Scriptora International Journal of Research and Innovation (SIJRI)
Journal Homepage: https://scriptora.org

Digital Forensics and Artificial Intelligence: Emerging Approaches to Cybercrime Investigation

Prof. Ashish Govindrao Kadam
Assistant Professor
Department of Computer Science & Engineering
CSMSS Chh. Shahu College of Engineering Chh. Sambhajinagar

Prof. Komal Ashish Kadam
Assistant Professor
Department of Artificial Intelligence & Data Science
CSMSS Chh. Shahu College of Engineering Chh. Sambhajinagar

Dr. Swati Vitthal Khidse
Associate Professor
Department of Computer Science & Engineering
CSMSS Chh. Shahu College of Engineering Chh. Sambhajinagar

Dr. Sandeep Prabhakarrao Abhang
Professor
Department of Computer Science & Engineering
CSMSS Chh. Shahu College of Engineering Chh. Sambhajinagar

Prof. Bhausaheb Shankarrao Deshmukh
Associate Professor
Department of Mechanical Engineering.
CSMSS Chh. Shahu College of Engineering Chh. Sambhajinagar

Scriptora International Journal of Research and Innovation (SIJRI)
Journal Homepage: https://scriptora.org

Abstract

Digital technologies have changed the nature of crime and present problems in the investigation and in gathering evidence in cybercrime. Advanced digital forensic techniques have become vital to tackle the growing challenges of cybercrime, identity theft and financial fraud, data breaches, ransomware and online exploitation. Artificial Intelligence (AI) is proving to be a helpful technology in Digital Investigations, enabling the precision, speed and effectiveness of digital investigations. This study delves into how the Digital Forensics and the Artificial Intelligence are evolving and the new techniques that will be utilized in Digital Evidence Analysis, Cybercrime Detection, and Cybercrime Investigative Decision making. It discusses the possibilities of using AI, NLP, intelligent pattern recognition and automated evidence analysis to detect suspicious behavior and to trace the history of a cybercrime incident. The research further emphasizes the capabilities of AI-driven forensic tools in handling vast amounts of digital data, uncovering hidden patterns, links, and behaviors, and saving time on intricate investigations. It also offers answers to some of the main concerns around the use of AI in forensic practice such as: data privacy; algorithmic bias; integrity of evidence; transparency of algorithms and processes; admissibility in court; and the credibility of automated results. The study highlights the need for a responsible use of intelligent technologies, need for standardization of forensic procedures and need for the proper legal framework. It highlights the need for the AI integration with the classical Digital Forensic tools and techniques to enhance the Digital Forensic capabilities in Cybercrime investigations, establishing a more proactive, reliable and efficient Digital Forensic system.

Keywords: Digital Forensics, Artificial Intelligence, Cybercrime Investigation, Machine Learning, Digital Evidence, Cybersecurity, Automated Forensic Analysis, Cybercrime Detection.

Publication History
Received: 14 September 2026 **Accepted:** 20 September 2026**, Published:** 25 October 2026

Open Access (BOAI Compliant) | © 2026 Author(s). Published by SIJRI under Creative Commons CC BY-NC 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/). Official signatory to BOAI.

1. Introduction

Digital technologies have transformed people, businesses and institutions in their interactions, transactions and the way they handle information in the digital sphere. The more dependent on digital platforms, however, has also brought new opportunities for cybercriminal activities such as ID theft, financial fraud, data breaches, ransomware, online harassment, and unauthorized access to computer networks. The traditional approach to cybercrime investigations is facing challenges with the increasing complexity and difficulty of cyber-attacks. Now investigators have a huge volume of digital data, advanced cyber-attack techniques, encrypted data, and ever-changing technology and environments. Digital forensics in this context has become a vital field in the identification, collection, preservation, examination and analysis of electronic evidence (EE) for the purposes of criminal investigations and lawsuits.

Digital forensics is a technology and science-based process that minimizes computer, mobile, network, cloud or other digital system incidents. Primarily, to identify relevant evidence while maintaining the integrity, authenticity and reliability of information obtained. Increased use of cloud computing, financial services online, the Internet of Things (IoT), social media and smartphones is driving the growth of digital forensic investigations. Evidence can be spread over different devices, different locations and digital platforms, making it complex to investigate the process. In addition, cybercriminals employ sophisticated artificial intelligence, virtual private networks, encryption methods, and technologies to likely conceal their activities and identities. An intelligent, adaptive and big data processing approach is required that can be more investigative for these developments.

Artificial Intelligence (AI) is rapidly emerging as an important technology that will improve the capabilities of a digital forensics examiner. There are new opportunities to detect suspicious activity and to analyse complex digital evidence with the aid of AI technologies, specifically machine learning, deep learning, natural language processing and intelligent pattern recognition. Such algorithms can sift through huge volumes of data, detect unusual activity, unusual patterns, and red flags for cybercrime. NLP can be used to analyse emails, online chats, social media communications and other text-

Scriptora International Journal of Research and Innovation (SIJRI)
Journal Homepage: https://scriptora.org

based data for investigators. Likewise, deep learning can be used to help analyze images, recognize faces, detect malware, and analyze multimedia information. AI will automate repetitive investigative procedures and save time in the analysis of evidence to free up forensic time for more complex investigative analysis.

The capabilities of AI for use in digital forensic investigations also open opportunities for proactive and predictive cybercrime detection. Traditional forensic practices tend to deal with digital evidence gathered following a security event. AI-powered systems, on the other hand, can be used to identify suspicious patterns, map seemingly unrelated online behaviours and proactively spot new cyber threats earlier.

While AI has many advantages in the field of digital forensics, it also comes with its own set of challenges, technical and ethical and legal. The reliability and accuracy of AI-generated conclusions depend on the information fed into intelligent systems. Algorithmic bias, false positives, lack of explainability and misclassifications could impact the trustworthiness of investigations. A second major problem is the ability to preserve a chain of custody and to present electronically-processed evidence in court. Digital evidence should be collected, examined and preserved by investigators' actions in an acceptable manner without alterations or unauthorized changes. Data privacy and security, surveillance, confidentiality and the responsible use of automated investigative technologies are all important issues that should be addressed. Therefore, it is important to remember that AI should not replace business judgment and human review and verification.

The complexity of cybercrime is increasing at an alarming rate and it is essential that a collaborative model is created that incorporates the principles of digital forensics, artificial intelligence, cyber security and legal aspects. The cooperation of law enforcement, forensic laboratories, experts in cybersecurity, research and judicial institutions is necessary to create effective investigative procedures and to enhance the technical resources. Lifelong professional training, harmonisation of forensic practices and protocols, as well as transparency of AI models and adequate regulatory safeguards are required to enable the responsible and effective deployment of intelligent forensic systems. The current research paper is about the dynamic connection between Artificial Intelligence and DF in cybercrime investigation titled “Digital Forensics and Artificial Intelligence: Emerging Approaches to Cybercrime Investigation”. It is centered on the identification, collection, preservation, examination and analysis of digital evidence with AI enabled technologies. New tactics in combating cybercrime, the potential for smart forensic techniques to be embraced and the technical and legal hurdles are also explored. The research will aim to explore the potential of AI to enhance the timeliness and accuracy of cybercrime investigations, to improve investigations' transparency and reliability, and to preserve the integrity and accountability of digital evidence in investigations.

2. Background of the study

The digital technologies, e-information, cloud computing, social networks and financial transactions on the internet have significantly transformed modern society. These changes have brought new potential avenues for communication, business and the exchange of information, but also added to the complexity and prevalence of cybercrime. Both individual and organizations and government institutions are facing problems due to identity theft, phishing, financial fraud, ransomware attack, data breaches, cyberstalking and unauthorized access to computer systems. With the ever-changing nature of cybercrime, traditional investigation techniques are having to evolve in order to meet the demands of the large volume of electronic evidence and increasingly sophisticated digital threats. Digital forensics is a crucial component of cybersecurity and criminal investigations that involves the discovery, preservation, examination, and presentation of digital evidence. It involves finding out about electronic gadgets and digital settings like computers, cell phones, servers, cloud systems, databases and network systems. The primary purpose of digital forensics is to make sense out of digital incidents, identify possible perpetrators, determine events and provide substantive and legally sound evidence that will assist in legal proceedings. However, with the growing complexity of the digital infrastructure has come a host of challenges, including the ability to manage huge data loads, retrieve lost data, monitor anonymized traffic and identify sophisticated cyber-attack trends. Solving these problems with technology is under investigation and that is where Artificial Intelligence (AI) is relevant. Cybercriminal investigations can be enhanced by the use of AI-powered tools such as machine learning, deep learning, NLP, pattern recognition, and automated anomaly detection. They can be used to detect suspicious activity, identify abnormal network events, identify the type of malware present, filter through the content of communication logs and find connections between seemingly unconnected digital events. Moreover, AI-powered forensic tools can be used for automated classification and prioritization of evidence, which can help with earlier stages of investigations and free up forensic specialists to focus

Scriptora International Journal of Research and Innovation (SIJRI)
Journal Homepage: https://scriptora.org

on more in-depth analysis. AI is a new trend in the field of digital forensics and crime investigation. Standard forensic methods are based on manual examination, set procedures and personal expertise of the investigators. AI-based methods, on the other hand, can analyze vast amounts of electronic information, find patterns and recognize signals that might not be easily detectable with traditional methods. The following investigations are of particular interest for this integration in the context of encrypted communications, attacks on distributed systems, digital financial crimes, attacks using malware or cross-platform crimes: But before AI outputs can be used as definitive evidence in an investigation, they should be rigorously examined by a critical and a credible and factual forensic evaluation. While AI tools offer significant benefits in the field of digital forensics, there are also significant concerns that need to be addressed, including data privacy, algorithmic bias, explainability, evidence integrity, and legal admissibility. The trustworthiness of AI-generated conclusion is tied to the quality of the training sets, transparency of analytical models and proper handling of digital evidence. Evidence may be altered, lost or improperly obtained during the process of investigation and could impact credibility. Thus, the overarching importance of retaining adherence to proper forensic procedures, audit trails, the chain of custody, and human supervision when using AI in cybercrime investigations still cannot be overstated. In this context, the present research investigates the relationship between Digital Forensics and Artificial Intelligence (AI) as applied in the newest methods of computer Science and technology used to investigate Cybercrime. It covers how analytic techniques using AI can be applied to improve the analysis of digital evidence; optimize the investigational process; identify and respond to advanced cyber threats; and Informed Forensic Decision Making. In addition, the study also takes into account the technical, ethical and legal issues involved with the implementation of intelligent forensic systems. The study will focus on these developments and its capacity to complement the existing digital forensic tools and processes to create novel cybercrime investigation mechanisms which are streamlined, accurate, transparent and reliable. The potential of AI in forensic research has also been given attention, with recent studies investigating its applications in the field. It has been researched for mobile device analysis, automated evidence analysis and intelligent pattern recognition and forensic reporting. Yet, scientists are pointing out the need for methods to validate the AI's results in a reliable fashion, transparent algorithms and proper supervision by humans to ensure proper forensic standards. The background serves to give an overall idea of the importance of research in the use of AI to aid in digital forensics, not to replace humans. This study has particular significance in terms of the Cybercrime detection and evidence management, the accuracy and credibility of the gathered evidence in trials and the emergence of intelligent approaches in detecting cybercrime.

3. Objectives of the Study

1. To develop an understanding of new applications of AI in digital forensics and cybercrime.
2. To explore the use of the AI tools in identification, collection, preservation and analysis of digital evidence on various electronic media and websites.
3. To research and gain insight on the application of machine learning and intelligent analytical tools to identify cyber threats, suspicious activity and trace digital crime.
4. To evaluate the efficacy of AI-based forensic tools to improve the accuracy, speed and efficiency of cybercrime investigations when compared to traditional forensic tools.
5. To appreciate the technical, ethical, legal and privacy issues that arise from the use of Artificial Intelligence in digital forensic practices.

6. Literature Review

The rise of digital technologies and the evolving nature of cyber threats have made digital forensics an integral part of contemporary cybercrime investigation. New challenges are created as a result of the widespread use of computers, smart phones, cloud platforms, social media and interconnected networks in relation to the identification, collection, preservation, analysis and presentation of digital evidence. Conventional methods of forensic investigation can be time-consuming and labour-intensive, especially when working with vast amounts of digital data. Artificial intelligence (AI), machine learning, and intelligent analytical techniques are becoming important methods to enhance the speed, accuracy, and effectiveness of digital forensic investigations in this context. In Cohen (2010), the difficulties of digital forensic investigations were explored, as well as the significance of systematic evidence examination, forensic process,

Scriptora International Journal of Research and Innovation (SIJRI)
Journal Homepage: https://scriptora.org

and sound analysis. The study made a number of points on the importance of preserving the integrity and evidential value of digital evidence. It serves as a solid basis for the use of sophisticated computational tools in the field of forensics while not disrupting on-going investigations. Casey (2011) laid out the evolution of digital evidence, and its significance in the field of criminal investigation, in relation to digital devices and electronic information. The author stressed the need to have adequate procedures in place to identify, gather, preserve and analyze digital evidence. This is a sign of the complexity of the Digital environment, and investigators need to keep up with and continuously develop their technical knowledge and analytical abilities. Garfinkel (2010) studied the research and development issues of digital forensic science. The author pointed out some of the following features were missing in current tools used for forensics: processing large amounts of data, reproducibility, and standardised investigation protocols. The study suggests that there is a need to further the development of forensic automation and analytical technologies to address the current and growing volume and diversity of electronic evidence. Quick and Choo (2014) studied the issues in cloud storage and digital forensic investigations. They discovered that the challenges of evidence acquisition, access and preservation of evidence exist in cloud computing environments because evidence may be located on numerous servers, across various geographic sites. The challenges highlight the potential of AI-powered forensic tools in finding relevant information and navigating through complex digital environments. Caviglione, Wendzel and Mazurczyk (2017) investigated the evolution of the relationship between cybercrime and digital forensic investigation. Their efforts have raised the awareness of the evolving nature of cyberattacks and the challenges of cybercrime investigations. The authors emphasized the importance of the use of advanced forensic techniques to keep up with the new ways of cybercriminals and sophisticated cyber technologies. With the emergence of machine learning, digital evidence analysis and suspicious activity detection has taken a new turn. Sommer and Paxson (2010) networked an IDS and talked about the difficulties they encountered with bringing the statistical learning to the real world of security. They found the quality of training data, evaluation methods and machine learning results interpretation were key. The observation is particularly relevant in the case of the investigation of cybercriminals using artificial intelligence, where the misclassification could affect the investigating decisions. Buczak and Guven (2016) summarized the data mining and machine learning techniques used in cyber security. They discussed some of the techniques such as decision trees, neural network, support vector machines, clustering, association rule mining, etc. These methods were explained by the authors and how they can be used to help detect intrusion, identify the malware or classify suspicious activity. They are involved in research in areas related to the application of machine learning to digital evidence identification and analysis, which brings to theory. Similarly, Sarker et al. (2020) discussed about Cybersecurity Data Science and Application in Identification and Response of new Cyber threats. They presented the results of their research on how powerful analytical tools can be in dealing with large amounts of security information, detecting atypical behavior and supporting predictive threat analysis. These capabilities can be adapted to DF investigations as they can help investigators identify what they might consider to be important evidence in a large volume of data. Quick and Choo (2016) conducted another study on the analysis of large-scale digital forensic evidence management (big forensic data reduction). They noted that the size of a digital forensic image has created difficulties for digital forensic investigators trying to locate relevant information in a large amount of information. The study revealed a need for proper methodology of data reduction for improved forensic examination. These can be enhanced by AI-powered tools that enable classification and prioritization to sift through vast amounts of irrelevant information to identify potentially relevant evidence, assisting investigators to focus their resources. AI has also helped to support cybercrime investigations, offering new resources for recognizing malicious software, unusual files, and analyzing unusual digital activity. Network intrusion detection systems need to be carefully evaluated: The real world is very different from the experimental world (Sommer and Paxson, 2010). They are especially important for the digital forensics community, and important for automated decisions in digital forensics—these need to be compared with contextual information before being accepted as true. Buczak and Guven (2016) did a comprehensive study about machine learning and data mining techniques for cybersecurity intrusion detection. They learned supervised and unsupervised learning algorithms, and how they can be used to detect malicious network traffic. Among the most important ones that was discussed among the authors was data accessibility and difficulties in the analytical methods and complexity. The results demonstrate that machine learning can play a part in assisting in forensic investigations by assisting in the identification of suspicious communication patterns, abnormal system activity, and suspicious indicators of cybercrime. Sarker et al. (2020) gave a detailed survey on Cybersecurity Data Science with the aid of machine learning. Their work provided them with an idea of the usefulness of patterns in security data, and how patterns can be utilized to make automated decisions. The authors emphasized the importance of data-driven cybersecurity frameworks that can be used for the

Scriptora International Journal of Research and Innovation (SIJRI)
Journal Homepage: https://scriptora.org

identification of new threats and improvement of security operations. Their results offer a helpful baseline for crafting AI-based models for forensic investigations, which can handle vast amounts of digital data, flag suspicious behaviors, and assist investigators in reconstructing cyber incidents. The other important aspect of the digital forensics using AI is investigating cloud-based cybercrime. Quick and Choo (2013) investigated challenges of cloud storage forensic collection, and showed that the retrieval of digital evidence from cloud platforms can pose problems regarding data integrity as well as metadata preservation. The results of their study show that investigators should be aware of the impact of data collection methods on the original digital evidences. In the context of cloud forensics, AI can assist in finding pertinent files, examining access history, and identifying irregular patterns or changes in the system in a cloud-based environment. Automatic analysis should be performed in combination, however, with proper evidence preservation procedure. Garfinkel (2010) discussed the standardised and modular research and processing in digital forensics. The author emphasized the need to have a "tool" and a "process" to be dependable in the field of forensics. This is particularly true for the field of forensic investigations where AI technologies are entering, where the analytical outputs obtained may vary depending on the type of algorithm they are applying, how they are trained, configured and processed. Thus, transparency and repeatability, along with validation should continue to be key expectations of forensic tools that utilize AI. As for the scientific principles of digital forensic evidence, Cohen (2010) mentioned the importance of establishing valid processes in examining evidence. This view strengthens the importance of making sure that technological advancements do not compromise forensic conclusions' credibility. The capacity to explain “why” files are identified as being “odd”, why the digital events are correlated, and why the evidence may be a potential piece of evidence are among the key attributes of AI-driven investigation. The human investigator should never solely rely on the automated results to make a judgment regarding the usefulness of the automated results in a criminal investigation, and should always be responsible for the evaluation of the automated results.

7. Material and Methodology

The present study is qualitative and descriptive in nature and study the role of AI in Digital forensics in Cyber-crime investigation. The research method was secondary data collection from literature, which included peer-reviewed research papers, academic journals, books, conference proceedings, cyber security reports and publications on digital forensic practices and AI investigative tools. It highlights the knowledge of machine learning, deep learning, natural language processing, automated pattern recognition and predictive analysis in identifying, collecting, preserving, examining and interpreting digital evidence. It also highlights the role of AI in malware analysis, network intrusion detection, cyber threat detection, authentication of digital evidence, and investigating complex cyberattacks. Comparative assessment of traditional forensic methodologies and AI-based methodologies are done to understand the advantages and disadvantages of AI methods in practice, as well as the issues of data privacy, algorithmic bias, evidence authenticity and legal acceptability. All the collected data is thoroughly analyzed, sorted and digested in a systematic manner to build a comprehensive understanding of the potential capabilities of AI to facilitate more precise, productive and reliable investigations into modern cybercrime.

8. Results and Discussion

Artificial Intelligence (AI) has now entered the world of digital forensic investigations, changing the way digital evidence is discovered, seized, preserved and investigated in cybercrime investigations. The findings of the present study suggest that AI tools have the potential to streamline the analysis process in forensic investigations, making them more efficient, timely, and effective in combating cybercrime. Conventional digital forensic techniques usually require investigating a significant amount of information manually, which can be time consuming and resource-intensive for investigators. However, AI solutions can process a lot of data, identify abnormal activity, notice out-of-the-ordinary behavior and find potential digital evidence in a much shorter time. Advanced technologies like machine learning algorithms, natural language processing, and automated pattern recognition have been useful in analysing electronic communication, network traffic, system logs, multimedia files and other digital forms of information.

Further, the study highlights the importance of machine learning in spotting emerging cybercrime trends and in the investigative process. In the cases of malicious file identification, detection of abnormal network activity, committing fraudulent transactions, and identification of signs of unauthorised access, supervised and unsupervised learning methods can be useful for forensic investigators. Below, are some of the more pertinent skills that are utilized in phishing, ransomware, identity theft, financial fraud and data breaches. AI driven analytical systems can also draw connections between seemingly unrelated online activity to better understand how cyberattacks are being conducted,

Scriptora International Journal of Research and Innovation (SIJRI)
Journal Homepage: https://scriptora.org

where and when, and why. However, the usefulness of these technologies depends on the quality of the data that is available, the right algorithms selected and the interpretation of the results produced by these algorithms.

The other noteworthy achievement is with regards to AI in Digital Evidence Examination and Multimedia Forensics. The modern cybercrime investigation often involves images, video, audio, emails, social media communications and even information in the cloud. The manual analysis of the above-mentioned types of materials can be difficult, particularly if evidence is discovered on multiple devices and platforms. Investigators may find it useful to review data using AI-powered image recognition, facial analysis, speech analysis, and metadata analysis, to help identify relevant information and discrepancies or changes in digital files. Likewise, NLP can be utilized to examine any kind of paper, electronic correspondence, as well as questionable emails that might contain key words, communication designs, and even prospective elements that might suggest criminal activity. However, automated results should be thoroughly reviewed and analyzed on their own to avoid misinterpretation and use of faulty evidence in legal cases.

The conversation also focuses on the use of AI to tackle the issues of volume and complexity of digital evidence. In addition to the introduction of cloud computing, Internet of Things (IoT) devices, mobile apps and encrypted communication channels, there are also several other new methods for retrieving forensic data. Traditional investigative techniques might not be able to handle the variety and ever-expanding amount of data. AI Forensic solutions offer opportunities for faster classification of data, prioritisation of evidence, detection of anomalies and multi-platform analysis. These abilities can be applied to improve investigative practices and in order to maximise the use of forensic resources. But investigators need to make sure that automated evidence processing systems are giving them an accurate picture, preserve the original evidence, and follow the procedure of digital forensics during the investigation.

Even with these benefits, there are several technical, ethical and legal issues with the use of Artificial Intelligence in digital forensics. Algorithmic bias, lack of transparency, false positive findings, privacy issues, and manipulation of digital evidence could affect the reliability of AI-driven investigations. In addition, the explainability of some AI models could result in issues when forensic evidence needs to be explained to courts and/or laws. Thus, information created with AI should not be considered definitive without proper human review. The proper chain of custody documentation, secure evidence storage, documenting investigative procedures and validating the analytical tools are all critical elements to ensuring that the credibility and admissibility of digital evidence is maintained.

The paper highlights the significant potential of AI for digital forensics and its applications to digital crime investigations in today's context. AI should not be a substitute for forensic investigators, but rather a technology that supports investigators and assists them with the analysis of the data, and repetitive examination tasks. The balance has to be struck among the smart and skilled manpower, analytical processes and legal compliance for having the correct investigative outcomes. When harnessed properly, combining technological advancements with the appropriate security measures and continued education, AI can enhance the cybercrime investigation process by making it more proactive, efficient, and evidence-based.

9. Conclusion

The integration of AI in digital forensics has paved the way for innovative advancements and improvements in the field of cybercrime investigations and digital evidence analysis. AI-powered tools assist investigators in navigating through extensive digital information, detecting suspicious activity, identifying unforeseen patterns, and more accurately and quickly analyzing intricate cyber incidents. New technologies like machine learning and deep learning, natural language processing and automated evidence analysis, are assisting in the detection of cyber threats and re-construction of digital events. For the technologies to be properly and effectively applied, however, privacy of data (including data sovereignty and security), integrity of evidence, transparency of algorithms, and lawfulness of admissibility need to be considered. There also needs to be a focus on addressing challenges, such as biased algorithms, false positives, evolving techniques of cyber attacks, and the improper use of AI tools, to ensure investigations are accurate. Eliminating barriers among cybersecurity professionals, forensics investigators and law enforcement and technology vendors is a necessary step to help create an effective investigation framework. Overall, the adoption of digital forensic practices and AI tools can help to streamline, optimize, and technologize the response to cybercrime, while not neglecting the important and irreplaceable human element in investigations and its ethical duties.

References

1. Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1
2. Beebe, N. L. (2009). Digital forensic research: The good, the bad and the unaddressed. In Proceedings of the 5th Annual IFIP WG 11.9 International Conference on Digital Forensics.
3. Billah, M. (2025). Explainable AI for digital forensics: Ensuring transparency in legal evidence analysis. Journal of Forensic Science Research, 9(2), 109–116. https://doi.org/10.29328/journal.jfsr.1001089.
4. Carrier, B. (2005). File system forensic analysis. Addison-Wesley.
5. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the Internet (3rd ed.). Academic Press.
6. Chernyshev, M., Baig, Z., Syed, N., Doss, R., & Shore, M. (2026). Large language models in digital forensics: Capabilities, challenges and future directions. Forensic Science International: Digital Investigation, 56, 302043. https://doi.org/10.1016/j.fsidi.2025.302043
7. Cohen, F. (2010). Digital forensics: A critical review. Fred Cohen & Associates.
8. Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Science International: Digital Investigation, 48, 301675. https://doi.org/10.1016/j.fsidi.2023.301675
9. European Network of Forensic Science Institutes. (2020). Best practice manual for the forensic examination of digital technology. ENFSI.
10. Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models. (2022). Forensic Science International: Digital Investigation, 42, 301403. https://doi.org/10.1016/j.fsidi.2022.301403
11. Fähndrich, J., Honekamp, W., Povalej, R., Rittelmeier, H., Berner, S., & Labudde, D. (2023). Digital forensics and strong AI: A structured literature review. Forensic Science International: Digital Investigation, 46, 301617. https://doi.org/10.1016/j.fsidi.2023.301617
12. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7, S64–S73. https://doi.org/10.1016/j.diin.2010.05.009
13. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
14. ISO/IEC. (2012). Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC Standard No. 27037:2012). International Organization for Standardization.
15. ISO/IEC. (2015). Information technology—Security techniques—Guidelines for the analysis and interpretation of digital evidence (ISO/IEC Standard No. 27042:2015). International Organization for Standardization.
16. ISO/IEC. (2015). Information technology—Security techniques—Incident investigation principles and processes (ISO/IEC Standard No. 27043:2015). International Organization for Standardization.
17. Johansen, G. (2020). Digital forensics and incident response (2nd ed.). Packt Publishing.
18. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86
19. Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In Advances in Neural Information Processing Systems (Vol. 30).
20. Lyle, J., Guttman, B., Butler, J., Sauerwein, K., Reed, C., & Lloyd, C. (2022). Digital investigation techniques: A NIST scientific foundation review (NIST Interagency/Internal Report 8354). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8354
21. Manna, R., Singh, A., Chetia, K. (2026). The Impact of Heatmap Metrics on Consumer Decision-Making in Metaverse Fashion Spaces. In: Jain, V., Heggde, G.S., Belk, R., Spais, G. (eds) Marketing in the Digital Age. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-95-6509-2_14
22. Manna,R.,Singh,A.,&Apte,M.(2024).Demystifyingmetaversedatafromuser-technology interaction. Applied Marketing Analytics, 9(4), 357-374.
23. Mitchell, T. M. (1997). Machine learning. McGraw-Hill.

Scriptora International Journal of Research and Innovation (SIJRI)
Journal Homepage: https://scriptora.org

24. Nallamala, S. K., Kodali, S., Punukollu, M., Burugu, S., Punukollu, P., & Yerneni, R. P. (2023). Advanced explainability methods for AI-based cyber forensics in incident investigation
25. Nelson, B., Phillips, A., & Steuart, C. (2015). Guide to computer forensics and investigations (5th ed.). Cengage Learning.
26. Pathak, A., Biswal, R., & Manna, R. (2026). Towards inclusive family support: intersectional and socio-ecological determinants of parental quality of life in India. Journal of Family Social Work, 29(5), 282–298. https://doi.org/10.1080/10522158.2026.2697719
27. Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302
28. Quick, D., & Choo, K.-K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation, 11(4), 273–294.
29. R. Manna, "“Effective learning through e-learning system: DEA Approach”: HCI technologies for education," 2012 4th International Conference on Intelligent Human Computer Interaction (IHCI), Kharagpur, India, 2012, pp. 1-6, doi: 10.1109/IHCI.2012.6481851.
30. Reshmi Manna. (2025). FINANCIAL FITNESS ANALYTICS FOR PERSPECTIVE ON EMPLOYEES' FINANCIAL LITERACY, HEALTH AND FIN-FIT TRAINING EFFECTIVENESS. European Economic Letters (EEL), 15(2), 2564–2579. https://doi.org/10.52783/eel.v15i2.3103
31. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 1135–1144). https://doi.org/10.1145/2939672.2939778
32. Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
33. Solanke, A. A. (2022). Digital forensics and artificial intelligence: Emerging applications and challenges in digital evidence analysis.
34. Solanke, A. A., & Biasiotti, M. A. (2022). Digital forensics AI: Evaluating, standardizing and optimizing digital evidence mining techniques. KI – Künstliche Intelligenz, 36, 143–161.
35. Towards a unified XAI-based framework for digital forensic investigations. (2024). Forensic Science International: Digital Investigation, 50, 301806. https://doi.org/10.1016/j.fsidi.2024.301806

SIJRI: Vol.2, Issue 10, October 2026 Page: 13-22 ISSN: 3107-9334

