YourLawArticle

Open Access Law Journal, ISSN (O): 3049-0057

Editor-in-Chief – Prof. (Dr.) Amit Kashyap; Publisher – Reet Parihar

Cyber Forensics With Artificial Intelligence: A Better Tool Of Investigation

Devesh Pandey, B.A.LL.B, Galgotias University

&

Shashwat Kumar Jha, B.A.LL.B, Galgotias University

Published on: 1st June 2024

Abstract

The Digital world is welcoming the new generation with ever-developing advanced technology and enhanced network connectivity. On one hand, individuals are getting involved in eh cyber world without much filter; on the other hand, the other side of the coin is also functioning effectively, i.e., cybercrimes. When the technology was not so advanced the most of the crimes were physical that could be detected and tackled by law enforcement agencies in effective ways, but with network enhancement and an increased amount of cybercrimes, law enforcement agencies have to get themselves updated every moment to tackle them. As per the reports, by 2020, 80% of adults on Earth will have a smartphone.[1]. On the other hand, to date, 49.7% of the total population is connected to the Internet, with a growth of 936% from 2000-2017[2]. Biggest worry for cybersecurity professionals. It is predicted that the projected costs of cyber-crimes will reach $2 trillion by 2019[3]. It is also observed that more than half of the firms – around 57% – have experienced a cyber-attack in the past year.[4]. These reports themselves suggest the requirement of increased and active participation of law agencies and cyber forensics to find out the real culprit and protect the victims. In this paper, the use of artificial intelligence in cyber forensics is discussed to provide an analytical view for this emerging area of forensics.

[1] RSA, *Current State of Cybercrime* (RSA Whitepaper, 2016)
[2] Internet World Stats, *World Internet Users and 2017 Population Stats* http://www.internetworldstats.com/stats.htm accessed 4 December 2024
[3] Steve Morgan, 'Cyber Crime Costs Projected To Reach $2 Trillion by 2019' *Forbes* (17 January 2016) https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/ accessed 4 December 2024
[4] Hiscox, *The Hiscox Cyber Readiness Report - 2017* https://www.hiscoxgroup.com/cyber-readiness accessed 4 December 2024

Keywords: *Cybercrime, Artificial Intelligence, Digital Forensics, Cybersecurity, Online Investigations*

1. INTRODUCTION

Cyber Forensic is a developing technology in the field of law enforcement industry and the merger of artificial intelligence into the same leads to the development of a more prominent tool for better investigation and law enforcement. Artificial intelligence, as the name itself suggests the generated intelligence which is developed with the information saved and provided to the computer, based on which it analyses the information and provides the desired results. In an era of massive cyber connectivity, cybersecurity has become a top priority for the security of the data, infrastructure and systems against cyberattacks. With the increasing adoption of cyber technologies by organisations to run their business, the impacts of cybercrime have gone deeper to imply losses, brand damage, and security issues. Not only cyber security issues but the increasing rate of crimes in different parts of the world, with the increasing cyberspace, requires the enrichment of the law enforcement agencies to be very active and particular in this field. To tackle this problem with an advanced system of merging artificial intelligence with cybersecurity and cyber forensics is beneficial for agencies as well as for society.

Manual investigation procedures are labour-intensive, time-consuming, and they are prone to human error, which impedes fast and appropriate organizations response to cybersecurity incidents in real time. In addition, the amount and complexity of data created in these cyber environments enlarge the gap between rational thinking and high-tech capabilities of human analysts, which can lead to delayed responses and/or inability to attribute cyber threats. Such technology is urgently required to tackle the problem of rising cybercrimes, as forensic systems develop at the pace of constantly changing cyber threats, as well as in other crime investigations. Through the application of AI advancements such as machine learning, natural language processing, and anomaly detection, organisations can significantly boost the effectiveness, accuracy, and scalability of investigations. This approach proves invaluable not just in cybersecurity incidents but also in a wide range of other investigative scenarios.

1.1 RESEARCH OBJECTIVE:

- To identify the scope of artificial intelligence in cyber forensics in the field of investigation.
- To identify the role of AI in investigation.
- To identify the applications of AI and cyber-forensics in investigations.

1.2 HYPOTHESIS:

AI is the technology which provides results by processing data stored and provided to the computer, and the result provided is obtained from that limited resource only. It does not include other resources on its own until commanded to do so by human intervention, leading to confined research and investigation.

1.3 RESEARCH QUESTION:

1.3.1 Whether the AI can be utilised in other fields of investigation than in cyber-related crimes?

1.3.2 Whether the investigation with AI can lead to more accurate results?

1.3.3 Can AI pose some challenges in the process of the investigation?

1.4 LIMITATION OF RESEARCH:

AI is the technology which provides results by processing data stored and provided to the computer, and the result obtained is obtained from that resource only, whereas the process of the investigation requires the expansion of the research area to unfold the truth and identification of the real culprit. This paper is limited for academic purposes, and the area of research is limited to the territorial boundaries of Bharat, i.e., India.

1.5 LITERATURE REVIEW:

1.5.1 The paper titled "Artificial Intelligence Based Cyber Forensic Framework" by Parag H. Rughani, Ph.D., IFS, from Gujarat Forensic Sciences University, highlights the growing concern of cybercrimes alongside the rise in internet and smartphone usage. It points out that the current resources, including manpower, are insufficient to keep up with the increasing rate of cybercrime. Existing tools and technologies rely heavily on human interaction, which significantly hampers the speed of investigations. To address this, the paper proposes a framework that incorporates Artificial Intelligence to optimise the performance and speed of cyber forensic tools. This AI-based framework minimises human involvement by automating most routine tasks through intelligence learned from training. However, the paper focuses solely on the process and does not delve into detailed applications or the challenges involved.[5]

1.5.2 The paper titled "Artificial Intelligence in Forensic Science," authored by Siddhant Gupta, Mrs. Vinny Sharma, and Dr. Prashant Johri from Galgotias University, explores how forensic

[5] ResearchGate, *ARTIFICIAL INTELLIGENCE BASED CYBER FORENSICS FRAMEWORK* https://www.researchgate.net/publication/320758716_ARTIFICIAL_INTELLIGENCE_BASED_CYBER_FORENSICS_FRAMEWORK accessed 4 December 2024

science techniques can be enhanced and expanded by integrating modern and emerging technologies, particularly Artificial Intelligence (AI). The authors discuss the current and potential future applications of AI across various branches of forensic science, emphasising how these advancements could revolutionise the field by improving its scope and effectiveness.[6]

1.5.3 The paper titled "A Pioneering Approach to Forensic Insight: Utilisation of AI for Cyber Security Incident Investigation," authored by Venkateshwara Naidu Kolluri, explores innovative strategies for enhancing cybersecurity investigations through the strategic application of Artificial Intelligence (AI). It highlights how traditional forensic analysis methods are struggling to keep up with the rapid pace and increasing frequency of cyberattacks. These conventional techniques fall short in promptly and effectively identifying, isolating, and analysing cybercrime. By harnessing the power of AI, particularly machine learning, natural language processing, and anomaly detection, investigations can be significantly strengthened and streamlined. The research in this paper is specifically focused on the context of the United States.[7]

1.5.4 The paper titled "AI-Driven Cyber Forensics," authored by Rohit Tahsildar Yadav from MIT ADT University, delves into the transformative role of Artificial Intelligence (AI) in the field of cyber forensics. With the increasing complexity of cyber threats and the growing volume of cyber data, AI integration has become a pivotal advancement. This paper offers a thorough examination of how AI is revolutionising cyber forensics, analysing its key roles, benefits, and the challenges it presents in this rapidly evolving domain.[8]

1.6 RESEARCH METHODOLOGY:

DATA COLLECTION: The data is collected from primary as well as secondary sources, including the quantitative and qualitative methods.

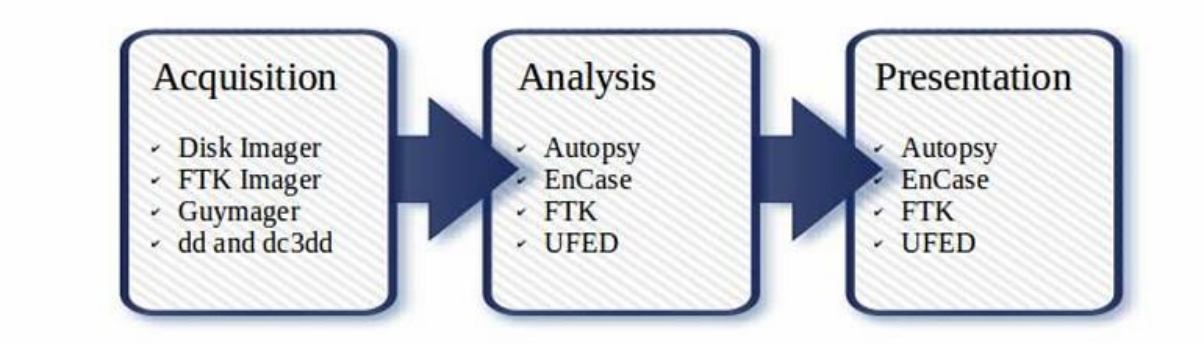
The method resorted fort here search together with the material for the paper is a doctrinal type involving analytical as well as descriptive study. The paper is based on secondary informative resources and data, including various journals and articles, in order to arrive at a precise conclusion.

[6]Siddhant Gupta, Vinny Sharma and Prashant Johri, 'Artificial Intelligence in Forensic Science' (Galgotias University)
[7]ResearchGate, *A Pioneering Approach to Forensic Insights Utilization: AI for Cybersecurity Incident Investigations* https://www.researchgate.net/publication/380729744_A_PIONEERING_APPROACH_TO_FORENSIC_INSIGHTS_UTILIZATION_AI_FOR_CYBERSECURITY_INCIDENT_INVESTIGATIONS accessed 4 December 2024
[8]IJSRET, 'Artificial Intelligence Based Digital Forensics Framework' https://ijsret.com/wp-content/uploads/2024/07/IJSRET_V10_issue4_353.pdf accessed 4 December 2024)

PROCESS OF THE USE OF CYBER FORENSICS WITH ARTIFICIAL INTELLIGENCE

According to the Oxford definition, forensics refers to "scientific tests or techniques used in connection with the detection of crime." When these scientific methods, particularly computer-based techniques, are applied to investigate cybercrimes, it is known as Cyber Forensics. In broader terms, cyber forensics involves the tools and methods used to address cybercrimes, typically consisting of three key stages: Acquisition, Analysis, and Presentation.

A wide range of both commercial and free tools is available for conducting digital forensics. Notable examples include EnCase, FTK, UFED, Nuix, IEF, Autopsy, and XRY, which are widely recognised and trusted in the field. The reports generated by these tools are often accepted as valid evidence in courts across many countries around the world.



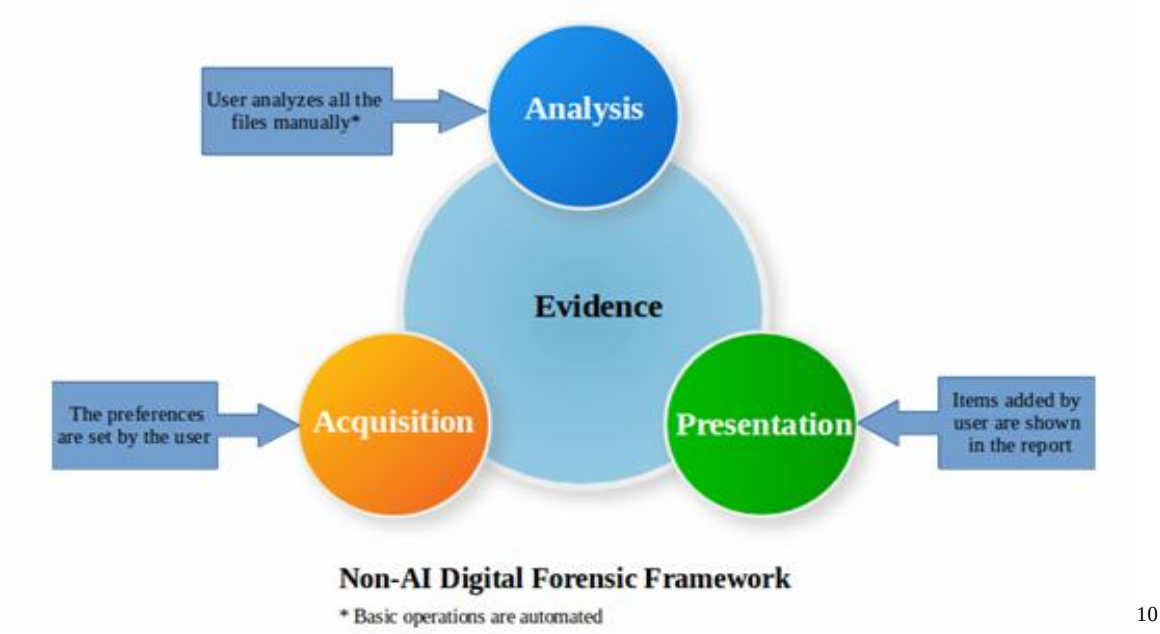
These tools offer user-friendly graphical interfaces (GUIs) and enable high-speed analysis. Key features of many of these digital forensics tools include custom filters, advanced reporting capabilities, and data carving. Additionally, they have been designed to automate certain processes. However, full automation is not yet realised, as user input is often still required to complete specific tasks.

In a traditional non-AI digital forensic investigation, the process begins with the acquisition of data, during which the user manually sets up preferences. Following this, the acquired files are analysed manually, and based on the results of this analysis, the relevant data is presented. The final step involves the preparation of a comprehensive report detailing the findings.[9]

The lack of intelligence in current digital forensics tools results in investigators having to perform repetitive and time-consuming tasks, even when handling identical evidence and cases. Another major limitation is the reliance on the user during the analysis phase. While these tools are highly capable and equipped with automation features—such as identifying broken files, detecting invalid

[9]Parag H. Rughani, *Artificial Intelligence Based Digital Forensics Framework* (IFS, Gujarat Forensic Sciences University, Gandhinagar, Gujarat – India)

file signatures, recovering files from unallocated space, retrieving deleted files, and categorizing data like multimedia files, logs, internet artifacts, and emails—they still require the user to thoroughly inspect every part of the evidence to identify relevant files and include them in the final report. Although each case is unique and criminals often employ different methods, reducing the investigator's workload by narrowing down the number of files to review, from thousands to a handful, would significantly improve both the speed and efficiency of the process. While user involvement cannot be fully eliminated, such a reduction would be invaluable in enhancing productivity.



[10]

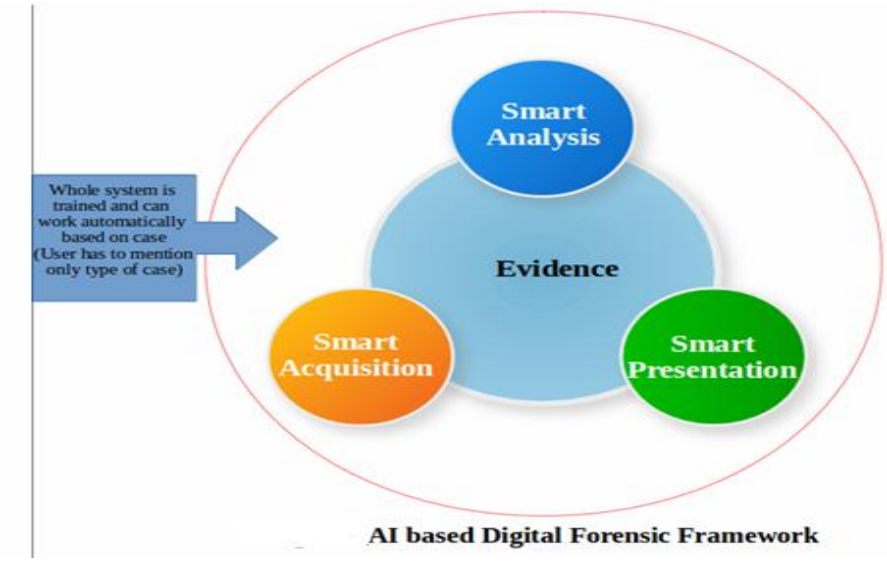
The AI-based Cyber Forensic Investigation framework is designed as an all-in-one solution for the entire digital forensic process, handling the three critical steps—acquisition, analysis, and presentation. While most existing forensic tools support these steps, they lack the intelligent capabilities that the proposed framework incorporates. The system is built on well-established AI and machine learning techniques, where it is trained using existing datasets. These datasets enable the system to understand how to make decisions based on different situations, enhancing its ability to perform effectively.

In this AI-driven framework, the investigator only needs to input the case name, and the system, utilising artificial intelligence, can automatically generate a comprehensive report from the data gathered across various branches of the investigation. For example, in the case of a threatening email—one of the most common cybercrimes—an investigator would typically file a case after

[10] *Ibid.*

receiving such an email. If a traditional, non-AI tool is used, the investigator would create a disk image from the storage device, often involving an entire 1 TB hard drive. This process is time-consuming and inefficient, as not all data on the disk is relevant to the case. The image would then need to be analysed, which could involve sifting through a massive amount of irrelevant data, like multimedia files or installed software.

In contrast, with the proposed AI-based framework, the acquisition tool would be trained on similar cases, making it an "experienced" tool capable of identifying the relevant data, such as the email in question, without needing to analyse the entire disk. By focusing only on the data pertinent to the case, such as email records, and ignoring unrelated data like multimedia files, the system significantly speeds up the process, allowing the investigator to quickly extract and present the necessary information.



APPLICATIONS OF AI WITH CYBER FORENSIC INVESTIGATION

Artificial Intelligence holds the potential to address challenges that experts have faced for decades. While forensic science plays a crucial role in uncovering information from crime scenes to clarify judgments and identify perpetrators, much of the work still relies on human effort. Humans, however, are prone to delays and errors during the investigative process. By integrating AI into forensic operations, the process can be expedited, streamlined, and made more accurate, significantly reducing the possibility of mistakes and enhancing the overall efficiency of investigations.

3.1 Crime Scene Reconstruction:

This system requires inputs such as the presence of specific objects at the crime scene, like a dead body or an object such as a broken glass. After analysing each aspect of the input data, the system can autonomously generate 3 to 4 animated videos, offering significant advantages over the current manual methods used to construct crime scene animations. Crime scene reconstruction is a critical

part of investigations, and in many criminal cases, there have been instances where suspects attempt to escape custody while being transported to the scene. The proposed AI tool could help mitigate such risks by providing realistic simulations that reduce the likelihood of dangerous encounters between suspects and law enforcement during the crime scene reconstruction process. This technology would enable more controlled and secure investigations, minimising the chances of risky situations arising.[11]

3.2 Data Acquisition & Recovery Purposes:

Cyber Forensic Experts often face a significant challenge when analysing files, particularly in determining which files are important, since this can only be decided after opening and inspecting the contents of each file. Another complication arises when a suspect changes the file extension, such as from .doc to .exe, making the task even more cumbersome. To address these issues, an Artificial Neural Network (ANN) can be employed to internally analyse the files and automatically display only the relevant content to the cyber expert. This approach streamlines the process, saving time and effort while ensuring that experts focus solely on the critical data.

3.3 Cyber Forensics:

In cybercrimes committed over the internet, Artificial Neural Networks (ANN) can be incredibly valuable. They can track and analyse the activities of web users, distinguishing between legal and illegal actions. For instance, it can identify when a user is employing proxy servers or generating suspicious amounts of traffic to potentially breach a server. In investigations involving phone call tracing and other activities, law enforcement and forensic experts often face political challenges that complicate the process. To address this, ANN can use its pattern recognition capabilities, along with remote sensing and satellite technology, to determine which phone calls warrant tracing and which do not. This intelligent system would help navigate the political complexities and streamline the decision-making process, ensuring that resources are used effectively and ethically.[12]

3.4 Data analysis:

Digital forensics is a rapidly evolving field that requires the analysis of vast and constantly changing data sets. Artificial Intelligence (AI) offers a powerful approach for managing and processing this complex data. For instance, AI can perform a meta-analysis of metadata collected from various

[11]Bruno W.-P. Hoelz, Célia G. Ralha and Rajiv Geeverghese, 'Artificial Intelligence Applied to Computer Forensics' in *Proceedings of the 2009 ACM Symposium on Applied Computing* (ACM, Honolulu, Hawaii, 2009) 883–888.
[12] Philip Turner, 'Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags)' (2005) 2(3) *Digital Investigation* 223–228

sources, aggregating and simplifying it to make sense of intricate and extensive data. This process allows for the transformation of large amounts of data into a more digestible and comprehensible format, enabling forensic experts to work more efficiently and effectively in a shorter time frame.[13]

3.5 Pattern recognition:

A fundamental aspect of forensic science is detecting patterns and trends within large data sets, which relies on solid evidence and probabilistic reasoning. Artificial Intelligence (AI) can significantly enhance the ability to identify these trends in complex data. AI can, for example, recognise various forms of items or interpret how humans understand knowledge. This might involve analysing image patterns, where algorithms attempt to identify distinct sections of an image or specific individuals. Similarly, AI can be used to detect patterns in textual data, such as email messages or audio recordings. Pattern recognition techniques strive to adapt to diverse data types, aiming for high accuracy in identifying meaningful patterns. Achieving this in practice, however, can be challenging, even when using machine learning or AI techniques. In these applications, AI can play a crucial role in minimising the occurrence of false positives or false negatives, ultimately improving the reliability and precision of forensic investigations.[14]

3.5 Improving contact among all investigating team members:

Forensic investigations require collaboration among various professionals, including forensic statisticians, attorneys, police investigators, and others. Miscommunication or lack of coordination between these parties can lead to incorrect decisions, misinterpretation of data, and ultimately, delays or inaccuracies in the pursuit of justice. Artificial Intelligence can play a pivotal role in bridging this gap by facilitating clearer communication and coordination between stakeholders. Through AI-driven systems, information can be streamlined and analysed more efficiently, ensuring that all parties are aligned, reducing the risk of errors, and enhancing the overall effectiveness of the investigative process.

3.6 Creating Repositories:

Artificial Intelligence can play a crucial role in creating an electronic archive that stores all forensic digital operations, records, assets, and reports. With the rapid expansion of storage capacities through devices like USB drives, hard drives, optical media, and flash drives, which can now hold vast

[13]DA Duce, FR Mitchell and P Turner, 'Digital Forensics: Challenges and Opportunities' in J Haggerty and M Merabti (eds), *ACSF 2007: Proceedings of the 2nd Conference on Advances in Computer Security and Forensics* (School of Computing & Mathematical Sciences, Liverpool John Moores University, UK, 2007).
[14]CM Bishop, *Neural Networks for Pattern Recognition* (Oxford University Press 1995).

amounts of data, it has become increasingly difficult for forensic researchers to manage and analyse this information. AI can serve as an effective tool for organising, interpreting, and utilising such large data volumes, providing a reliable resource for legal purposes. By automating data storage and analysis, AI can streamline the process, making it more efficient and manageable for forensic professionals.

CHALLENGES AND CONCLUSION

4.1 CHALLENGES

While integrating Artificial Intelligence (AI) into digital forensics brings a host of advantages, it also introduces a range of challenges that must be tackled to unlock its full potential. These challenges span across technical, ethical, and practical domains, each influencing the accuracy, efficiency, and trustworthiness of AI-driven forensic systems. Addressing these obstacles is critical to ensuring that such systems can operate effectively and reliably in real-world forensic applications.

4.1.1 Bias and Fairness:

A significant concern in applying AI to digital forensics is the risk of bias in algorithmic decision-making. Since AI systems learn from the data they are trained on, any inherent biases in this data can be unintentionally replicated or even magnified by the models. This raises critical questions about fairness and objectivity, potentially affecting the accuracy and equity of forensic investigations. Ensuring unbiased data and implementing safeguards against such biases are essential to maintaining the integrity of AI-driven forensic processes.

4.1.2 Interpretability and Transparency:

AI models, particularly deep learning networks, often operate as "black boxes," with decision-making processes that are difficult for humans to comprehend or interpret. This opacity creates significant challenges in forensic investigations, where transparency and reproducibility are essential. Forensic experts must be able to clearly explain how evidence was analysed and how conclusions were derived to ensure the credibility of AI-generated findings in court and among other stakeholders. The interpretability of AI systems is therefore a critical issue, as it directly impacts the reliability and acceptance of their use in legal and investigative contexts.

4.1.3 Data Privacy and Security:

AI-powered forensic tools rely heavily on analysing vast amounts of data, often including sensitive or personal information. Safeguarding the privacy and security of this data is paramount, particularly in compliance with data protection laws such as the General Data Protection Regulation (GDPR) in

the EU or the California Consumer Privacy Act (CCPA) in the US. Any mishandling or unauthorised access to this information could result in privacy violations and compromise the integrity of forensic investigations. Ensuring strict adherence to these regulations is essential to maintain trust and uphold the credibility of AI-driven forensic practices.

4.1.4 Ethical and Legal Considerations:

The use of AI in digital forensics brings substantial ethical considerations that cannot be overlooked. Concerns surrounding consent, privacy, and the potential misuse of AI technologies highlight the need for a thoughtful and principled approach. The implementation of AI in forensic investigations must be grounded in ethical guidelines to ensure responsible use that respects individual rights and safeguards against abuse. Striking this balance is critical to maintaining public trust and upholding the integrity of forensic practices in the age of AI.[15]

Given the rapid advancement of AI technologies, it is essential to establish specific legislation tailored to address the unique challenges posed by AI systems and their potential repercussions. As AI continues to evolve and integrate into various domains, including digital forensics, it is here to stay, and society must adapt accordingly. Proactive measures, including dedicated legal frameworks, are crucial to prevent potential misuse or mishaps. Such legislation will equip governments to manage AI-related issues effectively, ensuring safety, accountability, and responsible deployment of this transformative technology.

4.2 CONCLUSION:

Artificial Intelligence has proven to be an invaluable asset in the field of investigation, offering innovative pathways to uncover the truth with enhanced clarity. Its results are significantly more accurate and precise compared to those generated manually, making it a game-changer in criminal cases, especially those of a grave nature. AI's ability to save time—a critical factor in such matters—combined with its efficiency in preserving evidence and streamlining related processes, underscores its transformative potential.

While challenges exist, they can be effectively addressed through the active involvement of IT professionals and continuous training programs for law enforcement officers. AI is a cutting-edge technology, and its role in law enforcement should not be limited. Instead, it should be embraced as a powerful tool that can strengthen the pursuit of justice and improve investigative outcomes.

[15]IJSRET, 'Artificial Intelligence Based Digital Forensics Framework' https://ijsret.com/wp-content/uploads/2024/07/IJSRET_V10_issue4_353.pdf accessed 4 December 2024

BIBLIOGRAPHY:

1. https://www.researchgate.net/publication/320758716_ARTIFICIAL_INTELLIGENCE_BASED_CYBER_FORENSICS_FRAMEWORK (last visited: 04.12.2024)
2. Artificial Intelligence in Forensic Science" written by Siddhant Gupta, Mrs. Vinny Sharma, Dr. Prashant Johri of Galgotias University
3. https://www.researchgate.net/publication/380729744_A_PIONEERING_APPROACH_TO_FORENSIC_INSIGHTS_UTILIZATION_AI_FOR_CYBERSECURITY_INCIDENT_INVESTIGATIONS (last visited: 04.12.2024)
4. https://ijsret.com/wp-content/uploads/2024/07/IJSRET_V10_issue4_353.pdf (last visited: 04.12.2024)
5. ARTIFICIAL INTELLIGENCE BASED DIGITAL FORENSICS FRAMEWORK: Parag H. Rughani Ph. D., IFS, Gujarat Forensic Sciences University Gandhinagar, Gujarat – India
6. ARTIFICIAL INTELLIGENCE BASED DIGITAL FORENSICS FRAMEWORK: Parag H. Rughani Ph. D.,IFS, Gujarat Forensic Sciences University Gandhinagar, Gujarat – India
7. ARTIFICIAL INTELLIGENCE BASED DIGITAL FORENSICS FRAMEWORK : Parag H. Rughani Ph. D.,IFS, Gujarat Forensic Sciences University Gandhinagar, Gujarat – India
8. Bruno W.- P. Hoelz, Célia G. Ralha and Rajiv Geeverghese, Artificial Intelligence applied to computer forensics in Proceedings of the 2009 ACM symposium on Applied Computing, Honolulu, Hawaii, (ACM, 2009), pp 883-888.
9. Philip Turner, 'Unification of digital evidence from disparate sources (Digital Evidence Bags)', Digital Investigation (2005) 2(3), pp 223-228.
10. Duce DA, Mitchell FR, Turner P (2007) Digital forensics: challenges and opportunities. In: Haggerty J, Merabti M (Eds.), ACSF 2007: Proceedings of the 2nd Conference on Advances in Computer Security and Forensics, School of Computing & Mathematical Sciences, Liverpool John Moores University, UK.
11. Bishop, C.M. (1995). "Neural Networks for Pattern Recognition", Oxford University Press.
12. https://ijsret.com/wp-content/uploads/2024/07/IJSRET_V10_issue4_353.pdf (last visited: 04.12.2024)