International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 03-11-2023, Accepted: 18-11-2023, Published: 04-12-2023
Volume 5, Issue 4, 2023, Page No. 121-123

Role of Artificial Intelligence (AI) in Digital Forensic

Monika Khindre[1], Deepti Monga[2]
[1] Department of Law, University Institute of Legal Studies, Chandigarh University, Gharuan, Mohali, Punjab, India
[2] Professor, Department of Law, University Institute of Legal Studies, Chandigarh University, Gharuan, Mohali, Punjab, India

Abstract
The emergence of the digital age has thrust the discipline of digital forensics into the forefront of investigative techniques, necessitating the development of creative methods to handle the quantity and complexity of digital data. This piece examines how the field of digital forensics is developing and how AI is revolutionizing the way that investigations are conducted. The research described the foundations of digital forensics and emphasizing how important they are to both criminal and civil investigations. After recognizing the shortcomings of conventional methods, it goes over the fundamentals of AI and some of its uses that are pertinent to digital forensics. An extensive investigation is conducted on the incorporation of AI in digital forensics, encompassing automated data gathering, predictive analysis, and threat intelligence powered by AI. The study examines the many advantages which AI offers the industry, including improved speed, efficiency, and data handling capabilities. But conducting this research also means overcoming ethical issues and difficulties, such as privacy concerns and prejudice in AI algorithms.

Keywords: Digital forensics, artificial intelligence, cybersecurity, machine learning, automated analysis, ethical considerations, privacy concerns

Introduction

An essential part of forensic science is digital forensics, which is a complex procedure that involves the methodical examination of digital devices, networks, and electronic systems. This broad field seeks to systematically collect, store, and examine digital evidence in order to unearth information that is essential for looking into and combating fraud, cybercrimes, and other forms of digital misconduct. Due to the increasing reliance on digital platforms for communication, financial transactions, and information storage, the importance of digital forensics in today's technological world has increased to an unprecedented degree. The extent and complexity of possible cyber threats and criminal activity have unavoidably increased as a result of this rise, which emphasizes the urgent need for skilled digital forensic investigators who can handle digital evidence effectively and efficiently.

The introduction of AI is now causing a revolutionary change in the ever-evolving field of digital forensics. With its ability to learn and solve problems like human intellect, AI has the potential to completely change the way digital forensics are conducted. The way investigators handle digital evidence has changed dramatically as a result of this integration, which not only solves the difficulties brought on by the sheer amount and complexity of digital data but also greatly improves the efficiency and precision of investigative procedures. It is becoming more and more clear as we examine the complex interplay between AI and digital forensics that this combination holds the key to opening up previously unheard-of opportunities for threat mitigation and cyber investigation. When AI enters the field of digital forensics, it brings with it a dynamic element where data analysis tools, machine learning algorithms, and pattern recognition collaborate to navigate the complex digital terrain. AI enables investigators to concentrate their skills on more complex facets of digital evidence examination by automating repetitive activities and analyzing enormous information quickly. This speeds up investigations and makes it possible to look more closely at possible dangers and harmful activity. Furthermore, AI-driven solutions for digital forensics show a capacity for adaptation and evolution, enhancing their analytical powers with each inquiry through feedback and experience. Because of its adaptability, AI is positioned as a powerful ally in the never-ending game of cat and mouse between law enforcement and cybercriminals, offering a pre-emptive defence against constantly changing digital threats. There are difficulties and moral issues with integrating AI into digital forensics. Ensuring privacy rights are protected, ethical data management procedures are necessary, and AI algorithms must be visible and accountable. A crucial component of this developing discipline is maintaining a balance between protecting human rights and utilizing AI's ability for effective investigations.

Fundamentals & Challenges into Digital Forensics

Computer forensics, or digital forensics, is the use of investigative methods to gather, examine, and store electronic evidence so that it may be used in future court cases without compromising its integrity. In order to find, analyse, and record instances of digital crimes, it includes examining digital devices, networks, and electronic systems. Digital forensics covers a wide range of areas, such as business investigations, intelligence collection, and cybercrime, among others. In both criminal and civil matters, digital forensics is essential and has a big impact on how things turn out in court. It provides vital evidence to prove guilt in criminal situations, assisting law enforcement in locating and apprehending cybercriminals. Digital forensics is essential in civil proceedings to settle conflicts, support allegations, and guarantee the accuracy of digital evidence used in court. Modern civilization is heavily

dependent on digital technology, which emphasizes how crucial digital forensics are to preserving the credibility and integrity of the judicial system.[1]

The enormous amount and complexity of digital data is one of the main obstacles to traditional digital forensics. The exponential expansion of digital information has left investigators with the difficult challenge of sorting through massive volumes of data in order to find pertinent evidence. The complexity is further increased by the sheer variety of data sources, which includes cloud services, IoT devices, and smartphones. As a result, forensic specialists must continually adjust to the rapidly changing digital world. Conventional digital forensics procedures take a lot of time and include carefully inspecting and analyzing digital evidence. Timeliness for investigations can be extended by the labour-intensive process of manually extracting and analyzing data from storage devices. More effective and simplified digital forensic techniques are desperately needed as the requirement for quick reactions to cyber events and court cases grows. The ever-changing and dynamic landscape of cyber threats presents a constant challenge for professionals in the field of digital forensics. Because cybercriminals are fast to adapt and use complex strategies to hide their actions, forensic investigators must keep up with the most recent advancements in cybersecurity. The use of encryption, anonymization software, and other obfuscation techniques has increased, making it more difficult to identify and attribute digital crimes, necessitating the development of new techniques and equipment in the field of digital forensics.

Integration of AI in Digital Forensics

The goal of the multidisciplinary computer science discipline of AI is to build machines that can emulate human intellect. Fundamentally, AI aims to provide robots the capacity to learn from mistakes, adjust to shifting inputs, and carry out operations that normally demand for human intellect. AI is essentially defined by its ability to interpret data, make sense of complicated situations, and solve problems. A key component of AI is machine learning ML, which offers statistical models and algorithms that enable systems to learn from experience and get better over time without the need for explicit programming. Machine learning algorithms identify patterns, generate predictions, and improve their performance repeatedly over time by analyzing large datasets. In order to handle the dynamic and complex nature of digital forensics, where standard rule-based systems frequently fall short, this adaptive learning process is essential.

By tackling the inherent issues connected with data analysis and threat detection, AI is revolutionizing the field of digital forensics. This integration is complex and includes a number of elements that improve the effectiveness of forensic investigations.

1. Automated Data Collection and Analysis

Any digital forensic investigation begins with the massive and complex work of data triage, in which AI techniques are essential. By using machine learning techniques, automated systems may quickly classify and rank data according to relevance, saving a great deal of time and effort compared to the manual process of going through enormous datasets. This procedure expedites further research, guaranteeing that forensic specialists concentrate on the most relevant data as soon as possible.

Log files, which are frequently large and intricate, hold priceless records of digital activity. AI-driven log file analysis tools are highly skilled at interpreting patterns found in these logs, allowing investigators to reconstruct events, spot anomalies, and create timelines with previously unheardof speed and accuracy. AI's capacity to identify minute patterns and correlations in log data improves the precision of research endeavours and produces more solid and trustworthy findings.

2. Predictive Analysis in Digital Forensics

Digital forensics' mainstay, behavioural analysis, is another area where AI excels. Forensic investigators can create profiles of normal user behaviour by utilizing machine learning techniques. This makes it easier to identify deviations or inconsistencies that could indicate malicious activity. By identifying patterns that point to unusual or suspect behaviour, this predictive feature of AI helps identify possible risks in advance and allows for pre-emptive action before things get out of hand.

In digital forensics, AI systems' capacity to identify complex patterns in large datasets is critical. Algorithms that recognize patterns are excellent at spotting patterns and irregularities, which helps investigators put disparate pieces of evidence together. forensic specialists may gain a full and nuanced picture of the digital world with the use of AI's pattern recognition skills, which can be used to identify the tactics used in cyber-attacks or to find subtle correlations between seemingly unconnected data sources.

3. AI-Driven Threat Intelligence

In the never-ending cybersecurity game, AI steps up as a proactive sentinel. AIdriven threat intelligence technologies are able to anticipate possible attacks and weaknesses by continually evaluating changing threat landscapes and learning from previous instances. By taking a proactive approach, digital forensic specialists may strengthen defences in advance, reducing risks and the effect of cyberattacks before they materialize.[2] One of the most important aspects of AIdriven threat intelligence is anomaly detection, which is the process of identifying departures from the norm. AI systems are highly skilled at identifying anomalous activity that might indicate a security breach through the analysis of enormous datasets and real-time surveillance. Digital forensics professionals may increase the resilience of digital infrastructures by quickly detecting abnormalities, tracing the cause of irregularities, and putting preventive measures in place.

Benefits of AI in Digital Forensics

AI brings a host of benefits to the field of digital forensics that greatly increase the effectiveness of investigation procedures. Digital forensic investigations are undergoing a transformation thanks in large part to AI-driven tools and algorithms, which greatly increase speed and efficiency. Unlike conventional approaches, which can need time consuming manual analysis of large datasets, AI algorithms are excellent at quickly scanning and classifying data, which speeds up the early stages of investigations. This quicker speed is essential because it allows investigators to stay up to date with the always changing world of digital evidence, especially given how quickly cyber dangers are emerging. AI in digital forensics leads to a notable increase in analytical precision and accuracy. Machine learning

algorithms are able to identify complex patterns, irregularities, and relationships in datasets that are not visible to human observers. This improved degree of precision boosts the dependability of digital evidence offered in court by speeding up investigations and reducing the margin of error in conclusions. The capacity of AI to identify minute details results in forensic findings that are more reliable and comprehensive, which represents a major improvement in investigation capacities.

The sheer amount of data that investigators in digital forensics have to go through is one of the toughest obstacles. AI meets this difficulty by being exceptionally good at handling and processing large datasets, which makes it possible for investigators to quickly sort through large amounts of data. Investigators are freed up to focus on crucial elements of the case, since automated data triage and classification expedites the identification of pertinent evidence. With the exponential

development of data production in today's digital ecosystem, this competence becomes increasingly important for effective information extraction. Advanced technologies are needed.

AI integration speeds up investigations and makes it easier for digital forensics to monitor and respond in real time. AI systems keep a close eye on network activity, identify irregularities, and instantly notify investigators of any security problems in real time. By taking a proactive stance, forensic teams may react quickly to new threats, minimizing potential harm and protecting digital environments. AI enhances the conventionally reactive character of forensic operations by transforming digital investigations into dynamic and adaptable processes by offering a continuous monitoring system. The discipline is undergoing a paradigm change with the combination of AI with digital forensics, which will improve the overall effectiveness and responsiveness of investigation procedures in the constantly changing realm of cyber threats.

Challenges and Ethical Considerations

The application of AI to digital forensics raises the possibility of algorithmic bias, in which the underlying models unintentionally reinforce or magnify preconceptions found in the training data. Biased algorithms may unfairly target particular populations or demographics in the context of digital forensics, which might result in false charges. It is crucial to identify and reduce prejudice in order to guarantee the objectivity and justice of analysis powered by AI. This calls for constant oversight, improvement, and openness in the creation and application of AI algorithms, with an emphasis on getting rid of any biases.

Because digital forensics by its very nature examines personal data, there are serious privacy problems. When AI algorithms are used on large datasets, the privacy of people who are being investigated may unintentionally be compromised. It's difficult to strike a compromise between the need to find digital evidence and protecting people's privacy. Encryption, safe data processing procedures, privacypreserving strategies, and strict adherence to legal and ethical requirements all become critical. Digital forensic professionals need to exercise caution when navigating this ethical terrain in order to protect the privacy and rights of those who are engaged.

In digital forensics, interpretability and explain-ability are challenged by the innate complexity of AI systems. Forensic analysts, lawyers, and the impacted parties need to know how conclusions were arrived at when AI systems produce insights or make choices. Lack of openness can breed suspicion and mistrust, which will impede the field's acceptance and use of AI. Creating AI models with integrated interpretability characteristics is one way to tackle this difficulty and help practitioners understand and verify the decision-making process. In the field of digital forensics, working toward explainable AI not only improves accountability but also makes it easier for human specialists and AI systems to work together productively.

Conclusion

The field of cyber investigations has changed as a result of AI's incorporation into digital forensics. AI has developed into a vital tool for forensic experts, capable of automating repetitive operations and offering sophisticated analytical solutions. The efficiency of digital forensic procedures has been greatly enhanced by its ability to quicken the pace of investigations and deepen analysis. The application of AI in digital forensics is still in its early stages. AI tools' capabilities will grow as technology does. A dynamic approach is required due to the constant evolution, which encourages professionals to keep up to date on developing technologies, processes, and best practices. Being adaptive and flexible will be essential as the profession develops and encounters new difficulties.

The use of AI in digital forensics is expected to lead to ground-breaking developments as long as technology keeps advancing. Machine learning's subset, deep learning, is anticipated to be crucial. Digital forensic investigations will be increasingly accurate and efficient when more complex algorithms with contextual analysis and subtle pattern recognition capabilities are developed. Furthermore, the range of data that can be studied will increase with the integration of computer vision and natural language processing into AI technologies. This will allow researchers to glean insights from unstructured data sources and multimedia material.

References

1. Abiodun A. Solanke & Maria Angela
2. Biasiotti, "Digital Forensics AI: Evaluating, Standardizing and Optimizing Digital Evidence Mining Techniques"36, *KI - Künstliche Intelligenz*, 143 (2022).
3. Antonis Mouhtaropoulos; Chang-Tsun
4. Li; Marthie Grobler, "Digital Forensic
5. Readiness: Are We There Yet," 9, *Journal of International Commercial Law and Technology*, 173 (2014).
6. Faye Mitchell, "The Use of Artificial Intelligence in Digital Forensics: An
7. Introduction," 7, *Digital Evidence and Electronic Signature Law Review*, 35 (2010).
8. Luke Stark; Jevan Hutson,
9. "Physiognomic Artificial Intelligence," 32, *Fordham Intellectual Property,*
10. *Media & Entertainment Law Journal*, 922 (2022).
11. *The Role of Machine Learning in Digital Forensics*, 2020 8th
12. International Symposium on Digital Forensics and Security (ISDFS), Held on June 2020, *available at* <
13. http://dx.doi.org/10.1109/ISDFS49300 .2020.9116298> (last visited on November 26, 2023).