IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46AI/2025/4630425/
Vol. 2025 (34), Article ID 4630425

The Power of Machine Learning in Enhancing Digital Evidence Detection and Analysis*

Mohammad Ali A. HAMMOUDEH

Department of Information Technology, College of Computer, Qassim University
Buraydah 51941, Saudi Arabia

Correspondence should be addressed to: Mohammad Ali A. HAMMOUDEH, maah37@qu.edu.sa

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

The fast rise of digital data brings both chances and problems for law enforcement and forensic investigators. The large amount of digital evidence can give useful information about crimes, but the high volume and complexity of this data make manual analysis hard. Machine learning (ML) algorithms have become a strong tool for automating and improving digital forensic investigations, providing benefits like better accuracy, efficiency, and scalability. This paper looks into how well ML algorithms work in finding and analyzing digital evidence, examining their ability to simplify forensic processes and discover hidden patterns in complicated datasets.

Keywords: Machine Learning, Digital Forensics, Algorithmic Detection, Forensic Analysis, Computational Techniques.

Introduction

The digital world is now a big part of our lives, changing how we talk to each other, do business, and keep information. This change has also changed crime, created new types of cybercrime and made digital evidence more important in criminal cases. Digital evidence includes many types of data, like documents on computers, emails, social media updates, images, videos, and logs of network activity. The amount and complexity of digital evidence has greatly increased, creating major issues for police and forensic investigators (Rubén Arcos et al., 2023). Digital forensics is important in investigations today as it helps collect, keep, analyze, and understand digital evidence.

Traditional methods for forensics, while still useful, often have trouble keeping up with the growing needs of digital cases. Machine Learning (ML) algorithms can help with these issues by offering a way to handle data in digital forensics. ML can make many of the slow tasks in forensic work faster, like finding and getting useful data from large amounts of information, classifying and looking at digital items, and spotting strange patterns or activities (Miracle et al., 2024).

Materials and Methods

Today's businesses face many risks that require proper security methods. This study tries to show how machine learning algorithms helps find and analyze digital evidence. By using advanced computing methods, these algorithms can make the forensic analysis process better and more automated (Angelopoulou et al., 2020). The research looks closely at how different machine learning models work with various digital evidence types, which include text, images, and complicated network data. Through careful tests and analysis, the study

Cite this Article as: Mohammad Ali A. HAMMOUDEH, Vol. 2025 (34) "The Power of Machine Learning in Enhancing Digital Evidence Detection and Analysis " Communications of International Proceedings, Vol. 2025 (34), Article ID 4630425, https://doi.org/10.5171/2025.4630425

investigates how algorithms make decisions, looking at accuracy, precision, recall, and efficiency (Cao et al., 2020). This research aims to create a way to evaluate how reliable and useful machine learning methods are in different forensic cases.

Additionally, the study examines the problems that come with using machine learning algorithms in real cases of forensic investigation. It discusses issues like data quality, how results can be interpreted, and how algorithms can adapt to new technology (Angelopoulou et al., 2020). By highlighting these issues, the study offers valuable information for both professionals and researchers in the areas of machine learning and digital forensics. In summary, this research not only enhances our understanding of machine learning's role in digital forensics but also lays the groundwork for future developments in the field. The results provide a well-rounded view, recognizing the positive aspects of machine learning while seriously considering the practical issues that need to be solved for successful use.

Introduction to Machine Learning Algorithms

Types of Machine Learning Algorithms Important for Digital Forensics. Effective use in forensic processes. Figure 1. Different kinds of Computer Forensics. Forensics: Machine learning algorithms can learn patterns from data and provide a useful set of tools for digital forensic experts. Supervised learning methods, like support vector machines and decision trees, are good at classification tasks, which help categorize digital evidence. Unsupervised learning methods, such as clustering techniques, are helpful in spotting patterns and anomalies in large datasets, which helps find irregularities that humans might miss (Cresci et al., 2017). Moreover, deep learning algorithms, especially neural networks, are very capable of managing complex data types such as images and text. Their layered structures help pull out detailed features, improving the effectiveness of digital evidence evaluation (Dunsin et al., 2023). It is crucial to understand the details of each algorithm type to choose the right tool for specific forensic jobs, from malware detection to multimedia examination.

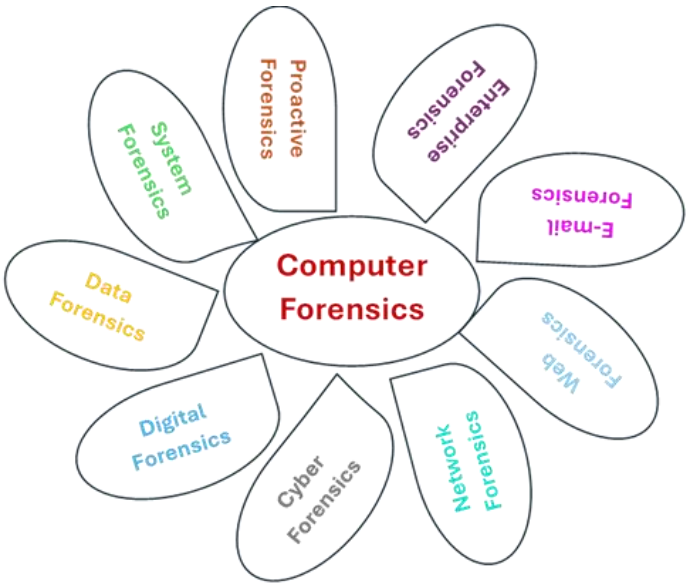

Fig 1. Various types of Computer Forensics. (Own Creation)

Applications and Advantages in Forensic Investigations

Machine learning methods have many uses in digital forensics, changing how investigations are done, making them faster and more precise. Automated data sorting helps by identifying important evidence from large amounts of data, speeding up the early stages of an investigation (Bamigbade et al., 2024). Pattern recognition methods help find trends and connections, giving useful information about how cybercriminals operate and their methods (Babuta and Oswald, 2020). Also, machine learning helps create predictive models that can forecast possible threats and weaknesses based on past information.

The speed and scalability of these methods allow for real-time analysis, helping investigators adapt to the fast changes in digital crime. While these uses show how machine learning can change digital forensics, it is

important to carefully think about ethical issues, data privacy, and how easy it is to understand the decisions made by algorithms in legal situations.

Results and Analysis

For Figure 2 and 3 Presents Findings on Algorithm Performance: The results from experiments show a detailed view of how well machine learning algorithms work in digital forensics. Both numerical and descriptive evaluations come together to show how effectively these algorithms operate in various forensic situations. Measurements like accuracy, precision, recall, and F1 scores act as standards, providing a complete assessment of the algorithms' ability to find and analyze digital evidence correctly (Cresci et al., 2017). The findings explore the details of algorithm performance, highlighting cases of successful evidence discovery and situations where algorithms may not perform well. Clear visual displays and statistical analysis reveal the strengths and weaknesses of each method, laying a solid groundwork for further discussions. Comparison of Different Machine Learning Methods: An important part of the research is a careful comparison of different machine learning methods used in digital forensics. This comparison helps identify the relative strengths and weaknesses of different algorithm models, pointing out the best strategies for particular forensic tasks. This analysis goes beyond just accuracy, taking into account factors like computational efficiency, scalability, and how well they adapt to changing digital environments (Babuta and Oswald, 2020). By comparing the performance of various machine learning algorithms, the research aids in forming best practices for picking algorithms suited for specific forensic situations. These comparative insights help practitioners navigate the broad field of digital forensics.

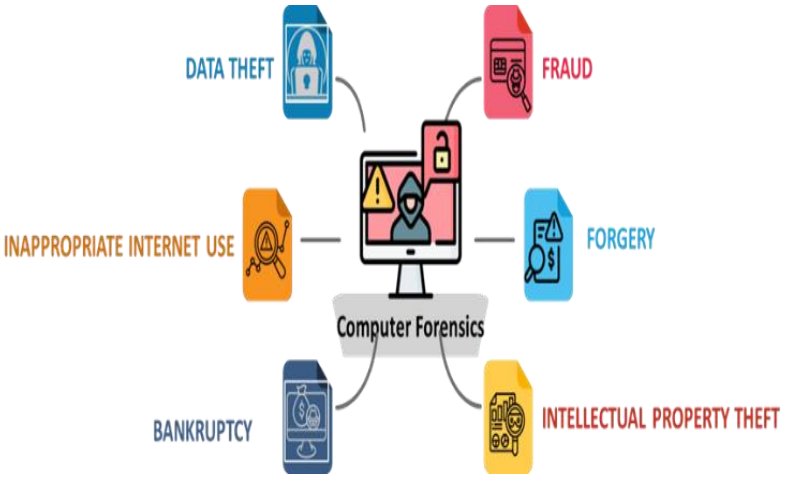

Fig 2. Types of Computers Forensic. (Own Creation)

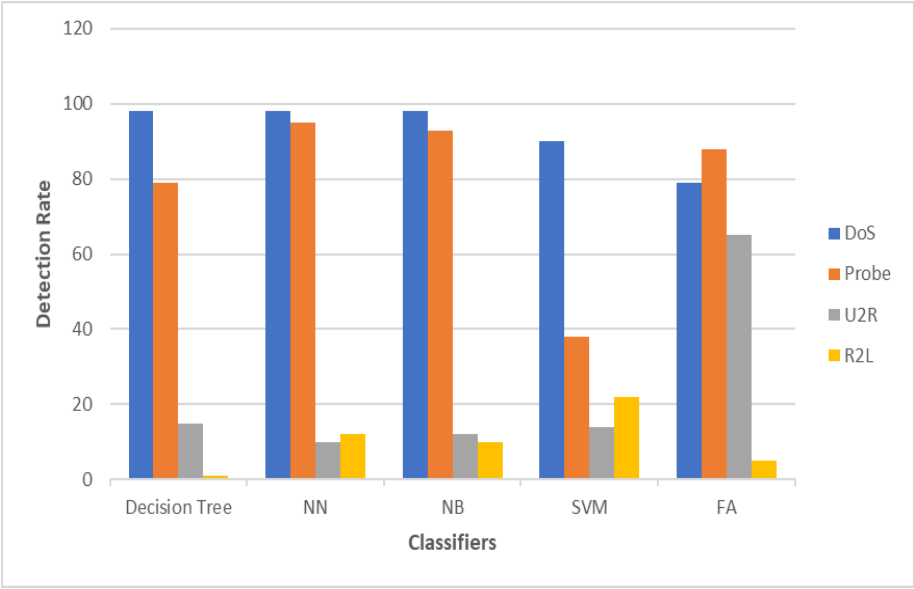

Fig 3. Performance comparison of common classifiers for different Attacks. (Own Creation)

Exploration of Factors Influencing Algorithmic Success

The details of algorithm success are shown by looking at the many different factors that affect how machine learning works in digital forensics. Factors like data quality, variety, and representativeness are key aspects that impact how strong algorithms are in real-life situations (Babuta and Oswald, 2020). Also, aspects like feature engineering, model settings, and ease of understanding play a role in knowing how algorithm design affects investigative success. This study goes beyond just looking at success or failure. It examines the complex factors that affect how reliable and useful machine learning algorithms are in digital forensics (Pasquale, 2019). The information gained from this study helps to improve algorithm methods and moves forward digital forensic practices.

Considerations For Real-World Application

The move of machine learning progress from tests to real-life usage needs careful thought about practical limits and operational facts. This part looks at how machine learning algorithms can work in real-world forensic investigations as in Figure 4, focusing on problems like scalability, necessary resources, and integration. Real-world concerns go beyond just how well the algorithms perform; they include compatibility with older systems, how humans and machines work together, and the timing pressures in forensic cases. By offering practical insights, this part helps those involved develop a plan to successfully use machine learning in regular forensic work. As highlighted by RUSI's studies, there is a need for uniform procedures to ensure the correct evaluation of algorithms in real-world settings (Babuta et al., 2020).

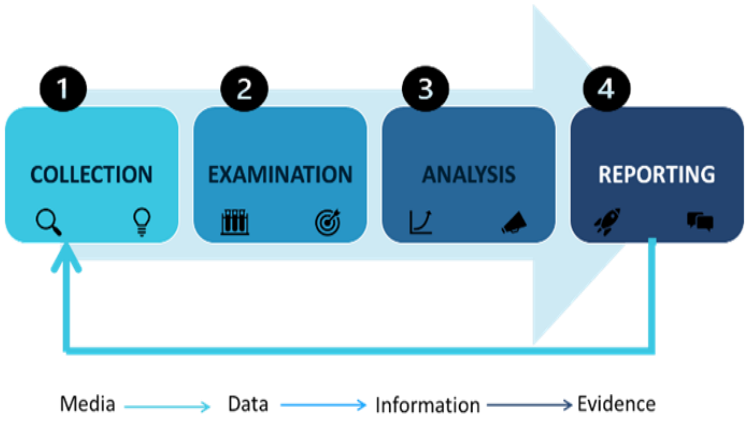

Fig 4. Digital investigation model phases. (Own Creation)

Moreover, while AI offers significant chances for data review, ongoing attention to privacy and human rights issues is required as new techniques are used.

Ethical Implications and Safeguards

The ethical side of using machine learning in digital forensics is very important, leading to a thoughtful discussion about risks and protections in algorithm decision-making. Concerns about privacy, reducing bias, and carefully managing sensitive information are crucial ethical priorities. This part looks at finding the right balance between seeking justice and protecting personal rights in the digital world. The talk includes creating ethical guidelines and protections, focusing on the need for clarity in algorithm decision-making and the need to prevent unexpected results (Babuta et al., 2020). By tackling these ethical issues directly, the research helps the careful growth of digital forensics, making sure that machine learning progress meets ethical norms and societal expectations as shown in Figure 5.

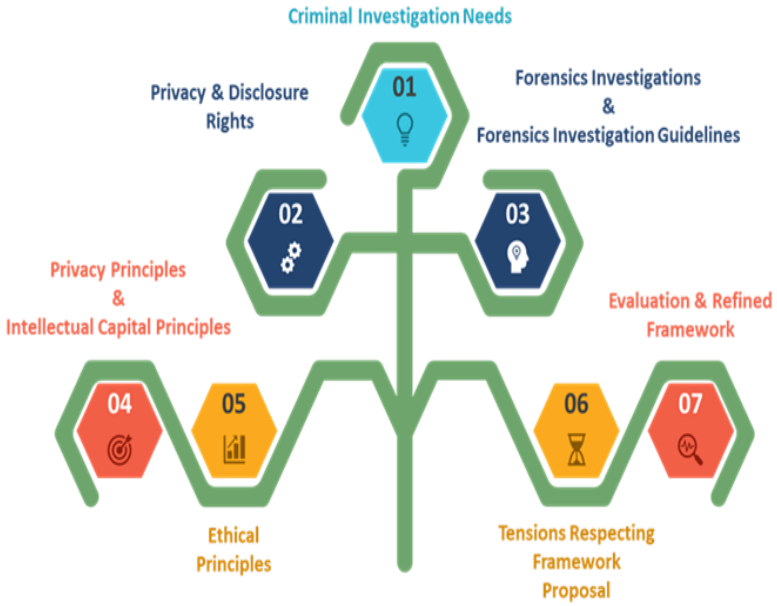

Fig 5. Ethical Framework. (Own Creation)

Conclusion

The study on how well machine learning methods can find and analyze digital evidence marks an important advance in digital forensics. The combination of results highlights how machine learning can change the game when tackling the difficult and large challenges in digital environments. The shown effectiveness of algorithms shows both the achievements and the natural difficulties along with limitations of machine learning models. Comparing different methods offers guidance for choosing the best strategies, recognizing the variety of tasks in digital forensics and the need for specific solutions. Looking into what affects algorithm success deepens our insight, stressing the importance of detailed factors when designing and using these algorithms.

Problems with using machine learning in digital forensics are recognized, and the conversation goes beyond theory to address the real-world details of applications. Issues like scalability, compatibility, and ethical protections highlight the necessity for a complete approach to integration. As we explore the edges of digital forensics, the ethical effects and protections discussed in this research need careful attention. The careful use of machine learning methods requires a focus on transparency, privacy, and reducing bias, which ensures that technology improves with fairness and respect for people's rights.

Overall, this study not only boosts our knowledge of the connection between machine learning and digital forensics but also moves the field toward a future where new technologies work well with ethical needs. By enhancing our understanding of the abilities, challenges, and ethical issues tied to machine learning methods in digital forensics, this research lays the groundwork for the ongoing improvement of investigative techniques.

References

- Babuta, A. and Oswald, M. (2020) Data analytics and algorithms in policing in England and Wales: Towards a new policy framework, Royal United Services Institute (RUSI). [Online]. [Accessed 8 December 2024]. Available at: https://core.ac.uk/download/305121462.pdf
- Babuta, A., Janjeva, A. and Oswald, M. (2020) Artificial intelligence and UK national security: Policy considerations, Korean Association of Rusists. [Online]. [Accessed 8 December 2024]. Available at: https://core.ac.uk/download/305121521.pdf
- Bamigbade, O., Scanlon, M. and Sheppard, J. (2024) Computer Vision for Multimedia Geolocation in Human Trafficking Investigation: A Systematic Literature Review. [Online]. [Accessed 8 December 2024]. Available at: http://arxiv.org/abs/2402.15448
- Cao, H., Dutt, N., Jafarlou, S., Lim, M. M., Rahmani, A. M., Shin, I. and Vishwanath, M. (2020) Investigation of Machine Learning Approaches for Traumatic Brain Injury Classification via EEG

Assessment in Mice, eScholarship, University of California. [Online]. [Accessed 8 December 2024]. Available at: https://core.ac.uk/download/323075717.pdf

- Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A. and Tesconi, M. (2017) 'Social Fingerprinting: Detection of Spambot Groups through DNA-Inspired Behavioral Modeling,' IEEE. [Online]. [Accessed 8 December 2024]. Available at: http://arxiv.org/abs/1703.04482
- Dunsin, D., Ghanem, M. C., Ouazzane, K. and Vassilev, V. (2023) A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response. [Online]. [Accessed 8 December 2024]. Available at: https://core.ac.uk/download/591678421.pdf
- Miracle, U., Shakhov, V. and Koo, I. (2024) 'Comparative Evaluation of Network-Based Intrusion Detection: Deep Learning vs Traditional Machine Learning Approach,' 2024 Fifteenth International Conference on Ubiquitous and Future Networks (ICUFN). [Online]. [Accessed 8 December 2024]. Available at: https://www.semanticscholar.org/paper/996cf952d9080906d1aa9a3ed4a398e880f7794f
- Pasquale, F. A. (2019) Professional Judgment in an Era of Artificial Intelligence and Machine Learning, DigitalCommons@UM Carey Law. [Online]. [Accessed 8 December 2024]. Available at: https://core.ac.uk/download/212819576.pdf
- Rubén Arcos, Chiru, I. and Ivan, C. (2023) Routledge Handbook of Disinformation and National Security, Taylor & Francis. [Online]. [Accessed 8 December 2024]. Available at: https://play.google.com/store/books/details?id=1pYIEQAAQBAJ
- Angelopoulou, A., Effraimidis, D., Flynn, M., Hemanth, J., Kapetanios, E., Towell, T. and Williams, D. (2020) 'Assessing the Effectiveness of Automated Emotion Recognition in Adults and Children for Clinical Investigation,' Frontiers Media SA. [Online]. [Accessed 8 December 2024]. Available at: https://core.ac.uk/download/305119273.pdf