Review Article

Indian Journal of Forensic Odontology
Volume 16 Number 2, July - December 2023
DOI: http://dx.doi.org/10.21088/ijfo.0974.505X.16223.2

Exploring the Global Use of Artificial Intelligence in Forensic Investigations

Debasis Bora[1], Sazida Yasmin[2]

How to cite this article:
Debasis Bora, Sazida Yasmin. Exploring the Global Use of Artificial Intelligence in Forensic Investigations. Ind J Forensic Odontol 2023;16(2):59–62.

Abstract

Widespread adoption, integration and implications of artificial intelligence (AI) in forensic investigations are gaining traction on a global scale. By examining existing literature and case studies, this review elucidates the multifaceted roles AI plays in enhancing forensic processes, ranging from crime scene analysis to digital forensics. This comprehensive review highlights the utilization of AI algorithms for evidence extraction, pattern recognition, and predictive analytics, enabling investigators to streamline workflows and uncover hidden insights from complex data sets. Furthermore, it discusses the ethical and legal considerations surrounding the deployment of AI in forensic contexts, emphasizing the need for transparency, accountability, and safeguards against potential biases. Drawing on references from various jurisdictions, the paper offers insights into the challenges and opportunities associated with integrating AI technologies into forensic practices worldwide. Ultimatelythis review contributes to a deeper understanding of the evolving landscape of AI-driven forensic investigations and underscores the importance of responsible AI implementation in the pursuit of justice.

Keywords: Artificial Intelligence; Forensic; Investigation; Evidence; Tool; Software; Future.

INTRODUCTION

AI Tools in Forensic Investigations[1]

AI tools are increasingly being utilized in forensic investigations to assist in solving crimes and analysing evidence. Here are some specialized essential AI tools commonly used in forensic investigation:

Facial Recognition Technology: This tool helps in identifying suspects or victims by comparing facial features in images or videos with databases of known individuals. Facial recognition technology playsa crucial and critical role in identifying, recognizing criminals and locating missing persons.

Voice Analysis Software: AI-powered voice analysis software can analyse characteristics of a person's voice, such as pitch, tone, and speech patterns, to help identify suspects or verify the authenticity of recordings.

Text Analysis and Natural Language Processing (NLP): Text analysis and NLP tools can analyse

Author's Affiliations: [1]Associate Professor, [2]UG Student, Programme of Forensic Science, Assam down town University, Guwahati 781026, Assam, India.

Corresponding Author: Debasis Bora, Associate Professor, Programme of Forensic Science, Assam down town University, Guwahati 781026, Assam, India.

E-mail: debasis.bora@adtu.in

Received on: 26.03.2024 **Accepted on:** 24.04.2024

© Red Flower Publication Pvt. Ltd.

written documents, emails, chat logs, and other text-based evidence to extract valuable information, identify patterns, or detect linguistic clues that may aid in an investigation.

Digital Forensics Tools: AI-powered digital forensics tools are used to recover, analyse, and interpret data from electronic devices such as computers, smartphones, and storage media. These tools can help investigators uncover deleted files, track digital footprints, and reconstruct digital activities.

Pattern Recognition Algorithms: AI algorithms can analyse large datasets to identify patterns or correlations that may be relevant to a forensic investigation. For example, pattern recognition algorithms can help identify trends in crime data or detect anomalies in financial transactions.

Machine Learning for DNA Analysis: Machine learning algorithms are increasingly being used in DNA analysis to assist forensic scientists in interpreting complex DNA profiles, predicting phenotypic traits from DNA samples, and matching DNA evidence to potential suspects or databases.

DNA analysis assists forensic scientists in interpreting complex DNA profiles, predicting phenotypic traits from DNA samples, and matching DNA evidence to potential suspects or databases.

Predictive Analytics: Predictive analytics tools use AI algorithms to analyse historical data and make predictions about future events or trends. In forensic investigation, predictive analytics can be used to anticipate criminal behaviour, prioritize leads, or allocate resources more effectively.

Geospatial Analysis: AI-powered geospatial analysis tools can analyse location based data, such as GPS coordinates, crime scene locations, or mobile phone tower pings, to map out connections between individuals, events, and locations, aiding investigators in reconstructing timelines and identifying suspects.

Applications of AI in Forensic Investigations[2,3]

Artificial Intelligence (AI) is increasingly being utilized in forensic investigations due to its ability to analyse large volumes of data quickly and accurately, aiding in solving crimes and delivering justice. Here are some detailed applications of AI in forensic investigations:

Facial Recognition: AI-powered facial recognition software can match faces captured in surveillance footage or photographs with existing databases of known individuals, aiding in identifying suspects or victims. This technology has been instrumental in solving cases involving missing persons, human trafficking, and terrorism. For example, Clearview AI's facial recognition technology has been used by law enforcement agencies to identify criminals by comparing images against a vast database of publicly available images.

Voice Analysis: AI algorithms can analyse voice recordings to determine characteristics such as age, gender, and emotional state, and even identify potential suspects based on voice patterns. This technology is used in forensic phonetics, helping in identifying speakers in anonymous calls, deciphering recorded conversations, and providing evidence in criminal investigations.

Digital Forensics: AI tools are employed to analyse digital evidence such as emails, social media posts, chat logs, and file metadata. Natural Language Processing (NLP) algorithms can extract relevant information, detect patterns, and identify potential leads in cybercrime investigations. Tools like Autopsy and EnCase utilize AI techniques to sift through vast amounts of digital data, helping investigators uncover crucial evidence in cases involving cyberattacks, fraud, and intellectual propertytheft.

Crime Prediction and Prevention: Predictive analytics algorithms, powered by AI, analyse historical crime data to identify patterns and predict future criminal activity hotspots. Law enforcement agencies use these insights to allocate resources effectively and prevent crimes before they occur.

Pattern Recognition in Forensic Evidence: AI algorithms are employed to analyse forensic evidence such as fingerprints, DNA sequences, and ballistics to identify patterns and match them to potential suspects or previous criminal cases. Machine learning techniques enable automated analysis of complex forensic data, reducing the time and resources required for manual examination. For example, AI-powered fingerprint analysis systems like AFIS (Automated Fingerprint Identification System) compare latent prints found at crime scenes with a database of known prints to identify potential matches accurately.

CHALLENGES AND LIMITATIONS

Data Quality and Quantity: Forensic investigations rely heavily on data, which may vary in quality and quantity. AI algorithms require large, diverse datasets to train effectively. However, in forensic investigations, data might be limited,

incomplete, or biased, which can affect the accuracy and reliability of AI systems.

Interpretability and Explainability: AI algorithms often operate as black boxes, making it difficult to understand the reasoning behind their decisions. In legal contexts, explainability is crucial for ensuring transparency and accountability. Interpretable AI models are necessary to provide understandable justifications for their conclusions in forensic investigations.

Bias and Fairness: AI algorithms can unintentionally perpetuate biases present in the training data, leading to unfair outcomes, especially in forensic investigations where decisions can have serious consequences for individuals. To ensure fairness in AI systems, it is crucial to address bias by carefully designing algorithms, selecting unbiased datasets, and implementing appropriate evaluation metrics.

Adversarial Attacks: Malicious actors may attempt to manipulate AI systems used in forensic investigations by introducing adversarial examples—subtle changes to input data designed to deceive the algorithm. Detecting and mitigating adversarial attacks is challenging but necessary to maintain the integrity and reliability of AI-driven forensic tools.

Ethical and Legal Considerations: AI applications in forensic investigations raise complex ethical and legal questions, such as privacy concerns, consent issues, and the potential for unintended consequences. It's crucial to establish clear guidelines and regulations governing the use of AI in forensics to ensure compliance with ethical standards and legal frameworks.

Resource Constraints: Developing and deploying AI systems for forensic investigations requires significant resources, including expertise, computational power, and financial investment. Many law enforcement agencies and forensic laboratories may lack the necessary resources to adopt AI technologies effectively, limiting their widespread implementation.

Cross-Domain Generalization: AI models trained on data from one forensic domain may not generalize well to other domains or contexts. For example, a model trained on fingerprint analysis may not perform as accurately when applied to facial recognition. Improving the generalization capabilities of AI systems across different forensic disciplines remains a challenge.

Future Trends in AI Forensic Investigations[3,4]

AI in forensic investigations has been evolving rapidly, and several trends are likely to shape its future. Here's an overview with details

Advanced Data Analysis Techniques: AI is increasingly being used for analysing massive volumes of data in forensic investigations, including digital evidence such as emails, social media posts, and CCTV footage. Techniques such as natural language processing (NLP), image recognition, and pattern recognition are being employed to extract meaningful insights from this data. Researchers are exploring ways to enhance these techniques further to improve accuracy and efficiency.

Deep Learning for Image and Video Analysis: Deep learning algorithms, particularly convolutional neural networks (CNNs), are revolutionizing image and video analysis in forensic investigations. These algorithms can automatically detect, classify, and analyse objects, faces, and activities in visual data, aiding investigators in identifying suspects and reconstructing events.

Blockchain for Evidence Integrity: Blockchain technology is gaining traction for maintaining the integrity and authenticity of digital evidence. By leveraging blockchain's decentralized and immutable ledger, forensic investigators can securely store and timestamp evidence, ensuring its integrity throughout the investigation process.

Explainable AI (XAI) in Forensic Decision Making: As AI systems play a more significant role in forensic decision making, there is a growing demand for transparency and accountability. Explainable AI (XAI) techniques aim to make AI algorithms more interpretable by providing explanations for their decisions. This not only enhances trust in AI driven forensic analyses but also enables investigators to understand the reasoning behind AI generated insights.

Privacy Preserving Techniques: With the increasing sensitivity of personal data involved in forensic investigations, preserving privacy is paramount. AI techniques such as federated learning, homomorphic encryption, and differential privacy are being explored to analyse sensitive data while protecting individual privacy.

Automated Evidence Collection and Processing: AI-powered tools are being developed to automate the collection and processing of digital evidence, streamlining the investigative process. These tools can automatically identify relevant evidence, extract key information, and generate reports,

saving investigators time and effort.

Multimodal Fusion for Enhanced Analysis: Combining information from multiple modalities, such as text, images, and audio, can provide a more comprehensive understanding of forensic evidence. Multimodal fusion techniques, including fusion at feature level, decision level, or semantic level, are being explored to integrate diverse sources of evidence and improve investigative outcomes.

These trends reflect the ongoing efforts to harness the power of AI to enhance the efficiency, accuracy, and reliability of forensic investigations.

CONCLUSION

The use of AI in forensic investigations is a significant advancement in modern law enforcement and judicial systems worldwide. By utilizing AI technologies such as machine learning, computer vision, and natural language processing, investigators can efficiently analyze vast amounts of data and uncover valuable insights that help in solving crimes and delivering justice. However, ethical concerns about privacy, bias mitigation, and transparency must be carefully addressed to ensure the responsible and equitable deployment of AI in forensic contexts. With ongoing research and collaboration between stakeholders, AI promises to revolutionize forensic investigations by improving accuracy, speed, and ultimately, the pursuit of truth in the criminal justice system.

REFERENCES

1. Vodanovic.M, Subasic.M, Milosevic.D, Galic. J., August 2023 Artificial Intelligence in Forensic medicine and forensic dentistry.
2. Deloitte Switzerland.,(2018) How can Forensic Investigators gain an edge using AI.
3. Mohsin.K., January(2021) Artificial Intelligence in Forensic Science.
4. Dwork, C. (2006). Differential privacy. In International Colloquium on Automata, Languages, and Programming (pp. 1-12). Springer, Berlin, Heidelberg.