

Advancing Forensic Science through Artificial Intelligence: A Systematic Review

Hagos Yisak Hailu^{1*} Gadisa Adamu Mitiku² Dereba Workineh Seboka² Messay Asgedom Gobena¹

Abstract

The main aim of this systematic research was to analyze the emerging trend of incorporating AI to advance forensic investigation. A search of relevant studies published up to December 2025 was performed across the manifold automated databases, including Scopus, Google Scholar, Web of Science, Research gate and PubMed/MEDLINE. This paper indicated that AI is transforming modern-day forensic science regardless of the challenges, including overwhelming volumes of data, trace evidence embedded in hectic and manifold environments, conventional laboratory systems, and limited specialist skills. Together, these factors can hamper investigations and increase the risk of failures of justice. However, deep learning and machine learning can help address these challenges. In a variety of forensic fields, case-based reasoning and neural networks are used to provide objective, reproducible, and errorless results. AI has recently been integrated into almost every major field of forensic sciences, using various approaches such as pattern recognition, data mining, data analysis, image processing, statistical analysis, computer vision, graphical modeling, computational, and mathematical methods. Furthermore, AI supports investigators and forensic experts by articulating logical evidence in fingerprint analysis, Deoxyribonucleic acid (DNA) analysis, footprint analysis, ballistics analysis, drug analysis, facial identification to recognize people in pictures, voice recognition and videos, autopsy, cause of death determination, and three-dimensional (3D) reconstructions of crime scenes. Therefore, in spite of its challenges, the introduction of AI into forensic analysis creates momentous development in the arena of crime investigation, opening up new opportunities for accuracy, efficiency, and scalability in solving sophisticated cases and providing justice.

Keywords: Artificial Intelligence, Digital Forensics, Emerging Technology, Forensic Expert, Forensic Science, Predictive Policing

DOI: <https://doi.org/10.20372/ejpos.v1iII.12989>

¹*Corresponding Author: College of Crime Investigation and Forensic Science, Ethiopian Police University, Email hagosy2006@gmail.com, Sendafa, Ethiopia, ORCID:0000-0001-9856-3407

² School of Electrical Engineering and Computing, Adama Science and Technology University, Adama, Ethiopia

² College of Applied Natural science, Science, Adama Science and Technology University, Adama, Ethiopia

¹ College of Crime Prevention and Public Security Studies, Ethiopian Police University, Sendafa, Ethiopia

Introduction

AI is the capability of technology to perceive and learn from practice, mimic human thought and be trained to solve given problems. AI combines machine learning with deep learning, with models trained on massive quantities of data to make intelligent decisions. The concept of ‘thinking machine’ originated in ancient Greece (Ahmed, 2022), and the term “AI” first appeared in 1956. It remains at the core of widespread practical implementation in a variety of sectors, including forensic science and criminology, even after the introduction of Google Translate and ChatGPT (Javadova, 2024). The primary objective of forensic analysis is to obtain truthful evidence using approaches proven to be consistent and reliable in the field. The proof is given to the court of justice, and the prosecutor must determine its reliability and admissibility. However, old, laborious, and manual data analysis techniques cannot manage today's forensic laboratory challenges and complexities as well as human professionals. These methods are frequently overly time-consuming and subject to human mistakes (Srivastava et al., 2022).

Criminal investigations have historically relied on forensic science, which offers vital resources for obtaining convictions and resolving crimes (Singh, Kumar, & Jadhav, 2020). Deep learning (DL), machine learning (ML), and natural language processing (NLP), among other AI-driven tools integrated into forensics, enable quick evidence analysis and fundamentally revolutionize the field of criminal investigation (Mohammad & Alqahtani, 2019). It marks a paradigm shift to enduring issues, signaling novel solutions in investigative works.

The AI model algorithms allow forensic scientists and law enforcement institutions to handle massive volumes of detection patterns, data, and identify useful patterns from huge datasets, thereby supporting in the illumination of critical evidence with extraordinary speed and accuracy (Dorothy, 2024; Mohammad & Alqahtani, 2019). AI systems have the capacity to learn and understand the consequences of prior actions and function autonomously (Volonnino et al., 2024). At a broader scope, AI can be classified into two areas: deep learning and machine learning. The success of AI is mainly data-driven, where outcomes are not explicitly programmed but provide by the data fed. The models are decisive, and data pre-processing is the foundational stage in machine learning (Du et al., 2020). A machine learning algorithm typically performs two core operations, i.e., learning and classification (Burrell, 2016). In the learning stage, algorithms are trained based on the input data, while deep-learning systems

usually use millions of adjustable weights using neural networks and large labeled examples to train the machine. Deep learning is a neural network considered scalable machine learning that consists of many layers and automates most of the process, like feature mining, excluding human involvement required, and lets the use of huge data storage. Recurrent neural networks (RNNs) are a class of deep learning models that are basically intended to handle progressive data and advance the field of machine learning (ML), like natural language processing, bioinformatics, speech recognition, autonomous systems, and time series prediction (Mienye, Swart, & Obaido, 2024).

From this perspective, digital forensics is expanding rapidly with AI-driven techniques significantly improving the proficiency of evidence collection, recognition, processing, and detection. The modern-day forensic technologies have advanced to meet the sophistication of digital crime, progressing from labor-intensive file analysis to advanced AI-driven techniques. AI-enhanced digital forensics makes use of automated approaches to facilitate investigation and evidence collection. A good component model, dataset selection, data collection, analysis methodologies, and ethical considerations are necessary. Each component is crucial to AI accuracy and ethical forensics practices. Selecting suitable datasets for training and testing AI models is crucial (Kadage, 2024).

The literature survey indicated that there was no well-organized review on the integration of AI in forensic sciences to ensure the justice system. Hence, this paper aimed to synthesize recently published studies on the integration of AI in the development of forensic science. Mainly, 1) AI technology in forensic investigation systems, 2) AI applications in smart forensic laboratories, 3) AI and predictive policing, 4) the future directions of AI in advancing forensic science in the pursuit of criminal justice and law enforcement.

Materials and Methods

This study has employed systematic literature review methodology for recently published research works. Screening of related papers from five relevant sources i.e., Scopus, Google Scholar, Web of Science, Research gate and PubMed/MEDLINE) was conducted. A search of relevant studies published up to December 2025 was performed across the manifold automated databases. The terms used in the search were artificial intelligence, forensic science, emerging technology, forensic expert, digital forensics predictive policing, smart forensic laboratories, and

machine learning. The references within the included articles were reviewed, and the corresponding abstracts and full articles were carefully read in case they were relevant.

Results and Discussion

From the proposed relevant sources (Scopus, Google Scholar, Web of Science, Research gate and PubMed/MEDLINE), a search of one hundred twenty-five (125) articles were performed. A total of 85 articles were checked through their title and abstracts. After excluding all non-relevant articles, the remaining 62 articles were carefully reviewed through the whole text. Based on the proposed title of the study, therefore, the whole text articles were concluded, and a final number of 58 papers were selected as relevant to the title and were included in the present systematic review.

AI: Emerging Technology in Forensic Investigation Systems

Technology and its advancements have provided the forensic sciences with many cutting-edge tools, devices, and applications, allowing forensics to gain a better and more accurate understanding of the crime scene, optimal data and information acquisition, and faster processing, allowing for more reliable conclusions and significantly improving the scientific investigation of crime. Figure 1 depicts ten types of technological advancements: 3D scanning and modeling, digital technologies, AI and data analysis, biometric technologies, nanotechnology, autopsy and radiology techniques, genetic identification technologies, voice and audio recognition technologies, and extended reality (XR) intelligence and data analysis (Chango et al., 2024). This entails that AI is currently assisting almost every major field of forensic science and criminal investigation via a variety of approaches, such as data analysis, pattern recognition, image processing, computer vision, data mining, statistical analysis and probabilistic methods, artificial olfaction, computational and mathematical methods, and graphical modeling. AI-based algorithms can thus detect vast volumes of data to identify hazards and are used to, prevent, and even forecast future crime or criminal behavior (Singh, Kumar, & Jadhav, 2020).

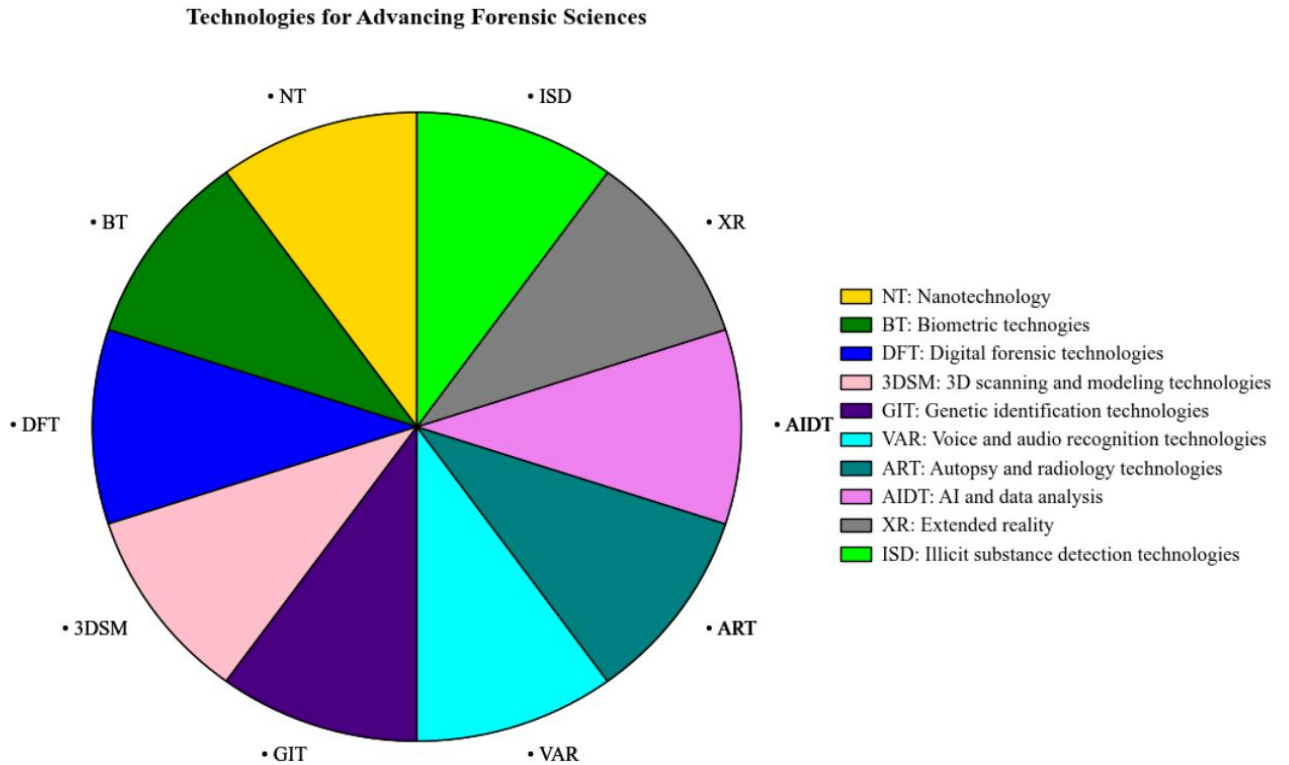


Figure 1. Technologies for Advancing Forensic Science

Figure 1 reveals some of the emerging technologies that are advancing forensic sciences. Nanotechnology (NT) plays a significant part in forensic science by enhancing the discovery and analysis of trace evidence at a bitsy position, enabling more precise examinations. In forensic investigations, distinctive physical characteristics such as fingerprints, iris patterns, facial recognition, and biometric technologies (BT) are essential for identifying individuals. This improves identity verification and forensic analysis security. In order to assist forensic professionals in recovering pertinent evidence stored in digital form, Digital Forensic Technologies (DFT) places a strong emphasis on locating, storing, and evaluating data from electronic devices such as laptops, desktop computers, and cellphones (Chango et al., 2024). Furthermore, by producing exact, accurate reconstructions of crime scenes and tangible evidence that enable virtual repairs and more extensive scrutiny, 3D scanning and modeling technologies (3DSM) are revolutionizing forensic investigations. Genetic identification technologies (GIT) are essential for DNA profiling in forensics, helping to identify suspects and victims and creating connections between evidence and individual characteristics. A voiceprint identification system is a digital signal processing concerned with recognizing a speaker by their speech features

through pre-processing, feature extraction, and a classifier to assure the veracity of audio evidence (Jha, Jain, & Srivastava, 2024). The big data analytics in forensics used by AI and Data Analysis (AIDT) transformed digital forensics, enabling predictive technologies that proactively prevent cybercrimes enrich crime investigation processes and develop effective decision-making, which finds insights that traditional approaches could overlook. The introduction of extended reality (XR) technologies, including augmented reality (AR), virtual reality (VR), and mixed reality (MR) is reshaping forensic investigation by advancing practices like professional training, evidence analysis, and crime scene reconstruction. Besides, the illegal material detection technologies focus on identifying and analyzing drugs and chemicals, aiding law enforcement and forensic experts in countering drug-related crimes. Together, these technologies upgrade the forensic skills, leading to well-organized, precise, and comprehensive investigations (Udaynadh et al., 2024).

The demand for advanced data analytics, resulting in the usage of machine learning and other emerging approaches, can be traced to the birth and subsequent rise of technologies such as Big Data, Business Intelligence, and automation-required applications. As per the explanation of (Vahid et al., 2018), machine learning is a subset of AI that uses computerized ways to solve problems based on previously collected data and knowledge without requiring needless changes to the core process. AI is simply the creation of algorithms and other computational approaches to improve machine intelligence. It contains algorithms that think, act, and complete tasks utilizing protocols that are normally out of human reach (Li & Pisztora, 2014).

Globally, the digital forensic backlogs spanning many years are becoming commonplace in law enforcement organizations. The number of cases that need the skills of digital forensic investigators is overwhelming, and this load is made worse by the amount of data that has to be examined. AI is often seen as the solution to many large data issues (Du et al., 2020). Automation and AI, which are roughly characterized as machine learning and deep learning, are two modern computing sciences that reinforce one another. In order to automate a wide range of tasks and jobs, AI-oriented software, applications, operating systems, and gadgets are being developed at a rapid pace. To increase the efficacy of digital forensics, for instance, US federal and state law enforcement organizations have started researching the application of AI-oriented technology. More digital investigations may be resolved as a result of this development, which

can increase the precision of digital forensic investigations (Jarrett & Choo, 2021). AI has the ability to greatly speed up and increase the precision of forensic investigations, making it possible to find compromised systems, attack routes, and data breaches more quickly (Syed & Kousar, 2024). The integration of AI into forensic sciences reveals a radical shift in forensic investigations. Its capacity to analyze extensive data sets, identify complex patterns, and generate swift insights has the capacity to transform the justice system. Though the classical forensic techniques are effective, they are faced with many challenges, like human errors and a shortage of time. Employing AI algorithms, like predictive analytics, facial recognition, machine learning, and natural language processing, the forensic professionals can make efficient use of data, search for patterns, and reconstruct the scene of a crime. Therefore, the emergence of AI in the forensic arena supports the analysis of texts, videos, images, electronic records, fingerprints, as well as DNA and facial recognition data so that it can improve evidence in courts, ensuring accountability and justice.

AI Applications in Smart Forensic Laboratories

The majority of modern criminal investigations rely on digital evidence (Casino et al., 2022). Long the mainstay of scientific research and industrial operations, traditional chemical analysis methods often face of difficulties, such as laborious sample preparation, human error, limited data processing capabilities, integration of analytical techniques, cost implications, and safety and environmental concerns (Chennuri et al., 2024; Wang & Zhang, 2019). The near incorporation of AI into smart laboratories has addressed long-standing difficulties using advanced algorithms, automation, and machine learning. This facilitates the extraction of important insights from complex datasets, speeds up experimental workflows, increases productivity and efficiency, improves analytical accuracy, maximizes resource utilization, enhances real-time monitoring and analysis, promotes interdisciplinary collaboration, and increases scalability and adaptability (Chennuri et al., 2024; Smith & Johnson, 2020). Due to this reason, the AI systems in smart laboratories are fundamentally transforming chemical analysis by transitioning from manual, repetitive, and time-intensive methods to automated, data-driven workflows. These systems leverage artificial intelligence (AI), machine learning (ML), and Internet of Things (IoT) connectivity to enhance accuracy, safety, and efficiency across research and development (Kim et al., 2025; Smith & Johnson, 2020).

Smart forensic laboratories (SFL) are promising in accelerating the application of scientific methods, teaching and learning activities in the field of science. Through the automation of experimental workflows, along with autonomous experimental planning, SFL hold the potential to greatly enhance the analysis, research, academic interaction, and practical works in forensics.

AI-Based Automation Technologies in Forensic Science

Digital Forensics is a segment of forensic science that relates to the collection, identification, analysis, and illumination of digital evidence hidden in different types of electronic devices (Du, Le-Khac, & Scanlon, 2017). AI technology has started revolutionizing in the world of digital forensics and plays an indispensable position in cybersecurity by figuring out and stopping threats in actual time (Dunsin, Ghanem, & Ouazzane, 2022). AI can automate common and time-consuming activities, like data sorting and initial analysis, to advance proficiency and mitigate the chance of human error. AI uses drones and robotic sensors to automate the collection of evidence without the need for human interaction (Kosta, Jain, & Suwalka, 2024; Qadir & Noor, 2021). These technologies can then analyze the collected data in real time. By cross-referencing databases, they find and identify possible evidence, such as fingerprints, and automate procedures like DNA profiling (Chen & Tseng, 2023; Kosta, Jain, & Suwalka, 2024; Sessa et al., 2024). Moreover, AI can employ advanced techniques along with deep acquisition of knowledge for photo and video analysis, language processing for statistics estimation, and predictive analytics for predicting future threats grade. The computer vision-based system has managed to detect weapons of two types (different guns and knives) to report the crimes ongoing inside the place for the responsible bodies (Kosta, Jain, & Suwalka, 2024; Yu & Pei, 2021).

Forensic medicine has rapidly emerged advanced imaging technologies to advance the accuracy and efficiency of investigations. Techniques like multi-detector computed tomography, virtual autopsy, and AI-driven imaging have revolutionized the identification of injuries and causes of death (Toraskar et al., 2019). AI tools help identify subtle fractures where specialists can perform more important tasks in an emergency department by reducing radiologic reading time in multifaceted cases (Kebande et al., 2020; Kumar & Vats, 2024). So as to harness investigation premises and recognize likely offenders, AI-based analytical modeling systems can analyze forensic evidence, including ballistic data, fingerprints, and DNA profiles (Chen et al., 2021; Kumar & Vats, 2024). Through the comparison of evidence offenders' databases and recognized behavioral patterns, these models can prioritize investigations and reduce the number of suspects

(Mohammad & Alqahtani, 2019). Lastly, Data mining complements the AI tools by detecting the hidden connections and trends within large datasets, thereby simplifying the identification of evidence that might otherwise remain concealed. Concurrently, Machine learning tools are used to generate an illegal activity network traffic data that divides packets into hazardous and non-malicious categories (Jada & Mayayise, 2024).

AI models are highly adaptable in forensic data analysis, leveraging machine learning and pattern recognition to detect fraudulent activities and cybercrimes within vast, complex datasets (Akeiber, 2025). These systems distinguish similarities and abnormalities in areas such as bank transactions, user behavior, and network logs to identify threats, often with greater speed and accuracy than human analysts (Islam & Rahman, 2025). These algorithms can also assist in identifying digital and forensic artifacts, like hidden files, erased data, and encryption techniques used to conceal evidence (Kosta, Jain, & Suwalka, 2024). Neural networks (NNs) are the foundation of the most effective AI systems for automated human face recognition, which have been investigated and developed by numerous scholars (Kasar, Bhattacharyya, & Kim, 2016). Pattern recognition is frequently used to identify and contrast different images of handwriting or signatures. Experts can ascertain the writer's gender with the use of certain pattern recognition algorithms and AI neural network models. Artificial neural network (ANN)-based AI algorithms can analyze a suspect's brain activity even during brain imaging to determine whether or not the suspect is acting normally (Hosseini et al., 2024). The amount of medicine that should be injected into the suspect is determined by ANN, which can also determine how much will have the desired effect (Singh et al., 2025). Based on a variety of physiological characteristics, the ANN can also correlate and identify lying and high-stress situations (Srivastava & Dubey, 2014). AI will also make it much simpler to anticipate a projectile's range in the ballistics industry. Without requiring human intervention, the ANN can assist experts in examining gunpowder and cartridge cases and compare bullet markings, firearm identification, and other ballistic evidence from the database using image processing (Singh et al., 2025).

Deep learning is helpful for several tasks in automated fingerprint recognition and classification systems because it automatically learns features and structures from sufficient input training data (Saeed, Hussain, & Aboalsamh, 2022). While maintaining exceptional accuracy, automated AI-

powered systems can drastically cut down on the number of comparisons made throughout the matching process (Wani et al., 2019). Furthermore, identifying and contrasting particular patterns in questionable data is one of the most crucial aspects of forensic science. To examine massive amounts of data, experts must use sophisticated statistical and probabilistic reasoning techniques. A fingerprint, a handwritten cursive word, a human face, or speech signals are examples of patterns. Numerous fields, such as speech recognition, face identification, fingerprint recognition, iris recognition, and visual situation interpretation, have employed neural networks (Singh et al., 2025).

Strong AI systems are utilized to identify people based on dental data during mass disaster investigations (Takano et al., 2019). It is also possible to train artificial neural networks to infer a person's sex from their skeletal remains. Neural network-based AI algorithms don't require a lot of expertise to implement. They can lessen human bias in the sex evaluation of skeletal remains and are fast and accurate. With applications spanning from archeology to forensic science, neural networks hold promise for the study of anthropology (Bewes et al., 2019). Additionally, the application of AI and 3D digital technology may enhance some forensic visualization processes. In order to enable real-time interaction with the reconstructed scenes, it may automatically generate 3D graphical models and animations. Virtual reality simulation in forensics involves graphically modeling 3D virtual objects and individuals using measurements and images, animating the models to mimic the crime scene or pertinent incidents (Maneli & Isafiade, 2022). The AI algorithm-designed device for measuring triglycerides, cholesterol, aspartate aminotransferase (AST), and lactate dehydrogenase (LDH) can be used to immediately analyze blood drawn from the femoral vein. The blood's pH level can be used to estimate the post-mortem interval by interpreting the data and comparing it to various databases (Hachem & Sharma, 2019). Additionally, by considering the experimental classification of bloodstains that have been scented, it may be possible to successfully employ AI learning algorithms in image processing and computer vision to automatically categorize bloodstains. However, the origin of the blood shade could be automatically ascertained using image processing techniques that combine computational intelligence. An early instrument that would carry out the string approach automatically might greatly enhance investigators' ability to handle bloodstain pattern

analysis problems and attempt to resolve complicated cases more quickly and accurately than they do now with manual methods (Acampora et al., 2021).

It is now possible to build robots or other machines that can analyze and characterize volatile scents created from a variety of sources for forensic reasons because of advancements in biochemistry, artificial intelligence, and aroma-sensor technologies (Wilson, 2014). The main purpose of these devices, sometimes known as electronic noses or e-noses, is to mimic the mammalian olfactory system in a way that gathers repeatable information so that scent blends can be detected and classified. Investigators are using these e-noses to help them find different explosive items as well as chemical and biological weapons (El Kazzy et al., 2020).

The integration of automation into forensic investigations signifies a transformative development in the field, providing the potential to enrich proficiency and efficiency in handling the increasing size of digital evidence. Regardless of the challenges existed, the forthcoming progress in forensic automation is promising. Innovations in machine learning and AI are expected to improve pattern recognition, anomaly detection, and data classification, with self-learning systems improving performance over time. Blockchain technology provides solutions for guaranteeing evidence integrity and upholding a secure chain of custody. A cross-disciplinary partnership among forensic experts, cyber security professionals, and legal specialists is critical to address these challenges and develop effective automated tools. This field can transfer more well-organized case resolutions and better-quality management of forensic evidences.

Artificial Intelligence and Forensic Expert Testimony

The application of science to law is a component of the legal system in many nations across the world and is growing in importance as a tool for improving the administration of justice. When a crime is committed, it is the duty of forensic experts to provide expert testimony that is crucial to the investigation process in order to elucidate the facts surrounding the crime (Kloosterman et al., 2015). Law enforcement agencies globally frequently confront multi-year digital forensic backlogs. Digital forensic investigators have many cases and data to process. AI is frequently seen as a solution to many big data concerns (Du et al., 2020). The current state of AI-enhanced digital forensics necessitates a review of its historical development. Over time, this discipline has changed dramatically, moving from simple file system analysis to complex methods driven by state-of-the-art algorithms. The constant interplay between offenders and investigators

guarantees these forensic methods are continually refreshed. Setting this trajectory in context highlights how dynamic and flexible contemporary forensic practice is (Wu et al., 2017). AI is currently unavoidably changing the court system and the nature of forensic expert evidence as part of larger technological advancements (Maltoni, Dappelli, & Meuwly, 2017). Forensic experts play a crucial, multifaceted role in the criminal justice system, acting as the bridge between crime scenes and courtrooms by transforming physical and digital traces into legally admissible evidence (Rao et al., 2023; Singh et al., 2025). Their work, which requires a blend of rigorous scientific knowledge (Tripathi et al., 2024), careful attention to detail, and clear communication skills, is vital for identifying perpetrators, exonerating the innocent, and providing objective and reliable data (Maltoni, Dappelli, & Meuwly, 2017). For example, digital forensics can retrieve vital information from computer devices (Waltke et al., 2018), and toxicological analysis can accurately identify drugs or poisons and connect a suspect to a crime scene (Rana, 2018). The accuracy and dependability of scientific studies are foundational to the legitimacy of judicial cases, as forensic evidence ranging from DNA to digital forensics increasingly dictates case outcomes (Maltoni, Dappelli, & Meuwly, 2017). For instance, next-generation sequencing offers more precise and comprehensive DNA analysis (Rana, 2018). Fingerprint matching has become faster and more accurate thanks to automated fingerprint recognition systems (Maltoni, Dappelli, & Meuwly, 2017). Similarly, thanks to developments in digital forensic technologies, even the most complicated cybercrimes may now be effectively examined (Dweikat, Eleyan, & Eleyan, 2021).

These developments have increased the scope of what specialists can do in addition to improving the accuracy of forensic analyses. As a result, forensic professionals should engage in continuous education, training, and certification to maintain competence in technological usage and ensure courtroom admissibility. This is because forensic experts play an indispensable role in the criminal justice system, linking the gap between crime scenes and courtrooms. Moreover, the developments in forensic technology have prominently enhanced their capabilities; the AI and machine learning systems employed in many of the forensic investigations, like crime scene reconstruction, voice identification, and deep-fake detection, offer the promise of improved promptness, proficiency, and analytical capability.

Artificial Intelligence and Predictive Policing

Predictive policing is not a single technology, but a convergence of several computational, analytical, and forensic tools designed to forecast criminal activity. Predictive policing algorithms analyze historical crime data to forecast future criminal activities, enabling more targeted and proactive law enforcement strategies. The algorithms help to identify individuals or perpetrators and the possible victims by analyzing patterns in historical dealings (Grace, 2021). AI in predictive policing leverages data analytics, machine learning, and algorithmic decision-making to predict and prevent crimes before they occur. Predictive policing uses social behavior patterns, historical crime data, and geographic trends to identify high-risk areas, potential offenders, and vulnerable victims, enabling law enforcement agencies to allocate resources more efficiently (Rigano, 2019). AI techniques like HunchLab and PredPol generate heat maps of crime-prone areas, guiding patrol routes and resource deployment. Moreover, AI can weigh the likelihood of reoffending by analyzing factors like criminal history, socioeconomic indicators, behavior patterns, and design targeted rehabilitation programs to reduce recidivism. Fingerprint tools are the most widely used instruments on a crime scene as fingerprints are the most common and important physical evidence on crime scenes. AI in fingerprinting is used in numerous ways, such as fingerprint formation, DNA sequencing, drug recognition, detecting evidence analysis, and spotting document credentials (El-Din, 2022; Singh et al., 2025). AI-driven models generate insights into potential crime hotspots and suspect profiles, enabling law enforcement to take preemptive measures. This approach not only simplifies resource allocation but also fosters a dynamic environment for crime prevention. AI technologies progressively encourage investigative professionals to focus on strategic decision-making rather than merely reactive measures, thereby increasing overall effectiveness in crime control efforts while maintaining public safety. It encompasses the realm of digital forensics and the Internet of Things (IoT) as well. Hence, the AI-powered geospatial crime mapping applies clustering techniques such as k-means and self-organizing maps (SOMs) to classify regions based on crime density. The time-series forecasting models like autoregressive integrated moving average (ARIMA), long short-term memory (LSTM) networks, and Prophet Models forecast seasonal crime flows and long-term crime trends (Rigano, 2019).

Predictive policing is the usage of data-driven algorithms and AI tools to predict illegal activities and deploy law enforcement assets more effectively. The AI-powered crime prevention approaches help to provide better safety and security. The law enforcement organizations and

technology innovators should work together to realize that the placement of AI in this area is equitable, responsible, and associated with the values of the communities they work for. Advocates argue that predictive policing can lead to significant mitigations in crime rates, as evidenced by successful enactments in many jurisdictions where data analytics have been working to optimize patrol strategies and resource allocation. Hence, it is possible to harness the benefits of AI while protecting against its potential drawbacks.

Challenges of Artificial Intelligence

Even though the forensic investigation has greatly benefited from artificial intelligence, there are still several problems and potential dangers that need to be addressed. The common challenges of AI are data privacy and security, where the AI systems require large amounts of data to operate, which leads to a breach of privacy or security (Kosta, Jain, & Suwalka, 2024). Besides, the bias, fairness, and ethical concerns of AI technologies and systems are not illuminated enough. This can lead to unfair outcomes, such as discrimination in hiring or lending (Kosta, Jain, & Suwalka, 2024; Parker, 2024). The AI systems are often considered black boxes. The logic of how they attain at their decision to solve a problem is not clear yet to most scholars and is the big issue of transparency. Furthermore, there is a lack of skilled professionals who can develop and implement AI systems in an industrial setup on top of existential risk, job displacement, regulation, and control. A cyclical issue in the sector is also finding a sense of balance between innovation and regulation (Kosta, Jain, & Suwalka, 2024).

The present literature survey has identified critical challenges of AI, like labor market shifts, algorithmic bias, privacy erosion, job displacement, systemic inequities, advanced surveillance capabilities, existential risks, autonomous weapons, and escalating global security dilemmas, lack of diverse representation, and lack of transparency (opaque decision-making). These challenges are examined for their thoughtful societal consequences, including worsened economic inequality, multifaceted ethical dilemmas, and tangible threats to global security and stability.

Future Directions of AI in Advancing Forensic Science

Deep fake technology has emerged as a major challenge for forensic investigations, enabling the formation of hyper-realistic fake videos, digitally manipulated images, and synthetic voice recordings that can betray law enforcement agencies, the judiciary, and forensic experts. To fight this issue, AI-powered forensic techniques are being advanced to analyze deep fakes by detecting

discrepancies in eye movements, lip-syncing, facial expressions, and audio waveforms. Recurrent neural networks (RNNs) and Convolutional neural networks (CNNs) are leveraged to scrutinize pixel-level distortions, frame anomalies, and compression artifacts that may be invisible to the human eye. Furthermore, AI-driven voice forensic tools analyze speech synthesis patterns, tone modulation, and background noise inconsistencies to detect deep fake audio. Future advancements in AI-powered forensic systems will further improve the accuracy of deep fake detection by incorporating adversarial machine learning techniques to stay ahead of evolving deep fake generation algorithms. Guaranteeing the authenticity of digital evidence through AI-based deep fake detection will be critical for upholding trust in forensic analysis and court proceedings (Alnaqbi et al., 2025). Future advancements in behavioral AI will likely include multimodal data fusion, integrating physiological sensors, real-time sentiment analysis, and eye-tracking systems to improve lie detection accuracy. These developments will provide law enforcement with additional tools to evaluate suspect testimonies and aid forensic psychologists in criminal profiling and suspect interrogation (Forte, 2006; Alnaqbi et al., 2025). AI-driven blockchain solutions will improve the credibility of forensic reports in legal proceedings, reinforcing the credibility of forensic science in the justice system. As quantum AI technology continues to emerge, it is expected to integrate with advanced forensic applications such as neural network training for deep fake detection, pattern recognition, and molecular forensics for chemical trace analysis in forensic linguistics (Alnaqbi et al., 2025). Therefore, Forensic investigations could be significantly accelerated, improved, and modernized by these developments.

Based on the systematic review made, therefore, it is possible to recommend developing a holistic framework (spanning policy interventions) to address the complicated challenges of AI through targeted research directions, industry best practices, and responsibly harnessing AI's transformative potential in the area of police institutions in general and forensic science in particular.

Conclusion

From the present review, it is possible to conclude that AI is transforming science in general and forensic science in particular. It is breaking bottlenecks in knowledge synthesis and experimentation, offering tools that enhance accuracy, efficiency, and objectivity. However,

responsible implementation, grounded in ethical considerations, transparency, reliability in investigations, and legal rigor, is critical. This paper sketches a foundation for forensic scientists, technologists, and legal professionals on how they can collaboratively shape the next generation of intelligent forensic systems. It outlines AI's transformative role in forensic science, acknowledges both benefits and challenges, and a viewpoint on the sustained evolution of AI-driven forensic tools. The future directions in this field involve the development of explainable AI techniques for legal settings, integration with blockchain for evidence traceability, training and certification programs for forensic AI usage, forming standards and regulations for AI use in forensic science in agreement with the international standards and regulatory frameworks, necessity for unbiased datasets, and development of interpretable AI models for legal admissibility. Hence, the law enforcement institutions, forensic experts, researchers, and judicial actors should establish a concrete ground for AI, machine learning, deep learning, and neural networks.

Conflict of Interests

The authors have declared that no conflict of interest exists.

References

- Acampora, G., Di Nunzio, C., Garofano, L., Saliva, M., & Vitiello, A. (2021). Applying density-based clustering for bloodstain pattern analysis. In *2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. pp. 28-33. IEEE.
- Ahmed Alaa El-Din, E. (2022). Artificial intelligence in forensic science: invasion or revolution? *Egyptian Society of Clinical Toxicology Journal*, 10(2). <https://doi.org/10.21608/esctj.2022.158178.1012>.
- Akeiber, H. J. (2025). A comprehensive study of cybercrime and digital forensics through machine learning and AI. *Al-Rafidain Journal of Engineering Sciences*, 3(1), 369–395. <https://doi.org/10.61268/hfflpp49>.
- Alnaqbi, A., Alblooshi, M., Nasser, H. A., Habtom, N., & Iqbal, F. (2025). Forensic investigations in the age of AI: Identifying and analyzing artifacts from AI-assisted crimes. In *2025 13th International Symposium on Digital Forensics and Security (ISDFS)*. 1-6.

- Bewes, J., Low, A., Morphett, A., Pate, F. D., & Henneberg, M. (2019). Artificial intelligence for sex determination of skeletal remains: Application of a deep learning artificial neural network to human skulls. *Journal of Forensic and Legal Medicine*, 62, 40-43.
- Bharath Kumar Chennuri, B., Sravanthi, A., Srivani, K., Madhavi, M., Sudha, B., Srinu, K., & Santosh Kumar, K. (2024). Smart laboratories: Integrating AI for efficient chemical analysis. *Journal of Chemical Health Risks*. 14(2), 1-4.
- Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 1–12. <https://doi.org/10.1177/2053951715622512>.
- Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, 10, 25464–25493. <https://doi.org/10.1109/ACCESS.2022.3154059>.
- Chango, X., Flor-Unda, O., Gil-Jiménez, P., & Gómez-Moreno, H. (2024). Technology in forensic sciences: innovation and precision. *Technologies*, 12(8), 120.
- Chen, R. J., Lu, M. Y., Chen, T. Y., Williamson, D. F., & Mahmood, F. (2021). Synthetic data in machine learning for medicine and healthcare. *Nature Biomedical Engineering*, 5(6), 493-497.
- Chen, Y.-F., & Tseng, P. K. (2023). The boundary of artificial intelligence in forensic science. *Dialogo*, 10(1), 83–90. <https://doi.org/10.51917/dialogo.2023.10.1.5>.
- Dorothy, B. (2024). Maximizing forensic analysis efficiency through integrated AI models. *International Research Journal of Modern Engineering and Technology Science*. <https://doi.org/10.56726/irjmets48804>.
- Du, X., Hargreaves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac, N. A., & Scanlon, M. (2020). SoK: Exploring the state of the art and the future potential of artificial intelligence in digital forensic investigation. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*. pp. 1–10.
- Du, X., Le-Khac, N. A., & Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. *European Conference on Information Warfare and Security*, 573–581.

- Dunsin, D., Ghanem, M. C., & Ouazzane, K. (2022). The use of artificial intelligence in digital forensics and incident response (DFIR) in a constrained environment. In *International Conference on Digital Forensics and Security of Cloud Computing (ICDFSCC)*. pp. 1-5.
- Dweikat, M., Eleyan, D., & Eleyan, A. (2021). Digital forensic tools used in analyzing cybercrime. *Journal of University of Shanghai for Science and Technology*, 23(3), 367–379. <https://doi.org/10.51201/jusst12621>.
- El Kazzy, M., Hurot, C., Weerakkody, J., Buhot, A., & Hou, Y. (2020). Biomimetic olfactory biosensors and bioelectronic noses. *Advances in Biosensors: Reviews Volume 3*, 3, 15-63.
- Forte, D. (2006). The state of the art in digital forensics. *Advances in Computers*, 67, 253-300. [https://doi.org/10.1016/S0065-2458\(05\)67006-4](https://doi.org/10.1016/S0065-2458(05)67006-4).
- Grace, J. (2021). Algorithmic impropriety' in UK policing contexts: A developing narrative?. In *Predictive Policing and Artificial Intelligence*. pp. 237-253.
- Hachem, M., & Sharma, B. K. (2019), February). Artificial intelligence in prediction of post-mortem interval (PMI) through blood biomarkers in forensic examination—a concept. In *2019 Amity International Conference on Artificial Intelligence (AICAI)*. pp. 255-258. IEEE.
- Hosseini, E. A., Schrimpf, M., Zhang, Y., Bowman, S., Zaslavsky, N., & Fedorenko, E. (2024). Artificial neural network language models predict human brain responses to language even after a developmentally realistic amount of training. *Neurobiology of Language*, 5(1), 43–63. https://doi.org/10.1162/nol_a_00137.
- Islam, M. S., & Rahman, N. (2025). AI-driven fraud detection in financial institutions: A comprehensive study. *Journal of Computer Science and Technology Studies*, 7(1), 100–112. <https://doi.org/10.32996/jcsts.2025.7.1.8>.
- Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organizational cyber security: an outcome of a systematic literature review. *Data and Information Management*, 8(2). <https://doi.org/10.1016/j.dim.2023.100063>.
- 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. <https://doi.org/10.1002/wfs2.1418>.
- Javadova, A. N. (2024). Using Artificial Intelligence in the Forensic Science for the Analysis of Microparticles: A Systematic Review. *Futurity Economics & Law*, 4(2), 229-246.

- Jha, K., Jain, A., & Srivastava, S. (2024). *Analysis of human voice for speaker recognition: Concepts and advancement. Journal of Electrical Systems, 20(1S), 582–599.*
- Kadage, A. D. (2024). AI-enhanced digital forensics: automated techniques for efficient investigation and evidence collection. *Journal of Electrical Systems, 20(1S), 211–229.* <https://doi.org/10.52783/jes.766>.
- Kasar, M. M., Bhattacharyya, D., & Kim, T. H. (2016). Face recognition using neural networks: a review. *International Journal of Security and Its Applications, 10(3).* <https://doi.org/10.14257/ijisia.2016.10.3.08>.
- Kebande, V. R., Ikuesan, R. A., Karie, N. M., Alawadi, S., Choo, K. K. R., & Al-Dhaqm, A. (2020). Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments. *Forensic Science International: Reports, 2, 100122.*
- Kim, Y. H., Lee, S. Y., Kim, J. Y., Cho, H., Chun, H. S., & Ahn, S. (2025). Nuclear magnetic resonance-based approaches for the structural and quantitative analysis of mycotoxins. *Magnetochemistry, 11(6), 47.*
- Kloosterman, A., Mapes, A., Geradts, Z., van Eijk, E., Koper, C., van den Berg, J., Verheij, S., van der Steen, M., & van Asten, A. (2015). The interface between forensic science and technology: How technology could cause a paradigm shift in the role of forensic institutes in the criminal justice system. *Philosophical Transactions of the Royal Society B: Biological Sciences, 370(1674), 20140264.* <https://doi.org/10.1098/rstb.2014.0264>.
- Kosta, S., Jain, S., & Suwalka, I. (2024). AI revolutionizing forensic analysis: enhancing efficiency and accuracy in crime investigation. *International Advanced Research Journal in Science, Engineering and Technology, 226–229.*
- Kumar, S., & Vats, S. (2024). A review article on the transformative impact of artificial intelligence-powered autopsy in forensic medicine. *International Journal For Multidisciplinary Research, 6(2), 1-7.*
- Li, J., & Pisztora, V. A. (2014). Unsupervised and semisupervised learning. *Wiley StatsRef: Statistics Reference Online, 1-18.*
- Maltoni, D., Cappelli, R., & Meuwly, D. (2017). Automated fingerprint identification systems: from fingerprints to fingermarks. *In Handbook of Biometrics for Forensic Science, pp. 37-61.*

- Maneli, M. A., & Isafiade, O. E. (2022). 3D forensic crime scene reconstruction involving immersive technology: A systematic literature review. *IEEE Access*, *10*, 88821-88857.
- Mienye, I. D., Swart, T. G., & Obaido, G. (2024). Recurrent neural networks: A comprehensive review of architectures, variants, and applications. *Information*, *15*(9), 517.
- Mohammad, R. M. A., & Alqahtani, M. (2019). A comparison of machine learning techniques for file system forensics analysis. *Journal of Information Security and Applications*, *46*. <https://doi.org/10.1016/j.jisa.2019.02.009>.
- Parker, O. (2024). *Data governance and ethical AI: developing legal frameworks to address algorithmic bias and discrimination*. 10.13140/RG.2.2.11601.34406.
- Qadir, S., & Noor, B. (2021). Applications of machine learning in digital forensics. In *2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2)*. pp. 1-8.
- Rana, A. K. (2018). Crime investigation through DNA methylation analysis: methods and applications in forensics. *Egyptian Journal of Forensic Sciences*, *8*(1), 7.
- Rao, K., Singh, R. R., Yadav, P. K., & Tripathi, S. K. (2023). Role of scientific evidence in the judiciary system: A systematic review. *Indian Journal of Forensic Medicine and Toxicology*, *17*(4). <https://doi.org/10.37506/ijfmt.v17i4.19945>.
- Rigano, C. (2019). Using artificial intelligence to address criminal justice needs. *National Institute of Justice Journal*, *280*(1-10), 17.
- Saeed, F., Hussain, M., & Aboalsamh, H. A. (2022). Automatic fingerprint classification using deep learning technology (DeepFKTNet). *Mathematics*, *10*(8), 1285. <https://doi.org/10.3390/math10081285>.
- Sessa, F., Esposito, M., Cocimano, G., Sablone, S., Karaboue, M. A. A., Chisari, M., Albano, D. G., & Salerno, M. (2024). Artificial intelligence and forensic genetics: Current applications and future perspectives. *Applied Sciences*, *14*(5), 2113. <https://doi.org/10.3390/app14052113>.
- Singh Sankhla, M., Kumar, R., & Jadhav, E. B. (2020). Artificial intelligence: advancing automation in forensic science & criminal investigation. *Seybold Reports*, *15*(8), 2064–2075.

- Singh, N., Khan, M. Z., Kaur, B., & Mishra, A. (2025). Revolutionizing crime investigation: The role of deep learning in forensic intelligence. In forensic intelligence and deep learning solutions in crime investigation. *IGI Global Scientific Publishing*, pp. 281-300.
- Smith, J., & Johnson, A. (2020). Integration of artificial intelligence in chemical analysis. *Journal of Analytical Chemistry*, 123–135.
- Srivastava, A., Harshey, A., Das, T., Kumar, A., Yadav, M. M., & Shrivastava, P. (2022). Impact of DNA evidence in criminal justice system: Indian legislative perspectives. *Egyptian Journal of Forensic Sciences*, 12(1), 51. <https://doi.org/10.1186/s41935-022-00309-y>.
- Srivastava, N., & Dubey, S. (2014). Lie detection system using artificial neural networks. *Journal of Global Research in Computer Science*, 5(8).
- Syed, F. M., & Faiza Kousar, E. S. (2024). AI-driven forensic analysis for cyber incidents in healthcare. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, 15(1), 473-499.
- Takano, H., Momota, Y., Ozaki, T., Shiozawa, S., & Terada, K. (2019). Personal identification from dental findings using AI and image analysis against great disasters in Japan. *Forensic Legal Investigative Science*, 5, 041.
- Toraskar, T., Bhangale, U., Patil, S., & More, N. (2019, July). Efficient computer forensic analysis using machine learning approaches. In *2019 IEEE Bombay Section Signature Conference (IBSSC)*. pp. 1-5.
- Tripathi, S. K., Rao, K., Singh, R. R., & Yadav, P. K. (2024). Artificial intelligence and its role in forensic karyotyping: A systematic review. *Indian Journal of Forensic Medicine and Toxicology*, 18(1). <https://doi.org/10.37506/900g7477>.
- Udaynadh, B., Chavan, V. A., Singh, A., V. A., & Adithi, E. (2024). Applications of nanomaterials in forensic science. *Future Trends in Chemical Materials Science and Nanotechnology*, 3B(13), 1–17. <https://doi.org/10.58532/v3becs13p1ch1>.
- Vahid, S., Nezhad, A., Abad, K., Yilmaz, M., Ann, Á., & Ann, Á. P. S. O. (2018). Prediction of the durability of limestone aggregates using computational techniques. *Neural Computing and Applications*, 29(2), 423–433. <https://doi.org/10.1007/s00521-016-2456-8>.

- Volonnino, G., De Paola, L., Spadazzi, F., Serri, F., Ottaviani, M., Zamponi, M. V., Arcangeli, M., & La Russa, R. (2024). Artificial intelligence and future perspectives in forensic medicine: A systematic review. *Clinical Therapeutics*, 175(3), 193–202. <https://doi.org/10.7417/CT.2024.5062>.
- Waltke, H., LaPorte, G., Weiss, D., Schwarting, D., Nguyen, M., & Scott, F. (2018). Sexual assault cases: Exploring the importance of non-DNA forensic evidence. *NIJ Journal*, 279, 1-14.
- Wang, L., & Zhang, Y. (2019). Applications of AI in smart laboratories: a review. *Analytical Methods*, 89–102.
- Wani, M. A., Bhat, F. A., Afzal, S., & Khan, A. I. (2019). Supervised deep learning in fingerprint recognition. In *Advances in Deep Learning*. pp. 111–132. Springer Singapore. <https://doi.org/10.1007/978-981-13-6794-6-7>.
- Wilson, A. D. (2014). Electronic-nose applications in forensic science and for analysis of volatile biomarkers in the human breath. *Journal of Forensic Science & Criminology*, 1(1), S103. <https://doi.org/10.15744/2348-9804.1.S103>.
- Wu, S., Zhang, Y., Wang, X., Xiong, X., & Du, L. (2017). Forensic analysis of WeChat on Android smartphones. *Digital Investigation*, 21, 3–10. <https://doi.org/10.1016/j.diin.2016.11.002>.
- Yu, C., & Pei, H. (2021). Face recognition framework based on effective computing and adversarial neural networks and its implementation in machine vision for social robots. *Computers & Electrical Engineering*, 92, 107128. <https://doi.org/10.1016/j.compeleceng.2021.107128>.