

AI-Driven Digital Forensics: Revolutionizing Cybercrime Investigations and Future Trends

Nishchal Soni*

Department of Forensic Science, School of Bioengineering and Biosciences, Lovely Professional University, Punjab, India

Abstract

AI-powered digital forensics represents a transformative approach in the investigation of cybercrimes, leveraging Artificial Intelligence (AI) to enhance data analysis, efficiency, and accuracy in forensic investigations. As cyber threats have evolved in complexity and scale, traditional methods of digital forensics historically centered on data extraction from standalone devices have had to adapt to an environment characterized by smartphones, cloud storage, and sophisticated malware. This adaptation has brought AI into the forefront, facilitating the automation of tasks that were once labor-intensive and time-consuming, thus enabling forensic experts to focus on critical analysis and decision-making. The integration of AI in digital forensics has revolutionized various facets of the field, including automated log analysis, malware detection, multimedia content evaluation, and network traffic analysis. These innovations not only expedite investigations but also improve the accuracy of evidence collection and analysis by uncovering patterns that may go unnoticed in manual reviews. However, the deployment of AI also raises significant legal and ethical challenges, including concerns over user privacy, algorithmic bias, and the admissibility of AI-generated evidence in court settings. Such controversies have led to ongoing debates about the balance between technological advancement and the preservation of ethical standards in forensic practices.

Looking toward the future, the landscape of digital forensics is expected to be shaped by continued advancements in AI and automation, with projections indicating substantial market growth in forensic technologies. Innovations such as blockchain for chain of custody and nanotechnology for evidence analysis are anticipated to further enhance the efficacy of forensic investigations. As the interplay between AI capabilities and human expertise evolves, forensic professionals must remain vigilant in addressing the associated challenges, ensuring that both technological and ethical considerations are integrated into their methodologies.

Keywords: Cybercrime investigations • Legal challenges in AI forensics • Blockchain • AI digital forensics

Introduction

The field of digital forensics has undergone significant transformation, driven by rapid advancements in technology and the escalating complexity of cybercrimes. Initially, digital forensics focused primarily on the recovery and analysis of data from standalone computers, a simpler era when data was often confined to physical devices like hard drives and USB storage. These early forensic techniques involved manual data extraction from physical storage mediums and were generally straightforward, allowing investigators to focus on reconstructing events from limited data sources. The scope of digital forensics was narrower, with investigations typically centering around a single device, which was often disconnected from external networks or the internet [1,2].

However, the proliferation of digital devices and the rise of interconnected systems brought about a profound change in the landscape of digital forensics. As smartphones, tablets, cloud-based storage, and smart devices became ubiquitous, investigators were tasked with analyzing data from a variety of platforms, each with its own unique challenges. This shift meant that digital forensics had to evolve to include a much broader range of environments, moving beyond the isolated analysis of a single device to encompass cloud infrastructures, social media platforms, and encrypted communication systems. Investigators now face the task of dealing with a sheer volume of data that is often dispersed across various networks and devices, adding layers of complexity to forensic investigations [3].

Address for Correspondence: Nishchal Soni, Department of Forensic Science, School of Bioengineering and Biosciences, Lovely Professional University, Punjab, India; E-mail: nishchalresearch@gmail.com

Copyright: © 2025 Soni N. This is an open-access article distributed under the terms of the creative commons attribution license which permits unrestricted use, distribution and reproduction in any medium, provided the original author and source are credited.

Received: 27 September, 2024, Manuscript No. JFR-24-148960; **Editor assigned:** 30 September, 2024, PreQC No. JFR-24-148960 (PQ); **Reviewed:** 15 October, 2024, QC No. JFR-24-148960; **Revised:** 11 April, 2025, Manuscript No. JFR-24-148960 (R); **Published:** 18 April, 2025, DOI: 10.37421/2157-7145.2025.16.654

The need for more advanced forensic techniques became even more urgent as cyber threats grew in sophistication. Hackers began employing encryption, steganography, and advanced malware, making it harder for forensic investigators to retrieve and analyze evidence using traditional methods. For example, criminals could encrypt entire hard drives or use malware designed to erase or manipulate digital evidence, effectively bypassing many of the earlier forensic techniques. As a result, new methods had to be developed to deal with encrypted data, malware analysis, and network traffic monitoring [4].

A turning point in the evolution of digital forensics came with the integration of Artificial Intelligence (AI) technologies. The introduction of AI into digital forensic practices marked a significant shift, as these technologies allowed for the automation of tasks that were previously labor-intensive and time-consuming [5]. AI has enabled forensic investigators to analyze massive datasets efficiently, uncovering patterns, anomalies, and connections that would be nearly impossible to detect manually. The application of machine learning algorithms, for example, allows for the real-time analysis of network traffic, log files, and malware code, expediting the identification of suspicious activities and evidence [6]. Furthermore, AI-driven Natural Language Processing (NLP) has facilitated the analysis of large volumes of text-based data, such as emails, messages, and social media content, enhancing the ability to identify key individuals, relationships, and potential threats more effectively.

Historically, early forensic methodologies were largely reactive, involving post-incident data recovery and analysis. With AI, digital forensics has evolved into a more proactive discipline, allowing investigators to predict potential cyberattacks and identify vulnerabilities before they can be exploited. Machine learning models can now be trained to recognize behaviors associated with cyber threats, enabling a more predictive approach to digital forensics. This shift has significantly improved both the speed and accuracy of forensic investigations, allowing for faster detection and response to cybercrimes.

Moreover, as the digital forensics field expanded, it became essential for forensic professionals to adapt to new roles that bridge the gap between human expertise and AI capabilities. The collaboration between human investigators and AI-driven systems has become crucial in ensuring that AI tools are applied effectively while maintaining the nuanced decision-making abilities that only human experts can provide [7]. This collaboration ensures that while AI handles data processing and pattern recognition, human investigators focus on interpreting the evidence, contextualizing findings, and making critical legal and ethical decisions.

As digital forensics continues to evolve, driven by advancements in AI and other emerging technologies, the discipline is likely to become even more integral to modern investigations. The future of digital forensics will not only depend on technological innovation but also on the ability of forensic professionals to integrate these technologies within ethical and legal frameworks that protect individual rights and ensure the integrity of forensic practices. The

collaboration between human expertise and AI will remain essential, with AI taking on increasingly sophisticated roles in data analysis, while human investigators continue to provide oversight, ethical judgment, and critical analysis in complex forensic cases.

Literature Review

Current applications

AI-powered technologies have revolutionized the field of digital forensics, enabling a variety of applications that enhance both the efficiency and accuracy of investigations. As the scope of digital evidence continues to grow, with massive volumes of data now stored across cloud services, networks, and diverse digital devices, AI has become an essential tool in managing and analyzing these complex datasets. From automated log analysis to network traffic monitoring, AI-driven tools have streamlined the investigative process, allowing forensic experts to focus on interpreting and contextualizing the findings. Below are some of the key current applications of AI in digital forensics.

Automated log analysis: One of the most prominent applications of AI in digital forensics is the automation of log analysis. Logs are records of events generated by systems, applications, and devices, and analyzing these logs is crucial for detecting security incidents and cyberattacks. However, the sheer volume of log data generated by modern IT infrastructures can make manual review both time-consuming and prone to human error. AI algorithms excel in processing these large datasets, automatically identifying patterns, anomalies, and potential threats [8]. By leveraging AI, forensic teams can automate the initial phases of log analysis, allowing them to quickly detect suspicious activities, such as unauthorized access, data exfiltration, or system tampering. This capability reduces the investigative time significantly, while improving the overall accuracy of the findings.

Malware detection: AI-powered malware detection has become a vital component of digital forensics, especially as malware evolves and becomes more sophisticated. Traditional signature-based malware detection methods often fail to recognize new or obfuscated malware strains. AI, however, enables a more dynamic and adaptive approach to identifying malicious software. Machine learning algorithms are trained on vast datasets of known malware, allowing them to identify new or previously unknown malware based on behavior analysis and code similarities [9]. By continuously learning from new datasets, AI systems can detect even subtle changes in malware behavior, providing early alerts to investigators before an attack escalates. This real-time detection capability is critical in minimizing the damage caused by malware and ensuring that forensic investigations can trace the origins and impact of the threat effectively.

Image and video analysis: The analysis of digital images and videos is a core aspect of many forensic investigations, especially in criminal cases involving surveillance footage, photos, or videos. AI-driven tools

have made significant advancements in this area by enabling rapid examination and classification of multimedia content. AI algorithms can identify faces, objects, text, and other elements within images and videos, helping investigators locate crucial evidence in a fraction of the time it would take manually. Facial recognition technology, for example, can match a suspect's face across multiple sources of video footage, speeding up the identification process. Additionally, AI can analyze large video datasets for patterns or key moments, allowing investigators to prioritize their review of the most relevant segments.

Natural Language Processing (NLP): Natural Language Processing (NLP) plays a crucial role in the forensic analysis of text-based data, such as emails, chat logs, and social media communications. Investigators often need to sift through enormous volumes of digital text to find evidence, a task that would be highly impractical to perform manually. AI-based NLP tools can automatically categorize and classify text data based on relevance, sentiment, and keyword analysis, making it easier for investigators to focus on critical information. NLP also enables the detection of relationships between individuals, uncovering communication patterns and connections that might otherwise go unnoticed. This technology has proven particularly useful in cases involving fraud, harassment, and organized crime, where large amounts of text-based evidence are involved.

Network traffic analysis: Monitoring and analyzing network traffic is another area where AI has made a profound impact in digital forensics. Cyberattacks often involve unusual patterns of network activity, such as spikes in data transmission, unusual access times, or unauthorized data movement. AI algorithms can be trained to automatically detect deviations from normal traffic patterns, flagging suspicious activity for further investigation [9]. This real-time network traffic analysis allows forensic teams to respond quickly to potential breaches, limiting damage and gathering evidence that is crucial for tracing the source of an attack. Additionally, AI-driven systems can correlate network events with known attack patterns, providing investigators with valuable insights into the methods and tools used by cybercriminals.

Forensic triage: Forensic triage is the process of identifying the most relevant evidence early in an investigation to prioritize resources and actions effectively. In digital forensics, where the volume of data can be overwhelming, AI technologies have become indispensable for speeding up this process. AI systems can analyze metadata and content attributes to flag files or data that are likely to be of high relevance to the investigation. By automating this initial assessment, forensic teams can focus their efforts on the most critical evidence, improving both the speed and accuracy of investigations. This application of AI is particularly beneficial in time-sensitive cases, where quick decisions can have a significant impact on the outcome of the investigation [10].

Discussion

Benefits of AI in digital forensics

The integration of AI into digital forensics offers several notable advantages, significantly enhancing data analysis, investigation efficiency, and overall investigative outcomes. By automating labor-intensive processes, AI minimizes human error, expedites forensic procedures, and provides investigative teams with insights that would be difficult or impossible to obtain manually. Below are the key benefits of AI in digital forensics.

Enhanced data analysis: AI technologies, including Machine Learning (ML) and Natural Language Processing (NLP), have revolutionized the way forensic experts handle vast amounts of digital evidence. These tools enable the swift and accurate analysis of large datasets, helping forensic professionals identify patterns, anomalies, and correlations that may indicate criminal activities, fraud, or breaches [11,12]. AI-powered systems can perform complex data analytics at a scale and speed beyond human capability, leading to more efficient investigations. For example, AI can reconstruct digital timelines, detect hidden relationships between individuals or data points, and piece together fragmented evidence into coherent narratives. This comprehensive approach provides investigators with a more complete understanding of events, which can be crucial in cases involving multiple suspects, intricate digital infrastructures, or extensive data sets.

Additionally, AI presents findings in formats that are easily comprehensible to non-experts, such as juries or judges, enhancing the credibility and persuasive power of forensic evidence in court. By transforming raw data into clear, concise, and reliable reports, AI tools help bridge the gap between complex technical evidence and legal decision-making processes [13]. This not only makes forensic evidence more accessible but also strengthens its role in judicial proceedings.

Efficiency in investigations: AI-powered tools significantly improve the efficiency of digital forensic investigations by automating routine and time-consuming tasks. Investigators often face overwhelming volumes of data, which must be processed, analyzed, and interpreted within tight deadlines. AI tools can automate processes such as evidence collection, data filtering, and the identification of suspicious content, which drastically reduces the time spent on manual reviews. For instance, AI can rapidly scan through logs, emails, images, and network traffic to highlight areas of concern, enabling investigators to focus on the most relevant information without sifting through mountains of extraneous data. This increased efficiency accelerates the investigative process, allowing teams to resolve cases faster while maintaining accuracy.

Furthermore, AI's ability to predict potential future threats or behaviors through predictive analytics enhances the proactive elements of digital forensics. By analyzing historical data patterns and current activity, AI systems can anticipate cyberattacks, helping organizations to implement preventive measures before incidents escalate [14]. This forward-looking capability not only aids in solving crimes but also contributes to preventing future breaches and improving overall security measures.

Addressing bias and enhancing fairness: While concerns over biases in AI algorithms are valid, AI technologies are continually evolving to address and minimize these issues. Developers of AI forensic tools are working to ensure that their models are fair, accurate, and inclusive by training them on diverse datasets and performing regular updates based on new data [12,7]. This ongoing refinement helps to mitigate the risk of algorithmic bias affecting forensic outcomes.

Efforts to enhance transparency and accountability in AI systems are also key to improving fairness. By developing AI models that explain their decision-making processes in understandable terms, forensic teams can verify and validate the outputs produced by these tools, reducing the likelihood of unjust outcomes. As AI tools become more transparent and interpretable, they will be better equipped to complement the work of human investigators without introducing undue biases into forensic investigations.

Collaboration between human investigators and AI: AI technologies are designed to augment, rather than replace, human investigators. In digital forensics, the most effective outcomes are achieved through a collaborative approach that combines AI's ability to process massive datasets quickly and accurately with the nuanced judgment and intuition of human experts. AI excels at detecting patterns, relationships, and anomalies that might go unnoticed by human investigators, especially in large and complex datasets [15]. However, human expertise remains essential for interpreting the context and significance of the data, making informed decisions, and applying ethical and legal standards to the investigation.

This collaborative model enhances decision-making, as AI tools can provide investigators with detailed insights while allowing them to focus on the strategic elements of a case. By handling the heavy lifting in terms of data analysis, AI frees up human investigators to apply their specialized knowledge, creativity, and critical thinking skills, ultimately leading to more comprehensive and effective forensic strategies [16].

Psychological relief for investigators: One of the more significant, yet often overlooked, advantages of AI in digital forensics is its ability to alleviate the psychological burden on investigators, especially when dealing with graphic or disturbing content. Forensic investigators often have to review explicit or traumatic material, such as images and videos related to violent crimes, exploitation, or accidents. The repeated exposure to such content can lead to psychological distress, trauma, or burnout.

AI-powered systems can automatically identify and flag graphic materials, allowing investigators to limit their direct exposure to harmful content. By automating the review and classification of these materials,

AI reduces the emotional strain on human investigators, improving their mental health and well-being. This not only helps forensic professionals maintain their focus and productivity but also enhances the overall efficiency of investigations, as investigators can concentrate on the more complex aspects of the case without the added emotional toll.

Through its diverse applications, AI continues to transform the field of digital forensics, bringing enhanced accuracy, efficiency, fairness, and psychological relief to investigative processes.

Conclusion

AI-driven digital forensics is revolutionizing the landscape of cybercrime investigations by significantly enhancing the speed, accuracy, and scope of forensic analysis. By leveraging machine learning, pattern recognition, and automated data processing, investigators can rapidly sift through massive volumes of digital evidence to uncover hidden connections and malicious activity. This technological advancement not only streamlines case resolution but also strengthens legal proceedings with more reliable and timely insights. As cyber threats become increasingly sophisticated, AI will continue to evolve, enabling proactive threat detection, predictive analytics, and adaptive forensic techniques. However, this evolution also demands ethical considerations, transparency, and collaboration between technologists, law enforcement, and policymakers. Looking forward, the integration of AI with blockchain, quantum computing, and real-time analytics holds the potential to redefine digital forensics entirely. Ultimately, AI stands as a powerful ally in the fight against cybercrime, reshaping the future of digital investigations with unprecedented capabilities.

Limitations

While the integration of AI in digital forensics offers numerous benefits, it also presents significant challenges and limitations that must be carefully addressed. These concerns encompass legal and ethical issues, the inherent limitations of AI frameworks, algorithmic bias, and the need to balance ethical principles in forensic practices.

Legal and ethical issues

The application of AI in digital forensics raises substantial legal and ethical challenges. Participants in a recent survey identified user privacy and data protection as paramount concerns within the forensic community. The unregulated use of non-accredited tools in court settings poses risks to the admissibility of evidence, as these tools may compromise the integrity of the evidence collected. The potential for misuse of AI tools for excessive data retrieval is another pressing ethical dilemma, especially when such practices may involve sensitive information unrelated to the case at hand.

Moreover, the implementation of AI technologies often necessitates access to vast amounts of personal data, which can infringe on individual privacy rights. Ensuring compliance with existing data protection regulations, such as the General Data Protection Regulation

(GDPR) in Europe, is crucial to maintaining ethical standards in digital investigations. However, the realities of digital investigations frequently lead to the acquisition of more data than is strictly necessary, complicating adherence to these legal standards.

Data minimization and permissions

A critical legal issue highlighted by experts is the lack of permissions for storing information related to investigations. Many forensic experts argue that the ability to store data securely, with proper oversight, could enhance investigative outcomes by providing necessary context for analysis. However, the principle of data minimization mandated by regulations like the GDPR requires that only essential data be collected for specific purposes. In practice, digital investigations often involve acquiring excessive data, which can lead to challenges in compliance and raise ethical questions about the scope of investigations.

Limitations of AI frameworks

The design of AI frameworks in digital forensics is intended to assist human investigators, rather than replace them. While AI tools can significantly enhance investigative efficiency and accuracy, their rapid evolution often outpaces the development of accompanying ethical and legal frameworks. This creates a challenging landscape for practitioners, who must adapt their methodologies to remain compliant with evolving legal standards and ethical expectations. Acknowledging these limitations, ongoing feedback and evaluation of AI tools are crucial for identifying potential failures and improving the robustness of the systems employed [8].

Algorithmic bias and transparency

Another significant concern is the potential for algorithmic bias, which can adversely affect the reliability of forensic outcomes. The perception that AI algorithms are infallible can lead to misplaced trust in their decisions; however, inherent biases in algorithm design can distort results and affect the integrity of forensic investigations. The challenge of maintaining transparency in AI systems, particularly those characterized as "black boxes," complicates the understanding of how decisions are made, thus impacting accountability in forensic processes. Transparency is essential for validating the efficacy and fairness of AI systems, as well as for addressing public concerns regarding the trustworthiness of AI-generated evidence.

Balancing ethical principles

To navigate these challenges, various ethical frameworks have been proposed that prioritize human dignity and respect for individuals' rights. Key principles such as beneficence, nonmaleficence, and justice are essential in guiding the ethical application of AI in digital forensics. However, the application of these principles can become complicated when different ethical codes conflict. For instance, the pursuit of justice in a digital investigation may require intrusive data collection methods that conflict with the principle of nonmaleficence, which aims to avoid causing harm.

Careful examination of the ethical implications of forensic practices is necessary to ensure that the deployment of AI technologies does not undermine individual rights or public trust in the forensic process. Striking the right balance between leveraging AI for investigative efficiency and maintaining ethical standards is a critical challenge for the future of digital forensics. As the field continues to evolve, ongoing dialogue among stakeholders, including technologists, legal experts, and ethicists, will be essential in addressing these multifaceted challenges.

Future trends

The landscape of digital forensics is undergoing a transformative shift, fueled by advancements in technology, particularly in Artificial Intelligence (AI) and automation. As the complexity and volume of cybercrimes continue to escalate, the demand for innovative forensic solutions will drive significant changes in the field. Several key trends are expected to shape the future of digital forensics.

Technological advancements in digital forensics: The global market for forensics technology is projected to reach \$42.1 billion by 2027, with a Compound Annual Growth Rate (CAGR) of 15%. This rapid growth is largely driven by rising crime rates and an increasing recognition of the importance of forensic evidence in criminal investigations. As organizations seek to improve their investigative capabilities, investment in advanced technologies will be crucial for keeping pace with evolving threats.

AI and automation: AI is emerging as a pivotal force in revolutionizing forensic investigations. Its capabilities enable the automation of various processes, from evidence collection to analysis, resulting in improved accuracy and efficiency. AI-powered tools can assist forensic professionals in managing the vast amounts of data generated in modern investigations, helping to identify relevant evidence quickly and accurately. The introduction of advanced AI tools, such as ChatGPT, illustrates how AI can augment forensic practices, suggesting applications even in niche fields such as digital forensics.

Automated systems will facilitate a more efficient workflow for investigators, allowing for quicker turnaround times and more accurate results. The adaptability of AI algorithms ensures that forensic approaches remain relevant amidst the evolving challenges posed by modern digital evidence, including cloud storage and encrypted communications. As these technologies continue to develop, the role of human investigators will shift, focusing more on strategy and interpretation while AI handles data analysis and pattern recognition.

Nanotechnology and advanced analysis: Another emerging trend in digital forensics is the incorporation of nanotechnology, which enhances the sensitivity of analytical methods. This technology will enable forensic professionals to detect and analyze minute traces of evidence, such as DNA or gunshot residue, which may be critical in solving cases. As analytical techniques continue to evolve, forensic

professionals will be better equipped to uncover vital evidence that may have previously gone unnoticed.

Blockchain and chain of custody: The adoption of blockchain technology in digital forensics is gaining traction, particularly for managing the chain of custody, which is crucial for maintaining the integrity of digital evidence. Blockchain offers a secure and immutable way to document the handling of evidence, ensuring that it remains untampered and easily traceable. By employing distributed ledgers, forensic investigators can enhance the reliability of the evidence collected, addressing challenges related to data manipulation and authenticity.

Multidisciplinary approach: Modern digital forensics is increasingly recognized as a multidisciplinary endeavor, integrating expertise from various fields, including law, computer science, and data mining. This collaborative approach is essential for addressing the complex challenges posed by contemporary cybercrime. Forensic professionals will need to continuously evolve their methodologies, drawing on knowledge from different disciplines to tackle emerging threats effectively.

Continuous innovation and preparedness: As the digital landscape becomes more intricate, the need for continuous innovation in forensic techniques is paramount. Organizations like Eclipse Forensics emphasize the importance of research and development in staying ahead of technological advancements. Preparedness and adaptability will be crucial for forensic professionals to effectively tackle the evolving challenges in digital investigations. Ongoing training, skill development, and collaboration between technologists and investigators will ensure that the forensic community remains at the forefront of technological advancements while upholding ethical standards and legal compliance.

In summary, the future of digital forensics will be shaped by technological advancements, the integration of AI and automation, the adoption of new analytical methods, and a multidisciplinary approach to investigations. As the field continues to evolve, forensic professionals must remain vigilant and proactive in adapting their practices to meet the challenges posed by an increasingly complex digital environment.

References

1. Ec-Council. "The Future of Digital Forensics: Trends and Emerging technologies." Cybersecurity Exchange. (2023).
2. Jobya. "Emerging Trends in Digital Forensics: Staying ahead in 2023." Jobya. (2024).
3. Vcl S. "Exploring Digital Forensics: A Global Perspective 2023." Virtual Cyber Labs. (2023).
4. Kadage, Anushka Deepak, Banoth Meghya Nayak, Vishal Sharad Hingmire, and Kirti Wanjale, et al. "AI-Enhanced Digital Forensics: Automated Techniques for Efficient Investigation and Evidence Collection." *J Electr Syst* 20 (2024): 211-229.
5. Simplyforensic, Simplyforensic. "The Intersection of Digital Forensics and Artificial intelligence (AI)-SimplyForensic." Simplyforensic. (2024).
6. Forensics P, Forensics P. "Mobile Forensics and AI: Impact on digital Investigations | Powerhouse Forensics." Powerhouse Forensics. (2023).
7. Angadi S. "6 Ways AI Can Revolutionize Digital Forensics." (2023).
8. Froklage P. "Digital Forensics Tools: The Ultimate Guide (2024)." Magnet Forensics. (2024).
9. Behl H. "From Sci-Fi to Crime-Solving: How AI is Transforming Digital Forensics for Law Enforcement." Lexology. (2024).
10. EclipseForensics. "How will AI transform digital forensics in 2023 and beyond?." Eclipse Forensics. (2024).
11. Maratsi, Maria Ioanna, Oliver Popov, Charalampos Alexopoulos, and Yannis Charalabidis. "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): 32-40.
12. Lowden O. "The Technology Trends Shaping the Future of Forensics." (2023).
13. Miller C. "Unraveling Digital Mysteries: How AI Copilots Can Revolutionize Digital Forensic Investigations*." DFRWS. (2023).
14. EclipseForensics. "Artificial intelligence in Digital Forensics: Leveraging AI for investigations." Eclipse Forensics. (2023).
15. Adel, Amr, Ali Ahsan, and Claire Davison. "ETHICore: Ethical Compliance and Oversight Framework for Digital Forensic Readiness." *Information* 15 (2024): 363.
16. Kelly L, Sachan S, Ni L, and Almaghrabi F, et al. "Explainable Artificial intelligence for Digital Forensics: Opportunities, challenges and a drug testing case study." In: IntechOpen eBooks. (2020).

How to cite this article: Soni, Nishchal. "AI-Driven Digital Forensics: Revolutionizing Cybercrime Investigations and Future Trends." *J Forensic Res* 16 (2025): 654.