Commentary
Volume 10:05, 2025

Journal of Forensic Medicine

ISSN: 2472-1026

Open Access

Digital Forensics: Modern Challenges Across Technologies

Rachel T. Nguyen*

Department of Forensic and Biomedical Sciences Coastal State University School of Medicine, USA

Introduction

The field of digital forensics is continually expanding, adapting to the rapid evolution of technology and the new challenges it presents. Modern investigations demand innovative approaches to ensure evidence integrity, address emerging threats, and navigate complex digital environments. This body of work surveys recent advancements and identifies key areas of focus within this critical domain.

One significant area of exploration is how blockchain technology can fundamentally reshape digital forensics [1].

It delves into the immutability, transparency, and decentralization properties of blockchain, showing how these attributes can enhance the integrity of evidence collection, storage, and chain of custody, effectively preventing tampering and ensuring auditability in digital investigations. The core idea here is to leverage a distributed ledger to create an unalterable record of forensic data, which is crucial for legal admissibility and trust.

Another pressing concern in today's digital landscape is the rise of deepfakes. This survey addresses the significant challenge deepfakes pose to digital forensics [2].

It explores current techniques for deepfake detection, ranging from visual artifacts to metadata analysis and Artificial Intelligence-based methods, while highlighting the evolving arms race between deepfake generation and detection, and the urgent need for robust forensic methodologies. The dynamic nature of deepfake creation means detection methods must constantly evolve to keep pace.

The Internet of Things (IoT) environment also brings unique complexities to digital forensics. One review systematically examines these challenges and approaches, identifying issues like heterogeneous devices, volatile data, and proprietary operating systems [3].

This research proposes a comprehensive overview of existing forensic frameworks and tools, pointing to future research directions for effective IoT investigations. Complementing this, other work provides a concise overview of the unique challenges and existing solutions in conducting digital forensics for IoT devices, emphasizing difficulties in data extraction and analysis from diverse and resource-constrained devices, and outlining essential steps for building effective IoT forensic capabilities [9].

Furthermore, a specific digital forensic process model tailored to the complexities of the IoT environment details a structured methodology for handling evidence from a multitude of IoT devices, integrating phases from identification and preservation to analysis and presentation, providing a clear roadmap for investigators in this challenging domain [10].

As distributed computing models become more prevalent, new forensic frontiers emerge. This paper explores the nascent field of forensics within federated learning (FL) [4].

It highlights the unique challenges in investigating data breaches, model poisoning, and privacy violations in distributed FL systems, while also identifying opportunities to integrate forensic readiness into FL architectures for enhanced accountability and security. Understanding how to conduct investigations in these decentralized machine learning environments is crucial.

Cloud computing environments also introduce significant complexities for digital forensics. Research proposes a specific cyber forensics model tailored for cloud computing environments, addressing the complexities introduced by virtualization, distributed storage, and multi-tenancy [5].

It outlines systematic steps for evidence acquisition, preservation, analysis, and reporting in the cloud, aiming to overcome traditional forensic limitations in highly dynamic cloud infrastructures. Building on this, a comprehensive study reviews various digital forensics process models specifically designed for cloud computing [6].

It dissects their methodologies, strengths, and weaknesses, providing insights into how each model handles the unique challenges of cloud investigations, from data volatility to jurisdictional issues, ultimately guiding practitioners in model selection.

The integration of Artificial Intelligence (AI) techniques into digital forensics is systematically explored [7].

This review categorizes and analyzes how AI is being used for automating tasks like data analysis, anomaly detection, and pattern recognition, aiming to improve efficiency and accuracy in complex forensic investigations, while also noting challenges related to explainability and bias. AI holds promise for sifting through vast amounts of data, but its application requires careful consideration. Finally, a survey provides an exhaustive overview of forensic analysis techniques applicable to mobile devices [8].

It covers various operating systems, data acquisition methods (physical, logical, filesystem), and tools used to extract and analyze digital evidence from smartphones and tablets, addressing the evolving security measures and data fragmentation challenges inherent in mobile forensics. These collective insights underscore the multi-faceted nature of modern digital forensics and the continuous need for research and development to keep pace with technological advancements.

Description

The comprehensive landscape of digital forensics today is characterized by its continuous adaptation to technological advancements and the inherent complexities these bring. Understanding the methodologies, challenges, and proposed solutions across various domains is key to effective digital investigations. Several studies highlight the transformative potential of emerging technologies and the persistent difficulties in traditional areas.

Blockchain technology, for example, offers a paradigm shift in how digital evidence is managed [1]. The inherent immutability and transparency of blockchain ensure that once evidence is recorded, it cannot be tampered with without detection. This decentralization aspect significantly enhances the chain of custody, providing an auditable and trustworthy record essential for legal proceedings. Such a framework could drastically reduce disputes over evidence integrity, a common challenge in digital investigations. By leveraging distributed ledger technology, forensic practitioners can establish a higher standard of evidence reliability, moving beyond centralized systems that may be vulnerable to single points of failure or manipulation.

The proliferation of deepfake technology introduces a formidable adversary for digital forensics. Research underscores the critical challenge deepfakes pose, exploring a range of detection techniques from subtle visual artifacts to complex metadata analysis and advanced Artificial Intelligence-based methodologies [2]. This field is an ongoing arms race, where new deepfake generation techniques necessitate equally sophisticated detection methods. The focus is on developing robust forensic tools that can discern authentic media from synthetically generated content, a task made increasingly difficult by the growing realism of deepfakes. Investigators must not only identify fabricated content but also trace its origins and methods of creation, adding layers of complexity to forensic analysis.

Internet of Things (IoT) environments present a unique blend of forensic challenges due to their vast and diverse nature. A systematic review identifies core issues such as the sheer heterogeneity of devices, the volatile nature of much of the data they produce, and the widespread use of proprietary operating systems [3]. These factors complicate data acquisition, preservation, and analysis. Specific overviews of digital forensics for IoT devices further emphasize difficulties in extracting and analyzing data from resource-constrained devices [9]. To address this, dedicated research proposes a structured digital forensic process model tailored for the IoT environment. This model details phases from identification and preservation to analysis and presentation, providing investigators a clear roadmap for handling evidence from a multitude of IoT devices [10]. The goal is to establish standardized procedures that can effectively navigate the fragmented and dynamic IoT ecosystem.

Beyond device-specific challenges, new computing paradigms also demand tailored forensic approaches. Federated learning (FL), a distributed machine learning approach, introduces unique investigative challenges surrounding data breaches, model poisoning, and privacy violations [4]. The decentralized nature of FL means traditional forensic methods designed for centralized systems are often insufficient. Studies call for integrating forensic readiness directly into FL architectures to ensure accountability and enhance security from the ground up. Similarly, cloud computing environments, characterized by virtualization, distributed storage, and multi-tenancy, necessitate specialized cyber forensics models [5]. These models outline systematic steps for evidence acquisition, preservation, analysis, and reporting in the cloud, aiming to overcome traditional forensic limitations in highly dynamic infrastructures. A comprehensive study on various digital forensics process models for cloud computing dissects their methodologies, strengths and weaknesses, offering insights into handling challenges from data volatility to jurisdictional issues, thereby guiding practitioners in model selection [6].

Artificial Intelligence (AI) is not just a target for forensics (like deepfakes) but also a powerful tool for forensic practitioners. A systematic review explores the increasing integration of AI techniques into digital forensics, categorizing and analyzing its use for automating tasks such as data analysis, anomaly detection, and pattern recognition [7]. AI promises improved efficiency and accuracy in complex investigations, though challenges related to explainability and bias remain critical considerations. Ensuring that AI tools are transparent and fair is paramount for their adoption in legal contexts. Finally, mobile devices continue to be central to many investigations, requiring specialized forensic analysis techniques [8]. Surveys provide an exhaustive overview of methods for various operating systems, covering data acquisition (physical, logical, filesystem) and the tools used to extract and analyze digital evidence. The continuous evolution of mobile security measures and the challenge of data fragmentation mean mobile forensics is a perpetually evolving field.

Conclusion

This collection of papers addresses the evolving landscape of digital forensics, covering critical areas like blockchain, deepfakes, Internet of Things (IoT), federated learning, cloud computing, Artificial Intelligence (AI), and mobile devices. Research highlights how blockchain technology can fundamentally reshape digital forensics by enhancing evidence integrity through immutability and transparency, preventing tampering, and ensuring auditability in investigations [1]. The challenge of deepfakes is also a major focus, with studies exploring detection techniques ranging from visual artifacts to AI-based methods, acknowledging the ongoing struggle between generation and detection technologies [2]. Digital forensics in IoT environments presents unique complexities due to heterogeneous devices, volatile data, and proprietary operating systems. Investigations detail existing frameworks and tools, proposing systematic reviews and specific process models to handle data extraction and analysis from diverse IoT ecosystems [3, 9, 10]. Cloud computing introduces its own set of challenges, including virtualization and distributed storage, leading to the development of tailored cyber forensics models and comprehensive studies of process models for effective evidence acquisition and analysis in dynamic cloud infrastructures [5, 6]. The papers also delve into specialized domains. Forensics within federated learning systems examines challenges like data breaches and model poisoning, advocating for integrated forensic readiness [4]. The integration of AI into digital forensics is explored, showing its use in automating tasks like data analysis and anomaly detection to improve efficiency and accuracy in investigations, while also noting issues of explainability and bias [7]. Furthermore, a comprehensive review of forensic analysis techniques for mobile devices covers various operating systems and data acquisition methods, highlighting the complexities of evolving security measures and data fragmentation [8]. Collectively, these papers provide a broad perspective on the current state, challenges, and advancements in digital forensics across modern technological paradigms.

Acknowledgement

None.

Conflict of Interest

None.

References

1. Mohammad Al-Fawa'reh, Adnan Al-Odat, Eyad Al-Okby. "Blockchain-Based Digital Forensics Framework: A Technical Survey." *Sensors* 23 (2023):5006.
2. Fadi Al-Ayyoub, Sawsan Abed-Al-Kareem, Yousef Al-Ayyoub. "Digital Forensics for Deepfakes: A Survey." *Sensors* 23 (2023):6800.
3. Abdun Naser, Feroz Ahmed, Mohammad Hafizur Rahman. "Digital forensics of IoT devices: A systematic review." *Sensors* 23 (2023):3613.
4. Toshihisa Takagi, Kenji Kitagawa, Masatoshi Kawai. "Forensics of Federated Learning: Opportunities and Challenges." *Sensors* 23 (2023):5937.
5. Mohammed Saleh Zameer, Yazen F. Abu-El-Basal, Anas M. Al-Quraan. "Cyber Forensics Model for Cloud Computing Environments." *Applied Sciences* 13 (2023):342.
6. Mohammed Saleh Zameer, Yazen F. Abu-El-Basal, Anas M. Al-Quraan. "A Comprehensive Study of Digital Forensics Process Models in the Cloud Computing Environment." *Applied Sciences* 13 (2023):7762.
7. Marwa El-Sayed, Tarek Gaber, Wael S. El-Shafai. "Artificial Intelligence for Digital Forensics: A Systematic Literature Review." *Applied Sciences* 13 (2023):9051.
8. Siti Nurulain Mohd Zulkifli, Rosli Omar, Rabiah Ahmad. "A Survey of Forensic Analysis Techniques on Mobile Devices." *IEEE Access* 8 (2020):110682-110697.
9. Manel Ayadi, Sami Faiz, Walid Barhoumi. "An Overview of Digital Forensics for IoT Devices." *Journal of Reliable Intelligent Environments* 7 (2021):117-130.
10. Zulkifli Zainal Abidin, Khairul Azhar Murad, Mazlan Harith. "A Digital Forensic Process Model for IoT Environment." *International Journal of Advanced Computer Science and Applications* 11 (2020):361-367.

How to cite this article: Nguyen, Rachel T.. "Digital Forensics: Modern Challenges Across Technologies." *J Forensic Med* 10 (2025):431.

Address for Correspondence: Rachel, T. Nguyen, Department of Forensic and Biomedical Sciences Coastal State University School of Medicine, USA, E-mail: rachel.nguyen@csu.edu

Received: 02-Sep-2025, Manuscript No. jfm-25-173750; **Editor assigned:** 04-Sep-2025, PreQC No. P-173750; **Reviewed:** 18-Sep-2025, QC No. Q-173750; **Revised:** 23-Sep-2025, Manuscript No. R-173750; **Published:** 30-Sep-2025, DOI: 10.37421/2472-1026.2025.10.431