APPLICATIONS AND POTENTIAL OF ARTIFICIAL INTELLIGENCE IN FORENSIC SCIENCE

Fayzullaev Nurbek[1]
Sambhram University | Jizzakh affiliation
nurbekfayzullayev89@gmail.com
Kuchkarov Muslimjon[2]
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract. *Artificial intelligence (AI) offers significant potential to enhance forensic science by increasing efficiency, pattern recognition, and reproducibility across digital forensics, pathology, biometric identification, and trace analysis. However, AI functions most effectively as a human-supervised decision-support system rather than an autonomous adjudicator. Despite demonstrated task-specific accuracy, widespread courtroom integration is constrained by black-box opacity, small or unrepresentative datasets, and a lack of standardized validation frameworks. The primary imperative is ensuring rigorous validation, explainability, and governance to prevent operational efficiency from compromising procedural fairness, evidentiary reliability, and human-supervised legal accountability.*

Keywords: *Artificial Intelligence, Forensic Science, Digital Forensics, Decision Support Systems, Biometric Identification, Forensic Imaging, Explainable AI, Evidence Validation.*

Artificial intelligence has clear potential in forensic expertise, but the literature supports it most strongly as a decision-support technology that improves speed, pattern recognition, and consistency in specific tasks rather than as a replacement for human experts.

Forensic expertise increasingly faces data volume, time pressure, and interpretive complexity that strain traditional methods, especially in digital evidence, imaging, identification, and large-scale pattern. AI has been introduced across forensic medicine, pathology, anthropology, odontology, genetics, digital forensics, document analysis, image forensics, and crime scene reconstruction because it can automate repetitive analysis, detect weak patterns, and reduce some forms of human subjectivity.

Current evidence suggests that AI improves accuracy, reproducibility, and efficiency in many bounded forensic tasks, including postmortem imaging, biometric recognition, digital evidence triage, dental comparison, file classification, and document forgery detection . At the same time, the field still lacks sufficient external

validation, representative datasets, standardized protocols, and robust legal frameworks for routine courtroom use.

The central problem is therefore not whether AI can be applied to forensic expertise, but whether it can be validated, explained, and governed well enough for trustworthy operational use. This thesis examines the applications, performance, limitations, and future potential of AI technologies in forensic expertise, with the working hypothesis that AI strengthens forensic decision-making when used as an interpretable, human-supervised support system rather than an autonomous adjudicator.

The topic matters because forensic conclusions affect liberty, liability, and public trust, so any technology that changes evidentiary analysis must improve both technical performance and procedural fairness.

Methods

This thesis can be framed as a systematic literature review with narrative synthesis of AI applications in forensic expertise. That design matches the current state of the field, where evidence is heterogeneous across domains, methods, and outcome measures.

The sample comprises peer-reviewed and conference literature on AI in forensic science, forensic medicine, digital forensics, forensic genetics, odontology, imaging, and related expert domains. Studies should be included if they evaluate or review AI-assisted forensic tasks such as identification, classification, detection, reconstruction, prediction, or decision support, and excluded if they are non-forensic, non-human where inapplicable, or lack enough methodological detail for appraisal.

Materials should include bibliographic databases such as PubMed, Scopus, Web of Science, ScienceDirect, Google Scholar, and Cochrane, along with structured search strings combining terms for artificial intelligence, machine learning, deep learning, and forensic science. Data extraction should record forensic domain, AI method, task, dataset type, comparator, performance metrics, validation strategy, and stated ethical or legal concerns.

The procedure should follow PRISMA-style screening, duplicate removal, title and abstract review, full-text eligibility assessment, and quality appraisal using an established critical framework where possible. Analysis should be primarily descriptive and thematic, because the evidence base spans highly different datasets and outcomes, although quantitative summaries of accuracy, precision, recall, F1-score, or error reduction can be reported where directly available.

AI methods compared across forensic domains

Domain	Typical AI Use	Reported Performance or Value	Key Limitation
Digital forensics	Triage, anomaly detection, file and behavior analysis	Faster large-scale evidence processing and improved scalability	Limited datasets and admissibility concerns
Forensic imaging/pathology	Injury detection, virtual autopsy, PMI, cause-of-death support	Reduced variability and improved diagnostic precision	Small or context-specific datasets
Identification sciences	Fingerprints, face, DNA, dental comparison, sketches	High task-specific accuracy in several studies	Demographic bias and weak generalization
Document and media forensics	Forgery, deepfake, audio-image analysis	Strong potential for authenticity verification	Interpretability and cross-domain robustness

Figure 1. AI applications and limits across forensic domains

Results

The literature consistently shows that AI applications in forensic expertise cluster around five practical domains: identification, pathology and imaging, digital forensics, pattern-rich trace analysis, and workflow support. Across these domains, the most common reported advantages are faster evidence processing, higher consistency, reduced observer dependence, and better handling of large or heterogeneous datasets. In digital forensics, AI appears especially valuable because conventional methods struggle with scale, heterogeneity, and real-time demands. Reviews describe uses in data collection and recovery, cybercrime timeline reconstruction, malware and anomaly detection, metadata analysis, email or behavior correlation, and network traffic analysis. One experimental study reported that deep reinforcement learning outperformed Faster R-CNN and YOLO for crime scene object detection, with higher precision, recall, and F1-score in complex scenes. Deep learning has also been proposed to improve corrupted file prediction and file-type identification beyond traditional digital approaches.

Digital and cyber-forensic applications

Application	Main Function	Example Finding
Evidence triage	Rapid scanning of large data volumes	AI can process vast datasets more quickly than manual review
Network forensics	Detect prior or potential attacks	AI-based models support timely network threat detection
Image and file forensics	Detect manipulations or corrupted files	Deep learning improves media and file authenticity analysis
Crime scene object analysis	Detect relevant objects automatically	Deep reinforcement learning outperformed standard detectors
Future sources	IoT, vehicles, smart homes	New evidence sources are a major future opportunity

Figure 2 Digital forensic AI uses and representative findings

In forensic identification, AI has shown promising task-level performance in fingerprints, facial recognition, sketch matching, clothing recognition, dental comparison, and DNA interpretation. Reported single-study results include 96.8% accuracy for fingerprint recognition, 92.3% for facial identification, above 70% for clothing classification from surveillance footage, and improved sketch-to-photo matching using CNNs, GANs, and autoencoders. In forensic odontology, current AI applications concentrate on bite marks, sex determination, age estimation, and dental comparison, with deep learning particularly useful for unstructured image data and transfer learning sometimes used to compensate for limited datasets.

In forensic genetics and related biomolecular fields, AI has been applied to STR interpretation, haplogroup analysis, DNA methylation-based age prediction, DNA extraction support, bacterial classification, and identity-related microbiome inference. However, the literature repeatedly stresses that these systems remain difficult to deploy in real cases because forensic samples are variable, statistical conclusions can be misunderstood in court, and domain communication gaps remain substantial.

In pathology, imaging, and cause-of-death support, AI has been used for injury detection, fracture recognition, time-of-injury estimation, PMI estimation, diatom

analysis in drowning, firearm lesion assessment, and virtual autopsy workflows. Reviews report lower inter-observer variability in postmortem fracture detection and PMI error reductions up to 15% in predictive models, while advanced imaging offers more precise and non-invasive examinations. Yet a scoping review found no AI application clearly established in the daily practice of forensic pathologists so far, indicating a wide translational gap between promising prototypes and medicolegal routine.

Discussion

Taken together, the evidence supports a moderate-to-strong claim that AI can enhance forensic expertise in narrow, well-defined tasks, especially when large datasets, image-heavy evidence, or repetitive classification problems are involved. The best-supported benefits are operational rather than epistemic: AI speeds workflows, scales evidence review, and improves consistency more often than it proves wholly new forensic truths. That pattern is consistent with the broader forensic literature, which repeatedly frames AI as an assistant to expert judgment rather than a substitute for it. This point remains important because forensic decision-making is legal as well as technical, and expert accountability, context interpretation, and communication in court remain human responsibilities. The main limitations recur across the full corpus. Many studies rely on small, homogeneous, simulated, or highly curated datasets, which weakens generalizability to real investigations. Black-box modeling, limited interpretability, and uneven procedural transparency also threaten admissibility and defense scrutiny. Legal frameworks remain underdeveloped, and many authors call for standards, bias testing, validation entities, and lifecycle monitoring before wider adoption.

Research gap priorities

Gap	Why It Matters	Direction
External validation	Lab performance often overstates field readiness	Test on real, diverse casework
Explainability	Courts require transparent reasoning	Prefer interpretable or XAI models
Data diversity	Bias and weak transfer threaten fairness	Build representative shared datasets
Standards and governance	Admissibility depends on procedure, not just accuracy	International protocols and oversight
Training	Tool misuse and mistrust slow adoption	Cross-train forensic and AI professionals

Figure 3 Key barriers to trustworthy forensic AI adoption

The strongest future opportunities lie in multimodal systems, deepfake detection, smart-home and IoT evidence correlation, explainable digital forensics, secure chain-of-custody support, and AI-assisted visualization of complex evidence. Generative AI may expand training, data augmentation, and multimodal synthesis, but its risks are also higher in high-stakes settings such as forensic psychiatry and image analysis

Conclusion

Artificial intelligence technologies have substantial applications and potential in forensic expertise, especially in digital forensics, identification, imaging, pathology, and evidence classification, but the literature supports assisted expertise far more strongly than autonomous forensic judgment. The most important shift is from manual, isolated, and subjective workflows toward scalable, data-driven, human-supervised analysis, while the biggest open question is how to validate and govern these systems so that efficiency gains do not compromise transparency, fairness, and legal reliability.

REFERENCES

1. **Bal, E., & Yalçın Sarıbey, A.** (2025). Artificial Intelligence in Forensic Science: Applications, Legal Framework and Criminal Liability Regime. 2025 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA).
2. **Malik, P., Dawar, H., Patel, P., Ahuja, D., & Jain, A.** (2024). Enhancing Forensic Analysis of Digital Evidence Using Machine Learning: Techniques, Applications, and Challenges. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences.
3. **Du, X., Hargreaves, C., Sheppard, J. W., Anda, F., Sayakkara, A. P., 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. Proceedings of the 15th International Conference on Availability, Reliability and Security.
4. **Karie, N., Kebande, V., Kebande, V., & Venter, H.** (2019). Diverging Deep Learning Cognitive Computing Techniques into Cyber Forensics. Forensic Science International: Synergy.
5. **Zaheen, U., Rakha, A., Hassan, Q., Khan, M. F., Akhtar, S., & Munawar, A.** (2025). A Systematic Review About the Evolving Role of Artificial Intelligence in Various Fields of Forensic Medicine. Journal of Forensic and Legal Medicine.
6. **Galante, N., Cotroneo, R., Furci, D., Lodetti, G., & Casali, M.** (2022). Applications of Artificial Intelligence in Forensic Sciences: Current

Potential Benefits, Limitations and Perspectives. International Journal of Legal Medicine.

7. **Arthanari, A., Raj, S., & Ravindran, V**. (2025). A Narrative Review in Application of Artificial Intelligence in Forensic Science: Enhancing Accuracy in Crime Scene Analysis and Evidence Interpretation. Journal of International Oral Health.
8. **Shepitko, M., & Latysh, K.** (2024). Use of Artificial Intelligence in Forensic Science. Theory and Practice of Forensic Science and Criminalistics.
9. **Kumar, D. R., Baplawat, A., Prabakaran, D. P., Sridhar, A. P., Saraswathi, B., & Roja, M.** (2025). Artificial Intelligence in Forensic Sciences: Bridging Systematic Challenges with Next-Generation Applications. Journal of Neonatal Surgery.
10. **Mohammad, N., Ahmad, R., Kurniawan, A., & Mohd Yusof, M . Y . P.** (2022). Applications of Contemporary Artificial Intelligence Technology in Forensic Odontology as Primary Forensic Identifier: A Scoping Review. Frontiers in Artificial Intelligence.
11. **Al Neaimi, M., Hamadi, H. A., Yeun, C., & Zemerly, M.** (2020). Digital Forensic Analysis of Files Using Deep Learning. 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS).
12. **Devi, S., & Sabiyath Fatima, N.** (2026). ForenXAI: An Intelligent Deep Learning Framework for Forensic Document Verification and Forgery Detection for Police Evidence. Journal of Internet Services and Information Security.
13. **Morán-Torres, R., Feld, K., Hesser, J. W., Taalab, Y. M., & Yen, K.** (2025). Artificial Intelligence and Computer Vision in Forensic Sciences. Rechtsmedizin.
14. **Kassem, M., & Lodhi, K.** (2024). Revolutionizing Forensic Science: The Role of Artificial Intelligence and Machine Learning. Journal of Artificial Intelligence, Machine Learning, and Bioinformatics.
15. **Tynan, P.** (2024). The Integration and Implications of Artificial Intelligence in Forensic Science. Forensic Science, Medicine and Pathology.