



Application of AI capabilities in forensics and criminal proceedings: Innovative technologies in forensic examinations

OÑATI SOCIO-LEGAL SERIES FORTHCOMING

DOI LINK: [HTTPS://DOI.ORG/10.35295/OSLS.IISL.2555](https://doi.org/10.35295/OSLS.IISL.2555)

RECEIVED 17 DECEMBER 2025, ACCEPTED 23 APRIL 2026, FIRST-ONLINE PUBLISHED 9 JUNE 2026

SARA BAKYT¹ 

AKYNKOZHA ZHANIBEKOV² 

AIGUL PARIDINOVA³ 

YERBOL KARZHAUBAYEV⁴ 

NURSULTAN POSHANOV⁵ 

Abstract

This study aims to identify and systematically present the modern domains of forensic examination where AI capabilities can be effectively utilized. Additionally, the study intends to provide a general assessment of the applicability of AI tools to forensic science in the future, particularly regarding the potential expansion of their role. The findings suggest that AI has the potential to substantially enhance the toolkit of forensic examinations within the techno-biological spectrum, especially in areas requiring the processing of large datasets, sample comparison, and the identification of complex patterns. However, AI is less applicable in fields that require an understanding of human psychology, behavior, or event context. This study interests professionals in forensic science and forensic examination from a practical standpoint. Furthermore, it highlights which branches of forensic science may require human involvement in the future, offering insights into the implications for the labor market and education in this field.

¹ Sara Bakyt. Higher School of Law, Turan University, Almaty, Kazakhstan. Email: sara.bakyt@bk.ru ORCID: <https://orcid.org/0000-0002-2252-2710>

² Akynkozha Zhanibekov. Department of Criminal Law, Criminal Procedure and Criminalistics, Al-Farabi Kazakh National University, Almaty, Kazakhstan. Email: Akynkozha.Zhanibekov@kaznu.edu.kz ORCID: <https://orcid.org/0000-0002-1116-2123>

³ Aigul Pardinova. Department of Tourism, International University of Tourism and Hospitality, Turkestan, Kazakhstan. Email: aigul.pardinova@iuth.edu.kz ORCID: <https://orcid.org/0009-0005-9483-6603>

⁴ Yerbol Karzhaubayev. Department of Law, Shoqan Ualikhanov Kokshetau State University, Astana, Kazakhstan. Email: Erbol-dok@mail.ru ORCID: <https://orcid.org/0009-0000-8794-1660>

⁵ Nursultan Poshanov. Corresponding author. Humanitarian School, International University of Tourism and Hospitality, Turkestan, Kazakhstan. Email: nuposhanov7@outlook.com, N.POSHANOV@IUTH.EDU.KZ ORCID: <https://orcid.org/0000-0001-6822-1019>

Key words

Artificial intelligence; deep learning; expert opinion; forensic examination; machine learning

Resumen

El objetivo de este estudio es identificar y presentar de forma sistemática los ámbitos actuales del análisis forense en los que se pueden utilizar eficazmente las capacidades de la IA. Además, el estudio pretende ofrecer una valoración general de la aplicabilidad de las herramientas de IA a la ciencia forense en el futuro, especialmente en lo que respecta a la posible ampliación de su papel. Los resultados sugieren que la IA tiene el potencial de mejorar sustancialmente el conjunto de herramientas de los exámenes forenses dentro del espectro tecno-biológico, especialmente en áreas que requieren el procesamiento de grandes conjuntos de datos, la comparación de muestras y la identificación de patrones complejos. Sin embargo, la IA es menos aplicable en campos que requieren una comprensión de la psicología humana, el comportamiento o el contexto de los hechos. Este estudio resulta de interés para los profesionales de la ciencia forense y el examen forense desde un punto de vista práctico. Además, destaca qué ramas de la ciencia forense pueden requerir la intervención humana en el futuro, ofreciendo una perspectiva sobre las implicaciones para el mercado laboral y la formación en este campo.

Palabras clave

Inteligencia artificial; aprendizaje profundo; opinión de expertos; examen forense; aprendizaje automático

Table of contents

1. Introduction	4
2. Methods and materials	5
3. Results	6
3.1. Physical and hybrid evidence analysis	9
3.2. Digital and data-intensive forensic domains	10
3.3. Behavioural and interpretative expertise	12
4. Discussion.....	14
5. Conclusions	16
References.....	17

1. Introduction

Modern forensic science is undergoing a phase of transformation driven by the rapid advancement of technology. Artificial intelligence (AI), machine learning, big data processing, and other innovative methods are increasingly integrated into criminal proceedings, enhancing the accuracy and efficiency of forensic investigations (Dunsin *et al.* 2024, Karpuntsov and Veresha 2023). These technologies enable the automation of evidence analysis, minimize human error, and accelerate the crime investigation process. Against this backdrop, new directions in forensic research, applied knowledge, and expert examination are emerging.

The rise in cybercrime, along with the growing significance of digital devices in “traditional” criminal investigations, has led to increased demand for digital forensics. This field involves the examination of digital data and devices in a manner that is legally admissible in court. It encompasses the processes of identifying, collecting, verifying, analyzing, interpreting, documenting, and presenting digital evidence (Rizvi *et al.* 2022). According to the U.S. Bureau of Labor Statistics (BLS), the number of forensic science jobs is expected to increase by 14% between 2022 and 2032, reaching approximately 18,600 positions—representing significant growth compared to previous years. BLS attributes this rise to advancements in forensic methods that have improved the accessibility and reliability of objective forensic information. Consequently, courts and law enforcement agencies must hire additional personnel to apply these methods in data analysis for use in legal proceedings (Gustafson 2024, US Bureau of Labor Statistics 2024).

In recent years, the volume of digital evidence has grown significantly, necessitating new approaches to its processing and interpretation. AI, with its capacity to automate analysis and identify patterns across large datasets, has emerged as a particularly suitable response to this challenge. It is already widely applied in forensic science, from facial recognition and handwriting analysis to ballistic examination and crime prediction modeling. However, alongside its advantages, the use of such technologies raises several concerns, including the legality and reliability of AI-derived conclusions, algorithm transparency, ethical considerations, and their admissibility in court. In applied forensic science across various countries, experts from a wide range of scientific disciplines—ranging from forensic anthropologists to cybersecurity specialists—are actively involved. This diversity has a logical explanation: due to the historically shaped characteristics of judicial systems (which, in many countries, share common principles and approaches), specialists from various fields of knowledge have been invited as experts in forensic investigations.

The emergence of AI has marked a new milestone in the history of forensic science, both as an academic discipline and as a practical field. It has drawn attention to adapting existing techniques, tactics, and methodologies to work with software applications and devices utilizing machine learning capabilities. Consequently, this transformation will inevitably impact the routine activities of forensic experts, requiring them to acquire new knowledge and skills.

Contemporary research on the application of AI in forensic science explores a variety of topics, including the role of explainable AI in forensics (Hall *et al.* 2022), the use of AI tools in network forensics (Rizvi *et al.* 2022), prospects for AI implementation in forensic

examination (Hamzah *et al.* 2022, Galante *et al.* 2023), the role of autonomous AI systems in detecting fraud on the dark web (Rawat *et al.* 2023), AI applicability in forensic medicine and toxicology (Wankhade *et al.* 2022), ethical considerations in forensic science in the AI era (Andrić and Ivanović 2023), challenges of implementing machine learning tools in different forensic fields (Ahmed Alaa El-Din 2022), the impact of automation and AI on digital forensics (Jarrett and Choo 2021), and the integration of AI tools into biological forensic analysis (McDonald *et al.* 2024). Thus, considerable attention has been given to the advantages of AI integration into specific areas of forensic science. However, existing research has largely overlooked the question of which forensic domains AI cannot be applied to (i.e., where its capabilities are inapplicable) or where its role may be significantly constrained.

This study focuses on the issue of improving forensics through the application of AI. Forensics itself is thus seen as one part of an overall security strategy to achieve the goals of justice and law enforcement. This study aims to systematically identify and present modern areas of forensic examination where AI capabilities can be effectively utilized. At the same time, it aims to highlight forensic fields where AI may encounter substantial limitations or prove entirely impractical. Additionally, the study seeks to provide a general assessment of the applicability of AI tools to forensic disciplines in the future, focusing on their potential for expansion.

2. Methods and materials

This study falls within the domain of theoretical research in forensic science. At the same time, given its comprehensive coverage of various branches of forensic science, the work is inherently interdisciplinary. This characteristic necessitates a complex methodological approach, which synthesizes multiple methods, including systems analysis, legal forecasting (in the context of applied disciplines), and elements of expert evaluation.

The research hypothesis is based on the premise that AI is applicable in certain forensic domains, while in others, it is either inapplicable or only marginally applicable. To substantiate this hypothesis, the study draws on a synthesis of academic literature, institutional reports, and documented practical implementations of AI tools, examining each forensic field against criteria such as data volume requirements, pattern recognition demands, and the degree of human judgment involved. The study provides examples of existing practical implementations of AI tools — specifically machine learning and deep learning — across various forensic disciplines. Additionally, it presents arguments supporting the potential expansion of these tools into other areas. The classification of AI applicability presented in Table 1 is based on a synthesis of three criteria applied consistently across all forensic disciplines: (1) the degree to which the task involves processing large volumes of structured or semi-structured data; (2) the availability of documented practical implementations or pilot projects; and (3) the extent to which human judgment, contextual interpretation, or ethical discretion is required. Fields rated “High” meet all three conditions favourably — substantial data volumes, existing implementations, and limited dependence on human discretion. Fields rated “Medium” show partial implementation or moderate data-processing demands. “Limited” applicability reflects fields where AI tools exist but perform inconsistently or require significant human oversight. “Low” or “Non-appropriate” ratings indicate fields where

the core task is inherently dependent on human understanding of psychology, intent, or context, and where no reliable AI implementations have been documented.

The issues of AI inapplicability or limited applicability in certain forensic fields are examined through a synthesis of existing scientific and practical knowledge, as well as through modal logic tools. This approach allows for the formulation of hypotheses concerning the future development of AI in specific forensic disciplines.

The documentary basis of this research includes analytical reports from private organizations operating in various fields of forensic science and forensic examination, as well as materials from government agencies and consulting firms specializing in forensic analysis. Key references include the FBI's Privacy Impact Assessment: Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability and PwC's Impact of Artificial Intelligence on Fraud and Scams.

Expert opinions from specialized forensic organizations and academic research are utilized in cases requiring the assessment of future trends. This comprehensive approach to evaluating AI implementation prospects in forensic science accounts for critical characteristics of real-world systems (in this case, the forensic system), such as stochasticity, uncertainty, nonlinearity, and variability.

The study involved two stages. The first stage was to explore the potential of AI for its application in the field of forensics. For this purpose, such new areas of forensics development as forensics of social networks, possibilities of predicting security threats on the basis of data analysis with the help of AI were considered. Separate areas of forensic research were identified, which became the basis for further categorisation of them depending on the applicability of AI to solve their tasks. The second stage of the research consisted of reviewing the performance of companies conducting forensic research. It was noted that forensic research in the XXI century is no longer the exclusive prerogative of the state, which allowed access to the above materials. In particular, the materials freely available on the Parabon NanoLabs website became the basis for the case study. As a separate example of the use of AI in forensic research, the possibility of machine reconstruction of human appearance was considered. The practical part of the research also includes the study of empirical data obtained from the use of artificial intelligence tools in forensic expertise - Parabon Case (Parabon Nanolabs 2024). Based on the analysis and synthesis of open data, it was summarised from the perspective of assessing the frequency of applicability of artificial intelligence in different areas of forensic science. The use of AI for different types of forensic analyses and the specifics of such applications were also considered.

3. Results

AI has become embedded across a wide range of industries — from healthcare and finance to logistics and consumer electronics. Forensic science has also become a beneficiary of these technologies, particularly in the detection and analysis of cybersecurity incidents (Rizvi *et al.* 2022, Galante *et al.* 2023). However, AI's potential extends beyond this application. Contemporary research increasingly highlights the growing significance of big data (BD), which was previously not strongly associated with traditional forensic science but is now becoming an essential component of forensic

and criminal investigations. As crime continues to migrate into the digital realm, forensic science—both as an academic discipline and an applied field—must adapt to these emerging digital landscapes.

Investigating cybercrime often involves addressing challenges related to big data, and proactive security event monitoring through AI-driven intrusion detection systems (IDS) can play a critical role in recovering essential digital evidence. This makes AI a natural tool for assisting investigators in processing large datasets to identify relevant pieces of information crucial to an investigation (Rizvi *et al.* 2022). A notable illustration of these emerging trends in forensic science is the rise of a relatively new subfield—social media forensics. With over 3.6 billion social media users worldwide, a number projected to increase to 4.5 billion by 2025, forensic experts now have access to an unprecedented volume of data for suspect profiling. Before the advent of social media, investigators and forensic analysts lacked such extensive datasets for criminal profiling (Veresha 2017). Today, social media data on specific individuals can significantly enhance investigative capabilities. To support the processing and interpretation of this information, researchers have developed AI models designed for analyzing data extracted from social media platforms. However, for automated data analysis to be considered admissible in court, it must be based on models that are reproducible, explainable, and verifiable (Gustafson 2024). From the points discussed above, two key conclusions can be drawn:

- a) Forensic science will increasingly engage with new, conventionally “non-physical” domains of criminal activity, requiring an adaptation of forensic methodologies, techniques, and tactics, as well as an overall modernization of forensic science education and professional training systems.
- b) Forensic science is acquiring a new set of digital tools capable of significantly streamlining both routine and specialized professional tasks through AI integration. AI can either be incorporated into existing forensic software or serve as the foundation for the development of AI-powered forensic applications from the outset.

Forensic science encompasses a broad range of disciplines, including — but not limited to — fingerprint and trace examination, ballistics, DNA analysis, digital forensics, forensic medicine, handwriting and document examination, phonoscopy, linguistic analysis, financial forensics, and psychological and psychiatric evaluation. The classification of these disciplines may vary across jurisdictions.

It is important to note that forensic expertise is no longer solely the prerogative of the state. This characteristic long distinguished many countries, particularly the post-Soviet states and former members of the Warsaw Pact. Currently, alongside state-run forensic institutions, private expert organizations providing forensic services operate in various countries worldwide. The competition fostered by this development, driving technological progress, has encouraged forensic institutions to implement the latest technical advancements from diverse applied research fields into their practices. Today, the technological tools applicable to forensic science are being developed across various industries—from medicine to telecommunications—and are now reaching a new milestone in their technical evolution by incorporating the capabilities of AI into forensic activities.

This study highlights several examples of companies (institutions) operating in the field of forensic science and related sectors (in the narrower sense, forensic laboratories) that are already utilizing AI for forensic expert purposes. One such company is Parabon NanoLabs. With financial support from the U.S. Department of Defense, the company developed the DNA phenotyping system Snapshot, which accurately predicts genetic ancestry, eye color, hair color, skin tone, freckle presence, and facial shape in individuals of any ethnic background, including those of mixed ancestry (Parabon Nanolabs 2024). In the high-profile case of M.D. Weidhofs in the U.S., dating back over 20 years, AI capabilities in forensic science have significantly aided law enforcement. By using AI and DNA samples, Parabon NanoLabs was able to model the suspect's face, which provided a new impetus for the investigation (Snohomish County 2022). At the same time, specialists at Parabon NanoLabs note that the modeling system does not provide absolute guarantees that the generated image will fully match the real person's appearance. In the case of criminals, at this stage of software development, there are too many risks that the system might produce incorrect results, leading the investigation down a false path. (An example comparing machine-generated facial reconstructions and photographs of real people, illustrating the current capabilities of forensic applied software, can be seen in Figure 1).

FIGURE 1

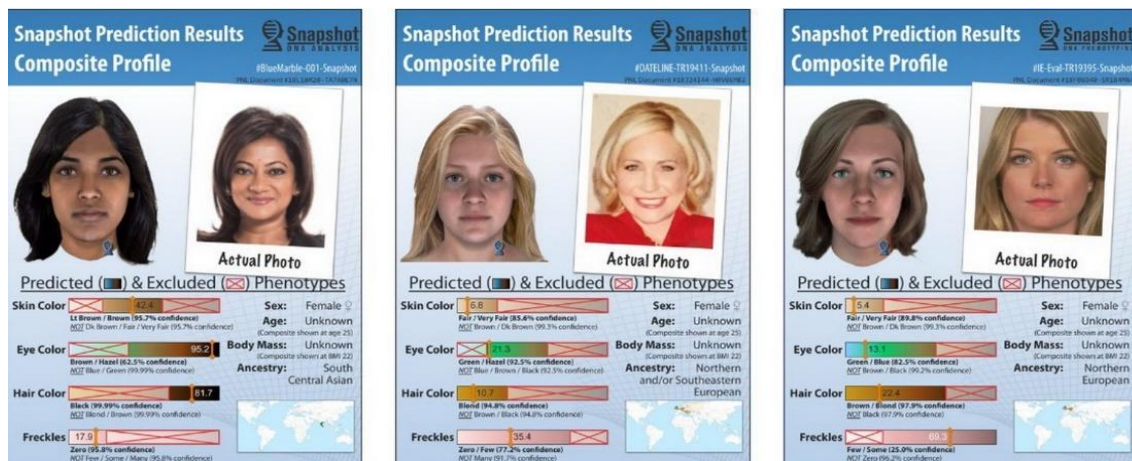


Figure 1. Example of comparison between machine-generated facial reconstruction and photographs of real individuals, demonstrating the current capabilities of forensic applied software (provided by Parabon NanoLabs for public access for informational purposes).

(Source: Parabon Nanolabs 2024.)

The program's ability to reliably determine hair color, eye color, skin tone, freckle count, and face shape provides undeniable advantages for law enforcement, assisting in the creation of photographic portraits of suspects who are wanted. Expanding on this topic, it is not an exaggeration to state that AI is already having a significant impact on forensic science, accelerating data analysis, reducing the likelihood of errors, and uncovering hidden patterns. In several areas, it is becoming not just an auxiliary tool but a fundamentally important factor that is transforming the investigation process. In this context, it is essential to highlight those types of forensic expertise where AI and machine learning capabilities undeniably hold potential for further development. Among them are fingerprint analysis, ballistics, computer forensics, biological (DNA) analysis, video forensics, voice analysis, linguistics, forensic chemistry, and financial-economic

expertise. In general, the frequency/possibility of using artificial intelligence tools in carrying out certain types of expertise can be summarised as follows (Table 1).

TABLE 1

High	Medium	Limited	Low	Non-appropriated
Digital DNA-analysis (biological) Photo-video- technical	Phonoscopy Linguistic	Chemical Ballistics Handwriting	Psychological, psychophysiological Traceology, analysis of traces of blast residue	psychiatric,

Table 1. Frequency/probability of application of artificial intelligence tools in carrying out certain types of expertise (developed by the author on the basis of Parabon NanoLabs data). Source: Parabon Nanolabs (2024).

A more detailed examination of this list requires a focus on certain types individually.

3.1. Physical and hybrid evidence analysis

Currently, automated systems employed in fingerprint analysis (such as AFIS [IAFIS] – Automated Fingerprint Identification System [Integrated Automated Fingerprint Identification System]) (FBI 2012, 2024) enable instant comparison of fingerprints with vast databases. AI can analyze partial and distorted fingerprint impressions, reconstructing damaged prints (Sparkes 2021). The use of neural networks significantly reduces identification time from several days to seconds. In particular, the enhancement of ABIS performance through AI is supported by experts from Thales, a major defense and aerospace company headquartered in Paris (Thales 2026). According to a study by Allied Research conducted in January 2022, the market for automated fingerprint identification systems (hardware and software) is projected to reach 68 billion USD by 2030, with a compound annual growth rate (CAGR) of 23.0% from 2021 to 2030 (Allied Market Research 2022).

Ballistics has historically relied on specialized professional training and personal examiner expertise. In the early 2000s, the capabilities of criminalists were enhanced by new technical tools, such as the IBIS (Integrated Ballistics Identification System) – an automated ballistic visualization and analysis system. At this stage, IBIS, based on its stated characteristics, does not use machine learning (ML). IBIS can search through large volumes of existing images and previous evidence from crime scenes, offering a small number of cases as potential matches. The forensic firearms expert then examines each potential match and decides whether a match truly exists (Allied Market Research 2022). AI could assist experts in this process. Its algorithms could potentially detect subtle differences between samples that are difficult to identify manually. Moreover, AI algorithms could be useful for automating the comparison of ballistic evidence,

improving accuracy, and reducing errors associated with human factors. Although comprehensive information on the use of AI in systems like IBIS is lacking in public sources, the idea that deep learning could enhance such systems is suggested in several studies (Dutta *et al.* 2021).

3.2. *Digital and data-intensive forensic domains*

The field of computer-technical expertise (digital forensics) is the most organic environment for the implementation of AI and machine learning (deep learning) capabilities. Already, AI analyzes vast amounts of data, identifying patterns in internet activity, financial transactions, correspondence, recovering deleted files, and detecting hidden data (e.g., in Bitcoin transactions). It also identifies traces of cyberattacks by analyzing network traffic and behavioral anomalies, as well as recognizing forged audio and video recordings (deepfake analysis). Companies such as Darktrace utilize AI for cybersecurity purposes (Industrial Cyber 2025). However, according to representatives of Malwarebytes, this potential is far from fully realized (Malwarebytes 2024). In this context, AI can provide forensic experts with a broad toolkit for the automatic search for evidence in the digital environment.

The next field is biological (DNA) expertise. In this case, it is important to note that there are already many examples of the effective use of AI in biological forensics today (Flinders University 2024a, 2024b). Machine learning accelerates the DNA identification process by analyzing complex genetic markers. AI can work with partially degraded or contaminated samples, and DNA analysis systems can identify distant relatives, helping to solve crimes even decades later. Practicing professionals in the field of applied genetics emphasize that AI and machine learning can significantly improve the sensitivity of PCR testing, which is of great importance in forensic medicine (Flinders University 2024a). Among the key advantages are the speed of sample processing and the comparison of DNA profiles.

The field of video technical expertise has almost entirely transitioned from analog video recording technologies and media to digital technologies, which expands AI's applicability to this domain. The enhancement of AI capabilities for analyzing surveillance camera footage, automatic face recognition, object identification, and vehicle recognition—specifically for forensic purposes—is currently being undertaken by major IT companies such as Icetana and SoftServe (Icetana AI 2024, Leno and Hnot 2024). As their experience shows, the use of AI is essential for improving image quality and restoring details, even when frames are blurred or damaged. AI aids in detecting manipulations with videos (e.g., tampering using deepfake technologies) (Qureshi *et al.* 2024, The IoT Academy 2024). Meanwhile, the main argument for supporting AI in this field of forensic expertise is automation and increased processing speed, specifically for the automatic processing and analysis of video files.

Regarding phonoscopic expertise (referred to as “audio forensics” in many English-language sources), this work found limited evidence of practical AI usage in the improvement of this type of forensic activity. Currently, experiments are being conducted to enhance audio forensics software using specialized platforms such as TensorBoard, which is associated with the design and implementation of neural networks (HPCC Systems 2024). The expansion of the phonoscopy toolkit through AI

for this industry is related to the capabilities of automatic audio analysis, speaker identification by voice, detection of counterfeit recordings, uncovering edits, and improved noise reduction (Gupta *et al.* 2024). It is also possible to discuss the potential for recognizing hidden messages and anomalies in speech. At the current stage, specialists are dealing with the lengthy process of manual spectrogram analysis.

Machine learning has the potential to expand the capabilities of linguistic expertise. Research conducted by the British Forensic Capability Network (FCN) has demonstrated that AI models can identify threatening and abusive messages up to 21 times faster than humans, which could significantly enhance the speed of police investigations (Forensic Capability Network 2024). Currently, applied software applications such as FLINT Systems are utilizing AI for forensic purposes (Nagel 2023). According to information from FCN, in the context of linguistic expertise, AI can improve text analysis mechanisms for detecting threats, extremist statements, manipulations, and falsifications, as well as identify the author of a text based on linguistic features. Looking ahead, it is possible to say that AI holds substantial potential for development in the automatic detection of fake news and disinformation.

AI also holds considerable promise for enhancing the capabilities of forensic chemical analysis. This potential is notably highlighted in materials from the U.S. National Institute of Standards and Technology (Taylor *et al.* 2024). At this stage, no AI-enhanced software applications specifically for forensic chemical analysis have been identified. However, it appears that the development of such applications is a matter of near-future prospects. AI could likely strengthen systems such as LIMS (Laboratory Information Management System), a widely used specialized software for managing laboratory workflows and documents. Additionally, AI could be employed for the analysis of chemical compounds, the detection of traces of drugs, poisons, and explosives, the automatic recognition of a substance's composition from spectral data, and particularly, for the identification of rare or modified chemical compounds. This conclusion is drawn from a review of research studies (Wankhade *et al.* 2022).

In the context outlined above, the applicability of AI to the field of financial and economic expertise appears to be quite organic, especially with the emergence of new types of financial transactions such as cryptocurrency deals, P2P payments, and the expansion of digital accounting tools (PwC 2023). Major companies in the consulting and corporate investigation sectors also note this. For example, materials from the international consulting firm Kroll highlight that AI has demonstrated its transformative power, particularly in combating financial crimes. AI-based systems can accurately analyze vast amounts of financial data in real-time, quickly detecting suspicious or potentially criminal activity. As a result, AI has become an essential tool for preventing fraud, detecting money laundering risks, and conducting Know Your Customer (KYC) checks (Bock *et al.* 2024). According to data from the financial intelligence company Valid8 Financial, 60% of companies engaged in forensic accounting are already using AI-based tools for fraud investigation (Valid8 2024). AI-enhanced platforms such as Quantifind's Graphyte already automate the detection of financial crimes by analyzing news, legal documents, and sanction lists (McShane *et al.* 2022). Future applications are expected to extend to transaction analysis, anomaly detection in financial statements, and identification of forged documents.

In conclusion, AI-enhanced applications have become an integral part of the toolkit across almost all major fields of modern forensic science. This applies to both its traditional sectors and to newer disciplines that emerged with the so-called third industrial revolution, such as computer and digital forensics. While AI is actively used in forensic science, there are areas where its application is limited or inapplicable for several reasons: the complexity of analysis, the need for human judgment, ethical concerns, and the insufficient reliability of algorithms. In these circumstances, even some of the previously highlighted types of forensic expertise can be characterized as hybrid or, in general, as those where AI capabilities are not applicable. The former category includes, for example, the aforementioned forensic phonoscopic expertise, while the latter encompasses psychological and psychiatric expertise, psychophysiological expertise, and several others.

3.3. Behavioural and interpretative expertise

Regarding psychological and psychiatric expertise, it should be noted that, at present, there are no clear arguments in favor of AI being useful for assessing psychological traits, pathologies, and related tasks. While some studies allow for the potential use of AI in psychological and psychiatric expertise, they mainly focus on the design of predictive AI systems, particularly in relation to the collection and processing of training data, the selection of machine learning methods, and the determination of requirements for explainability, rather than addressing ad hoc solutions. Furthermore, such integration is fraught with ethical challenges (Starke *et al.* 2023). Overall, the diagnosis of mental disorders requires a deep understanding of an individual's personality, motives, and emotions, which AI cannot replicate. It is not possible for AI to objectively assess the mental competence of a defendant or the degree of trauma experienced by a witness, while decisions and expert conclusions regarding the actions and personality of the subject of examination depend on the individual approach of the specialist, rather than solely on data analysis.

The field of handwriting analysis, although not fundamentally unsuitable for the implementation of AI (as evidenced by the development of applications such as TextOracle) (Lim 2024) may find AI's capabilities to be ineffective in complex cases. Handwriting can change due to factors such as stress, illness, or age, making automated analysis unreliable. Moreover, hand-executed forgeries can be so skillfully crafted that they require subjective judgment from the expert. There is evidence that AI performs well with typical samples, but in complex cases (such as intentionally altered handwriting or imitations), its accuracy sharply decreases (Zhao and Li 2023).

Obvious challenges for the implementation of AI are present in the field of linguistic expertise, particularly due to the inability to assess subtext and intent. AI can analyze text for keywords, but to date, there is no evidence to suggest that AI is capable of fully understanding context, tone, sarcasm, or hidden meaning. In legal practice, the author's intent is crucial, and AI cannot reliably determine this. Furthermore, AI is incapable of accounting for cultural and linguistic nuances, which can lead to erroneous conclusions (Denning and Arquilla 2022).

The field of forensic medicine also faces challenges related to the subject of research, especially in complex cases. For instance, determining the cause of death, particularly in

cases of complicated or combined injuries, requires not only data analysis but also expert judgment. The analysis of injuries and the interpretation of their causality depend on numerous factors (such as the mechanics of the impact, tissue interaction, etc.), which are difficult to formalize into algorithms. Certain cases (e.g., poisoning with rare substances) require an unconventional approach, which exceeds the capabilities of AI (Hussain and Jyotishana 2024). This also applies to the field of psychophysiological expertise, particularly in the interpretation of polygraph results. Polygraph studies rely on physiological reactions (e.g., pulse, sweating), but they do not provide 100% accuracy. Emotional responses may depend on a variety of factors (stress, fear, physiological condition), which AI cannot correctly interpret (Europolygraph 2024, Hamzelou 2024). As a result, errors in interpretation may lead to false accusations or the acquittal of criminals.

AI is of limited use in traceology when clear data is absent. Traces of footwear, vehicles, or tools are often blurred, partially erased, or deformed, making automated analysis difficult. In some cases, manual restoration of traces is required, which goes beyond the capabilities of AI algorithms (Bennett and Budka 2024). Additionally, unique or non-standard objects (e.g., homemade weapons) may not have analogs in databases, rendering machine analysis ineffective. The same applies to the expertise of explosives and chemical compounds (for example, in the case of complex mixtures). In practice, certain compositions of explosives or poisons contain components that AI may not recognize if they are not included in the training database. Combinations of chemical compounds may produce unexpected reactions that require an unconventional approach. Particularly, such opinions are outlined in profile research. There is noted that the chemical variability of homemade explosives and the complex reactions between components complicates adequate modeling by AI, especially in the field conditions (Aljanaahi *et al.* 2025, Prior *et al.* 2025). Modern methods, such as near-infrared spectroscopy with machine learning, demonstrate high accuracy in detecting key explosive precursors, but their effectiveness depends on the quality and diversity of training data (Prior *et al.* 2025). Furthermore, the analysis of the explosion mechanism and the assessment of damage also require human expertise (US Department of Homeland Security 2023). The research also notes that the use of AI in forensic chemistry is associated with risks such as algorithmic errors, misinterpretation of data, and the “black box” effect, where model results are difficult to explain and verify (Kleinstreuer and Hartung 2024, Sisodia 2025). These issues, in turn, can lead to erroneous conclusions, which is particularly critical in legal proceedings where high reliability and transparency of evidence are required. To mitigate these risks, it is proposed to use explainable AI (XAI), rigorous model validation, and continuous oversight by human experts (Hartung 2023, Hartung and Kleinstreuer 2025).

As for phonoscopic expertise, it was previously noted that AI could significantly enhance the capabilities of analysis in this field, but there may be certain “pitfalls” here as well. For instance, when dealing with deepfake voice forgery. It is widely known that modern deepfake technologies allow the creation of realistic voice forgeries that can deceive even AI, especially when such deepfakes are themselves generated using AI (Brodsky 2023). Meanwhile, the analysis of the emotional state of the speaker (e.g., stress, lying) has not yet reached a high level of accuracy. In situations where the court

demands a high degree of reliability, which AI cannot yet guarantee, machine analysis may not be accepted by the court as valid evidence.

Thus, this study combines the theoretical justification of the relevance of the use of AI in forensic analysis and offers a relevant classification of types of forensic analysis depending on the frequency/possibility of using AI tools in its conduct. In conclusion, the existing and potential capabilities of AI for forensics are indeed impressive. Although comprehensive quantitative measurements of its effectiveness have not yet been conducted, it is becoming evident that AI-powered applications can significantly accelerate processes in the work of forensic experts, not to mention the opportunities for clearer and more detailed analysis of the data obtained. However, as can be understood, the capabilities of AI are limited in areas where a deep understanding of the human psyche is required, complex interpretation of multilayered data is necessary, or in cases involving unique situations where there is insufficient training data, as well as where legal and ethical responsibilities for errors are present. Therefore, AI remains a tool that complements, rather than replaces, experts in forensic science. Looking ahead, there are no compelling reasons to believe this arrangement will change in the foreseeable future.

4. Discussion

Contemporary research on AI in forensic science reveals a consistent pattern: the technology's applicability is strongly correlated with the degree to which a forensic task can be reduced to data processing, pattern recognition, or large-scale comparison. Where these conditions are met — as in digital forensics, DNA analysis, or financial crime detection - AI integration is already substantial. Where they are not - as in psychological assessment, handwriting analysis, or polygraph interpretation - human judgment remains irreplaceable. As is rightly noted, despite the significant assimilation of artificial intelligence in digital forensics, the use of machine intelligence in “traditional” forensics remains limited (Hamzah *et al.* 2022). Forensic experts still rely on traditional methods, which are constrained in certain aspects, such as data analysis. However, it is encouraging that scholars and legal professionals are gradually recognizing the advantages of AI-powered applications (Farber 2025, Renukadevi *et al.* 2024).

Overall, there is no controversy regarding the fact that, at present, AI cannot fully replace the work of forensic experts in various fields. However, a systematic analysis of this issue, encompassing forensic science as both an applied discipline and a professional activity, has yet to be found. The arguments concerning the applicability or non-applicability of AI to a given activity typically address specific professional areas. This pattern is consistently supported across the literature. AI has demonstrated clear applicability in data-intensive forensic fields. In fingerprinting, neural network-based systems have reduced identification time from days to seconds while improving accuracy on partial prints (Maiti and Das 2022, Siegel *et al.* 2022). In digital forensics, AI enables automated detection of cyberattack traces and recovery of hidden data at a scale unachievable by manual methods (Dunsin *et al.* 2022). DNA analysis benefits from AI's ability to process degraded samples and identify distant genetic relatives (Alketbi 2024, McDonald *et al.* 2024, Sessa *et al.* 2024), while in financial forensics, AI-powered platforms flag anomalies across vast transaction datasets in real time (Mubarrat 2024). Across these domains, the common denominator is volume and pattern: AI excels precisely where human analysts face cognitive and temporal limits. However, as

previously noted, at this stage, no AI-enhanced software applications for forensic chemistry have been identified, nor has there been any evidence of AI implementation in software used for ballistic expertise. This is also supported by the lack of relevant studies confirming the existence of such applications or pilot projects. Nevertheless, compelling arguments are made that such products are needed and will likely emerge soon (Patsiouras *et al.* 2024, Raghav *et al.* 2025). A notable gap in the literature, however, is the relative neglect of AI's limitations. Research tends to foreground opportunities over constraints, yet the evidence points to a clear boundary: fields requiring contextual human judgment — psychological assessment, linguistic interpretation, polygraph analysis — consistently resist meaningful AI integration. Nevertheless, a number of studies support the finding that AI's applicability is limited in fields requiring contextual human judgment. In forensic psychiatry, Starke *et al.* (2023) argue that AI models cannot replicate the externalist reasoning required to assess mental competence, while Wang *et al.* (2023) demonstrate that AI systematically fails to interpret linguistic intent and cultural subtext. Chen and Tseng (2023) identify the boundary of AI in forensic medicine as lying precisely where causal interpretation of complex injuries begins. Across these fields, the limitation is not technical but epistemological: the tasks require understanding that cannot be reduced to pattern matching in training data. For example, many AI models used in forensic psychiatry are considered “black boxes,” which complicates their interpretation and raises concerns about the reliability of their conclusions. This is particularly critical in decision-making contexts that can have serious consequences for individuals' lives. The use of AI in forensics raises questions about accountability in the case of errors in analysis. A key issue is who will bear responsibility for potential mistakes or complaints regarding the results. This raises concerns regarding ethical accountability and legal consequences, including the fact that AI requires extensive databases for training. If the input data falls outside the scope of trained datasets, it may lead to false positives or false negatives in interpretation (Ahmed Alaa El-Din 2022, Andrić and Ivanović 2023). Beyond these dataset-related risks, the literature identifies a broader range of threats associated with AI deployment across forensic disciplines. These include the misinterpretation of algorithmically generated outputs by practitioners unfamiliar with the underlying models, the propagation of errors through automated pipelines without human oversight, and the risk of over-reliance on AI conclusions in courtroom settings where explainability remains insufficient. Such concerns have been documented across multiple forensic domains, including digital forensics (Dunsin *et al.* 2024), forensic medicine (Hussain and Jyotishana 2024), and phonoscopy (Öztürk *et al.* 2024), suggesting that the challenge is systemic rather than field-specific. The legal admissibility of AI-generated evidence raises three interconnected concerns that warrant explicit discussion. First, explainability: courts increasingly require that expert conclusions be transparent and reproducible, yet many AI models operate as “black boxes” whose internal logic cannot be articulated in legal proceedings (Hall *et al.* 2022). Second, admissibility: for AI-derived evidence to be accepted in court, the underlying models must be reproducible, validated, and verifiable — conditions that are not yet consistently met across forensic disciplines (Gustafson 2024). Third, accountability: when AI-assisted analysis produces erroneous results, the question of who bears legal and professional responsibility — the developer, the forensic expert, or the institution — remains unresolved in most jurisdictions (Andrić and Ivanović 2023). Addressing these three dimensions is a precondition for the responsible

integration of AI into forensic practice and legal proceedings. Alongside legal admissibility, the ethical and governance dimensions of AI in forensics require closer attention. Dataset bias poses a particular risk: if training data overrepresents certain demographic groups or crime types, AI models may produce systematically skewed results, with potentially discriminatory consequences in legal proceedings (Andrić and Ivanović 2023). Transparency is equally critical — forensic conclusions derived from opaque models undermine the principle of verifiability that is foundational to expert evidence. At the governance level, the absence of unified regulatory frameworks for AI use in forensic contexts creates significant uncertainty: currently, neither the conditions for certifying AI-based forensic tools nor the standards for their validation are consistently defined across jurisdictions (Hall *et al.* 2022). Addressing these gaps is essential for ensuring that AI integration into forensic practice remains consistent with the principles of fairness, accountability, and the rule of law. At the same time, no studies have been found that consider the applicability of AI's capabilities for forensic science as a whole, consolidating information on the applicability or non-applicability of AI to various fields. Such comprehensive studies contribute to the development of unified approaches to AI integration in forensic science, supporting the transparency and verifiability of expert conclusions. They are also essential for establishing methods and standards that uphold the key principles of forensic expert activities. In general, contemporary works rightly emphasize the need for cooperation between various specialists to maximize the potential of machine intelligence in forensic science, particularly in the rapidly growing field of digital forensics (Hamzah *et al.* 2022, Rizvi *et al.* 2022, Galante *et al.* 2023). It is noted that there is an urgent need to overcome the current limitations of the forensic tools used, expand the utilization of available resources, and develop more reliable algorithms to enhance the efficiency of forensic investigations. Taken together, these findings suggest that the most productive framework for AI in forensics is not substitution but augmentation: AI handles scale, speed, and pattern recognition, while human experts provide judgment, context, and accountability (Hamzah *et al.* 2022).

5. Conclusions

Thus, a number of areas in forensic science and forensic examination have been identified where AI capabilities are already implemented, and their role is highly likely to continue to grow. AI is becoming an indispensable tool, particularly in fields that require the processing of large volumes of data, sample comparison, and the identification of complex patterns. Although AI does not yet replace experts, it accelerates investigations to a certain extent, reduces the likelihood of errors, and provides new tools for investigating crimes that have remained unsolved for long periods. As can be inferred, forensic science will increasingly deal with new types of activities moving into the digital domain in the future, adapting methodological and applied tools accordingly. As machine learning advances, forensic science gains new tools for handling both routine and specialized tasks. AI may be integrated into existing software or built into purpose-designed AI-powered applications from the outset. AI is becoming part of the working toolkit of almost all major areas of modern forensic science, covering both its “traditional” sectors and types of expertise, as well as those emerging from human activities in the digital environment.

Despite the active use of AI in forensic science today, there are areas where its application is limited or inapplicable. This is due to factors such as the complexity of analysis, the need for human judgment, ethical issues, and the insufficient reliability of algorithms. Based on the results of this research, it can be noted that AI capabilities are already widely used in conducting such types of expertise as fingerprinting, computer and technical expertise, biological, video technical, financial-economic, and several others. Moreover, the dependence of these fields on AI tools is likely to increase. This is evidenced by both the development and practical implementation of software applications for these sectors, scientific assessments of the state, and prospects of AI implementation within them. At the same time, for a number of forensic examinations and applied fields (psychological and psychiatric, handwriting analysis, linguistic, etc.), AI capabilities remain limited due to the specific nature of forensic fields, which are more dependent on human discretion and require an understanding of human psychology and the context of certain events in various parameters. From a practical application perspective, this work highlights which areas of forensic science will require involvement in the future, which will undoubtedly be important for understanding this segment of the labor market and education.

References

- Ahmed Alaa El-Din, E., 2022. Artificial intelligence in forensic science: Invasion or revolution? *Egyptian Society of Clinical Toxicology Journal* [online], 10(2), 20–32. Available at: <https://doi.org/10.21608/esctj.2022.158178.1012>
- Aljanaahi, A., et al., 2025. A review of analytical and chemometric strategies for forensic classification of homemade explosives. *Analytical Science Advances* [online], 6(1), e70010. Available at: <https://doi.org/10.1002/ansa.70010>
- Alketbi, S. K., 2024. Emerging technologies in forensic DNA analysis. *Perspectives in Legal and Forensic Sciences* [online], 1(1), 1–24. Available at: <https://doi.org/10.70322/plfs.2024.10007>
- Allied Market Research, 2022. *Automated Fingerprint Identification Systems (AFIS) Market Outlook – 2030* [online] Available at: <https://www.alliedmarketresearch.com/automated-fingerprint-identification-system-market-A12196>
- Andrić, S. D., and Ivanović, A. B., 2023. Forensic sciences and ethics in the era of application of artificial intelligence. *Kriminalističke Teme* [online], 23(3-4), 95–102. Available at: <https://doi.org/10.51235/kt.2023.23.3-4.95>
- Bennett, M. R., and Budka, M., 2024. *AI trained to recognise footprints, but it won't replace forensic experts yet* [online]. Available at: <https://www.europeandissemination.eu/ai-trained-to-recognise-footprints-but-it-wont-replace-forensic-experts-yet/14799>
- Bock, T., Conolly, P., and Barroso, F., 2024. *Why high-quality data is crucial to fighting financial crime* [online]. 26 June. Available at: <https://www.kroll.com/en/insights/publications/ai-financial-crime-prevention>

- Brodsky, S., 2023. *Deepfake audio powered by AI can fool you – Here’s why you should care* [online]. 7 August. Available at: <https://www.lifewire.com/ai-powered-deepfake-audio-7570357>
- Chen, Y., and Tseng, P., 2023. The boundary of artificial intelligence in forensic science. *Dialogo* [online], 10(1), 83–90. Available at: <https://doi.org/10.51917/dialogo.2023.10.1.5>
- Denning, P. J., and Arquilla, J., 2022. *The context problem in artificial intelligence* [online]. 1 December. Available at: <https://cacm.acm.org/opinion/the-context-problem-in-artificial-intelligence/>
- Dunsin, D., et al., 2024. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation* [online], 48, 301675. Available at: <https://doi.org/10.1016/j.fsidi.2023.301675>
- Dunsin, D., Ghanem, M. C., and Ouazzane, K., 2022. *The use of artificial intelligence in digital forensics and incident response (DFIR) in a constrained environment* [online]. International Conference on Digital Forensics and Security of Cloud Computing (ICDFSCC). London Met Repository, 1–5. Available at: <https://repository.londonmet.ac.uk/7708/>
- Dutta, S. K., et al., 2021. Study on enhanced deep learning approaches for value-added identification and segmentation of striation marks in bullets for precise firearm classification. *Applied Soft Computing* [online], 112, 107789. Available at: <https://doi.org/10.1016/j.asoc.2021.107789>
- Europolygraph, 2024. *The polygraph: A reliable tool for truth detection in the 21st century* [online]. 27 September. Available at: <https://europolygraph.org/en/the-polygraph-a-reliable-tool-for-truth-detection-in-the-21st-century/>
- Farber, S., 2025. AI as a decision support tool in forensic image analysis: A pilot study on integrating large language models into crime scene investigation workflows. *Journal of Forensic Sciences* [online], 70(3), 932–943. Available at: <https://doi.org/10.1111/1556-4029.70035>
- FBI, 2012. *Privacy Impact Assessment Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability* [online]. Available at: <https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/freedom-of-information-privacy-act/department-of-justice-fbi-privacy-impact-assessments/iafis-ngi-biometric-interoperability>
- FBI, 2024. *The integrated automated fingerprint identification system* [online]. Available at: https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/iafis_0808_one-pager825
- Flinders University, 2024a. *AI promises to ramp up PCR tests for faster DNA diagnostics and forensics* [online]. 30 September. Available at: <https://www.clinicallab.com/ai-promises-to-ramp-up-pcr-tests-for-faster-dna-diagnostics-and-forensics-28038>

-
- Flinders University, 2024b. *AI used to upgrade DNA forensics* [online]. 12 October. Available at: <https://news.flinders.edu.au/blog/2024/10/12/ai-used-to-upgrade-dna-forensics/>
- Forensic Capability Network, 2024. *AI can detect abusive messages 21 times faster than humans* [online]. 16 July. Available at: <https://www.fcn.police.uk/news/2024-07/ai-can-detect-abusive-messages-21-times-faster-humans>
- Galante, N., et al., 2023. Applications of artificial intelligence in forensic sciences: Current potential benefits, limitations and perspectives. *International Journal of Legal Medicine* [online], 137(2), 445–458. Available at: <https://doi.org/10.1007/s00414-022-02928-5>
- Gupta, R., et al., 2024. Voice disorder recognition using machine learning: A scoping review protocol. *BMJ Open* [online], 14(2), e076998. Available at: <https://doi.org/10.1136/bmjopen-2023-076998>
- Gustafson, K., 2024. *Modern forensic science technologies* [online]. 7 January. Available at: <https://www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies>
- Hall, S. W., Sakzad, A., and Choo, K. R., 2022. Explainable artificial intelligence for digital forensics. *WIREs Forensic Science* [online], 4(2), e1434. Available at: <https://doi.org/10.1002/wfs2.1434>
- Hamzah, N. H., et al., 2022. Artificial intelligence in forensic science: Current applications and future direction. *Buletin Sains Kesehatan* [online], 6(2), 39–46. Available at: <https://myjms.mohe.gov.my/index.php/bsk/article/view/16561>
- Hamzelou, J., 2024. *AI lie detectors are better than humans at spotting lies* [online]. 5 July. Available at: <https://www.technologyreview.com/2024/07/05/1094703/ai-lie-detectors-are-better-than-humans-at-spotting-lies/>
- Hartung, T., 2023. Artificial intelligence as the new frontier in chemical risk assessment. *Frontiers in Artificial Intelligence* [online], 6, 1269932. Available at: <https://doi.org/10.3389/frai.2023.1269932>
- Hartung, T., and Kleinstreuer, N., 2025. Challenges and opportunities for validation of AI-based new approach methods. *ALTEX - Alternatives to Animal Experimentation* [online], 42(1), 3–21. Available at: <https://doi.org/10.14573/altex.2412291>
- HPCC Systems, 2024. *Machine learning and the forensic application of audio classification* [online]. Available at: <https://hpccsystems.com/resources/machine-learning-and-the-forensic-application-of-audio-classification/>
- Hussain, D. A., and Jyotishana, J., 2024. The application of artificial intelligence in the forensic medicine and toxicology: Need of the hour. *International Journal of Forensic Medicine* [online], 6(2), 25–29. Available at: <https://doi.org/10.33545/27074447.2024.v6.i2a.91>
- Icetana AI, 2024. *Icetana AI are experts in AI CCTV Systems* [online]. Available at: <https://www.icetana.ai/ai-cctv-analytics>
-

- Industrial Cyber, 2025. *Darktrace 2025 Report: AI threats surge, but cyber resilience grows amidst skills gap* [online]. 5 March. Available at: <https://industrialcyber.co/ai/darktrace-2025-report-ai-threats-surge-but-cyber-resilience-grows-amidst-skills-gap/>
- Jarrett, A., and Choo, K. K. R., 2021. The impact of automation and artificial intelligence on digital forensics. *WIREs Forensic Science* [online], 3(6), e1418. Available at: <https://doi.org/10.1002/wfs2.1418>
- Karpunsov, V., & Veresha, R. 2023. Legal Aspects of Virtual Assets Regulation in Ukraine. *DANUBE*, 14(3), 235–252. Available at: <https://doi.org/10.2478/danb-2023-0014>
- Kleinstreuer, N., and Hartung, T., 2024. Artificial intelligence (AI)—it’s the end of the tox as we know it (and I feel fine)*. *Archives of Toxicology* [online], 98, 735–754. Available at: <https://doi.org/10.1007/s00204-023-03666-2>
- Leno, S., and Hnot, T., 2024. *Future of VQA: How multimodal AI is transforming video analysis* [online]. 30 October. SoftServe. Available at: <https://www.softserveinc.com/en-us/blog/multimodal-ai-for-video-analysis>
- Lim, A., 2024. *TextOracle: Using AI to support forensic handwriting analysis* [online]. HTX. 19 January. Available at: <https://www.htx.gov.sg/whats-happening/all-news---events/all-news/2024/featured-news--textoracle--using-ai-to-support-forensic-handwriting-analysis>
- Maiti, D., and Das, D., 2022. Gender and hand identification based on dactyloscopy using deep convolutional neural network. In: A. K. Das *et al.*, eds., *Computational intelligence in pattern recognition: Proceedings of CIPR 2023* [online]. Cham: Springer, 145–155. Available at: https://doi.org/10.1007/978-981-99-3734-9_13
- Malwarebytes, 2024. *II v kiberbezopasnosti — riski i vozmozhnosti [AI in cybersecurity: Understanding the risks]* [online]. Available at: <https://www.malwarebytes.com/ru/cybersecurity/basics/risks-of-ai-in-cyber-security>
- McDonald, C., *et al.*, 2024. Developing a machine learning ‘smart’ polymerase chain reaction thermocycler part 2: Putting the theoretical framework into practice. *Genes* [online], 15(9), 1199. Available at: <https://doi.org/10.3390/genes15091199>
- McShane, E. J., *et al.*, 2022. Quantifying graphite solid-electrolyte interphase chemistry and its impact on fast charging. *ACS Energy Letters* [online], 7(8), 2734–2744. Available at: <https://doi.org/10.1021/acsenergylett.2c01059>
- Mubarrat, A. A., 2024. *Role of artificial intelligence and big data in modern forensic accountancy*. Available at: <https://doi.org/10.2139/ssrn.5078259>
- Nagel, D., 2023. AI writing detection tool uses ‘forensic linguistic’ techniques to check authorship. *THE Journal* [online], 7 March. Available at: <https://thejournal.com/articles/2023/03/07/ai-writing-detection-tool-uses-forensic-linguistic-techniques-to-check-authorship.aspx>
- Öztürk, S., Özyer, B., and Temiz, Ö., 2024. Detection of voices generated by artificial intelligence with deep learning methods. In: A. E. Çetin and E. Erdem, eds., 2024

-
- 32nd Signal Processing and Communications Applications Conference (SIU) [online]. Mersin: IEEE, 1–4. Available at: <https://doi.org/10.1109/SIU61531.2024.10601078>
- Parabon Nanolabs, 2024. *The snapshot DNA phenotyping service* [online]. Available at: <https://snapshot.parabon-nanolabs.com/#phenotyping>
- Patsiouras, E., *et al.*, 2024. Integrating AI and computer vision for ballistic and bloodstain analysis in 3D digital forensics. In: S. Livatino, P. Arpaia and L. T. De Paolis, eds., *2024 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRINE)* [online]. St Albans: IEEE, 734–739. Available at: <https://doi.org/10.1109/MetroXRINE62247.2024.10796512>
- Prior, A., *et al.*, 2025. Improving first responder forensic capabilities: On-site detection and quantification of explosive precursors using portable near-infrared spectroscopy and machine learning. *Forensic Science International* [online], 368, 112378. Available at: <https://doi.org/10.1016/j.forsciint.2025.112378>
- PwC, 2023. *Impact of Artificial Intelligence on fraud and scams* [online]. December. Available at: <https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf>
- Qureshi, S. M., *et al.*, 2024. Deepfake forensics: A survey of digital forensic methods for multimodal deepfake identification on social media. *PeerJ Computer Science* [online], 10, e2037. Available at: <https://doi.org/10.7717/peerj-cs.2037>
- Raghav, A., *et al.*, 2025. Forensic ballistics and artificial intelligence: Legal challenges and enhancing international framework for scientific evidence. In: C. Kaunert, ed., *Forensic intelligence and deep learning solutions in crime investigation* [online]. Hershey: IGI Global, 163–182. Available at: <https://doi.org/10.4018/979-8-3693-9405-2.ch009>
- Rawat, R., *et al.*, 2023. Autonomous artificial intelligence systems for fraud detection and forensics in dark web environments. *Informatika* [online], 47(9), 51–62. Available at: <https://doi.org/10.31449/inf.v46i9.4538>
- Renukadevi, P., John, S., and Shivani, N., 2024. Forensic Science: AI-Powered Image and Audio Analysis. *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)* [online]. Trichy: IEEE, 1519–1525. Available at: <https://doi.org/10.1109/icosec61587.2024.10722068>
- Rizvi, S., *et al.*, 2022. Application of artificial intelligence to network forensics: Survey, challenges and future directions. *IEEE Access* [online], 10, 110362–110384. Available at: <https://doi.org/10.1109/ACCESS.2022.3214506>
- Sessa, F., *et al.*, 2024. Artificial intelligence and forensic genetics: Current applications and future perspectives. *Applied Sciences* [online], 14(5), 2113. Available at: <https://doi.org/10.3390/app14052113>
- Siegel, D., *et al.*, 2022. Forensic data model for artificial intelligence based media forensics-Illustrated on the example of DeepFake detection. *Electronic Imaging* [online], 34, 1–6. Available at: <https://doi.org/10.2352/EI.2022.34.4.MWSF-324>
-

- Sisodia, N., 2025. Artificial Intelligence in Forensic Toxic Science: Emerging Trends and Analytical Techniques. *International Journal for Research in Applied Science and Engineering Technology* [online], 13(9), 1571–1579. Available at: <https://doi.org/10.22214/ijraset.2025.74270>
- Snohomish County, 2022. *Suspect identified in 1990 homicide cold case* [online]. 30 June. Available at: <https://www.snohomishcountywa.gov/Archive.aspx?ADID=6870>
- Sparkes, M., 2021. AI clears up images of fingerprints to help with identification. *New Scientist* [online], 28 June. Available at: <https://www.newscientist.com/article/2282218-ai-clears-up-images-of-fingerprints-to-help-with-identification/>
- Starke, G., D’Imperio, A., and Ienca, M. 2023. Out of their minds? Externalist challenges for using AI in forensic psychiatry. *Frontiers in Psychiatry* [online], 14, 1209862. Available at: <https://doi.org/10.3389/fpsy.2023.1209862>
- Taylor, M., Osborne, N., and Waltke, H., 2024. *Artificial Intelligence (AI) in forensic science use case explorer* [online]. National Institute of Standards and Technology (NIST). Available at: <https://forensicrti.org/wp-content/uploads/2024/10/Artificial-Intelligence-AI-in-Forensic-Science-Use-Case-Explorer.pdf>
- Thales, 2026. *CABIS. The next generation of ABIS* [online]. Available at: <https://www.thalesgroup.com/en/solutions-catalogue/public-security/national-security/cabis>
- The IoT Academy, 2024. *Deepfake detection technology – Working/uses/tools* [online]. 20 September. Available at: <https://www.theiotacademy.co/blog/deepfake-detection/>
- US Bureau of Labor Statistics, 2024. *Forensic science technicians* [online]. Available at: <https://www.bls.gov/ooh/life-physical-and-social-science/forensic-science-technicians.htm>
- US Department of Homeland Security, 2023. *Leveraging artificial intelligence is smart for explosive detection* [online]. 14 December. Available at: <https://www.dhs.gov/science-and-technology/news/2023/12/14/feature-article-leveraging-artificial-intelligence-smart-explosive-detection>
- Valid8, 2024. *The impact of AI on fraud investigations: What forensic accountants need to know* [online]. Available at: <https://www.valid8financial.com/guides/m/ai-and-fraud-investigations>
- Veresha, R. 2017. Criminal and legal characteristics of criminal intent. *Journal of financial crime*, 24(1), 118–128. Available at: <https://doi.org/10.1108/JFC-02-2016-0013>
- Wang, J., et al., 2023. Breaking boundaries between linguistics and artificial intelligence. *Journal of Organizational and End User Computing* [online], 35(1), 1–20. Available at: <https://doi.org/10.4018/joec.334013>
- Wankhade, T. D., et al., 2022. Artificial intelligence in forensic medicine and toxicology: the future of forensic medicine. *Cureus* [online], 14(8), 28376. Available at: <https://doi.org/10.7759/cureus.28376>

Zhao, H., and Li, H., 2023. Handwriting identification and verification using artificial intelligence-assisted textural features. *Scientific Reports* [online], 13(1), 21739. Available at: <https://doi.org/10.1038/s41598-023-48789-9>