Impact of Artificial Intelligence in Digital Forensics: a Review Study

Akarshan Suryal, Pramatma Vishwakarma and Anindita Malik

July 10, 2024

Impact of Artificial Intelligence in Digital Forensics: A Review Study

Akarshan Suryal[1, a)], Pramatma Vishwakarma[2, b)], Anindita Malik [1, c)]

[1] Department of Bioscience and Bioengineering, Lovely Professional University, Phagwara, India, 144411
[2] *Department of Computer Application, Lovely Professional University, Phagwara, India, 144411*
[a)]akarshansuryal6@gmail.com
[b)]vpramatma@gmail.com
[c)]anindita.27976@lpu.co.in

Abstract. Digital forensics is a critical component of modern law enforcement and cybersecurity. As technology continues to advance, the amount of data that Shall be Capable to be collected and scrutinized in investigations is increasing at an exponential rate. Artificial Intelligence has emerged as a powerful tool in digital forensics, offering new ways to scrutinize and process data so as to identify potential evidence and patterns. We conducted a study on the how AI is giving Impact on Digital forensics, where we discussed tool of AI used in creating the framework for the digital forensic investigations like ML, DL, NLP, Data Mining etc. Also discussed the possible area of Forensics Sciences where AI can play huge, impacted roles, also discussed all benefits and limitations of the Study.

Keywords: Artificial Intelligence Investigation, Natural Language Processing (NLP), Artificial Intelligences, Deep Learning (DL), Digital Forensics, Machine Learning (ML), Cyber Crime.

INTRODUCTION

Digital forensics is a critical component of modern law enforcement and cybersecurity. As technology continues to advance, the amount of data that Shall be Capable to be collected and scrutinized in investigations is increasing at an exponential rate. This presents signify be Capable to challenges for investigators, who must be Capable to process and scrutinize large volumes of data quickly and accurately so as to identify potential evidence and solve complex cases.(Anghel, 2019)

Artificial Intelligence has emerged as a powerful tool in digital forensics, offering new ways to scrutinize and process data so as to identify potential evidence and patterns. AI algorithms Shall be Capable to scrutinize large volumes of data in real-time, providing investigators with new insights and helping to streamline the investigation process. So as to free up investigators to concentrate on more difficult activities that call for human skill, artificial intelligence Shall be Capable to also be utilized to automate elementary operations like data collecting and analysis. (Ganesh, 2017; Kaur et al., 2016)

AI technology is being used in diverse ways in digital forensics, including Data Recovery, Multimedia Analysis, Threat Intelligence, Malware Analysis, Network Analysis, Log Analysis and NLP (Written and Spoken Communication to identify). AI Shall be Capable to be utilized to scrutinize video footage and recognize prospects suspects or automobiles involved in a crime. Also, shall be Capable to be utilized to monitor network traffic and recognize prospects threats or suspicious activity in real-time.(Ganesh, 2017; Kasper & Laurits, 2016)

Digital Forensics

Applying examination and analysis methods to obtain and preserve data from the relevant computer device in a manner that is relevant for presenting in court is known as digital forensics. To determine precisely what Shall be capable to be acquired on a digital device and who was to charge for it, digital forensics conducts a thorough inquiry while preserving a documented chain of evidence. Examiners and analysts now regularly employ digital forensics technologies.[5]

Digital forensics is the utilization of investigation and analysis techniques to gather and secure proof from a specific electronic device in a manner that is appropriate for presenting in a formal courtroom. The goal of digital forensics is to conduct a structural inquiry while maintaining a rely chain of evidence to determine precisely what take place on a digital device and who accounted for it. Several authors proposed diverse scientific methods for conducting digital forensic investigations and specified phases for the process, which are illustrated in Fig. 1 and briefly discussed below.[6]

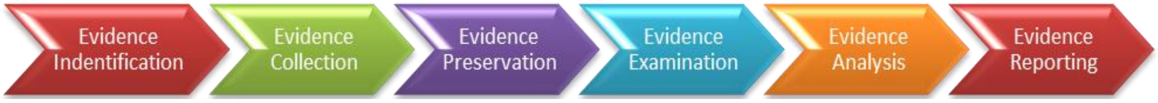

FIGURE 1. Digital Forensic Investigation Process

Artificial Intelligence

Artificial intelligence refers to the creation of advanced computer systems that Shall be to execute tasks beyond the capabilities of most humans. It involves simulating human intelligence in machines so that they Shall be to respond to questions similar to how humans would. This field aims to replicate cognitive processes like reasoning, understanding, summarizing, and learning from experience. The concept of AI dates back to the 1940s, and since then, computers have been programmed to perform complex tasks such as proving mathematical theories and playing chess with great proficiency.[7]

Artificial Intelligence, or AI, is an exciting and rapidly growing field of IT that seeks to develop intellectual machines that Shall be to execute undertakings that classically entail human intelligence. The foundation of AI idea of building machines with intelligence that Shall be to recognize configurations in data, learn from that data, and act on that. ML, a technique for instructing computers to understand and enhance their performance over time, is among the essential elements of AI. In ML, algorithms are created to evaluate data, gain knowledge from it, and base predictions and judgments on it.[8]

Artificial Intelligence is modernizing the approach we approach diverse phases of life, including digital forensics. Digital forensic is the practice of extracting, analyzing, and preserving digital evidence from computers, mobile phones, and other electronic devices to be applied in legal proceedings. AI Shall be to help automate the procedure of analyzing digital evidence, reducing the time and resources essential ed to identify relevant data. This article explores the task of A.I in digital forensics, the challenges faced, and the opportunity of A.I in this field.[3]

REVIEW METHODLOGY

The drive of this methodology is to outline the steps involved in conducting “A Study on Impact of AI in Digital Forensics” The study Shall aim to scrutinize and synthesize existing literature on the topic to provide a comprehensive overview of the current state of knowledge in this area. The following sections Shall outline the key steps involved in conducting this study.

Selection of Digital Archives

For this study data was gathered from five distinct digital archives, such as IEEE Xplore, ACM, Science Direct (SD), Springer Link (SL) and Google Scholar. IEEE Xplore provides comprehensive databases for papers on diverse topics like Artificial Intelligence with Digital Forensic. And it contains a vast collection of different papers. ACM Digital Library gives access to high quality paper in the ground of computing. SD offers accessibility to extremely dependent articles in engineering, medicine, and computing. Springer Link (SL) gives access to diverse fields Engineering, Law, Life Science, Computer Science. Google scholar provides a credible source in all scientific areas, including biomedical engineering, computational science, as well as health technology. These sources were chosen for their accept scope and uniqueness of the investigations.

Search Code Strategy

On Feb 16, 2023, the authentic research papers accessible since the start of time were gathered from databases (IEEE, ACM, SD, SL, Google Scholar). Numerous queries have been employed to improve the search-related inquiry for numerous types of AI tools that aid in digital or computer forensics. The following were essential search terms utilized for data lookup: ("Artificial Intelligence" **AND "**Digital Forensic" **OR "**Computer Forensic" **AND** "Forensic Analysis" **OR** "Data Recovery" **OR** "Evidence Collection" **OR** "Malware Analysis" **OR** "Log Analysis" **OR** "Intrusion Detection" **OR** "Evidence Analysis" **OR** NLP). These keywords were identified in the titles, abstracts, and keywords of published works. Furthermore, only original research publications pertaining to Artificial Intelligence tools that aid within digital forensics were selected, while review articles and books were excluded from the collection.

Eligibility Criteria and Article Screening

The literature selection technique was initiated by running search code queries on the aforementioned digital databases, as illustrated in the figure below. The first query yielded 468 items; however, after deleting duplicates, only 386 documents were left. After filtering based on title, abstract, and keywords, 311 papers were eliminated. We selected 75 papers for the entire text research, and after carefully reviewing each one, only 22 high-quality articles were chosen for our systematic review. Thereafter we generate a t where summary of what all authors want to convey is studies.

Searching and Selection Strategy for Systematic Review

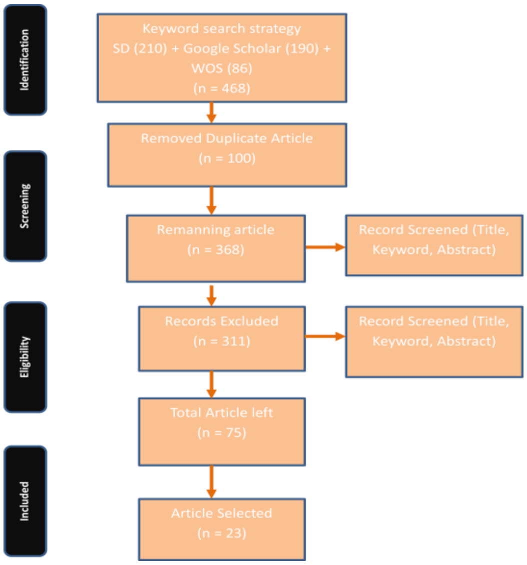

***FIGURE* 2.** A Comprehensive Review and Selection Strategy

RELATED WORK

TABLE 1. Summary of Artificial Intelligence with Digital Forensics Papers

Tool Used	Result	Limitation
Decision trees Neural networks Genetic algorithms Fuzzy logic	AI Techniques Shall be to be utilized to scrutinize data and identify patterns that may be relevant to an investigation[3]	• The essential for high-quality data and the ability for bias in ML algorithms

ML, DL, NLP Decision Trees Privacy-Preserving Techniques	Proposed framework involves data collection, data preprocessing, feature extraction, and decision-making utilizing ML algorithms[9]	• Lack of experimental results and comparison with traditional forensics methods • Privacy disputes
ML, NLP Data mining Expert systems	The essential for a shift from traditional digital forensics to intelligent forensics[10]	• Lack of empirical evidence, data, • Limited discussion on ethical, legal and implications, implementation challenges.
Classification, Clustering, Anomaly Detection algorithms, DL	Enhance efficiency and effectiveness. and highlights some of the challenges that essential to be addressed to safeguard the reliability and accuracy of ML-based approaches in this field [11]	• Limited discussion of ethical issues and narrow focus.
ML, NLP, Computer vision Expert systems	Potential benefits and challenges of using AI in investigations, and the value data digital forensics Shall be to provide for AI applications [12]	• Conceptual paper without empirical results and limited discussion of ethical, and social implications. • Lacks of comprehensive scrutiny of the strengths.
Mining Techniques, ML	A framework for evaluating and standardizing digital evidence mining techniques in digital forensics. It provides valuable insights for future study and growth [13]	• Does not offer specific experimental results to support the proposed framework. • Do not provide an in-depth assessment of the potential ethical, legal, and social implications of using AI-based tools in digital forensics
DL, Rule-Based Systems, Transfer Learning, Edge Computing, Hybrid AI Models	It proposes solutions and approaches for using Artificial Intelligence (AI) within digital forensics and Incident Response in constrained environments, based on existing research and literature in the ground [14]	• Lacks empirical data, technical details, a comparative analysis, • Has a limited scope.
ML, DL, NLP, Expert systems, Computer vision	Explores the potential benefits and challenges of using AI in digital forensics. It discusses diverse AI techniques, such as ML and NLP, and highlights the essential for a responsible and ethical approach to AI within digital forensics[15]	• Does not delve into specific applications. • Does not address the technical complexities. • Limitations of employing AI in digital forensic.
ML, NLP, Expert systems, Computer vision	Argues that AI develops the capability to help address specific of the current challenges in this domain, for instance the essential to scrutinize large volumes of complex data and the difficulty of identifying relevant prove in a timely manner[16]	• Lack of specific examples and data to support the author's claims, and its high-level overview of A.I in digital forensics. • Does not provide detailed technical information or practical implementation strategies.
Robotics process automation, ML, NLP, Expert systems, Computer vision	Discussed the influence of automation & artificial intelligence on digital forensics, which is the progression of identifying, collecting, analyzing, and preserving electronic evidence [17]	• Lack of empirical evidence also does not address potential drawbacks and challenges in-depth.
XAI techniques, feature importance analysis, rule extraction, and visualization tools	XAI techniques to mitigate the problem of distrust in AI-based digital forensics analysis. A case studies demonstrated that XAI techniques improved transparency and trust in the analysis by providing a clearer understanding of how the AI model arrived at its decision [18]	• The difficulty of developing effective XAI techniques for complex AI models. • Extra time and capitals required for developing and implementing XAI techniques to validate the effectiveness of XAI techniques.
ML, NLP, Expert systems, Neural Networks, Data mining	Discusses the utilization of artificial intelligence in computer forensics, highlighting the latent benefits and limitations of using AI technologies [19]	• Does not provide specific instances of AI technologies used in computer forensics. • Lack of Ethical Concerns

ML, NLP, Neural Networks, Fuzzy logic	Propose frameworks were able to identification, analysis, and understand digital evidence. The framework's effectiveness was evaluated using datasets, and the results showed its potential to improve the proficiency and precision of digital forensic examinations [20]	• No comparison with existing digital forensics frameworks and practical implementation was demonstrated. • Framework's accuracy was evaluated using limited datasets.
ML, NLP, DL Rules based learning	XAI employed to provide transparent and understand explanations for AI-based analysis. Also propose diverse XAI techniques, such as rule extraction, local model approximation, and attention mechanisms, to make AI systems more interpret. [21]	• Does not provide a detailed scrutiny of the practical limitations and challenges that may arise in implementing XAI in this area.
DL, CNN	Approach using CNN was effective in detecting missing frames in surveillance videos. They compared their method to traditional methods for missing frame detection and establish that the DL approach provided more accurate and rely on results[22]	• Lack of quantitative performance metrics, absence of a comparison with state-of-the-art methods, • Limited validation on real-world scenarios, which may affect the generalizability of the proposed approach.
Semantic Web Technologies, ML, NLP, DL, Fuzzy Logic, Computer Vision	Provide a synopsis of existing AI-based tools and approaches in digital forensic and highlight their potential in automating evidence processing and increasing case processing capacities [23]	• The paper does not supply a detailed comparison of the effectiveness of different AI technologies and report the ethical and legal implications of using AI in digital forensics. • Lack of a specific framework for implementing AI in digital forensics.
N. A	Primary result of this paper is the proposed framework itself, which provides a novel approach to reconstructing digital forensics evidence based on a goal-oriented model[24]	• The paper lacks a detailed evaluation of the proposed framework's performance in real-world scenarios. • It does not discuss the potential limitations and challenges in employing the model in practical settings.
Inductive logic programming (∂ILP)	Proposes an AI-based forensic investigative system that automates the forensic analysis process by emulating attacks to recognize and collect relevant evidence. The proposed methodology successfully generates rules that assist forensic examiners in identifying evidence to emulate attacks without execution [25]	• lacks details about the enactment of the proposed AI-based forensic investigative system, such as the specific tools used. • Additionally, the experimental results are limited to a specific environment and may not generalize well to other contexts.
NLP-based systems	Covering their role, applications, challenges, and future directions. It discusses various NLP-based techniques used in these fields, serving as a guide for researchers and practitioners and providing a roadmap for future research [26]	• lacks specific details about the execution and evaluation of these systems. • Additionally, the literature review is limited to published research and may not capture all current developments in the field.
N.A	Presents a taxonomy for classifying AI-related crime into two categories: AI as tool crime and AI as target crime. The paper analyzes the characters of AI crimes and also presents questions that are tricky to solve with conventional forensic practices. The authors emphasize the need to establish novel strategies for AI forensics to address these challenges [27]	• Paper is that it primarily focuses on theoretical discussions and literature review and does not provide empirical evidence or case studies to support its proposed taxonomy and inquiry of AI-related crime.
N. A	Proposes an AI-based system to optimize the digital forensics procedure. The system aims to increase the proficiency and productivity of digital	• It does not provide any experimental results or evaluation of the proposed AI-based system.

	forensics investigations by incorporating clustering techniques and computational intelligence [28]	• Additionally, the paper does not mention any specific tool or software used in the research.
System-Fault-Risk framework machine learning	Analyses the defensive and offensive use of Artificial Intelligence and ML Software in cybersecurity. The authors sort AI/MLS-powered cyberattacks hooked on seven classes using the System-Fault-Risk framework and discuss their practical implications [29]	• Does not go into detail about the technical aspects of how this expertise can be employed in attacks. • Additionally, the paper does not provide specific recommendations for mitigation strategies against AI/MLS-powered attacks.
N. A	The paper suggests that blockchain technology can be utilized to provide reliable cyber security, anti-fake, anti-alteration, and transaction accounting transparency repute for medical records with personal identifiable information in the NHS. The paper provides valuable insights for IT engineers, ICT students, and computer science academic researchers interested in AI security and blockchain technology [30]	• Does not provide a detailed analysis or employment of the proposed solution, making it difficult to evaluate the effectiveness of the suggested approach. • Additionally, the paper focuses only on the healthcare activity and does not explore the potential applicability of the proposed solution in other industries.

DISCUSSION AND CHALLENGES

The use of AI in digital forensics has the potential to improve the efficiency, accuracy, and speed of investigations. AI can automate time-consuming and labor-intensive tasks, enabling investigators to focus on more important tasks. It can also help with scalability by allowing investigators to review massive volumes of data quickly and accurately, as well as identifying patterns and anomalies in data sets. The use of AI can improve accuracy by automating data processing procedures and reducing the likelihood of human error. It can also accelerate investigations by helping investigators find pertinent evidence more quickly.

However, there are challenges with the use of AI in digital forensics, particularly with interpretability and transparency. Investigators need to understand how AI systems work and how they arrived at their conclusions to conduct digital forensics effectively. Additionally, there are difficulties with privacy and civil liberties, particularly as digital data becomes more prevalent and sensitive. It is essential to ensure that artificial intelligence is overseen appropriately, ethically, and with sufficient safeguards to defend civil rights.

Overall, the use of AI in digital forensics has the potential to improve investigations significantly. However, it is crucial to address the challenges and obstacles that may arise to ensure the ethical and legal implications of its use are adequately considered. The study on the impact of AI in digital forensics is necessary to provide guidance for future study and practice in the area.

Interoperability: Another difficulty in using AI within digital forensics is compatibility. distinct digital forensics technologies may use distinct data formats and procedures, making integration of AI systems into current processes problematic[10]

Limited data availability: Data availability is another research gap in the utilization of AI in digital forensics. The availability of large-scale, diversified datasets is crucial for the development and evaluation of AI-based digital forensics systems, but such datasets are frequently small and limited in scope [10]

Limited testing and evaluation: Another barrier to using AI within digital forensics is the deprivation of testing and evaluation of AI-based solutions. More rigorous testing and assessment of AI-based systems is required to determine their usefulness and reliability in real-world circumstances [10]

APPLICATION OF ARTIFICAL INTELLIGENCE IN DIGITAL FORENSICS

- **Automated analysis:** AI Shall be to scrutinize digital evidence like hard drives, mobile devices, and cloud storage. This Shall be to save prosecutors time and lessen the possibility of human error.
- **Pattern recognition:** AI may be employed to detect patterns in data that human analysts may overlook. AI algorithms, for example, shall be to Shall be to network traffic to spot abnormal communication patterns.

- **NLP:** AI Shall be to evaluate text data such as emails, chat logs, and social media messages. NLP (NLP) algorithms Shall be to extract crucial information from messages such as the sender, recipient, and timestamp, as well as perform sentiment analysis to determine emotional content.
- **Image and Video Analysis:** AI may be utilized to scrutinize photographs and videos the purpose of identify items, persons, and locations. This Shall be to be especially value in circumstances when digital evidence includes images or videos.
- **Malware detection:** AI Shall be to detect malware and other dangerous software. ML algorithms Shall be instructed to recognize patterns in code that indicate malware.
- **Detection of Abnormalities in Data:** AI Shall be to be employed to discover anomalies in data that may suggest suspicious activities. AI systems, for example, shall be to evaluate network user behavior to spot deviations from usual patterns of activity.
- **Evidence Prioritization:** Artificial intelligence (AI) Shall be employed to prioritize digital evidence based on its relevance and signify be to an inquiry. This Shall be to assist investigators in concentrating their efforts on the most important evidence.
- **Incident Response:** Artificial intelligence (AI) Shall be to help incident response teams by automating tasks like detecting affected systems and gathering data for investigation.
- **Continuous Monitoring:** Artificial intelligence Shall be to be employed to continuously monitor systems and networks, alerting investigators to any issues in real time. This Shall be to aid in the prevention and mitigation of cyber-attacks and other security events.
- **Data Recovery:** Artificial intelligence (AI) Shall be employed to recover data from damaged or corrupted digital devices. ML algorithms Shall be instructed to recognize patterns in corrupted data and reconstruct it in us form.
- **Voice and Audio Analysis:** AI Shall be to be employed to scrutinize voice and audio data the purpose of determine critical information such as speaker identity, conversational content, and speaker location.
- **Virtual Assistants:** By automating repetitive processes, delivering real-time notifications, and helping with data analysis, AI-powered virtual assistants Shall be to be employed to support digital forensics investigations.
- **Fraud Detection:** By examining vast volumes of data and spotting trends that might point to fraud, AI Shall be to be employed to identify fraudulent conduct, such as financial fraud. To help investigators find and stop fraud, ML algorithms Shall be instructed to recognize irregularities in financial transactions.
- **Cross-Device Analysis:** Using AI, data from numerous devices, including tots, laptops, and smartphones, may be scrutinized to find pertinent information and relationships among them. ML algorithms Shall be instructed to spot patterns and irregularities in data from many sources, assisting investigators in putting together a case's whole image.
- **Geographical Analysis:** Using AI, geographical data, such as GPS coordinates or location information from social media, may be scrutinized to find patterns and connections among diverse locations. ML algorithms Shall be instructed to recognize connections between diverse sites and people, assisting investigators in constructing a more thorough picture of a case.
- **Blockchain Analysis:** Using AI, it is vi to discover patterns and relationships between diverse transactions by analyzing data from blockchain networks, such as Bitcoin transactions. The purpose of helping investigators, stop and detect criminality, ML algorithms Shall be to be instructed to recognize suspicious activity on blockchain networks.
- **Cloud Forensics:** Using AI, data saved in cloud services like Google Drive or Dropbox may be scrutinized to find pertinent data and connections between diverse people and devices. The purpose of help investigators, create a more thorough picture of a case, ML algorithms Shall be to be instructed to admit patterns in cloud data.
- **Biometric Analysis:** AI shall be employed to identify suspects or witnesses in digital data using biometric analysis techniques like facial recognition and voice analysis. ML algorithms that evaluate biometric data Shall be to be instructed to help investigators find pertinent subjects and support a more thorough picture of a case.
- **Threat Hunting:** By automating the development of spotting potential dangers and anomalies in data, AI may enhance threat hunting. Security teams Shall respond more quickly and efficiently when using ML algorithms, which Shall be to be instructed to realize patterns and behavior that may suggest a cyber-attack.
- **Memory Forensics:** Using AI, it is vi to examine memory dumps, such as those gleaned from a computer's RAM, the purpose of spotting any potential security lapses or other unusual behaviors. It is vi to teach ML algorithms

to find trends in memory dumps, assist investigators in spotting and preventing cyberattacks.

- **Material Classification:** By looking at the content of digital material like emails or documents, AI Shall be to classify and categorize it. The purpose of helping investigators concentrate on the most crucial bits of information in a case, ML algorithms Shall be to be instructed to recognize pertinent information in data.
- **Behavioral Analysis:** Using AI, it is via to spot prospective suspects or witnesses by studying people's behavior, such as their online activities or digital interactions. The purpose of help investigators, create a more thorough picture of a case, ML algorithms Shall be to be instructed to recognize patterns and abnormalities in behavior.
- **Network Analysis:** AI Shall be to be employed to examine network traffic data, including logs or packets, to find any unusual activity or potential security breaches. To help investigators find and stop cyberattacks, ML algorithms Shall be instructed to recognize patterns in network data.
- **Analysis of Digital Signatures:** Using AI, it is to check the authenticity of digital signatures, including those in emails and electronic documents, and identify potential forgeries. ML algorithms Shall be instructed to discover patterns and discrepancies in digital signatures, aiding investigators in spotting and preventing fraud.
- **File System Analysis:** Using AI, potential evidence Shall be to be found by analyzing file system data, such as deleted files or file metadata. Investigators Shall be to recover and evaluate pertinent information by using ML algorithms that have been trained to recognize patterns and abnormalities in file system data.
- **Cyberthreat Intelligence:** AI Shall be to be applied to this field to gather information about potential cyberthreats and vulnerabilities. Security teams Shall be to prevent and respond to cyberattacks by using ML algorithms that have been trained to monitor vast.
- **Cryptography Analysis:** AI Shall be to be employed to examine data related to cryptography, such as passwords or encrypted messages, the purpose of find any potential flaws or vulnerabilities. Investigators Shall be to use ML techniques to train them to spot patterns and anomalies in cryptography data, which Shall be to aid in information recovery or decryption.

CONCLUSION

In conclusion, applying artificial intelligence to the scrutiny of digital forensics has the probable to greatly enhance the effectiveness and efficiency of investigations. Using AI-based tools and procedures, forensic examiners are now examining massive amounts of digital data, spotting anomalies, and finding pertinent evidence that might not have been present using more conventional procedures. The overall conclusion of the literature evaluation is that the applicability of digital forensics is a promising area of study with immense potential to increase the efficacy and efficiency of investigations. Adopting AI-based solutions is not without its difficulties, however, including the need for additional effective data shield and privacy safeguards and the danger of bias and errors in AI decision-making. Therefore, further research is essential ed to address these challenges and ensure accountable and moral use within the discipline of digital forensics.

REFERENCES

[1] Anghel C. Digital Forensics–A Literature Review. *The Annals of "Dunarea de Jos "University of Galati Fascicle III, Electrotechnics, Electronics, Automatic Control, Informatics* 2019; 42: 23–27.

[2] Kaur M, Kaur N, Khurana S. A literature review on cyber forensic and its analysis tools. *International Journal of Advanced Research in Computer and Communication Engineering* 2016; 5: 23–28.

[3] Ganesh V. Artificial intelligence applied to computer forensics. *International Journal*; 5.

[4] Kasper A, Laurits E. Challenges in collecting digital evidence: a legal perspective. *The future of law and eTechnologies* 2016; 195–233.

[5] Lovanshi M, Bansal P. Comparative study of digital forensic tools. *Data, Engineering and Applications: Volume 2* 2019; 195–204.

[6] Singh S, Kumar S. Qualitative Assessment of Digital Forensic Tools. *Asian Journal of Electrical Sciences* 2020; 9: 25–32.

[7] Russell SJ. *Artificial intelligence a modern approach*. Pearson Education, Inc., 2010.

[8] Winston PH. *Artificial intelligence*. Addison-Wesley Longman Publishing Co., Inc., 1992.

[9] Kim S, Jo W, Lee J, et al. AI-enabled device digital forensics for smart cities. *J Supercomput* 2022; 1–16.

[10] Irons A, Lallie HS. Digital forensics to intelligent forensics. *Future Internet* 2014; 6: 584–596.

[11] Qadir AM, Varol A. The role of machine learning in digital forensics. In: *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*. 2020, pp. 1–5.

[12] Costantini S, De Gasperis G, Olivieri R. Digital forensics and investigations meet artificial intelligence. *Ann Math Artif Intell* 2019; 86: 193–229.

[13] Dunsin D, Ghanem M, Ouazzane K, et al. The use of artificial intelligence in digital forensics and incident response (DFIR) in a constrained environment.

[14] Mitchell F. The use of artificial intelligence in digital forensics: An introduction. *Digital Evidence & Elec Signature L Rev* 2010; 7: 35.

[15] Mohsin K. Artificial Intelligence in Forensic Science. *Available at SSRN 3910244*.

[16] Jarrett A, Choo K-KR. The impact of automation and artificial intelligence on digital forensics. *Wiley Interdisciplinary Reviews: Forensic Science* 2021; 3: e1418.

[17] Solanke AA. Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models. *Forensic Science International: Digital Investigation* 2022; 42: 301403.

[18] Hoelz BWP, Ralha CG, Geeverghese R. Artificial intelligence applied to computer forensics. In: *Proceedings of the 2009 ACM symposium on Applied Computing*. 2009, pp. 883–888.

[19] Rughani PH. ARTIFICIAL INTELLIGENCE BASED DIGITAL FORENSICS FRAMEWORK. *International Journal of Advanced Research in Computer Science*; 8.

[20] Hall SW, Sakzad A, Choo K-KR. Explainable artificial intelligence for digital forensics. *Wiley Interdisciplinary Reviews: Forensic Science* 2022; 4: e1434.

[21] Zhang Z, Feng H, Pan S, et al. Missing Frame Detection of Surveillance Videos Based on Deep Learning in Forensic Science. In: *Proceedings of the 2020 6th International Conference on Computing and Artificial Intelligence*. 2020, pp. 298–304.

[22] Maratsi MI, Popov O, Alexopoulos C, et al. Ethical and Legal Aspects of Digital Forensics Algorithms: The Case of Digital Evidence Acquisition. In: *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*. 2022, pp. 32–40.

[23] Ogundiran A, Chi H, Yan J, et al. A Framework to Reconstruct Digital Forensics Evidence via Goal-Oriented Modeling. In: *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*. 2023, pp. 1–11.

[24] Alnafrani R, Wijesekera D. AIFIS: Artificial Intelligence (AI)-Based Forensic Investigative System. In: *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*. 2022, pp. 1–6.

[25] Ukwen DO, Karabatak M. Review of NLP-based systems in digital forensics and cybersecurity. In: *2021 9th International symposium on digital forensics and security (ISDFS)*. 2021, pp. 1–9.

[26] Jeong D. Artificial intelligence security threat, crime, and forensics: Taxonomy and open issues. *IEEE Access* 2020; 8: 184560–184574.

[27] Punjabi SK, Chaure S. Forensic Intelligence-Combining Artificial Intelligence with Digital Forensics. In: *2022 2nd International Conference on Intelligent Technologies (CONIT)*. 2022, pp. 1–5.

[28] Kamoun F, Iqbal F, Esseghir MA, et al. AI and machine learning: A mixed blessing for cybersecurity. In: *2020 International Symposium on Networks, Computers and Communications (ISNCC)*. 2020, pp. 1–7.

[29] Xiaohua F, Marc C, Elias E, et al. Artificial intelligence and Blockchain for future cyber security application. In: *2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. 2021, pp. 802–805.

[30] Kebande VR, Venter HS. On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges. *Australian Journal of Forensic Sciences* 2018; 50: 209–238.