INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 2, February 2026 | ISSN: 2456-4184 | IJNRD.ORG

THE ROLE OF ARTIFICIAL INTELLIGENCE IN DIGITAL FORENSIC INVESTIGATIONS: LEGAL AND ETHICAL CHALLENGES

Dr. Veena Kumari, Associate Professor, UILS, Chaura Maidan, Shimla, H.P.

Sh.Vijay Kumar, Ph.D, Research Scholar, H.P.U. Shimla, H.P.

Abstract : Artificial Intelligence (AI) is one of the key tools that is being implemented in the area of digital forensics to provide improved functionality in conducting investigations of a wide range of electronic content, identify irregularities in cybercrime, etc. Machine learning, pattern recognition and automated data processing techniques have made digital evidence extraction easier and faster than conventional forensic techniques, from computers to mobile devices, networks, and cloud storage. By using AI, we can catch cyber intrusions, map digital footprints, and verify the authenticity of electronic records, while we can further enhance the quality of the legal process. Yet, the introduction of AI into digital forensics also raises significant ethical and legal issues. The use of AI-based evidence is inherently uncertain in a number of situations such as algorithmic bias, data privacy, transparency, accountability, and how it should be used by the courts. Moreover, the potential for nefarious abuse deserves relevant controls and set expectations. The paper explores how AI transformed investigations of digital law, through looking at legal and ethical challenges. AI can improve the accuracy of investigations, reduce human mistakes, assist in justice, improve judicial procedures, safeguard human rights and ethics standards, and protect standards and moral rights when balancing the oversight over it.

Keywords: Artificial Intelligence, Digital Forensics, Cybercrime Investigation, Legal Challenges, Ethical Issues, Machine Learning, Evidence Admissibility, Data Privacy.

Introduction: The AI Revolution and the Crisis of Digital Evidence

Artificial intelligence involves creating advanced computer systems that can perform tasks beyond the capabilities of most humans. It focuses on replicating human intelligence, enabling machines to answer questions similarly to how people do. The primary aim is to emulate cognitive processes including reasoning, understanding, summarizing, and learning from experiences. The concept of AI dates back to the 1940s, and since then, computers have been designed to address intricate problems such as validating mathematical theories and competing in chess at an elite level. Digital forensics is a subset of forensic science that encompasses the identification, analysis, recovery, and investigation of digital evidence found on electronic devices. This type of evidence typically pertains to cybercrimes. Initially synonymous with computer forensics, digital forensics has evolved to include investigations involving various digital devices. It represents the application of scientific methodologies from computer science aimed at resolving legal inquiries, which generally involve the acquisition, examination, and presentation of digital evidence.[1] In the field of digital forensics, the objective is not to label an individual as either guilty or innocent. Instead, it seeks to provide quantitative evidence to forensic teams in a manner that allows for a thorough and unbiased interpretation of the findings. The adjudication of guilt or innocence is ultimately determined by judicial authorities, who receive these evidences through established digital forensic methodologies.[2]

As defined by the Oxford Dictionary, "forensic" pertains to the application of scientific techniques in investigating crimes and presenting these methods in legal settings. Within digital forensics, two significant areas are forensic data analysis and mobile forensics, which focus on various types of digital devices.[3]

Digital forensics, often referred to as digital forensic science, is a subset of computer forensic science that involves the recovery and examination of data found on digital devices, frequently associated with cybercrime incidents. Environments utilizing Information and Communications Technology encounter challenges stemming from extensive computer use for non-work-related purposes. User activities may include personal web browsing and using search engines for professional information; however, such browsing sessions encompass more than just these specified actions.[4]

The Core Legal Challenge: Admissibility and Due Process

Digital forensics plays an essential role in contemporary law enforcement and cybersecurity. As technological advancements continue, the volume of data available for collection and examination during investigations is growing rapidly. This surge poses significant challenges for investigators, who must efficiently and accurately process vast amounts of information to uncover

[1] Frederik Armknecht,Andreas Dewald, “Privacy-preserving email forensics”p-128, Available at https://d-nb.info/1229836004/34 (last Visited 13-04-2025).

[2] Asaf Varol ,Yeşim Ulgen Sonmez, “ Review of Evidence Collection and Protection Phases in Digital Forensics Process”.p-39. Available at https://www.researchgate.net /publication/356289285 (last Visited 13-04-2025).

[3] Dr. Nilakshi Jain, Dr.Dhananjay R. Kalbande, et.al., *Digital Forensics* 21 (Wiley India Pvt. Ltd., 1stedn., 2017).

[4] Id. At 19.

potential evidence and resolve intricate cases. Artificial Intelligence (AI) has emerged as a formidable asset in digital forensics, presenting innovative methods to analyze and process data in order to discover relevant evidence and discern patterns. AI algorithms can assess large datasets in real-time, offering investigators new perspectives while facilitating a more efficient investigative process. This enables investigators to focus on more complex tasks that require human expertise, as AI can also automate basic functions such as data gathering and analysis.[5]

The integration of AI into digital forensic investigations encompasses several aspects throughout different phases of the investigation lifecycle: collecting digital evidence, preserving it, analyzing it, and presenting findings. The proficiency and expertise of the computer forensic investigator are crucial to the success of each phase. Nonetheless, there is optimism that incorporating artificial intelligence into these investigations will provide effective tools to tackle complexity issues while addressing the challenges associated with the speed and volume of digital cases by pinpointing the most pertinent areas for inquiry and filtering out less relevant ones. This method has been partially utilized before through hash algorithms that eliminate inactive files and static system files from digital investigations. If one assumes that the knowledge applied by a digital investigator can be formally organized, it could contribute to knowledge representation. Likewise, if this knowledge is structured in such a way as to facilitate reasoning, then the concept of ontology within artificial intelligence can be employed.[6]

Artificial Intelligence (AI) represents an exciting and swiftly evolving area within IT aimed at creating intelligent machines capable of performing tasks traditionally requiring human intellect. The essence of AI lies in developing machines with cognitive abilities that enable them to recognize patterns in data, learn from those patterns, and execute actions based on their findings. Machine Learning (ML), a technique designed to teach computers how to interpret data and progressively enhance their performance over time, forms a core component of AI. Within ML frameworks, algorithms are designed to analyze data, extract insights from it, and make predictions or decisions accordingly. Artificial intelligence is revolutionizing our approach across various facets of life, including digital forensics.[7] AI also improves the capabilities for conducting predictive analytics and risk assessments within the realm of digital forensics. By analyzing historical data and recognizing trends, AI models can forecast potential security breaches or fraudulent actions. This proactive strategy allows forensic investigators to take preventive steps and respond effectively to emerging threats. Furthermore, AI can streamline legal documentation by generating comprehensive summaries of findings, which aids in expediting decision-making processes and bolstering legal proceedings.[8]

Digital forensics serves as a crucial resource for probing potential incidents in today’s technology-driven environment. However, professionals in this field must be equipped to face various challenges, including the intricacies and sheer volume of digital information, swiftly evolving technologies, and the ethical as well as legal concerns related to data collection and preservation. By adhering to established best practices for data management, digital forensic experts can assist organizations in safeguarding their digital resources and mitigating cybercrime.[9]

Ethical Responsibility and Accountability in the Legal System

There is a significant concern regarding the potential misuse of Artificial Intelligence (AI) technologies in criminal investigations. An unregulated or overly reliant approach to AI tools can lead to biased results, violations of privacy, insufficient transparency, and the wrongful incrimination of individuals. In India, the governing legal framework aligns with Articles 14 and 21 of the Constitution, which mandate fairness, equality, and due process during investigative activities. Indian legal scholars have acknowledged that technological innovations must function within constitutional and ethical boundaries.[10] Experts in cyber law and criminal justice stress that investigative bodies and AI specialists have an ethical obligation to ensure data integrity, accountability for algorithms, safeguarding of personal information, and essential human oversight when implementing AI systems.[11] From this perspective, it follows that investigation teams should regard AI as a supportive instrument rather than as an authoritative decision-maker. They need to critically assess AI-generated information before making decisions based on it. Concurrently, AI developers are responsible for creating systems that are transparent, comprehensible, and free from bias. Thus, maintaining ethical standards in AI-assisted investigations is crucial to avert misuse, uphold individual rights, and foster public trust in the criminal justice system.[12]

A key challenge associated with integrating artificial intelligence into computer forensics lies in clearly articulating how AI algorithms are utilized within forensic processes. This issue can be addressed by focusing on the role of AI in anomaly detection within computer forensics. There are two primary dimensions to consider: legal anomalies and computational anomalies. Legal anomalies refer to actions that violate laws specific to a jurisdiction, such as underage drinking or illegal driving. In contrast, computational anomalies encompass irregularities found within computing systems, such as sectors storing data improperly on a disk or anomalously formatted data packets that deviate from expected parameters—whether in dynamic streams or static storage—or personal relational data indicating atypical connections. Detecting these anomalies employs a variety of artificial intelligence techniques. Knowledge-based systems can be developed to encapsulate a legal expert's insights into law principles while identifying unusual behaviors. Neural networks may be trained to differentiate between appropriate and inappropriate behavior patterns while

[5] Akarshan Suryal, Pramatma Vishwakarma (et. al.), Impact of Artificial Intelligence in Digital Forensics: A Review Study, p. 1 Available at https://easychair.org/publications/preprint/52Gz (last visited 30-08-2025).

[6] Alastair Irons,Harjinder Singh Lallie, Digital Forensics to Intelligent Forensics,p. 592. Available at https://www.academia.edu/98369387 /Article_Digital_Forensics_to_Intelligent_Forensics? nav_from=cf993c00-b924- 46fd-a98f-f9c5a0ea7ff0 (last visited 30-08-2025).

[7] Supra note 5 at 1.

[8] Manasi Pritam Zirpe, Shravani Santosh Potdar (et.al), A I in Digital Forensics IJSRMST | Vol. 3 | Issue 5 | May 2024, p. 5 Available at https://www.researchgate.net/ publication/383837318 _AI_IN_DIGITAL_FORENSICS. (last visited 30-08-2025).

[9] Id at 6.

[10] M.P. Jain, *Indian Constitutional Law* 1123 (LexisNexis, New Delhi, 8th edn., 2018).

[11] R.K. Chaubey, *An Introduction to Cyber Law* 215 (Kamal Law House, Kolkata, 3rd edn., 2016).

[12] T. Ramachandran, *Cyber Crimes and Digital Evidence* 156 (Eastern Book Company, Lucknow, 1st edn., 2018).

modeling user interactions, enabling them to flag irregular usage by currently logged-in individuals. Additionally, data mining and machine learning methods can uncover behavior patterns and highlight deviations from norms. When combined with big data analytics and high-performance computing infrastructures, it becomes feasible to create systems that continuously adapt and enhance their performance capabilities to align with evolving trends in the field of computer forensics.[13]

There is a significant concern regarding the necessity of maintaining neutrality and fairness in the application of investigative tools. The presence of biased or unclear tools can compromise the integrity of investigations, leading to arbitrary or discriminatory results. In India, the relevant legal framework is based on Articles 14 and 21 of the Constitution, which guarantee equality before the law and a fair process. Indian legal experts have consistently argued that investigative methods should align with natural justice principles, transparency, and accountability.[14] As technological and digital tools become more prevalent, discussions surrounding cyber law and criminal justice highlight the importance of subjecting these investigative instruments to regular audits, establishing clear standard operating procedures, and ensuring human oversight to mitigate misuse and systemic bias.[15] To promote fairness, it has been proposed that measures such as independent oversight, investigator training, tool validation, and adherence to ethical standards be implemented. This indicates that impartiality in investigative tools cannot be assumed but needs to be actively enforced through legal protections and ethical frameworks. Investigative agencies are responsible for implementing corrective actions while technical experts should develop tools that are neutral, understandable, and respectful of rights. Ultimately, ensuring fairness in investigative tools enhances public trust in the justice system and reinforces constitutional principles.[16]

Applying artificial intelligence in the field of digital forensics holds significant promise for improving both the effectiveness and efficiency of investigative processes. Forensic analysts are leveraging AI-driven tools and methodologies to sift through vast quantities of digital information, identifying irregularities and uncovering relevant evidence that might have been overlooked with traditional techniques. The realm of digital forensics presents a compelling area for exploration, with substantial potential to enhance investigative outcomes. However, the implementation of AI solutions comes with challenges, such as the necessity for stronger data protection measures and privacy protocols, along with the risks associated with bias and inaccuracies in AI-generated decisions. Consequently, it is crucial to pursue further research to tackle these issues and promote ethical practices within the field of digital forensics.[17]

Conclusion and Suggestions

AI plays a transformative role in digital forensics with massive efficiency, precision, and ability to scan and categorize large volumes of digital evidence. Automation, pattern identification, predictive analysis Artificial intelligence has improved the forensic investigator's performance to identify cybercrimes and uncover hidden digital footprints that may be invisible. Nevertheless, with the addition of AI to the field of digital forensics are also an array of difficult legal and ethical dilemmas that are not easily addressed. Problems such as the admissibility of AI-produced evidence, transparency of algorithms and their resulting biases pose real problems for the systems of justice that are built upon fairness and due process. Also, the significant employment of individual and sensitive information in AI forensic procedures increases the likelihood of privacy violations and unethical surveillance practices. Left unchecked, the abuse or misinterpretation of its outputs could erode public confidence in forensic investigations and judicial decisions. Thus, the successful integration of AI technology in digital forensics mandates a balance between innovative technology and strict legal support and ethical duty. Transparent models of regulation, explainable AI, data protection practices and interdisciplinary collaboration are needed if AI is to be used as a trustworthy and fair mechanism to collect digital evidence and attain a sense of justice in an ever-more complicated digital landscape.

- Use of artificial intelligence for digital forensics must be governed by clear and comprehensive legal frameworks that define how the digital evidence that is obtained via these means shall be gathered, analyzed, and presented. Laws of this kind are important for a court to admit the evidence produced by AI and to be accountable if errors are made or misuse occurs.
- Investigators must be able to be aware of how and why the AI-augmented forensic tools have been created, and the AI-enhanced forensic tools should be transparent and explainable. Such transparency enables assurance of the quality of forensic evidence and allows for the inspection and challenge of AI outputs during legal proceedings.
- We must also acknowledge, regulate and eliminate biases in AI-powered forensic systems, especially when trained on historical crime data, which might be biased and/or reflect existing social or institutional biases. Independent audits and regular testing of heterogeneous training datasets in systems can safeguard the fairness of the process and possibly guard against wrongful accusation.
- Digital forensics of AI applications, in which sensitive personal data is involved, need to be implemented with strong data privacy and ethical safeguards in place. Access policies, data minimization, compliance to privacy legislation and so forth, and others are necessary to protect the individuals' rights and in the event of abuse protection have to be enforced.
- There needs to be on-going education and cross-disciplinary cooperation among human beings in digital forensics, in law enforcement, in legal systems, and in AI development, so that we will continue to educate, support, and stimulate cross-disciplinary, interdisciplinary collaboration. This allows more accurate interpretation of the results of AI outputs which complies with general principles of responsible and ethical application of AI technologies in the forensic investigation.

[13] Supra note 6 at 592.

[14] S.K. Verma, *Law and Justice in a Globalizing World* 72 (Oxford University Press, New Delhi, 1st edn., 2005).

[15] K.I. Vibhute, *Criminal Justice: A Human Rights Perspective* 301 (LexisNexis Butterworths Wadhwa, Nagpur, 1st edn., 2009).

[16] T. Ramachandran, *Cyber Crimes and Digital Evidence* 164 (Eastern Book Company, Lucknow, 1st edn., 2018).

[17] Supra note 5 at 8.

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.