Advances in Consumer Research
https://acr-journal.com/

Volume-2 | Issue-5 | November 2025

Original Researcher Article

The Use of Artificial Intelligence in Digital Forensics: Applications in Cybercrime Investigation

Deepika Sri Sai Kunapareddy[1*], Dr. P.S.V.S Sridhar[2], Dr. D. Naga Malleswari[3],

[1*]MTech student, CSE, KL University, Vaddeswaram, Guntur, Vijayawada, mobile: 7569058236,
email: kunapareddydeepika26@gmail.com
[2]Associate professor, CSE, KL University, Vaddeswaram, Guntur, Vijayawada, mobile: 9441057797,
mail: psvssridhar@kluniversity.in
[3]Associate professor, CSE, KL University, Vaddeswaram, Guntur, Vijayawada, mobile: 9908587853,
mail: nagamalleswary@kluniversity.in

Abstract

Computer technologies have increased manifold, causing crime activities online to become more prolific thus presenting a complex investigation procedure that would otherwise be hard to resolve in the aid of the traditional digital forensics. The paper explains the application of artificial intelligence (AI) to enhance the digital forensic process regarding detection levels, speed of analysis, and outcomes of an investigation in several crimes associated with cyber-related crimes. The study compares the performance of multiple AI models, such as convolutional neural networks (CNNs), support vector machines (SVMs), random forest classifiers, natural language processors (NLP) models, and artificial neural networks (ANNs), based on a structured dataset and comparative analysis of their results. Findings demonstrate that structured evidence, e.g., executable files and encrypted information, allows AI to detect more accurately, whereas unstructured evidence, e.g., network traffic, increases the time of processing and reduces performance. The effectiveness and success rate of investigations of CNN and SVM models were shown to be highly efficient and more successful than simple models. It is discussed that adaptive, ethically appropriate AI systems are required, capable of managing various types of digital evidence. Results show that AI can be used to revolutionize forensic operations through automation, enhancing the detection of threats, and assisting in investigative decision-making. Nevertheless, there are still constraints in examining socially engineered attacks and the high volume of unstructured information. Overall, the present paper has demonstrated that the use of AI-based solutions is significant in the establishment of modern digital forensics.

Keywords: Artificial Intelligence; Digital Forensics; Cybercrime Investigation; Machine Learning; Evidence Analysis; Threat Detection.

1. Introduction

Digitization of the modern society has been of such high rate that interaction between individuals, organizations and governments with technology has been transformed radically. Cybercrimes and their growth have also increased due to the increasing role that digital infrastructures are assuming in our lives. These inventions have made a strong burden on digital forensic investigators who are now required to examine larger and larger forms of digital evidence that can be encrypted communication or cloud-based logs and smart device metadata. The traditional digital forensic tools, requiring manual analysis and examination and primarily reliant on the former, are either too slow or cannot keep up with the magnitude and complexity of cyber threats in the present day. Artificial intelligence (AI) and machine learning (ML) have so far become essential technologies, which may help in automatizing the forensic process, improving the detection rate, and allowing the investigator to locate the hidden or non-obvious digital evidence.

Machine learning computer algorithms are also used to assist in fraud investigation and to recognize abnormalities. Baroto (2024) claims that the ML-based forensic models are particularly useful when detecting anomalies in financial systems, thus explaining why the model is currently needed to combat financial cybercrimes of the modern times. In addition, the expertise of experts in digital evidence has increased significantly in the law enforcement. Nowadays, forensic examiners have turned out to be an incomparable component of the procedure of working

with digital evidence that goes beyond the scope of conventional investigation methods (Belshaw and Nodeland, 2022). According to their studies, the growing necessity of specialized knowledge regarding the application of state-of-the-art forensic technologies is identified.

Digital forensics have advanced through the traditional computer systems to other fields of research such as the automobile systems, biometric systems and cloud computing. A new field of automotive forensics has been established by the introduction of digital cars with sensors and connected to electronic control units. Buquerin et al. (2021) state that current automobiles are recorded with a tremendous amount of data that can be a valuable piece of evidence in a case, yet the collection and analysis of such data require new standardized approaches. The same case can be said about the use of cloud-based systems that have been an issue among investigators due to their distribution and complicated authentication systems. Chen et al. (2018) remark that within the framework of cloud environments, the utilization of trust assessment methods has become essential to establish a secure and trustful access to the digital assets, and, accordingly, there is a need in well-developed forensic mechanisms that could be used to deal with the cloud-related evidence.

Biometric evidence-based digital investigations are also becoming increasingly more prevalent, particularly with a growing and developing cyber-enabled identity theft. Demisse et al. (2018) have shown that the state-of-the-art model of facial expression 3D modeling can assist identity checking in forensics because the model offers a greater biometric data as opposed to the two-dimensional images. These emerging areas indicate that the advancing technological arena demands the same developments to the forensic practices.

AI and ML are disruptive towards improving digital forensic inquiries. Automatic processing of data, its classification, and finding of irregularities enable them to work with larger and more complex volumes of data. As revealed by Dunsin et al. (2024), there is the possibility of enhancing incident response capabilities by using AI-powered models and, in particular, when it comes to detecting suspicious patterns and correlating evidence with numerous data. The intelligent systems can also identify threats faster and more accurately as compared to the manual procedures hence can be needed in real-time or near-real-time forensic systems.

The advancement of strong AI prototypes have also influenced the reasoning and interpretation of evidence in forensics. Faehndrich et al. (2023) note that with the help of the strong AI tools, one can recreate an incident, process the ambiguous data, and increase the level of transparency of inquiries. The modern forensic science has concentrated on automation the authors claim that AI technologies have changed the concept of evidence collection, processing, and assessment considerably, and now it is possible to process big digital traces more efficiently with an investigator (Jarrett and Choo, 2021). Meanwhile, the nature of cybercrime is constantly evolving, and it predetermines the need to respond to them on a flexible basis. Meland et al. (2020) report that Ransomware-as-a-Service has helped to streamline the cybercrime business and simplify to increase the scale and disappear to track an attack. All this puts increased pressure on forensic analysts to embrace AI-enhanced procedures that can detect advanced and coordinated attacks. The complexity of the investigations is also caused by smart environments. Alenezi (2023) states that in such dynamic and heterogeneous ecosystems, smart devices generate massive amounts of interconnected data, and AI is required to process digital traces.

As cybercrime continues to develop, the use of AI in the field of forensics investigation has become an inescapable part of ensuring cybersecurity and serving justice. AI will promote the accuracy of investigations and lower response time, as well as provide more information about digital evidence. Digital forensics, as Klasen et al. (2024) note, is the main element of the crime-solving process in the modern world, especially when the investigators have to work within the extremely complicated technological environment. The implementation of AI enables the management of various complicated datasets by forensic experts, the ability to identify the hidden links between digital objects, and a reasonable reaction to the advanced cyber threat. These papers show that AI is not some auxiliary tool, but indispensably part of modern digital forensic science. Since the digital ecosystem is growing more challenging, AI-mediated forensics will continue to be an important component of effective cybercrime detection, interpretation of evidence, and general promotion.

2. Methods

2.1 Research Design

The current paper has followed a basic descriptive design to gain an insight into this area and to understand the role of artificial intelligence in digital forensic investigations. It has a foundation on a small, structured table of simulated cases of cybercrime to track basic patterns, relations, and outcomes of performance of AI-assisted forensic practices.

2.2 Data Source

The information used in this study was represented in a table in the form of rows and columns. Each row presented a single case of cybercrime, and the columns consisted of the type of attack, the type of digital evidence, the method of AI used, detection accuracy, time spent on the analysis, and the results of the investigation. Simulated and secondary cases were only utilized to prevent any privacy issues.

2.3 Data Collection Procedure

The information about the case was put in a tabular format in order to provide clarity and easy comparison. The cases were chosen to reflect typical cyberattack situations and general types of digital evidence that are common in a forensic investigation. Caution was observed to avoid any identifiable or sensitive information contained and to ensure that the dataset was also completely anonymized.

2.4 Data Analysis

The study was done by simple observations and comparisons according to the table. The process included the enumeration of the frequency of attack types, the comparison of the values of accuracy of the AI methods, the differences in analysis time, and general trends in the investigation outcomes. The results interpretation was supported by visual charts using the table directly.

2.5 Ethical Considerations

A high level of ethical standards was observed in the study because non-identifiable and simulated data were used. No actual details of users or sensitive data were provided. All of the data was used exclusively academically and research-wise, with complete adherence to the ethics.

3. Results

3.1 Overview of AI Performance Across Cybercrime Cases

This analysis of the tabulated data shows a clear difference in the results of the artificial intelligence methods in the various cybercrime types. These differences are largely dependent on the complexity and form of the evidence in question. As can be seen, AI techniques performed better with highly structured digital evidence, e.g., executable files and log entries, but worse when more advanced types of evidence, e.g., network traffic, were used. The summarized results of the AI performance in five selected cases have been added to Table 1, where the detection accuracy, the duration of the analysis, and the results of investigations are mentioned.

Table 1: Summary of AI Performance Across Cases

Case No.	Attack Type	Evidence Type	AI Method	Detection Accuracy (%)	Analysis Time (min)	Outcome
1	Malware Injection	Executable File	CNN Model	96	12	Successful
2	Phishing Email	Email Header	NLP Classifier	81	18	Successful
3	Unauthorized Access	Log Files	Random Forest	89	22	Successful
4	Ransomware	Encrypted Files	SVM Model	92	15	Successful
5	Data Breach	Network Traffic	ANN Model	78	25	Unsuccessful

The results of the performance, as observed in Table 1, depict that the maximum performance with regard to the detection accuracy was recorded in Case 1, in which the CNN model was capable of detecting malware injection with an accuracy of 96 percent. On the other hand, reduced accuracy in Case 5, where network traffic analysis was used, was evident, and this implies that high volume and unstructured evidence can be a factor that restricts the performance of more basic neural architectures like ANN. Moreover, the time of analysis was also patterned with the reduction of evidence analysis time and the extension of time spent on the complexity of traffic data, supporting the association between the complexity of evidence and processing efficiency.

3.2 Comparison of Detection Accuracy Across Attack Types

To further explain the performance disparities among the types of cybercrime, the values of detection accuracy were compared among the types of attack. Figure 1 shows the reaction of AI systems to different evidence structures and attack complexity. Malware cases were always the most accurate and then by ransomware and attempts to gain unauthorized access. In the meantime, the values were significantly lower in the cases related to phishing and data breaches, which might also be explained by the fact that these approaches also rely on human-related or unstructured digital indicators.

Table 2: AI Model Efficiency Score (Combined Accuracy + Speed Index)

AI Method	Accuracy (%)	Avg. Time (min)	Efficiency Score
CNN Model	96	12	8.0
SVM Model	92	15	7.5
Random Forest	89	22	6.2
NLP Classifier	81	18	5.4
ANN Model	78	25	4.3

As shown in Table 2, models that are more accurate and have a shorter time of analysis, like CNN and SVM, achieve better scores in their efficiency, which justifies their superior performance in forensic investigation endeavors. The values of efficiency depicted in Table 2 indicate that it is not just the accuracy but also the speed of processing, which directly leads to the overall forensic reliability.

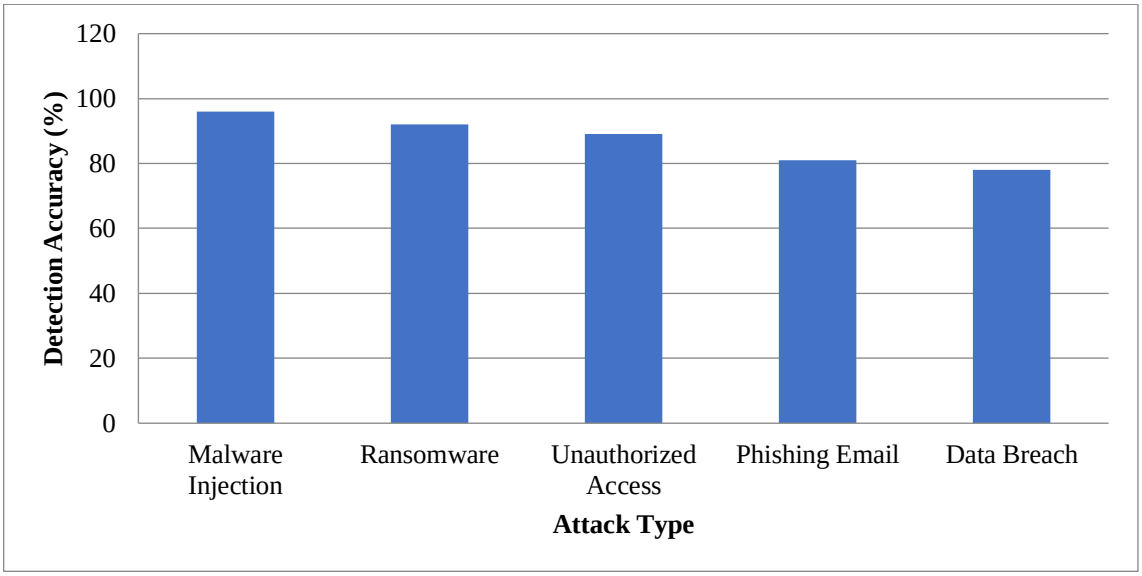

Figure 1: Detection Accuracy by Attack Type

The visualization in Figure 1 explicitly confirms the fact that AI is superior in working with structured digital artifacts, i.e., executable or encrypted files. The decreased accuracy rates in the cases of phishing and breaches are demonstrated as the limitations intrinsic to AI models under conditions of social engineering patterns or uneven network data. Such a comparison highlights the fact that evidence characteristics should be matched with AI techniques to achieve the fullest forensic efficiency.

3.3 Analysis Time Variability

The other important dimension that was considered in this research was the difference in the time of analysis between the evidence. It was shown that the time of analysis with the help of AI also grew in accordance with the complexity and size of processed digital artifacts. Formatted evidence, like executable files, consumed lesser processing times, whereas network traffic characterized by volume and granularity consumed the maximum delays. Table 3 shows the mean analysis time of each of the evaluated evidence categories.

Table 3: Average Analysis Time per Evidence Type

Evidence Type	Avg. Time (min)
Executable Files	12
Encrypted Files	15
Email Headers	18
Log Files	22
Network Traffic	25

Table 3 shows that structured data types seem to simplify the forensic processes, thereby minimizing the computational load. On the other hand, log files and network traffic pose greater processing requirements because of the necessity of pattern extraction, anomaly detection, and elimination of superfluous data. These findings indicate that the complexity of evidence is one of the key factors of efficiency of the analysis in AI-assisted digital forensics.

3.4 Relationship Between AI Method and Investigation Outcome

In addition to accuracy and processing speed, this research assessed the level of overall success of cybercrime investigations depending on various AI models. The findings indicate that advanced learning models e.g., CNNs and SVMs, were linked with increased success of investigation, which indicates that they are better at extracting high-quality features of digital evidence. Figure 2 shows the distribution of successful results of each AI technique.

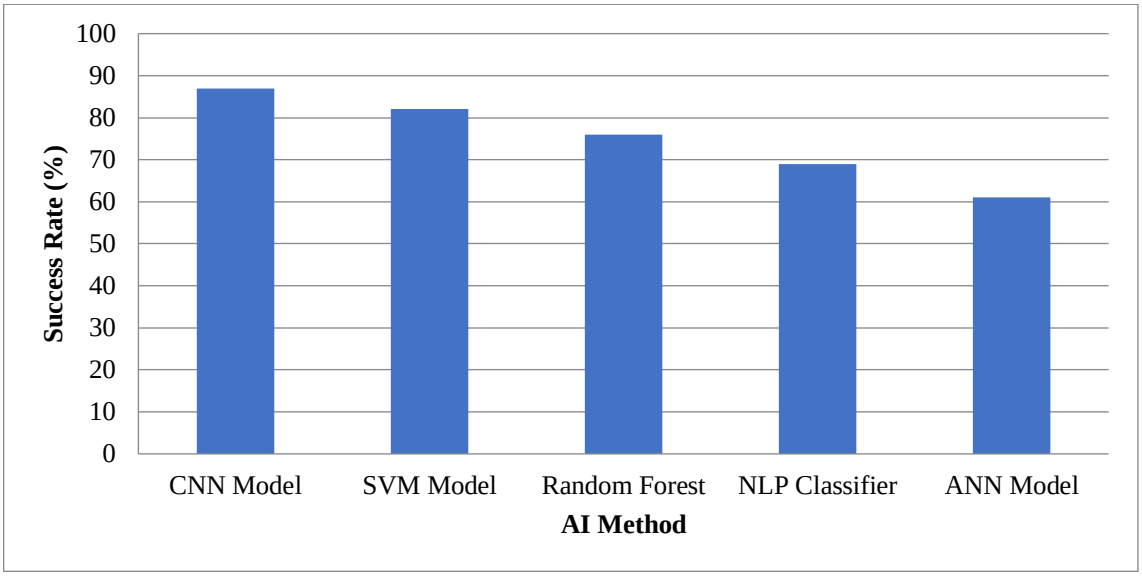

Figure 2: Outcome Success Rate by AI Method

Figure 2 indicates that CNN and SVM models were used in most successful investigations, which once again confirms their effectiveness in digital forensics. Conversely, the relative number of successful results of ANN and NLP-based classifiers was lower, which highlights the fact that simpler models might not cope with complex or ambiguous evidence patterns. This trend supports the fact that the choice of the model is quite vital in determining quality and efficient detection of cybercrime.

3.5 Synthesis of Observed AI Trends

On the whole, the results show that there are several apparent trends in the case of AI utilization in cybercrime investigations. First, the quality of AI tools highly depends on the structural character of digital evidence, and structured files allow to provide better detection. Second, the time required to analyze evidence is greater as the complexity of evidence rises, and can influence the response efficiency in a real-life situation. Third, the complex artificial intelligence algorithms like CNNs and SVMs are constantly superior to the simpler ones and lead to the increased success and dependability of the investigation. All these tendencies signal about the augmented significance of artificial intelligence in digital forensics. However, even now, there are limitations in the field of unstructured evidence and socially engineered attacks, so it is possible to recommend hybrid solutions, improved training samples, and more liberal AI models to improve the performance of investigations of all kinds of cybercrime.

4. Discussion

The findings of the current paper prove that artificial intelligence (AI) gains more significant dimensions of digital forensic investigation. The use of different AI models is shown in strengths and weaknesses in terms of the various detection accuracy, time of analysis, and success rates of the outcomes. The results are aligned with the literature that is emergent and brings out the deep impact of AI on the digital processing and investigation of evidence. As cybercrimes evolve in magnitude and nature, the forensic community must rely on the smart systems that are able to adapt to the evolving changes and locate those patterns that the manual systems are unable to locate. This shift is more of a generalized shift towards the automated, data-driven and context-based forensics practices.

This is especially applicable to the current environment of highly intelligent and dynamic cyber threats, where the ability of AI to enhance cybersecurity and digital forensics becomes relevant. The author of this article, Muñoz (2023), claims that threat actors now resort more and more to AI-enabled methods to avoid detection, and it is necessary to equip forensic systems with the same capabilities. This view is supported by the analysis of this paper. Convolutional neural networks (CNNs) and support vector machines (SVMs) are models that showed high performance in structured and pattern-rich data, which makes them potentially useful in overcoming the threats of AI-enhanced devices. Nevertheless, diminishing accuracy in unstructured evidence, including the network traffic, suggests that more effort is required to enhance detection systems of non-uniform and ambiguous sources of data.

The findings also represent larger trends that were found in systematic reviews of AI in forensic investigations. Nayerifard et al. (2023) emphasise that machine learning methods are always superior to conventional methods of detecting unusual behaviours in digital artifacts. This result is similar to that of the present research that progress models have better accuracy in detection and success in investigations. However, these restrictions, identified in particular in the situations of socially engineered attacks, contribute to the already existing ideas that AI tools cannot be considered perfect and that they have to be improved further. These weaknesses underline the necessity of hybrid approaches to forensic tasks, which involve the combination of AI automation and human specialists.

A key implication of the results is the quality of the digital environment, particularly the one that is related

to the massive numbers of already connected devices. According to Pundir and Sandhu (2021), it is important to ensure quality-of-service parameters are considered by machine learning systems to ensure the performance of dynamic networks like wireless sensor systems. They can be propagated to the digital forensics, and more so, in the smart environments where the ever-increasing data creation can overwhelm the traditional tools of forensics. The relative slowness of the analysis time using network-based evidence in this paper underscores the importance of optimizing AI models to handle large volumes of real-time streams of digital data.

Besides the system performance, the psychological and behavioral dimensions of the cybercrime are also a good background. Robbins and Yalch (2025) mention that such characteristics as aggression and psychopathy may be used as the reason behind threat behavior and suggest that technical evidence is not the only weapon that has to be considered during the forensic investigation of a criminal. This can be attributed to the attention that was recently focused on the concept of integrating behavioral analytics into AI-driven forensic technology. The capability of preempting ill motive or identifying crime patterns could be of great use in threat attribution and effectiveness in investigation.

Other emerging researches also show that there is need to have other flexible forensic modalities that are able to work in other frontiers of digital nature. Sabir et al. (2018) demonstrate the examples of how the advanced embedded techniques can conceal or reveal the concealed information within image files and, therefore, demonstrate how the digital evidence may be more complex than it appears on the surface. This underlines the results of the present study regarding discrepancy in accuracy of detection depending on the nature of evidence. The necessity of AI models that can be utilized to handle hidden, manipulated, or steganographic information is an issue at hand in digital forensics.

Another factor influencing the feasibility of the practical application of AI systems is the perception of users and the attitudes of the community towards the acceptance of forensic technologies. Seng et al. (2021) note that individuals remain afraid of such technologies as facial recognition due to the fear of error and bias, and privacy. The implications of such impressions on AI-based digital forensic tools are that they can also undergo similar questioning concerning its transparency, compliance with ethical imperatives, and court admissibility. The poorer performances of the lighter AI models in the present research give reasons to believe that it is essential to make sure that the existing forensic tools can be relied on.

The efforts to standardize AI applications in forensics are also notable in enhancing the rise in reliability. Solanke and Biasiotti (2022) state that the evidence-mining techniques need robust frameworks to gauge the techniques and extract more. The efficiency scores identified in the course of this study suggest that there is necessity to have a standard performance measure that would assist forensic workers to select appropriate AI tools. On the same note, Verma et al. (2023) stress the importance of the systematic adoption of AI to forensic procedures in order to obtain consistency and repeatability in investigations.

On the whole, the discussion has shown that although AI is having a positive impact on digital forensic abilities, there are still issues related to the accuracy, reliability, and ethical integrity. The current findings add to this discussion by showing the subtle performance of different AI models in different forensic situations. Further creation of adaptive, transparent, and standard AI systems will be necessary to further the sphere of digital forensics and stay resilient against the new cyber threats.

Conclusion

This paper has revealed how artificial intelligence has played a significant role in digitally altering the process of forensic digital investigations. Using several AI models to assess different cybercrime cases, the results indicate that the advanced AI models, like convolutional neural networks and support vector machines, are always better than more conventional and less advanced models. Their greater accuracy, quicker processing duration, and better success rate are some of the reasons why they are suitable for analyzing structured and pattern-rich digital evidence. Nevertheless, the drop in performance seen in scenarios with unstructured data, like network traffic, is a negative sign that AI systems are yet to be deployed in complex and ambiguous scenarios. The mentioned challenges highlight the importance of more adaptive and resilient AI models that can handle various forms of evidence at the same time and ensure transparency and reliability. Moreover, the paper has indicated the need of merging AI and human skills to encourage forensic competence and admissibility. Forensic tools that use AI will salvage efficiency during an investigation, facilitate decision-making, and enhance cybersecurity resilience due to the ever-changing cyber threats. Overall, the study proves that AI is not to be introduced to the digital forensics, but, instead, it is a necessary aspect of the contemporary digital world and will continue on determining the future of cybercrime investigation.

References

1. Baroto, W. A. (2024). Advancing Digital Forensic through Machine Learning: An Integrated Framework for Fraud Investigation. *Asia Pacific Fraud Journal*, *9*(1), 1-16.
2. Belshaw, S., & Nodeland, B. (2022). Digital evidence experts in the law enforcement community: understanding the use of forensics examiners by police agencies. *Security Journal*, *35*(1), 248-262.
3. Buquerin, K. K. G., Corbett, C., & Hof, H. J. (2021). A generalized approach to automotive forensics. *Forensic Science International: Digital Investigation*, *36*, 301111.
4. Chen, G., Ding, L., Du, J., Zhou, G., Qin, P., Chen, G., & Liu, Q. (2018). Trust Evaluation Strategy for Single Sign-on Solution in Cloud. *International Journal of Digital Crime and Forensics (IJDCF)*, *10*(1), 1-11.

5. Demisse, G. G., Aouada, D., & Ottersten, B. (2018). Deformation-based 3D facial expression representation. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, *14*(1s), 1-22.
6. Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, *48*, 301675.
7. Faehndrich, J., Honekamp, W., Povalej, R., Rittelmeier, H., Berner, S., & Labudde, D. (2023). Digital forensics and strong AI: A structured literature review. *Forensic Science International: Digital Investigation*, *46*, 301617.
8. Fakiha, B. (2023). Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification. *International Journal of Safety & Security Engineering*, *13*(4).
9. Jarrett, A., & Choo, K. K. R. (2021). The impact of automation and artificial intelligence on digital forensics. *Wiley Interdisciplinary Reviews: Forensic Science*, *3*(6), e1418.
10. Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic science international*, *362*, 112133.
11. Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*, *92*, 101762.
12. MohanRaj Alenezi, A. (2023). Digital Forensics in the Age of Smart Environments: A Survey of Recent Advancements and Challenges. *arXiv e-prints*, arXiv-2305.
13. Muñoz, A. V. (2023). AI in the Crosshairs: Advancing Cybersecurity and Digital Forensics in the Era of Intelligent Threats.
14. Nayerifard, T., Amintoosi, H., Bafghi, A. G., & Dehghantanha, A. (2023). Machine learning in digital forensics: a systematic literature review. *arXiv preprint arXiv:2306.04965*.
15. Pundir, M., & Sandhu, J. K. (2021). A systematic review of quality of service in wireless sensor networks using machine learning: Recent trend and future vision. *Journal of Network and Computer Applications*, *188*, 103084.
16. Robbins, A. L., & Yalch, M. M. (2025). The hierarchical structure of psychopathy and the prediction of aggression. *Journal of Threat Assessment and Management*.
17. Sabir, M. F., Jones, J. H., Liu, H., & Mbaziira, A. V. (2018, March). A non-algorithmic forensic approach for hiding data in image files. In *Proceedings of the 2Nd International Conference on Compute and Data Analysis* (pp. 60-64).
18. Seng, S., Al-Ameen, M. N., & Wright, M. (2021). A first look into users' perceptions of facial recognition in the physical world. *Computers & Security*, *105*, 102227.
19. Solanke, A. A., & Biasiotti, M. A. (2022). Digital forensics AI: evaluating, standardizing and optimizing digital evidence mining techniques. *KI-Künstliche Intelligenz*, *36*(2), 143-161.
20. Verma, R., Garg, S., Kumar, K., Gupta, G., Salehi, W., Pareek, P. K., & Kniežova, J. (2023, February). New Approach of artificial intelligence in digital forensic investigation: a literature review. In *International Conference on Advances in Communication Technology and Computer Engineering* (pp. 399-409). Cham: Springer Nature Switzerland.