigations are recognized as a defined technique that uses systematic principles and technology to identify, collect, preserve, and analyze electronic evidence in the aftermath of an Internet-connected crime. Data from computers and other electronic storage devices is acquired as part of these investigations to help determine what malicious actions were taken on a computer and who was accountable for them (Baig et al., 2017). But as more and more people make use of computers, the quantity and variety of data available for forensic examinations have grown exponentially. The growth of this phenomenon may be traced back to the proliferation of online and social media platforms (Bindu et al., 2017).

Accordingly, forensic investigators have challenges while attempting to analyze these platforms due to the information sources contained within them. However, there may be a greater weight on backlogs for digital forensic investigations (Mohammad, 2020). Social media platforms can provide valuable information about potential suspects, victims, and witnesses. These platforms offer a continuously updated collection of user-generated data sources, such as posts, friends, photos, demographics, chats, and more (Arshad et al., 2019). However, intelligent technologies like machine learning (ML) and natural language processing (NLP) have demonstrated their potential to enhance digital forensic investigations, particularly on social media platforms (Shahbazi & Byun, 2022; Sun et al., 2021). Therefore, the same problem exists when looking at massive volumes of data, including online interactions and chat histories. In contrast, these tools may automate the processes often used in digital forensics investigations. In addition, they may expedite the process and help law enforcement with the management of criminal exploitations that frequently occur on online media platforms (Nowroozi et al., 2021). Strategic utilization of email and various online networks offers significant advantages in information exchange and communication. ML text classification plays a crucial role in enhancing the security measures needed for daily interactions on social media platforms. Notable incidents, such as the misinformation spread during the US Clinton campaign and other high-profile cases, underscore the importance of interdisci-

plinary and digital forensics research. These incidents, reported and widely circulated on social media, highlight the urgent need for relevant stakeholders to support research efforts aimed at curbing the dissemination of false information and addressing the underlying issues it reveals (Lazer et al., 2018). Similar findings emerged during the recent COVID-19 pandemic, as presented in Song and Fergnani (2022)'s article on the strategies of underlining collective understanding of disease outbreaks. Additionally, concerns have been raised about terrorists and criminal syndicates exploiting social media for their activities. They create private communication channels to coordinate and exchange information, underscoring the need for vigilant monitoring and intervention (Goodman, 2019; Keatinge & Keen, 2019).

1.2. Digital Forensics

Digital forensics involves the examination of crimes involving digital technologies. Its primary objective is to identify, gather, and assess evidence from digital sources, obtain evidence for legal proceedings, and present findings in a court of the relevant jurisdiction (Hargreaves & Patterson, 2012). The use of digital devices as tools for crime has increased criminals' ability to execute different criminal offenses, such as stealing information, modifying user data, and unauthorized access to private information. The significance of digital forensics and the use of digital evidence in the field of forensics has been growing steadily, with technology playing a crucial role for both cybercriminals and security experts (Bankole et al., 2022). As a result, the importance of emphasizing cybersecurity and digital forensics cannot be overstated. Effective cybersecurity measures are essential to protect digital assets and sensitive information from malicious access. Simultaneously, digital forensics is pivotal for investigating cybercrimes, collecting digital evidence, and supporting legal proceedings. To stay ahead of cyber threats, ongoing advancements in digital forensics methodologies are necessary, along with collaboration between law enforcement, cybersecurity experts, and digital forensics specialists. Recognizing the importance of these fields and investing in research, training, and collaboration is crucial for defending against cyber threats and ensuring the integrity of digital environments.

However, it is necessary to protect businesses from cyber-attacks while also learning from digital evidence left after the incidents and being digitally forensically prepared for any kind of cyber/digital incident (Casino et al., 2022). Generally, the field of digital forensics has involved

collecting and analyzing evidence of illegal conduct on digital media using a range of tools and methodologies for presentation in a court of competent jurisdiction. It is difficult to underline the importance of digital forensics in the context of a modern criminal investigation due to the environment in which they operate. In general, everything that can be retrieved from digital devices and is connected to computer technology is referred to as "digital evidence," including files and data in digital form. This data is recorded and transmitted in digital form and is admissible in court (Khanafseh et al., 2019). Moreover, investigators who are currently working on developing models for digital forensics are increasingly recognizing its significance. Previous literature outlines four fundamental stages in digital forensics: acquisition, identification, evaluation, and admission. However, recent advancements have led to the development of various models describing techniques used to collect, examine, analyze, and report data from different digital devices. Recent studies have highlighted the impact of cognitive and human factors on investigative tasks, emphasizing the importance of identifying physical activities in the digital forensic investigation process, as noted (Horsman & Sunde, 2022). For digital forensics to be effective in criminal investigations, it must rely on clear and credible techniques. The processes of digital forensic investigation are illustrated in Fig. 1.

1.3. Crimes Committed on Social Media Platforms

The following are the most prevalent tactics and strategies used by social media criminals to commit crimes to exploit people:

- Criminals have used social media to persuade or engage victims to commit crimes, and they frequently disguise their identities while committing these crimes.
- In some circumstances, organizations may advertise and promote their services on suspicious websites while acquiring customer data for potential use in illegal activities. They promote and sell fake items through e-commerce platforms, which is a crime against the economy.
- Social media posts have the potential to insult marginalized individuals, persuade others, incite actual crimes, and facilitate various illegal activities, including hate speech and sexual harassment. Additionally, social media is often utilized as a disguise for engaging in unlawful behavior.

Flow of investigation process

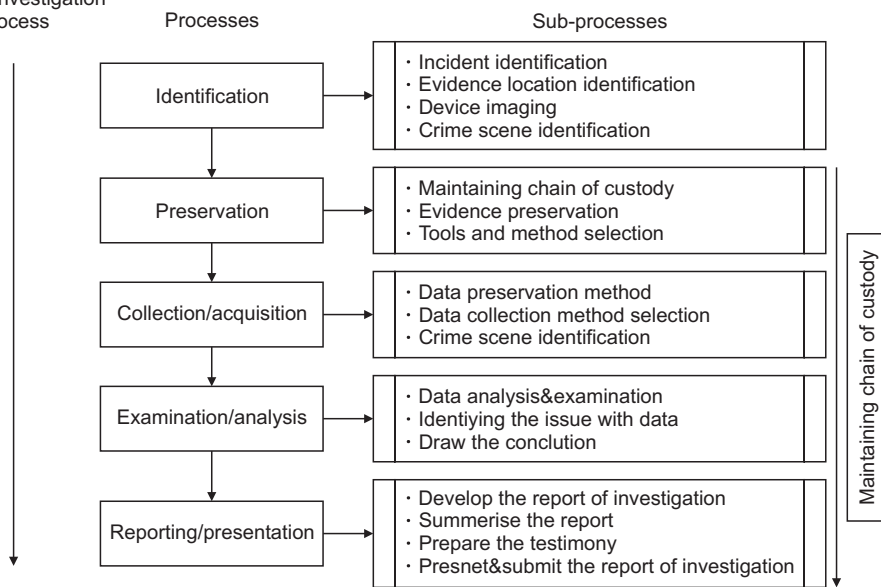


Fig. 1. Digital forensic investigation process.

Therefore, this study aims to conduct a comprehensive survey of ML technologies, algorithms, and NLP methods utilized to tackle criminal activities within Online social networks (OSNs), as outlined in the work by Shahbazi and Byun (2022). The research not only outlines these approaches but also examines their effectiveness in addressing various challenges. A significant contribution of this study to the field of social media forensics lies in evaluating the applicability of ML techniques and NLP approaches to identify suspicious behavior in OSN interactions, aiding in the discovery of crime suspects for court presentations in relevant jurisdictions.

1.4. Research Purpose

The purpose of this research is to explore and advance the use of ML techniques in digital forensics, specifically on social media platforms. However, the study will investigate how ML approaches can be used to effectively extract and analyze digital evidence from social media platforms. It will also study emerging ML methodologies and techniques that can enhance the capabilities of digital forensic investigators in handling and processing large volumes of data from social media platforms.

1.5. Research Objectives

- To explore the ML models that can be used to automatically detect criminal activity on social media platforms. This would free up investigators to focus on more complex tasks and would allow law enforcement agencies to investigate a wider range of

crimes more effectively.

- To identify the challenges and limitations of ML-based digital forensic investigation on social media platforms. This would help researchers to develop new ML techniques that are more effective and efficient.
- To identify the best practices for using ML in digital forensic investigations on social media platforms. This would help law enforcement agencies to get the most out of ML and would help to ensure that the results of ML-based investigations are reliable and accurate.

2. RELATED LITERATURE

This section presents an in-depth review of some significant studies for digital forensics investigations on OSNs with ML integration, as well as an assessment of their benefits and drawbacks. This research examines the current state of social media forensics. Global and individual digital forensics investigation processes and methodologies, such as those developed for social media forensics, are the techniques used during an investigation (Sun et al., 2021). Globally oriented digital forensics investigation focuses on a larger collection and analysis of collected data, which may be diverse and unstructured, with the primary goal of identifying and extracting as many hidden relationships between individuals as needed (Liu et al., 2019; Sun et al., 2021). Individually focused digital forensic investigation, on the other hand, involves collect-

ing data from a single computing device, such as a mobile device, to retrieve digital content and artifacts from the user's account (Arshad et al., 2020; Stoyanova, 2020). When there is a reporting case on a criminal breach of trust, global data collection and analysis might also aid in discovering potential criminal syndicate members within an organization.

The study conducted by Taha and Yoo (2019) introduces a graphical overview that identifies individuals in a social network with close affiliations to widely recognized criminals. This research contributes to improving communication and the identification of leaders within the network (Taha & Yoo, 2019). Furthermore, techniques like artificial intelligence, deep learning, NLP, and ML have been employed to pinpoint suspicious activities in social networks, as observed in the work by Bindu et al. (2017). They developed a supervised ML algorithm to automatically identify abnormal users in a static social network, assuming the network structure remains stable. Additionally, a hybrid approach for detecting automated spammers on Twitter was proposed (Fazil & Abulaish, 2018). This method analyses crucial factors, including community-based elements, using ML, considering metadata, content, and interaction-based features. Regardless of the machine's level of automation or complexity, Ruan et al. (2016) utilizes ML approaches to detect bot-maintained accounts on Twitter to identify spammers.

Several feature representations have been proposed for building a trustworthy bot detection model. A linguistic and content analytic strategy for investigating online predatory chats using Linguistic Inquiry and Word Count was proposed by Black et al. (2015). The authors wanted to see if there was any connection between predator behavior patterns offline and online by using O'Connell (2003)'s five sexual grooming phases. Computer crime, particularly on social media, is on the rise as a result of the global accessibility of computing resources. The Computer Misuse Act of 1990 in the United Kingdom establishes many penalties involving personal data stored by both public and commercial companies. Even though this legislation was formed in the United States and the United Kingdom, it has extraterritorial effects and can be utilized anywhere in the world. This generic offense includes spear phishing. The Computer Misuse Act considers spear phishing a violation due to its aim to obtain unauthorized access to computer systems.

Misuse of computers and the Internet may refer to a variety of unethical or unlawful behaviors involving the use of computer networks, systems, and the Internet.

Some examples of online and computer abuse include cyberbullying, which is the practice of harassing someone online, often through social media or messaging services. However, hacking is also another term for gaining unauthorized access to a computer system or network with the intent to steal data or cause harm. A phishing attack is also another Internet misuse practice of tricking individuals into divulging personal information, including passwords or credit card details, via the use of phony emails, texts, or websites. These are just a handful of the numerous ways that people abuse computers and the Internet. It is important to be informed about these concerns and to take precautions to safeguard one's online identity and personal data. Investigators must use standardized and clearly defined forensic processes to deal with various crimes using digital devices. Finding and collecting evidence from the resources is a key component of any digital crime investigation procedure.

3. ONLINE SOCIAL MEDIA FORENSICS

In recent years, social media has emerged as a valuable tool for individuals seeking to promote both positive and negative ideas. This form of advertising is designed to raise awareness about various concepts and activities, engage supporters in specific causes, and generate financial backing (Keatinge & Keen, 2019). Due to its ease of use in conveying messages and attracting supporters, social media proves to be an excellent platform for profit-making endeavors. OSNs, including popular websites like Twitter and Facebook, constitute one of these social structures (Shahbazi & Byun, 2020; Suryanto et al., 2021). The extraction of forensic data from social media platforms has emerged as a significant field of study in forensic science (Shahbazi & Byun, 2020; Suryanto et al., 2021). Most of the information is acquired through standard digital forensics, which is a very sophisticated kind of evidence when dealing with criminal cases online. Despite this, the globally spread nature of OSN shared contents and data volume makes the extraction procedure more complex. Due to privacy standards based on worldwide data protection legislation, only a limited degree of access is authorized when acquiring data from individuals without a legitimate purpose (Li et al., 2018b). During forensic data collection, the system operator is called to ask about formatting issues and data authenticity (Lorch et al., 2022).

For the past few years, researchers have been focusing on collecting artifacts from client devices since they might have physical access to those devices (Sandoval-Orozco et

al., 2020). On the other hand, the law enforcement community, evidence modeling, and forensic analysis based on cloud computing approaches are now on the focal line to enable investigators to find a suitable method for conducting a digital investigation on the platforms (Hemdan & Manjaiah, 2021; Purnaye & Kulkarni, 2022; Sun et al., 2021). To collect DF data, several critical steps must be taken to establish criminal cases in terms of their location, data sources, security, and so on (Shahbazi & Byun, 2021). Users can access and understand the data that social media networks provide more easily due to the scalability of the computing resources available. Similarly, as a result of the Global Data Protection Regulation that protects users, it is now mandatory to use this act under the law and formal processes (Misra & Arumugam, 2022). To ensure consistency and effectiveness, this process should be carried out by a highly qualified person who has a deep understanding of technical and legal issues (Sun et al., 2021). During the digital forensic investigation, the primary sources for social media content are recognized as artifacts (Horan & Saiedian, 2021).

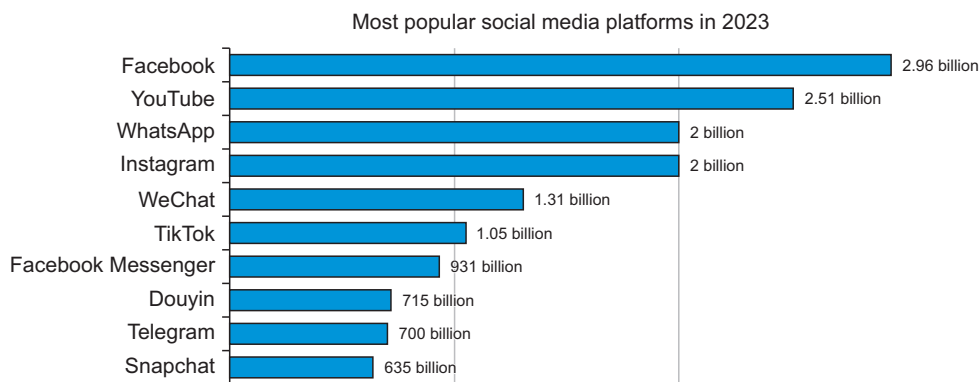
3.1. Online Social Media Statistics

According to Statista's 2022 estimate, Facebook was the first social media network to surpass one billion registered accounts, boasting over 2.89 billion monthly active users. Currently, the company oversees four of the most popular social media platforms: Facebook (the main platform), Facebook Messenger, WhatsApp, and Instagram, all of which have more than one billion monthly active users. In the third quarter of 2021, Facebook reported a staggering 3.58 billion monthly active users (Statista, 2022). Major social media sites are typically accessible in numerous languages, enabling users to connect with friends and others irrespective of geographical, political, or economic bound-

aries. As of 2022, social networking sites were estimated to have 3.96 billion users, a number expected to rise due to the increasing popularity of mobile devices and mobile social networks in underdeveloped countries. The growing usage of social media indicates a profound integration of these platforms into people's daily lives. Projections suggest that by 2023, there will be 4.89 billion social media users worldwide, reflecting a 6.5% increase from the current year. Notably, there has been a significant 79.1% increase in social media users over just five years, from 1.7 billion in 2012 to 2.2 billion in 2019. Throughout that period, there was an average yearly growth rate of 10.2%. While the total number of people using social media will rise in the future, its pace of expansion is likely to level out. Forecasts indicate a 5% compound annual growth rate between 2023 and 2027. Fig. 2 illustrates the most widely used social networks worldwide (Oberlo, 2023).

3.2. Video Analysis Forensics with Machine Learning

In recent years, ML has played a significant role in problem-solving across diverse domains, notably in industries such as industrial and forensic science (Sandoval-Orozco et al., 2020). ML is a data analysis method that automates the creation of analytical models, incorporating techniques such as supervised learning, unsupervised learning, reinforcement learning, and semi-supervised learning, finding extensive applications across global sectors (Javed et al., 2021). Currently, it is a widely utilized tool for video analysis (Bengio & LeCun, 2017). In a similar vein, Güera and Delp (2018) introduced a temporal-aware pipeline architecture for detecting deepfake videos in movies and retrieving frame-level data. This method employs a Convolutional Neural Network (CNN) and a Recurrent Neural Network (RNN) trained to determine video modifications. Additionally, Hosler et al. (2019)



Source: DataReportal



Fig. 2. Popular social networks worldwide (Reprint from Oberlo, [2023] *How many people use social media in 2024?* <https://www.oberlo.com/statistics/how-many-people-use-social-media>).

provided a technique for identifying video sources and confirming their legality. However, developing and testing advanced video forensic algorithms is challenging without access to common digital video databases. To address this need, the authors proposed the video authentication and camera identification database, offering a diverse collection of movies, which is especially beneficial for developing camera model identification algorithms.

While there is limited research on forensic tools utilizing ML to detect image provenance, most of these approaches can be applied to already collected film frame data due to the complexity of direct operations on video. Comparatively, Li et al. (2018a) introduced a novel methodology classifying video source output identification methods based on wavelet transformations, convincing artifacts, color filter arrays, sensor flaws, and metadata. Attributes like mobile devices, sensor flaws, and cameras are commonly employed in evaluating video source output, with sensor flaws being a notable consideration (Xiao et al., 2019). However, the application of deep learning should be controlled carefully to prevent unintended consequences, such as damaging scene properties during frame removal. In the realm of video forensics, evidence extraction from videos is crucial, involving techniques like face recognition and keyframe detection to aid investigators in gathering evidence from crime scene recordings. Keyframe extraction, representing video sequences through summary keyframes, is a powerful method in this context. Many organizations are grappling with the challenge of establishing meaningful societal frameworks (Javed et al., 2021; Shi et al., 2017). The steps of the video tampering detection technique are depicted in Fig. 3 as a block diagram.

3.3. Image Forensics Analysis with Machine Learning

Image forensics plays a vital role in both criminal investigations and civil cases, especially when manipulated images are used to promote hatred, prejudice, or false narratives about specific ethnic backgrounds or political entities (e.g., defamation). The integration of ML methods in image forensics is becoming more prevalent. However,

ML-based systems have their limitations and drawbacks, such as distinguishing ad (image) instances, and they carry real-world implications (Nowroozi et al., 2021). In this digital age, aided by various devices and software, it is now possible to track pattern-of-life data points with precision, down to seconds, contributing to a wealth of information for analysis. The surge in online images and videos has transformed the nature of evidence analyzed in forensic investigations. Within digital pictures, two types of fingerprints are visible on the sensor. Utilizing the inherent Photo Response Non-Uniformity for image authentication and source camera identification has become a significant focus (Ahmed et al., 2021; Gupta & Tiwari, 2018). Moreover, efforts have been made to determine the acquisition period of digital images. Significant contributions to determining the acquisition period of digital images have been proposed by Ahmed et al. (2021) to identify the age of digital images; the concept combines a sophisticated defective pixel identification approach with ML techniques.

The concept of local variation features has been introduced as an effective method for identifying potentially compromised pixels in image dating. In preparation for the reconstruction process, tangible events were assigned virtual timestamps. A video, in essence, is an image sequence originating from a multimedia visual source, which collectively forms a moving image. These individual images are commonly referred to as frames. Temporal classification analysis of specific devices or sets of devices is an integral aspect of the forensic investigator's toolkit. This analysis aids in framing the timeline of a given crime incident or other events, involving the gathering of information within a particular timeframe to pinpoint when the crime or related occurrences occurred (Ryser et al., 2020). In forensic analysis, there are three fundamental approaches: relational, functional, and temporal analysis. Relational analysis seeks to unveil connections or interactions between various elements. Functional analysis helps in understanding the operation or functioning of a system or object. Temporal analysis relies on temporal information and the passage of time, enabling investigators to

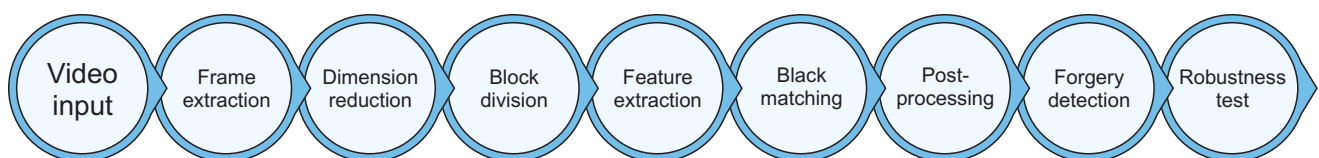


Fig. 3. Video tampering detection block diagram (Reprinted from Javed et al., [2021] *Engineering Applications of Artificial Intelligence*, 106, 104456).

construct a chronological sequence of events and identify patterns that provide a comprehensive view of events related to a crime (Ryser et al., 2020).

4. NATURAL LANGUAGE PROCESSING APPROACHES

In digital forensics, NLP techniques play a pivotal role in analyzing and extracting information from text-based evidence. This encompasses text classification, where textual data is categorized into different groups or classes, as outlined by Shahbazi and Byun (2021). NLP techniques are particularly useful in classifying various forms of textual evidence such as emails, chat logs, and social media posts based on their content. This classification aids in establishing legal cases and comprehending the context of crimes. Additionally, sentiment analysis, a part of NLP, is utilized to assess the emotional tone of a text. In the realm of digital forensics, sentiment analysis is applied to chat logs, emails, and social media posts to distinguish the emotional state of suspects or victims. This data proves valuable in building cases and understanding the circumstances surrounding a crime (Amato et al., 2019; Sun et al., 2021). Named Entity Recognition (NER) is another technique used to identify and classify named entities within text, including names, addresses, and phone numbers. NER is applied in digital forensics to identify suspects and victims by extracting relevant information from emails, chat logs, and other textual data sources. Language identification, which determines the language used in a piece of text, is employed in digital forensics to identify the language in emails, chat logs, and other text-based evidence. This information aids in understanding the context of crimes and helps in suspect identification (Sun et al., 2021).

Furthermore, the technique of topic modeling is utilized to identify subjects discussed in textual content. In digital forensics, it is applied to analyze chat logs, emails, and social media posts to determine the topics of conversation (Sun et al., 2021). This analysis assists in constructing cases and comprehending the motives behind crimes. In social network analysis, NLP is employed to authenticate social media account owners. Tools like the Stanford Part-of-Speech tagger are developed to extract elements from social media posts, enabling the identification of individual writing styles. Additionally, text mining techniques are used to recover compromised social media accounts, combining message content and other attributes effectively (Keretna et al., 2013). Furthermore, in the

context of malware detection, NLP is utilized to extract text-level information from Hypertext Transfer Protocol transactions generated by mobile apps (Sun et al., 2021; Xie et al., 2018). By employing text semantic features from network traffic, efficient malware detection models are constructed, contributing to the cybersecurity domain (van der Walt et al., 2018). Additionally, in the context of social network data, NLP and ML approaches are combined using Twitter data. Techniques like Latent Dirichlet Allocation and Support Vector Machine (SVM) are employed for analyzing user interaction and conversation data. These methods help uncover linguistic trends related to fake or authentic news (Lau et al., 2014). Similarly, Random Forest and NLP techniques are utilized to identify fake news by employing the research informed design matrix technique to identify similarities across documents (Antony Vijay et al., 2021).

In the context of cyberbullying detection, NLP techniques are pivotal. Cyberbullying, involving the use of digital platforms to humiliate or ridicule others, is a pressing concern (Ptaszynski et al., 2017). Social media platforms, including Twitter, Facebook, Instagram, and YouTube, have stringent anti-hate speech policies. The emergence of social media has given rise to cyberbullying, affecting both individuals and organizations globally (Chokshi & Mathew, 2020). Efforts to counter cyberbullying are essential, and NLP methods are employed to detect this form of abuse without involving the victims directly. In contrast to traditional digital forensics investigations, guidelines provided by organizations like National Institute of Standards and Technology (NIST) aid in conducting cyberbullying investigations without involving victims directly, ensuring the safety and privacy of those affected. These guidelines are critical in addressing the challenges posed by cyberbullying in the digital age. Cyberbullying is described as a form of targeted abuse that involves the use of OSNs to expose personal and private information. Because it predominantly affects children and teens, cyberbullying is sometimes dismissed as a normal part of growing up. If neglected, cyberbullying can lead to significant psychological and emotional consequences. It is defined as a targeted form of abuse utilizing OSNs to reveal personal and private information (Muneer & Fati, 2020). Various attempts have been made to intervene, prevent, or minimize this threat, often relying on connections between victims. It is essential to identify cyberbullying without involving the victims directly. In contrast to digital forensics investigation, the NIST offers an investigation guideline, illustrated in the Fig. 4.

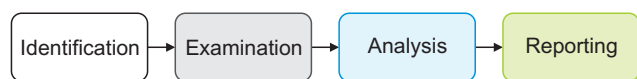


Fig. 4. National Institute of Standards and Technology digital forensics process.

5. CLOUD SERVICE MODELS

Cloud service models are used in response to digital forensics investigations in a variety of ways. The specific cloud service model that is used in a particular investigation will depend on the nature of the crime and the resources that are available to the investigators. In addition to the cloud service model, several other factors can affect the success of a digital forensic investigation in the cloud. These factors include the cooperation of the cloud service provider, the availability of cloud logs and data, and the expertise of the investigators. Cloud computing refers to the utilization of the Internet to offer instant access to shared computing resources like servers, storage, applications, and services. There are three primary categories of cloud service models. Each cloud service model provides the user with varying degrees of control, flexibility, and accountability. Businesses may choose the model that best meets their needs and specifications.

5.1. Infrastructure as a Service

Infrastructure as a Service (IaaS) is a model that provides virtualized computer resources such as virtual machines, servers, storage, and networking to users. Clients can customize, manage, and deploy their software and applications on these resources. Examples of IaaS providers include Amazon Web Services (AWS), Microsoft Azure, and Google Compute Engine (GCE). In this model, cloud service providers supply clients with servers, storage, and hardware for their operating systems and software. However, in IaaS clients are solely responsible for maintaining the infrastructure (Simou et al., 2016). Hardware as a Service is another term for IaaS, providing Internet-based computer infrastructure with hardware and software support to users. One of the main advantages of IaaS adoption is the avoidance of the complexity and cost associated with owning and operating physical servers (Baig et al., 2017). Key features of IaaS include highly scalable resources, adaptive services, dynamic functionalities, graphical user interface, and Application Programming Interface-based access. Moreover, operational functionalities are entirely automated. Leading providers in this domain include AWS, Microsoft Azure, GCE, Linode, DigitalOcean, and

Rackspace (Pichan et al., 2015).

5.2. Software as a Service

Software as a Service (SaaS) is a revolutionary concept that provides clients with convenient online access to software applications. In this model, the software is hosted and managed by the supplier and is accessible to the consumer through a web browser or dedicated application (Son & Buyya, 2018). Well-known SaaS vendors include Salesforce, Dropbox, and Google Workspace. An alternative term for this approach is “on-demand software,” as it is hosted by a cloud service provider, and users can effortlessly access these applications by connecting to the Internet via a web browser (Manoj & Bhaskari, 2016). SaaS exhibits several distinctive characteristics, including central management, hosting on remote servers, and availability over the Internet. Clients are relieved of the responsibility for hardware and software upgrades, as these are performed automatically. This service model aligns with the pay-per-use concept, enabling users to access an array of services from providers like BigCommerce, Salesforce, Google Apps, Dropbox, ZenDesk, Cisco WebEx, GoTo-Meeting, Slack, and many others. SaaS revolutionizes the way users access and utilize software applications, providing efficiency, scalability, and seamless updates without the need for client-side management (Ab Rahman et al., 2017).

5.3. Platform as a Service

This method provides users with a holistic platform for creating, operating, and overseeing applications, all without the need to build and sustain the foundational infrastructure. The operating system, programming language runtime, database, web server, and other required components are often included in the platform. Heroku, Google App Engine, and Microsoft Azure App Service are examples of PaaS providers. Cloud platform services, also known as Platform as a Service (PaaS), are today’s most popular service model. This model is primarily intended for developers, and it provides a framework for testing, deploying, and customizing applications using industry standards (Stoyanova et al., 2020). The development platform provides programming languages, libraries, and tools to developers. According to the PaaS paradigm, customers may also manage or control their deployed programs and, eventually, the application hosting environment settings rather than the underlying cloud infrastructure, network, servers, operating systems, or storage. According to Chung et al. (2017)’s analysis of key trends in public cloud

services, the PaaS market will expand exponentially. Similarly, based on major trends in public cloud services, the report also predicts that the amount of PaaS services will grow between 2018 and 2022. Table 1 provides an overview of the cloud service deployment models described above, along with the important roles of each stakeholder participating in the execution process.

6. PHASES OF DIGITAL FORENSIC INVESTIGATION ON SOCIAL MEDIA PLATFORMS

These stages ensure a systematic and legal approach, maintaining the integrity and accuracy of collected digital evidence on social media platforms investigation. The phases of digital forensics on social media include identification, collection, interpretation, evaluation of digital evidence, presentation, and reporting. Recently, it was found that cybercriminals are employing a sophisticated and intelligent strategy to target digital and physical infrastructures, individuals, and systems. Consequently, the analysis technique faces challenges as the data analysis paradigm

relies on acquiring minimal evidence from billions of networked devices that give very little amount of evidence. To adapt to conventional forensic investigation, the following steps are typically proposed in the literature for digital forensic investigation on social media platforms, particularly when combining ML methodologies. Fig. 5 illustrates the phases and substages involved in handling digital investigations on social media platforms.

6.1. Phase I: Identification

The primary phase in digital forensic investigation is identification, where the forensic process commences by recognizing potential sources of digital evidence, including systems, media, and mobile devices. This identification process involves four distinct steps:

- Identifying the incident itself.
- Identifying the essential evidence to substantiate the occurrence.
- Obtaining the identified set of all computers and system files suspected of carrying relevant evidence.
- The process of digital forensic investigation neces-

Table 1. Different service models investigation levels

Service model	Clients activities	Service provider	Platforms
SaaS	<ul style="list-style-type: none"> • The client lacks a comprehensive understanding of the system’s underlying architecture • Requesting single sign-on access control is recommended • The client must participate in the forensic procedure, such as by putting Proofs of Retrievability into place 	<ul style="list-style-type: none"> • On the provider’s infrastructure, logging tools should be running and active • The metadata of all devices and IP traces of clients accessing information is not permitted to be disclosed by providers 	<ul style="list-style-type: none"> • Gmail, Slack, and Microsoft Office 365
PaaS	<ul style="list-style-type: none"> • The clients have total control of their applications on this service model • The clients have no direct relationship and control of the underlying runtime environment • The logging mechanisms and additional encryption for security purposes can be implemented 	<ul style="list-style-type: none"> • Some cloud service provider’s have diagnostic capabilities that enable the collection and storage of various diagnostics data in a very configurable method 	<ul style="list-style-type: none"> • Google Compute Engine, Amazon, Web Services, Microsoft Azure
IaaS	<ul style="list-style-type: none"> • Compared to PaaS and SaaS models, IaaS instances provide a substantial amount of information that may be utilized as forensic evidence • Some examples include the customer’s ability to install and configure the image for forensic purposes, to run the snapshot of a virtual machine, and the fact that RFC 3227 contains several best practices applicable to an IaaS useful for responding to a security incident, particularly in the case of live investigating systems 	<ul style="list-style-type: none"> • Since persistent data must be kept in long-term storage, virtual IaaS instances frequently lack persistent storage, risking the loss of volatile data • Because of potential privacy concerns, providers could be reluctant to share forensic data, such as recent disc snapshots • Some issues might result from the ambiguity around the provider’s policy on terminating client contracts and the customer’s inability to confirm that all of the sensitive data kept on a virtual machine has been destroyed 	<ul style="list-style-type: none"> • Elastic compute Cloud EC2, Google Compute Engine, Rack space, Microsoft Azure, Amazon Web Services, Joyent

SaaS, Software as a Service; PaaS, Platform as a Service; IaaS, Infrastructure as a Service.

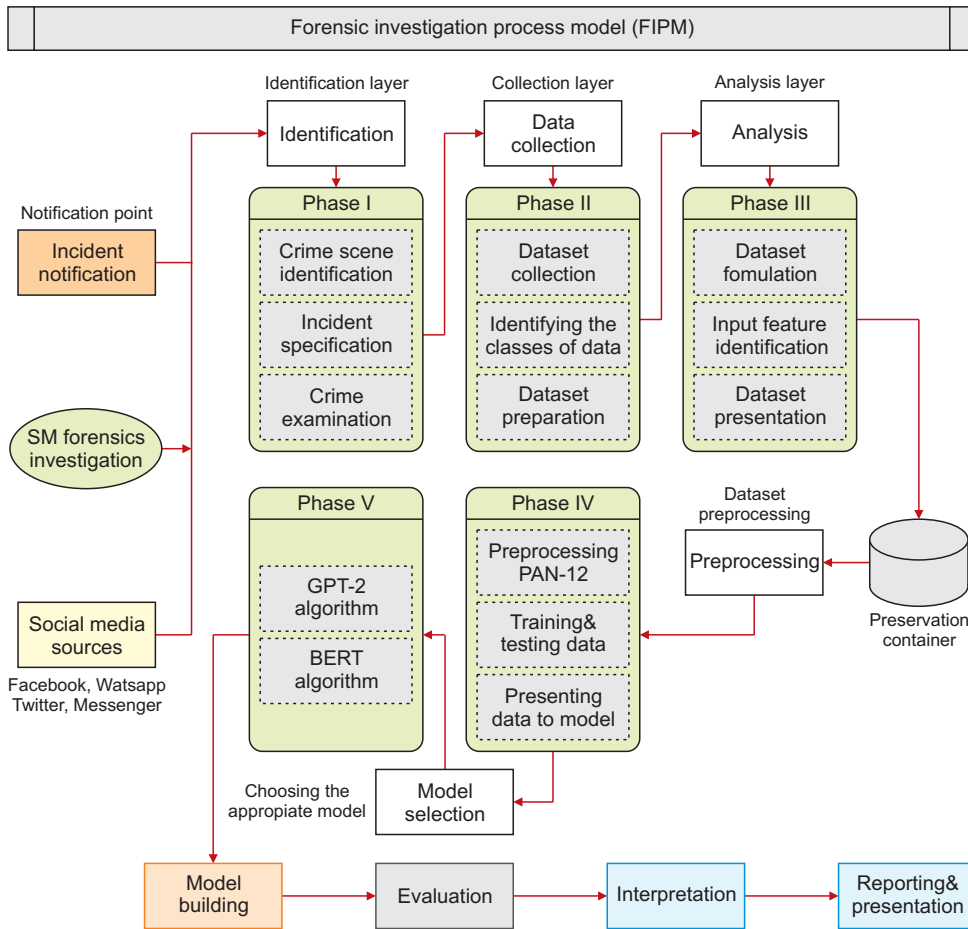


Fig. 5. Forensic Investigation on Online Social Media Platforms. SM, social media; GPT, generative pretrained transformer; BERT, bidirectional encoder representation from transformer.

sitates identifying evidence across various media sources such as cloud servers, network devices, and mobile devices. Identifying evidence involves understanding its current location, type, and format.

6.2. Phase II: Collection

The collection step in digital forensics is critical because it entails obtaining digital evidence from multiple sources such as computers, cell phones, and other electronic devices. The goal of the collecting phase is to acquire all necessary information without modifying or corrupting the original data. The following are some critical steps in the digital forensics collection stage:

- Identify possible evidence sources: The initial step is to identify all prospective digital evidence sources, such as PCs, servers, mobile devices, cloud storage, and social media accounts.
- Establish the chain of custody: To preserve the integrity and admissibility of evidence in court, a proper chain of custody must be maintained throughout the

collecting process. This includes recording who has access to the evidence, where it is held, and how it is transmitted.

- Collecting the data: After identifying prospective sources of evidence, the next stage is to collect data using appropriate tools and methodologies. This may entail making a forensic image of the device, copying certain files or directories, or collecting network traffic.
- Check the data: It is critical to validate the data to confirm that it was acquired accurately and completely. This includes validating the correctness of the timestamps and ensuring that all relevant data has been obtained.
- Secure the data: After the data has been collected and confirmed, it must be securely kept and safeguarded so that it cannot be tampered with or changed.

Ultimately, the collecting step is crucial in digital forensics since it serves as the basis for all later studies and

investigations. To guarantee that evidence is admissible in court, best practices must be followed and a proper chain of custody must be maintained. The traditional digital forensics procedure encounters several difficulties because of the cloud's distributed nature. Although data collection is simply the real acquisition of investigation-related data, most investigators are expected to rely on cloud service providers. This reliance never assures 100% availability of resources, nor their retention after data collection. Another critical consideration is the storage capacity of the collecting device, as no data is stored in a single location in cloud architecture.

6.3. Phase III: Analysis

In digital forensics, the analysis phase is a vital component of the investigative process that involves examining digital evidence collected during the collection phase. The major goal of this phase is to extract and evaluate pertinent data from the acquired digital evidence to support the investigation. However, during the analysis phase, the digital forensic investigator examines the data using different tools and methods to find any artifacts that may provide evidence of criminal activity. The procedure involves data recovery, data analysis, and result interpretation. Data recovery is the process of identifying and extracting data from acquired evidence, which may include deleted files, hidden files, and temporary files. After the data has been recovered, the investigator performs an in-depth analysis of the data to identify any substantial trends, abnormalities, or evidence of criminal activity. In addition to data analysis, the forensic investigator must preserve a complete record of all activities taken throughout the analysis phase. This record, also known as case documentation, serves as an audit trail of the investigative process and as evidence in court. Ultimately, the analysis phase is an important part of the digital forensics investigation process since it gives vital information on the nature of the crime and the individuals involved. All relevant information is analyzed using appropriate and legally permissible methodologies, allowing the necessary suspicious hosts or data to be discovered through this investigative approach. Investigators must be able to respond to all questions presented during the court presentation of the analytical report.

6.3.1. Examining the Dataset

Following the collection of the needed available data with the assistance of cloud service providers, this data is processed using a combination of manual and automated

procedures. The basic goal of examining is to collect and evaluate information on the classified event scene. Throughout this procedure, integrity must be maintained. During an investigation, the dataset collected will be subjected to a thorough examination to maintain consistency and originality. The forensic principles mandated all the acquired data should be original without being contaminated to maintain the chain of custody.

6.3.2. Hypothesis

Several tests on the chatlogs dataset are necessary to extract characteristics that more clearly illustrate how ML models would recognize abusive conversations to identify criminal behavior in online chat conversations. In this situation, it would be possible to obtain insightful information that forensic investigators could find beneficial. To acquire the necessary ideal outcome for assessment, supervised ML approaches can also be applied. Nevertheless, the hypothesis is developed using chat logs of Internet interactions.

6.3.3. Dataset Preparation

The effectiveness of the developed ML models is significantly influenced by the quality of the dataset. Thus, preparing the data set is a crucial step in creating effective and precise models. Additionally, data preparation would improve the ability of the developed models to generalize.

6.3.4. Dataset Pre-Processing

In preparing data for ML algorithms, it is essential to discretize attributes like file size and actual data size. Pre-processing poses a challenge when dealing with characteristics that include text values, as most ML algorithms operate solely on numerical data. Discretization involves grouping values to decrease the number of potential states for a feature, resulting in discrete values. While some features do permit text values, the range of acceptable values is restricted, including attributes like flags, access control type, and DOS file permissions.

6.3.5. Dataset Normalization

When the number of features in a dataset differs considerably, one feature may be prioritized over another. As a result, a suitable standardization and normalization procedure may be utilized to prevent certain characteristics with higher ranges from dominating. When expressed as numeric values, date, and time aspects, for example, may have a wider data range. Scaling the record values within a given range is one of the most frequent approaches for

example, or [1... 1]. In a suggested investigation, the min-max approach is utilized to normalize the obtained data.

6.3.6. Dividing the Dataset into Training and Testing Dataset

Most data mining and ML techniques suffer from overfitting issues. To put it another way, even while the model's error rate decreases throughout training, it still produces incorrect results when applied to an unknown input. This problem may be solved using the "hold-out" validation strategy (Mohammad & Alqahtani, 2019), which divides the obtained data into training and testing subsets. Examples are picked at random for each data collection. In most earlier studies, it was observed that the authors utilized 30% of the data to analyze the "tests" data and 70% of the data to train and validate the model.

6.3.7. Features Selection

The technique of feature selection offers several advantages, including reducing processing time and storage requirements. Moreover, it ensures that the developed models are straightforward and concise. Importantly, this technique aims to identify a subset of input features that play a significant role in predicting the value of the output variable (class variable) (Zuo et al., 2018). Feature selection also reduces the dataset's dimensionality, saving time and memory during the training of ML algorithms. Using all attributes can lead to a high-dimensional training dataset, known as the "curse of dimensionality." Therefore, much of the research focuses on identifying the most effective traits for constructing successful models (Sun et al., 2021). Information gain (IG) is commonly employed in this process to select crucial aspects from a pool of data. IG is a well-known feature evaluation method used in various classification problems, including heart disease classification, phishing website detection, and anomaly detection. However, addressing the reduction of dimensionality becomes necessary as certain characteristics during the training phase may not significantly contribute to explaining the target variables (Burns et al., 2018).

6.4. Phase IV: Digital Evidence Evaluation

In this section, the evaluation metrics employed to assess model quality are discussed. Each supervised classification model relies on four classification outcomes derived from the confusion matrix. True Positive (TP) signifies correctly identified positive cases, False Negative (FN) indicates positive cases mistakenly classified as negative, False Positive (FP) represents negative cases inaccurately

identified as positive, and True Negative (TN) signifies accurately classified negative cases. Various evaluation metrics can be derived from the confusion matrix. The following metrics are considered:

- If the dataset is imbalanced, accuracy alone is insufficient to assess the model quality. Therefore, the area under the curve should be used. Because TP are what is important, the following metrics do not contain FP. According to the equation, accuracy is the overall percentage of properly identified examples relative to the total number of occurrences in the test dataset, as shown in Equation 1.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (1)$$

- The overall number of relevant positively predicted incidents is determined by precision. Equation 1 calculates the precision as the percentage of relevant instances among the retrieved instances.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (2)$$

- Sensitivity or recall determines how good a model is at predicting the positives in ML when making predictions. It is also called a TP rate. Sensitivity is calculated based on the following given formula.

$$\text{Sensitivity} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (3)$$

- F1score is the harmonic mean of recall and precision. However, F1score is used if there is a high variance between precision and sensitivity in skewed data sets. The formulation is calculated as follows in Equation 4.

$$\text{F1score} = 2 \times \frac{\text{Precision} \times \text{Sensitivity}}{\text{Precision} + \text{Sensitivity}} \quad (4)$$

The confusion matrix is typically used to demonstrate the classifier's performance. The non-diagonal elements reflect instances where the classifier mislabeled an object, while the diagonal elements (TN & TP) show the number of situations where the predicted label matches the true label, where:

- i. TP is the number of examples predicted to be positive.
- ii. TN is the number of examples predicted to be negative rather than positive.
- iii. FP is the number of positive examples that were predicted to be predatory.
- iv. FN is the number of predator examples that were predicted to be non-predatory.

It is important that digital forensics examiners formally validate digital forensic models to demonstrate that they are accurate and reliable. It is also important that examiners consider the limitations of the approaches, especially models that are not explicitly designed for digital forensic examination. To assess the error rate accurately and impartially, different cross-validation techniques are proposed to validate the proposed model for effective and efficient model performance. This technique is commonly used to determine and evaluate the performance of ML algorithms.

6.5. Phase V: Presentation and Reporting

These are the final steps of any investigation. The report must include all of the information on the investigative procedure (explanation of what, why, and how). The detailed report must be provided to the jurisdiction section with authenticity and correctness, without tampering with the evidence, which is the most important aspect of the investigation (Datta et al., 2016). In a presentation before a court or other audience, the forensic analyst will outline the facts of the case and explain how his or her conclusions were reached. Specifically, the forensic investigators will provide the court with relevant information and maintain the chain of custody in their findings.

7. MACHINE LEARNING TECHNIQUES FOR DETECTING CRIMINAL ACTIVITIES ON SOCIAL MEDIA PLATFORMS

ML models have shown promising potential in the field of digital forensics for detecting and preventing various types of cybercrimes (Sandoval-Orozco et al., 2020). Here are some ML techniques commonly used for detecting crimes in digital forensics (Del Mar-Raave et al., 2021).

7.1. Signature-Based Detection

Signature-Based Detection: This is a cybersecurity method that involves identifying and thwarting known threats by matching them against predetermined patterns

or signatures (Zhang et al., 2017). These signatures are distinctive markers linked to recognized malicious entities or behaviors. This strategy is widely applied in antivirus programs and intrusion detection systems to rapidly identify and counter established threats (Kebande & Venter, 2018). Similar to antivirus software, signature-based detection involves creating a database of known attack signatures and comparing incoming data against these signatures (Kebande & Venter, 2018). If a match is found, the system can identify and respond to the attack. While effective against known attacks, this method may struggle with new and evolving threats (Javed et al., 2022).

7.2. Machine Learning Classifiers

ML classifiers are algorithms used to categorize data into predefined classes based on their features (Gilpin et al., 2018). Common types include decision trees, SVMs, Naive Bayes, and neural networks. These classifiers are trained on labeled data to make predictions on new data. The choice of classifier depends on data complexity and task requirements. Classification algorithms, such as decision trees, Naive Bayes, random forests, and SVMs, can be trained on labeled data to categorize digital artifacts or activities as benign or malicious (Del Mar-Raave et al., 2021; Sandoval-Orozco et al., 2020). These models rely on features extracted from data such as network traffic, log files, or system activities (Ahmed et al., 2021; Qadir & Varol, 2020).

7.3. Natural Language Processing

NLP is a branch of artificial intelligence that enables computers to understand and work with human language (Shahbazi & Byun, 2022). It involves tasks like classifying text, recognizing names and sentiments, generating language, and translating speech (Sun et al., 2021). However, it has proven to be a valuable tool in the field of digital forensics, where it helps in the analysis and interpretation of textual information for investigative purposes. NLP relies on techniques such as tokenization, word embeddings, RNNs, transformer models, and attention mechanisms. NLP has applications in chatbots, sentiment analysis, translation, and more, making human-computer communication more natural and efficient (Sun et al., 2021). NLP techniques can be employed to analyze text data from communication channels, documents, or online activities (Antony Vijay et al., 2021; Shahbazi & Byun, 2022). Sentiment analysis, topic modeling, and NER can help identify suspicious conversations or intent (Sun et al., 2021).

7.4. Deep Learning Approach

Deep learning models have become crucial in digital forensics due to their ability to extract complex patterns from data (MacDermott et al., 2022). They are used for various tasks, including image analysis, malware detection, file carving, network traffic analysis, detecting digital image forgeries, steganalysis, text analysis, behavioral analysis, and multimodal analysis (Aditya et al., 2018). These models offer enhanced capabilities in identifying anomalies, uncovering manipulation, and improving analysis in digital investigations (Shahbazi & Byun, 2020). However, they require substantial resources and expert interpretation for optimal performance. Deep learning techniques like CNNs and RNNs can be used for image analysis, sequence data (such as logs), and more complex patterns (Hoppe & Toussaint, 2020). Deep learning models can automatically extract meaningful features from raw data, diminishing the requirement for manual feature engineering (Ferreira et al., 2020).

7.5. Anomaly Detection

Anomaly detection techniques involve building a model of “normal” behavior and identifying instances that deviate from this norm (Karami, 2018). This approach is useful for identifying unusual patterns that might indicate malicious activities. Techniques like Isolation Forests, One-Class SVMs, and autoencoders can be employed for this purpose (Abraham et al., 2021; Wu et al., 2020).

8. ADMISSIBILITY OF DIGITAL EVIDENCE

The term “digital evidence” refers to any kind of data that is stored and sent electronically, such as text messages, emails, social media postings, computer files, and photos or videos taken with a digital camera. Digital evidence’s admissibility in court is based on several variables, including the evidence’s veracity, dependability, and applicability. The following aspects are considered when analyzing digital evidence: admissibility, authenticity, completeness, reliability, and credibility. Physical proof of existence that has been recorded or transmitted digitally is referred to as digital evidence. Another definition is “binary data saved or received that is admissible in court” (Arshad et al., 2019; Casey et al., 2018). It may also be described as computer or digital-based evidence that supports or refutes assumptions about how crimes were committed or addresses important components of crimes, such as motivation or alibi (Casey, 2019). Under RFC 3227’s instructions for collecting and keeping evidence, the legal considerations as

follows should be taken regarding the acquired evidence.

8.1. The Evidence Must Be Complete

The evidence should represent the complete set of results, not just one point of view or a subset of the findings. The location and features of the evidence must be presented to the courts (Abiodun et al., 2022). As a result, it is up to attorneys and investigators to make tough decisions, such as: What information is required to establish the factual foundation of a case? Can the “whole” evidence presented be appropriately authenticated? How far should a timeline go in terms of privacy rights, and where is the line between too much freedom and too much restriction? Is it possible for a jury to accurately analyze scanty evidence and condemn a defendant? (Would, for example, the conviction be maintained on appeal?) What does this all mean for digital forensics examiners and attorneys (Arshad et al., 2020)?

8.2. The Evidence Must Be Admissible

Evidence is considered acceptable if it supports a legitimate claim, remains unmodified during the digital forensic investigation, and the outcomes are verifiable, valid, and subject to peer review. Furthermore, evidence is admissible in court when it is presented to illustrate the facts of a case and does not violate the law or other legal criteria. As a result, before it can be produced in court, the evidence must fulfill a variety of legislative standards (Abiodun et al., 2022). Digital evidence must be relevant to the current legal dispute. This implies that it must have a logical relationship to the facts of the case and must be directly tied to the issues being fought. It is essential to remember that the legitimacy, dependability, or significance of digital evidence may be questioned. The admissibility of the evidence may be contested, for instance, if the technique employed to acquire the evidence is questioned.

8.3. The Evidence Must Be Authentic

Authenticity: It must be shown that the digital evidence is exactly what it claims to be. However, digital signatures, metadata analysis, and forensic analysis are just a few of the techniques that can be utilized for it. When it comes to authenticating evidence, two conditions must be met. To begin with, electronic evidence must be legally obtained with the aid of a signed permit from the investigators (Abiodun et al., 2022; Bankole et al., 2022). IT and computer science experts must then independently verify the authenticity of the document before taking further action. If neither of the two conditions is fulfilled, the evidence is

invalid and not complete. The digital evidence must precisely depict the incidents or activities it is meant to record to be considered reliable. The capacity to demonstrate that digital evidence was generated, maintained, and transferred following industry standards establishes its dependability. In general, the admissibility of digital evidence is decided on a case-by-case basis, considering the unique circumstances of each case.

9. MACHINE LEARNING APPROACHES ANALYSIS IN DIGITAL FORENSICS INVESTIGATION

Digital forensic investigation on social media platforms has become increasingly important in today's digital age, as these platforms have become a significant source of evidence in various criminal investigations and legal proceedings. Traditional digital forensic techniques often struggle to keep up with the massive amounts of data generated on social media platforms, making it challenging for investigators to extract relevant information efficiently. However, emerging ML approaches offer promising solutions to enhance the analysis of social media data in digital forensic investigations. Some ML approaches that can significantly benefit digital forensic investigation on social media platforms consist of the following.

1. **Sentiment Analysis:** Sentiment analysis techniques, a subset of NLP, can be employed to gauge the sentiment or emotions expressed in social media posts. ML models can be trained to automatically classify posts as positive, negative, or neutral. This analysis can help investigators understand the emotions and attitudes of individuals involved in a case, potentially revealing valuable insights.

2. **User Profiling:** ML techniques can be employed to create user profiles based on social media data. By analyzing patterns in user behavior, content preferences, connections, and interactions, ML models can help investigators build profiles of individuals and understand their online activities, affiliations, and potential associations with other users or groups.

3. **Fake News and Misinformation Detection:** ML algorithms can be trained to detect fake news and misinformation spread on social media platforms. These models can analyze the content, source, and context of posts to identify potentially misleading information. Detecting fake news and misinformation is crucial in ensuring the integrity of digital evidence and preventing the spread of misinformation that can influence public opinion.

4. **Network Analysis:** ML-based network analysis techniques can uncover hidden connections and relationships between individuals on social media platforms. By examining patterns in user interactions, ML models can identify influential users, communities, or potential collaborators involved in illegal activities. Network analysis can be particularly useful in cases involving organized crime, terrorism, or cybercrime.

5. **Anomaly Detection:** ML approaches can assist in identifying anomalies in social media data that may indicate suspicious or abnormal behavior. By training models on normal user behavior, deviations from the norm can be detected, potentially indicating fraudulent activities, hacking attempts, or other malicious actions. To leverage these ML approaches effectively in digital forensic investigations on social media platforms, several challenges must be addressed. These challenges include data privacy concerns, ethical considerations, the need for large, labeled datasets for training ML models, the dynamic nature of social media platforms, and the need for robust and interpretable ML models that can stand up to legal scrutiny.

10. CONCLUSION

In conclusion, emerging ML approaches offer enormous potential to enhance the analysis of social media data in digital forensic investigations. By leveraging sentiment analysis, topic modeling, user profiling, fake news detection, network analysis, and anomaly detection, investigators can extract valuable insights and evidence from the vast amount of social media data available. However, careful attention must be paid to addressing the challenges associated with the application of ML in digital forensics to ensure the reliability, privacy, and ethical use of the evidence obtained from social media platforms. Similarly, as our society becomes more interconnected and relies heavily on information and communication technology, the importance of cybersecurity has grown significantly. However, the existing digital forensics tools are inadequate to address the complexities of our modern cyber-physical civilization. Therefore, it is vital to prioritize research investments that focus on improving the implementation of digital forensics and investigative procedures, particularly concerning cybercrime.

ACKNOWLEDGEMENT

The authors wish to extend their gratitude to the personnel and students of the Security & Forensic Research

Group (SFRG) Laboratory, School of Computer Sciences, Universiti Sains Malaysia, Penang, for their support in obtaining the materials needed for this work. We also thank the reviewers for their informative comments and ideas, which improved the way this research endeavor was presented.

CONFLICTS OF INTEREST

No potential conflict of interest relevant to this article was reported.

REFERENCES

- Ab Rahman, N. H., Cahyani, N. D. W., & Choo, K. K. R. (2017). Cloud incident handling and forensic-by-design: Cloud storage as a case study. *Concurrency and Computation: Practice and Experience*, 29(14), e3868. <https://doi.org/10.1002/cpe.3868>
- Abiodun, O. I., Alawida, M., Omolara, A. E., & Alabdulatif, A. (2022). Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey. *Journal of King Saud University - Computer and Information Sciences*, 34(10 Pt B), 10217-10245. <https://doi.org/10.1016/j.jksuci.2022.10.018>
- Abraham, J., Ng, R., Morelato, M., Tahtouh, M., & Roux, C. (2021). Automatically classifying crime scene images using machine learning methodologies. *Forensic Science International: Digital Investigation*, 39, 301273. <https://doi.org/10.1016/j.fsidi.2021.301273>
- Aditya, K., Grzonkowski, S., & Lekhac, N. A. (2018, August 1-3). Enabling trust in deep learning models: A digital forensics case study. *Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (Trust-Com/BigDataSE)* (pp. 1250-1255). IEEE.
- Ahmed, F. N., Khelifi, F., Lawgaly, A., & Bouridane, A. (2021). A machine learning-based approach for picture acquisition timeslot prediction using defective pixels. *Forensic Science International: Digital Investigation*, 39, 301311. <https://doi.org/10.1016/j.fsidi.2021.301311>
- Amato, F., Cozzolino, G., Moscato, V., & Moscato, F. (2019). Analyse digital forensic evidences through a semantic-based methodology and NLP techniques. *Future Generation Computer Systems*, 98, 297-307. <https://doi.org/10.1016/j.future.2019.02.040>
- Antony Vijay, J., Anwar Basha, H., & Arun Nehru, J. (2021). A dynamic approach for detecting the fake news using random forest classifier and NLP. In V. Singh, V. K. Asari, S. Kumar, & R. B. Patel (Eds.), *Computational Methods and Data Engineering. Advances in Intelligent Systems and Computing: Proceedings of ICMDE 2020* (Vol. 2, pp. 331-341). Springer.
- Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. *Digital Investigation*, 28, 126-138. <https://doi.org/10.1016/j.diin.2019.02.001>
- Arshad, H., Omlara, E., Abiodun, I. O., & Aminu, A. (2020). A semi-automated forensic investigation model for online social networks. *Computers & Security*, 97, 101946. <https://doi.org/10.1016/j.cose.2020.101946>
- Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N., & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, 22, 3-13. <https://doi.org/10.1016/j.diin.2017.06.015>
- Bankole, F., Taiwo, A., & Claims, I. (2022). An extended digital forensic readiness and maturity model. *Forensic Science International: Digital Investigation*, 40, 301348. <https://doi.org/10.1016/j.fsidi.2022.301348>
- Bengio, Y., & LeCun, Y. (2007). Scaling learning algorithms towards AI. In L. Bottou, O. Chapelle, D. DeCoste, & J. Weston (Eds.), *Large-scale kernel machines* (pp. 1-41). MIT Press.
- Bindu, P. V., Santhi Thilagam, P., & Ahuja, D. (2017). Discovering suspicious behavior in multilayer social networks. *Computers in Human Behavior*, 73, 568-582. <https://doi.org/10.1016/j.chb.2017.04.001>
- Black, P. J., Wollis, M., Woodworth, M., & Hancock, J. T. (2015). A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly computer-mediated world. *Child Abuse & Neglect*, 44, 140-149. <https://doi.org/10.1016/j.chiabu.2014.12.004>
- Burns, M., Griffor, E., Balduccini, M., Vishik, C., Huth, M., & Wollman, D. (2018, June 18-20). Reasoning about smart city. *Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP 2018)* (pp. 381-386). IEEE.
- Casey, E. (2019). Interrelations between digital investigation and forensic science. *Digital Investigation*, 28, A1-A2. <https://doi.org/10.1016/j.diin.2019.03.008>
- Casey, E., Ribaux, O., & Roux, C. (2018). Digital transformations and the viability of forensic science laboratories: Crisis-opportunity through decentralization. *Forensic Science International*, 289, e24-e25. <https://doi.org/10.1016/j.fsi.2018.08.001>

- j.forsciint.2018.04.055
- Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Bořoč, I., Solanas, A., Conti, M., & Pat-sakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, 10, 25464-25493. <https://doi.org/10.1109/ACCESS.2022.3154059>
- Chokshi, A., & Mathew, R. (2020, December 10-11). Deep learning and natural language processing for fake news detection: A survey. *Proceedings of the International Conference on IoT based Control Networks and Intelligent Systems (ICICNIS 2020)* (pp. 716-728). ICICNIS.
- Chung, H., Park, J., & Lee, S. (2017). Digital forensic approaches for Amazon Alexa ecosystem. *Digital Investigation*, 22(Suppl), S15-S25. <https://doi.org/10.1016/j.diin.2017.06.010>
- Datta, S., Majumder, K., & De, D. (2016). Review on cloud forensics: An open discussion on challenges and capabilities. *International Journal of Computer Applications*, 145(1), 1-8. <https://doi.org/10.5120/ijca2016910521>
- Del Mar-Raave, J. R., Bahşi, H., Mršić, L., & Hausknecht, K. (2021). A machine learning-based forensic tool for image classification - A design science approach. *Forensic Science International: Digital Investigation*, 38, 301265. <https://doi.org/10.1016/j.fsidi.2021.301265>
- Drury, B., Drury, S. M., Rahman, M. A., & Ullah, I. (2022). A social network of crime: A review of the use of social networks for crime and the detection of crime. *Online Social Networks and Media*, 30, 100211. <https://doi.org/10.1016/j.osnem.2022.100211>
- Fazil, M., & Abulaish, M. (2018). A hybrid approach for detecting automated spammers in Twitter. *IEEE Transactions on Information Forensics and Security*, 13(11), 2707-2719. <https://doi.org/10.1109/TIFS.2018.2825958>
- Ferreira, W. D., Ferreira, C. B. R., da Cruz Júnior, G., & Soares, F. (2020). A review of digital image forensics. *Computers & Electrical Engineering*, 85, 106685. <https://doi.org/10.1016/j.compeleceng.2020.106685>
- Flores, R., Siami Namin, A., Tavakoli, N., Siami-Namini, S., & Jones, K. S. (2021). Using experiential learning to teach and learn digital forensics: Educator and student perspectives. *Computers and Education Open*, 2, 100045. <https://doi.org/10.1016/j.caeo.2021.100045>
- Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018, October 1-3). Explaining explanations: An overview of interpretability of machine learning. *Proceedings of the 2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA)* (pp. 80-89). IEEE.
- Goodman, A. E. J. (2019). When you give a terrorist a Twitter: Holding social media companies liable for their support of terrorism. *Pepperdine Law Review*, 46(1), 147-202. <https://digitalcommons.pepperdine.edu/plr/vol46/iss1/4/>
- Gupta, B., & Tiwari, M. (2018). Improving source camera identification performance using DCT based image frequency components dependent sensor pattern noise extraction method. *Digital Investigation*, 24, 121-127. <https://doi.org/10.1016/j.diin.2018.02.003>
- Güera, D., & Delp, E. J. (2018, November 27-30). Deepfake video detection using recurrent neural networks. *Proceedings of the 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)* (pp. 1-6). IEEE.
- Hargreaves, C., & Patterson, J. (2012). An automated timeline reconstruction approach for digital forensic investigations. *Digital Investigation*, 9 Suppl, S69-S79. <https://doi.org/10.1016/j.diin.2012.05.006>
- Hemdan, E. E. D., & Manjaiah, D. H. (2021). An efficient digital forensic model for cybercrimes investigation in cloud computing. *Multimedia Tools and Applications*, 80(9), 14255-14282. <https://doi.org/10.1007/s11042-020-10358-x>
- Hoppe, S., & Toussaint, M. (2020). Qgraph-bounded Q-learning: Stabilizing model-free off-policy deep reinforcement learning. *arXiv*. <https://doi.org/10.48550/arXiv.2007.07582>
- Horan, C., & Saiedian, H. (2021). Cyber crime investigation: Landscape, challenges, and future research directions. *Journal of Cybersecurity and Privacy*, 1(4), 580-596. <https://doi.org/10.3390/jcp1040029>
- Horsman, G., & Sunde, N. (2022). Unboxing the digital forensic investigation process. *Science & Justice*, 62(2), 171-180. <https://doi.org/10.1016/j.scijus.2022.01.002>
- Hosler, B. C., Zhao, X., Mayer, O., Chen, C., Shackelford, J. A., & Stamm, M. C. (2019). The video authentication and camera identification database: A new database for video forensics. *IEEE Access*, 7, 76937-76948. <https://doi.org/10.1109/ACCESS.2019.2922145>
- Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access*, 10, 11065-11089. <https://doi.org/10.1109/ACCESS.2022.3142508>
- Javed, A. R., Jalil, Z., Zehra, W., Gadekallu, T. R., Suh, D. Y., & Piran, M. J. (2021). A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions. *Engineering Applications of Artificial Intelligence*, 106, 104456. <https://doi.org/10.1016/j.engappai.2021.104456>
- Karami, A. (2018). An anomaly-based intrusion detection system in presence of benign outliers with visualization capabilities. *Expert Systems with Applications*, 108, 36-60. <https://doi.org/10.1016/j.eswa.2018.04.038>

- Keatinge, T., & Keen, F. (2019). Social media and (counter) terrorist finance: A fund-raising and disruption tool. *Studies in Conflict & Terrorism*, 42(1-2), 178-205. <https://doi.org/10.1080/1057610X.2018.1513698>
- Kebande, V. R., & Venter, H. S. (2018). On digital forensic readiness in the cloud using a distributed agent-based solution: Issues and challenges. *Australian Journal of Forensic Sciences*, 50(2), 209-238. <https://doi.org/10.1080/00450618.2016.1194473>
- Keretna, S., Hossny, A., & Creighton, D. (2013, October 13-16). Recognising user identity in Twitter social networks via text mining. *Proceedings of the 2013 IEEE International Conference on Systems, Man, and Cybernetics* (pp. 3079-3082). IEEE.
- Khanafseh, M., Qataweh, M., & Almobaideen, W. (2019). A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics. *International Journal of Advanced Computer Science and Applications*, 10(8), 610-629. <https://doi.org/10.14569/ijacsa.2019.0100880>
- Lau, R. Y. K., Xia, Y., & Ye, Y. (2014). A probabilistic generative model for mining cybercriminal networks from online social media. *IEEE Computational Intelligence Magazine*, 9(1), 31-43. <https://doi.org/10.1109/MCI.2013.2291689>
- Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018). The science of fake news. *Science*, 359(6380), 1094-1096. <https://doi.org/10.1126/science.aao2998>
- Li, J., Ma, B., & Wang, C. (2018a). Extraction of PRNU noise from partly decoded video. *Journal of Visual Communication and Image Representation*, 57, 183-191. <https://doi.org/10.1016/j.jvcir.2018.10.023>
- Li, S., Sun, Q., & Xu, X. (2018b, June 28-30). Forensic analysis of digital images over smart devices and online social networks. *Proceedings of the 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* (pp. 1015-1021). IEEE.
- Liu, B., Zhou, Q., Ding, R. X., Palomares, I., & Herrera, F. (2019). Large-scale group decision making model based on social network analysis: Trust relationship-based conflict detection and elimination. *European Journal of Operational Research*, 275(2), 737-754. <https://doi.org/10.1016/j.ejor.2018.11.075>
- Lorch, B., Scheler, N., & Riess, C. (2022). Compliance challenges in forensic image analysis under the artificial intelligence act. *arXiv*. <https://doi.org/10.48550/arXiv.2203.00469>
- MacDermott, Á., Motylinski, M., Iqbal, F., Stamp, K., Hussain, M., & Marrington, A. (2022). Using deep learning to detect social media 'trolls'. *Forensic Science International: Digital Investigation*, 43 Suppl, 301446. <https://doi.org/10.1016/j.fsidi.2022.301446>
- Manoj, S. K. A., & Bhaskari, D. L. (2016). Cloud forensics-A framework for investigating cyber attacks in cloud environment. *Procedia Computer Science*, 85, 149-154. <https://doi.org/10.1016/j.procs.2016.05.202>
- Misra, S., & Arumugam, C. (2022). *Illumination of artificial intelligence in cybersecurity and forensics*. Springer.
- Mohammad, R. M. A. (2020). An improved multi-class classification algorithm based on association classification approach and its application to spam emails. *IAENG International Journal of Computer Science*, 47(2), 07. https://www.iaeng.org/IJCS/issues_v47/issue_2/IJCS_47_2_07.pdf
- Mohammad, R. M. A., & Alqahtani, M. (2019). A comparison of machine learning techniques for file system forensics analysis. *Journal of Information Security and Applications*, 46, 53-61. <https://doi.org/10.1016/j.jisa.2019.02.009>
- Muneer, A., & Fati, S. M. (2020). A comparative analysis of machine learning techniques for cyberbullying detection on Twitter. *Future Internet*, 12(11), 187. <https://doi.org/10.3390/fi12110187>
- Ngejane, C. H., Mabuza-Hocquet, G., Eloff, J. H. P., & Lefophane, S. (2018, August 6-7). Mitigating online sexual grooming cybercrime on social media using machine learning: A desktop survey. *Proceedings of the 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)* (pp. 1-6). IEEE.
- Nowroozi, E., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2021). A survey of machine learning techniques in adversarial image forensics. *Computers & Security*, 100, 102092. <https://doi.org/10.1016/j.cose.2020.102092>
- Oberlo. (2023). *How many people use social media in 2024?* <https://www.oberlo.com/statistics/how-many-people-use-social-media>
- O'Connell, R. (2003). *A typology of child cyberexploitation and online grooming practices*. <http://image.guardian.co.uk/sys-files/Society/documents/2003/07/24/Netpaedoreport.pdf>
- Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation*, 13, 38-57. <https://doi.org/10.1016/j.diin.2015.03.002>
- Ptaszynski, M., Eronen, J. K. K., & Masui, F. (2017, August 21).

- Learning deep on cyberbullying is always better than brute force. In R. Rzepka, J. Vallverdu, & A. Włodarczyk (Eds.), *Proceedings of the Linguistic and Cognitive Approaches To Dialog Agents Workshop co-located with the 26th International Joint Conference on Artificial Intelligence (IJCAI 2017)* (pp. 3-10). CEUR-WS.
- Purnaye, P., & Kulkarni, V. (2022). A comprehensive study of cloud forensics. *Archives of Computational Methods in Engineering*, 29(1), 33-46. <https://doi.org/10.1007/s11831-021-09575-w>
- Qadir, A. M., & Varol, A. (2020, June 1-2). The role of machine learning in digital forensics. *Proceedings of the 2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.
- Ruan, X., Wu, Z., Wang, H., & Jajodia, S. (2016). Profiling online social behaviors for compromised account detection. *IEEE Transactions on Information Forensics and Security*, 11(1), 176-187. <https://doi.org/10.1109/TIFS.2015.2482465>
- Ryser, E., Spichiger, H., & Casey, E. (2020). Structured decision making in investigations involving digital and multimedia evidence. *Forensic Science International: Digital Investigation*, 34, 301015. <https://doi.org/10.1016/j.fsidi.2020.301015>
- Sandoval-Orozco, A. L., Quinto Huamán, C., Povedano Álvarez, D., & García Villalba, L. J. (2020). A machine learning forensics technique to detect post-processing in digital videos. *Future Generation Computer Systems*, 111, 199-212. <https://doi.org/10.1016/j.future.2020.04.041>
- Shahbazi, Z., & Byun, Y. C. (2020). Deep learning method to estimate the focus time of paragraph. *International Journal of Machine Learning*, 10(1), 75-80. <https://doi.org/10.18178/ijmlc.2020.10.1.901>
- Shahbazi, Z., & Byun, Y. C. (2021). Fake media detection based on natural language processing and blockchain approaches. *IEEE Access*, 9, 128442-128453. <https://doi.org/10.1109/ACCESS.2021.3112607>
- Shahbazi, Z., & Byun, Y. C. (2022). NLP-based digital forensic analysis for online social network based on system security. *International Journal of Environmental Research and Public Health*, 19(12), 7027. <https://doi.org/10.3390/ijerph19127027>
- Shi, Y., Yang, H., Gong, M., Liu, X., & Xia, Y. (2017). A fast and robust key frame extraction method for video copyright protection. *Journal of Electrical and Computer Engineering*, 2017, 1231794. <https://doi.org/10.1155/2017/1231794>
- Simou, S., Kalloniatis, C., Gritzalis, S., & Mouratidis, H. (2016). A survey on cloud forensics challenges and solutions. *Security and Communication Networks*, 9(18), 6285-6314. <https://doi.org/10.1002/sec.1688>
- Son, J., & Buyya, R. (2018). A taxonomy of software-defined networking (SDN)-Enabled cloud computing. *ACM Computing Surveys*, 51(3), 59. <https://doi.org/10.1145/3190617>
- Song, Z., & Fergnani, A. (2022). How pandemic films help us understand outbreaks: Implications for futures and foresight. *World Futures Review*, 14(1), 9-28. <https://doi.org/10.1177/19467567221076569>
- Statista. (2022). *Most popular social networks worldwide as of January 2024, ranked by number of monthly active users*. <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>
- Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the Internet of things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, 22(2), 1191-1221. <https://doi.org/10.1109/COMST.2019.2962586>
- Sun, D., Zhang, X., Choo, K. K. R., Hu, L., & Wang, F. (2021). NLP-based digital forensic investigation platform for online communications. *Computers & Security*, 104, 102210. <https://doi.org/10.1016/j.cose.2021.102210>
- Suryanto, H., Degeng, I. N. S., Djatmika, E. T., & Kuswandi, D. (2021). The effect of creative problem solving with the intervention social skills on the performance of creative tasks. *Creativity Studies*, 14(2), 323-335. <https://doi.org/10.3846/cs.2021.12364>
- Taha, K., & Yoo, P. D. (2019). Shortlisting the influential members of criminal organizations and identifying their important communication channels. *IEEE Transactions on Information Forensics and Security*, 14(8), 1988-1999. <https://doi.org/10.1109/TIFS.2018.2890811>
- van der Walt, E., Eloff, J. H. P., & Grobler, J. (2018). Cyber-security: Identity deception detection on social media platforms. *Computers & Security*, 78, 76-89. <https://doi.org/10.1016/j.cose.2018.05.015>
- Wu, X., Sun, C., Zou, T., Li, L., Wang, L., & Liu, H. (2020). SVM-based image partitioning for vision recognition of AGV guide paths under complex illumination conditions. *Robotics and Computer-Integrated Manufacturing*, 61, 101856. <https://doi.org/10.1016/j.rcim.2019.101856>
- Xiao, J., Li, S., & Xu, Q. (2019). Video-based evidence analysis and extraction in digital forensic investigation. *IEEE Access*, 7, 55432-55442. <https://doi.org/10.1109/ACCESS.2019.2913648>
- Xie, Y., Feng, D., Liao, X., & Qin, L. (2018). Efficient monitoring and forensic analysis via accurate network-attached provenance collection with minimal storage overhead. *Digital Investigation*, 26, 19-28. <https://doi.org/10.1016/j.diin.2018.05.001>
- Zhang, Y., Wu, S., Jin, B., & Du, J. (2017, December 13-16). A blockchain-based process provenance for cloud forensics.

Proceedings of the 2017 3rd IEEE International Conference on Computer and Communications (ICCC) (pp. 2470-2473). IEEE.

Zuo, Z., Li, J., Anderson, P., Yang, L., & Naik, N. (2018, July

8-13). Grooming detection using fuzzy-rough feature selection and text classification. *Proceedings of the 2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1-8). IEEE.