iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71562

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Digital Forensic: Techniques, Challenges, and Future Direction

Abdul Sallam Said Hamed[1], Dr. Omprakash Dewangan[2]
Kalinga University, Naya Raipur, India

Abstract: ***Digital forensics is now a crucial field of study in cybersecurity and criminal investigation, which helps identify, analyze, and preserve digital evidence. This systematic literature review discusses the current techniques, challenges, and future directions of research in digital forensics. Contemporary forensic techniques include disk forensics, network forensics, memory forensics, and cloud forensics, with the help of artificial intelligence (AI) and machine learning (ML) to improve evidence identification and analysis. Yet, digital forensics is confronted by various challenges, such as the quick development of technology, encryption intricacies, anti-forensic methods, and the volatility of digital data. Growing reliance on cloud computing, Internet of Things (IoT) devices, and encrypted communication channels only makes forensic examinations more challenging. Also, issues of legal and ethical considerations, like jurisdictional disputes and privacy, hinder the efficacy of forensic procedures. Future research will have to address the development of sophisticated automation methods, trans-border legal instruments, and AI-based forensic software for processing massive amounts of data. Blockchain-based technology for maintaining evidence integrity and normalized forensic processes in jurisdictions can further improve investigation effectiveness. The findings of this study emphasize the imperative of ongoing innovation and convergence among academia, law enforcement agencies, and technology providers to solve evolving digital forensic challenges.***
Keyword: Digital Forensics, Cyber Security, Cyber Crime, Tools, Investigations

I. INTRODUCTION

Digital forensics is a fast-growing discipline that is vital to contemporary cybersecurity, criminal investigations, and litigation. It is the process of identifying, acquiring, preserving, analyzing, and presenting digital evidence to aid investigative activities (Casey, 2011). The use of digital devices, cloud computing, and encrypted communications has increased the complexity and difficulty of digital forensic investigations (Garfinkel, 2010). When more cybercrimes are committed, law enforcement services and forensic scientists need to counter new technologies with innovative forensic science methods to mitigate advanced cybercrime (Baryamureeba & Tushabe, 2004). There is a need for a systematic review of digital forensic methods to grasp the state of the art in the field, determine the major challenges, and consider future research avenues. Forensic methods that are currently in use are disk forensics, network forensics, memory forensics, and mobile forensics, with each dealing with various aspects of digital evidence gathering and analysis (Rogers et al., 2006). Nevertheless, the growing employment of anti-forensic tools, including data encryption and obfuscation, poses great challenges to forensic examinations (Harris, 2006). Legal and ethical issues, including data privacy and jurisdictional disputes across borders, further complicate digital forensic processes (Kenneally & Brown, 2005). Our study aims to provide a comprehensive overview of digital forensic techniques, highlight major challenges, and propose future research directions. By synthesizing findings from existing studies, this review seeks to contribute to the development of more effective forensic methodologies and enhance the reliability of digital evidence in legal proceedings. The review follows a structured methodology, including the identification and selection of relevant studies, analysis of forensic techniques, and assessment of challenges and emerging trends in the field.

A. Research Questions

The study aims to address the following key research questions (RQs):

- RQ1: What are the most common digital forensic techniques currently in use?
- RQ2: What are the major challenges faced in digital forensic investigations?
- RQ3: What are the emerging trends and future research directions in digital forensics?

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

II. RELATED WORK

Digital forensics is a critical discipline in cybersecurity that facilitates the identification, collection, and analysis of digital evidence for legal and investigative use. A number of studies have investigated various forensic approaches, challenges, and directions for future research.

A. Digital Forensic Techniques

Traditional forensic techniques focus on data acquisition, disk imaging, and artifact analysis from digital storage devices (Casey, 2011). These techniques have evolved with the increasing adoption of cloud computing, mobile devices, and the Internet of Things (IoT). Mobile forensics has gained prominence due to the widespread use of smartphones, leading to new methodologies such as cloud-based forensic analysis and real-time evidence extraction (Sohal et al., 2021). Similarly, network forensics analyzes packet captures, logs, and encrypted traffic to detect cyber threats and digital crimes (Kaur & Singh, 2022). Advanced forensic techniques now incorporate artificial intelligence (AI) and machine learning (ML) for automated analysis and anomaly detection (Alazab et al., 2020).

B. Challenges in Digital Forensics

Several challenges hinder effective forensic investigations. The increasing use of anti-forensic techniques, such as encryption, steganography, and obfuscation, complicates evidence acquisition (Harris, 2006). Cloud computing introduces jurisdictional and legal challenges, as forensic analysts may struggle to access cross-border data stored in third-party servers (Zawoad & Hasan, 2015). Additionally, the sheer volume of digital evidence poses storage and processing challenges, necessitating the development of scalable forensic tools (Lillis et al., 2016). Forensic readiness, which ensures organizations are prepared to conduct investigations, remains a significant concern in corporate and law enforcement settings (Valjarevic & Venter, 2015).

C. Future Research Directions

The future of digital forensics lies in the adoption of AI-driven forensic analysis, blockchain for evidence integrity, and enhanced forensic automation (Quick & Choo, 2018). The use of AI and ML for automated malware classification and behavioral analysis can improve forensic efficiency (Alazab et al., 2020). Blockchain technology has the potential to ensure data integrity and secure the chain of custody in forensic investigations (Agarwal et al., 2021). Additionally, standardization of forensic methodologies and cross-border legal frameworks is necessary to improve forensic collaboration at a global scale (Baryamureeba & Tushabe, 2004). Emerging areas, such as quantum computing and deepfake forensics, require further research to address new threats posed by advancing technologies (Mohanty et al., 2020).

III. METHODOLOGY

This research employs a systematic literature review (SLR) method for the identification, evaluation, and synthesis of past research on digital forensic methods, issues, and future trends. The method uses the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Moher et al., 2009) for transparency and reproducibility. The four-phase review process is identification, screening, eligibility, and inclusion.

A. Data Sources and Search Strategy

A thorough search was done in various academic databases, such as IEEE Xplore, SpringerLink, ACM Digital Library, ScienceDirect (Elsevier), and Google Scholar to provide extensive coverage of the relevant literature. Keywords used in the search queries were "digital forensics," "forensic challenges," "cybercrime investigation," "forensic automation," "blockchain in forensics," and "AI for forensic analysis." Boolean operators (AND, OR) were employed to narrow down the results to include studies pertaining to forensic methodologies, new technologies, and challenges. Search results were filtered to encompass peer-reviewed journal articles, conference papers, and book chapters between 2010 and 2024 to ensure relevance.

B. Inclusion and Exclusion Criteria

1) Inclusion Criteria

- Peer-reviewed journal articles, conference papers, and book chapters.
- Studies published between 2010 and 2024 to ensure up-to-date findings.
- Papers discussing digital forensic techniques, challenges, and future trends.

2) Exclusion Criteria

- Non-English papers due to translation limitations.
- Studies unrelated to digital forensics (e.g., general cybersecurity research).
- Duplicate studies across different databases.

C. Data Extraction and Synthesis

Relevant studies were examined in order to obtain primary findings associated with forensic techniques, challenges, and future research directions. Data extraction was concentrated on the identification of conventional and contemporary forensic approaches, technical and legal hurdles, and upcoming trends like AI and blockchain in forensics. Thematic synthesis was employed in order to sort findings into the most important themes, enabling structured analysis. Patterns and trends among the chosen studies were contrasted to determine areas of gaps and areas for research. Studies were also examined in terms of methodological rigor and relevance to include only high-quality research.

IV. RESULTS AND DISCUSSION

A. Results

The systematic review revealed a number of important digital forensic methods, issues, and new trends in forensic investigations. Conventional techniques like disk imaging and live memory analysis are still common (Casey, 2011). Nevertheless, with the rise in encrypted communication and cloud storage, forensic investigators have embraced more sophisticated methods, such as volatile memory extraction and remote forensic analysis (Zawoad & Hasan, 2015). Artificial intelligence (AI)-based forensic software has also become well-known, which can automatically extract evidence and identify anomalies (Alazab et al., 2020).

Digital forensic analysis encounters various challenges like anti-forensic measures, legal and jurisdictional problems, and high-volume data. Anti-forensic activities like encryption, data concealing, and steganography complicate the process of collecting evidence (Harris, 2006). Legal impediments, especially cross-border cloud forensics, are challenges based on uneven global legislation (Quick & Choo, 2018). Also, the growing amount of digital evidence has developed a requirement for scalable forensic solutions that can manage large volumes of data effectively (Lillis et al., 2016).

The review emphasizes AI and machine learning, blockchain, and forensic automation as critical research areas of the future. AI-powered forensic models are improving malware detection, data classification, and anomaly identification, enhancing investigation effectiveness (Alazab et al., 2020). Blockchain technology is proving to be a promising solution for guaranteeing data integrity, chain of custody, and tamper-proof evidence management (Agarwal et al., 2021). In addition, there should be standardized forensic models to resolve legal disparities and facilitate effective international cooperation (Valjarevic & Venter, 2015). Table 1 summarized the key findings.

Category	Findings	References
Forensic Technique	Disk forensics, memory forensics, network forensics, mobile forensics, cloud forensics, AI-powered forensic tools	Casey (2011), Zawoad & Hasan (2015), Alazab et al. (2020)
Challenges	Anti-forensic techniques (encryption, data hiding), legal and jurisdictional issues, large-scale data processing	Harris (2006), Quick & Choo (2018), Lillis et al. (2016)
Emerging Trends	AI and machine learning, blockchain for forensic integrity, forensic automation, standardization efforts	Alazab et al. (2020), Agarwal et al. (2021), Valjarevic & Venter (2015)

Table 1: Summary the key findings

B. Discussion

The results show a shift from conventional forensic practices to more sophisticated, AI-based solutions. Although AI and machine learning have enhanced forensic investigations, there are still legal hurdles, privacy issues, and forensic preparedness. There is a need for cooperation between law enforcement agencies, policymakers, and researchers in addressing jurisdictional and technological issues. In addition, as digital crime techniques evolve, forensic practices must be regularly upgraded to stay effective.

Another key area that needs to be addressed is the creation of standardized forensic frameworks. The absence of global guidelines makes investigations inefficient, particularly in cross-border cybercrimes. Blockchain technology has been suggested as a means of providing forensic evidence integrity; however, its use is not widespread because it is challenging to implement (Agarwal et al., 2021).

The research also emphasizes the need for investigation into new threats like deepfake forensics, Internet of Things (IoT) investigations, and quantum computing threats (Mohanty et al., 2020). Resolving these problems will be crucial in maintaining the future efficacy and dependability of digital forensic investigations.

V. CONCLUSION AND FUTURE WORK

This systematic review of literature discussed digital forensic methods, issues, and future trends through examination of research already conducted in this area. The research categorized numerous forensic techniques, such as disk forensics, memory forensics, network forensics, mobile forensics, and cloud forensics, and noted the shift towards AI-based tools for extracting evidence and detecting anomalies. Although these advances increase forensic potential, digital forensics still confronts numerous challenges, including anti-forensic measures, high-volume data processing, and jurisdictional and legal issues. The review also highlighted new trends such as blockchain for forensic integrity, forensic automation, and the requirement of standardized frameworks to facilitate international cooperation in cybercrime investigations.

In spite of the technological progress, digital forensics is still a developing field that needs constant adjustments to meet the new cyber threats. The growing application of encryption, cloud storage, and decentralized systems calls for stronger forensic tools. Legal and ethical aspects, particularly in cross-border investigations, are also major challenges that need international cooperation and harmonized policies.

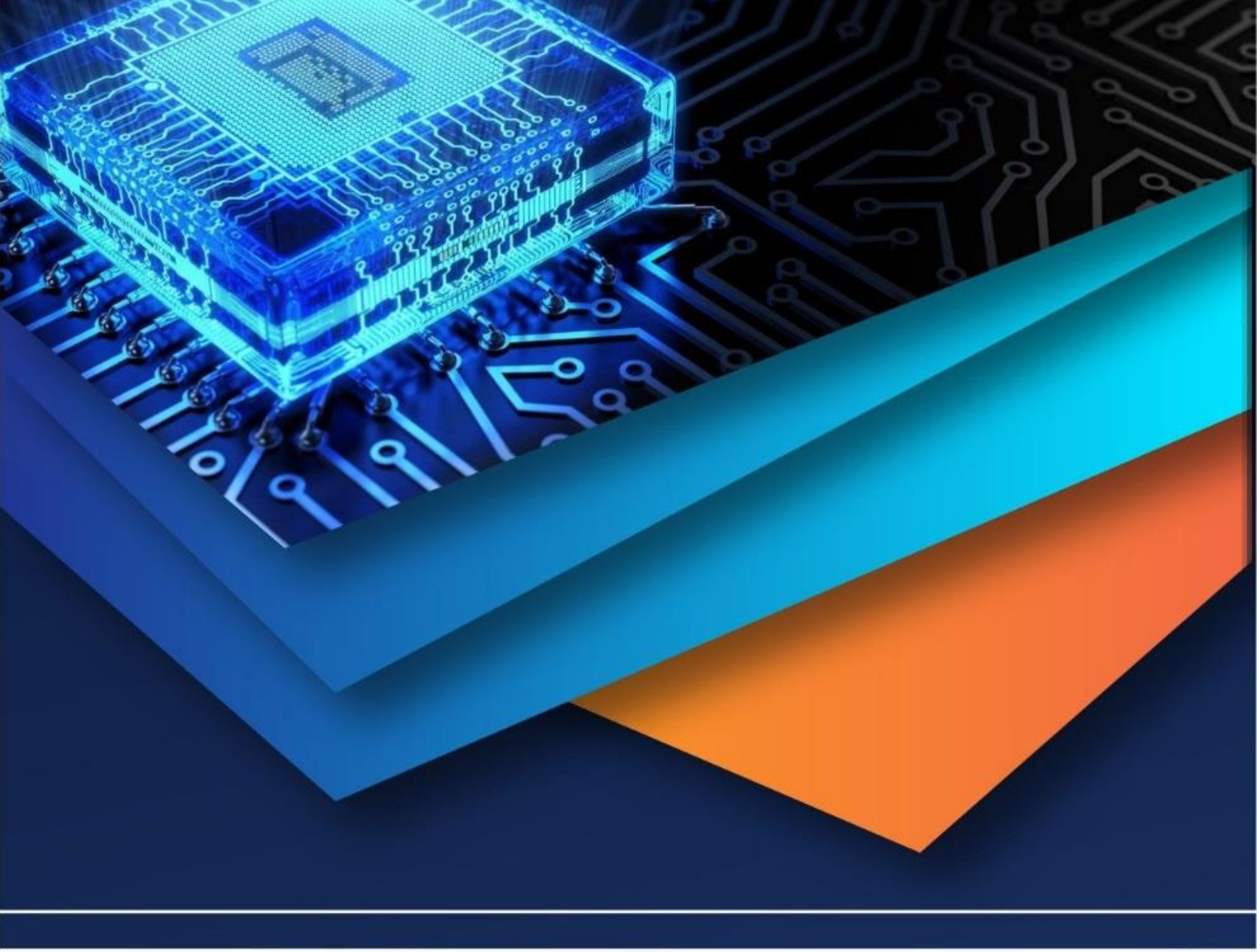
A. Future work

Future studies on digital forensics should revolve around strengthening AI and machine learning models to support forensic examination, providing enhanced accuracy, explainability, and flexibility in confronting new cyber-attacks. The utilization of blockchain technology for integrity preservation and tamper-proof data storage needs to be explored further for the creation of practical applications. Moreover, the emergence of deepfake media and AI-based forgeries requires innovation in multimedia forensics to enhance detection and authentication methods. With the proliferation of IoT devices and cloud infrastructures, new forensic approaches need to be formulated to effectively deal with distributed, encrypted, and ephemeral data. In addition, forensic preparedness and legal frameworks need to be regularly revised to comply with global regulations and changing cyber laws. Enhancing interdisciplinarity among digital forensic specialists, policymakers, and technology researchers will be essential in overcoming these challenges and developing better digital forensic practice.

REFERENCES

[1] Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. Digital Investigation, 1(1), 1-11.
[2] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press.
[3] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7, S64-S73.
[4] Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. Digital Investigation, 3(1), 44-49.
[5] Kenneally, E., & Brown, C. L. (2005). Risk-sensitive digital evidence collection. Digital Investigation, 2(2), 101-119.
[6] Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. Journal of Digital Forensics, Security and Law, 1(2), 19-38.
[7] Agarwal, S., Rajan, R., & Ahmed, M. (2021). Blockchain technology in digital forensics: Challenges and opportunities. Forensic Science International: Digital Investigation, 37, 301-312.
[8] Alazab, M., Tang, M., & Venkatraman, S. (2020). Machine learning for digital forensics: Techniques and applications. Future Generation Computer Systems, 107, 278-288.
[9] Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. Digital Investigation, 1(1), 1-11.
[10] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press.
[11] Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. Digital Investigation, 3(1), 44-49.
[12] Kaur, H., & Singh, K. (2022). Network forensic techniques: A review of methods and challenges. Journal of Cybersecurity and Privacy, 2(1), 45-62.

[13] Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas in digital forensics. The Computer Journal, 61(1), 298-308.
[14] Mohanty, S. P., Choppali, U., & Kougianos, E. (2020). Deep learning for digital forensics: Challenges and future directions. IEEE Consumer Electronics Magazine, 9(3), 33-41.
[15] Quick, D., & Choo, K. K. R. (2018). Digital forensic intelligence: Data subsets and Open Source Intelligence (OSINT) analysis. Future Generation Computer Systems, 78, 558-567.
[16] Sohal, S., Sandhu, R., & Kaur, P. (2021). Mobile forensics: A review of forensic methodologies, challenges, and tools. Journal of Digital Forensics, Security and Law, 16(2), 72-95.
[17] Valjarevic, A., & Venter, H. S. (2015). Implementation guidelines for a digital forensic readiness capability. Computers & Security, 53, 65-78.
[18] Zawoad, S., & Hasan, R. (2015). Digital forensics in the cloud: State-of-the-art and future directions. Journal of Network and Computer Applications, 66, 214-232.
[19] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.
[20] CASP. (2018). Critical Appraisal Skills Programme (CASP) Checklists. Retrieved from https://casp-uk.net.
[21] Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & The PRISMA Group. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Medicine, 6(7), e1000097.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY