ISSLP

OPEN PEER REVIEW

Opportunities of Artificial Intelligence in Scientific Crime Detection: A Review of Global Experiences and Localization Capacities in Iran

Alireza. Gholamhoseini[1], Ali. Najafi Tavana[2*], Atefe. Aminia[2]

[1] Department of Law, UAE.C., Islamic Azad University, Dubai, United Arab Emirates
[2] Department of Law, CT.C., Islamic Azad University, Tehran, Iran

*** Corresponding author email address**: 5809885586@iau.ir

Received: 2026-05-04 **Revised:** 2026-10-01 **Accepted:** 2026-10-07 **Initial Publish:** 2026-11-03 **Final Publish:** 2027-01-01

EDITOR:
Asghar Jafari
Associate Professor, Department of Psychology, Kashan University, Iran. Email: as_jafari@sbu.ac.ir
REVIEWER 1:
Asghar Jafari
Associate Professor, Department of Psychology, Kashan University, Iran. Email: as_jafari@sbu.ac.ir
REVIEWER 2:
Asghar Jafari
Associate Professor, Department of Psychology, Kashan University, Iran. Email: as_jafari@sbu.ac.ir

1. Round 1

1.1. Reviewer 1

Reviewer:

In the Introduction paragraph beginning with “Scientific crime detection may be understood as the systematic application of scientific knowledge,” the proposed definition appears to be formulated by the authors rather than derived from an established conceptual or legal framework. Because this concept constitutes the dependent analytical domain of the entire article, the manuscript should provide a more rigorous operational definition and specify its constituent stages, such as recognition of criminal events, collection and preservation of evidence, forensic analysis, suspect identification, reconstruction of events, case linkage, and production of evidence suitable for criminal proceedings. The article should then consistently evaluate AI applications against these stages rather than discussing AI capabilities in general terms.

The paragraph beginning “The significance of this transformation is particularly visible in cybercrime investigations” gives cybercrime a disproportionately prominent role relative to the title and stated scope of the article. Cybercrime is an important application area, but the article concerns scientific crime detection generally. The authors should either explain why cybercrime is analytically privileged or rebalance the discussion by giving comparable attention to homicide investigation, organized crime, financial crime, forensic identification, narcotics investigations, trafficking, and other evidentiary contexts. Otherwise, the article risks becoming partly a cybercrime paper embedded within a broader conceptual framework.

The final paragraph of the Introduction presents the objective, central question, scope, and methodology in one extended paragraph. The methodological statement—“The study adopts a descriptive-analytical and comparative approach based on the examination of relevant scholarship and the analytical reconstruction of technical, procedural, legal, and institutional dimensions”—requires substantially greater specification. The manuscript should explain how comparative jurisdictions were selected, how sources were identified, what inclusion and exclusion criteria were applied, the temporal scope of the literature,

and how conclusions concerning Iran were derived. Even for a doctrinal or narrative review, methodological transparency is necessary to distinguish systematic analysis from selective literature synthesis.

In the second section, the opening sentence "The most immediate contribution of artificial intelligence to scientific crime detection lies in its capacity to process evidence at a scale that exceeds ordinary human analytical ability" is plausible but should be reformulated to avoid an unqualified comparative claim. Processing volume and speed may exceed human capability, but contextual reasoning, evidentiary interpretation, causal inference, and recognition of unusual case-specific circumstances may not. The manuscript should consistently distinguish computational superiority in narrowly specified tasks from broader investigative competence. This would strengthen the article's later human-in-the-loop argument.

The discussion of machine learning in the paragraph beginning "Machine learning occupies a central position in this transformation" would benefit from greater technical precision. The article currently combines supervised classification, unsupervised anomaly detection, prediction, and relational analysis without explaining their methodological differences. A concise clarification of supervised learning, unsupervised learning, anomaly detection, clustering, and probabilistic classification would help readers understand why different applications generate different evidentiary risks. This is especially important because error profiles, training-data requirements, and interpretability differ substantially across these methods.

In the paragraph on computer vision and biometric surveillance, the statement that "Accuracy should therefore be treated as an evidentiary and rights-based issue rather than merely a technical performance metric" is an important proposition that deserves deeper development. The manuscript should specify relevant performance concepts such as false-positive rate, false-negative rate, precision, recall, threshold selection, demographic performance disparities, and confidence scores. In criminal investigation, system accuracy should not be discussed as a single aggregate percentage because different error types have very different consequences. Adding this methodological distinction would significantly strengthen the scientific rigor of the article.

The paragraph on generative AI states that "A conventional forensic instrument is generally expected to produce reproducible results when the same validated procedure is applied under the same conditions," followed by a contrast with generative systems. This is analytically useful, but the authors should distinguish reproducibility, repeatability, validity, reliability, and explainability. These concepts are presently treated as closely interchangeable. A generative model may produce non-identical textual outputs while still allowing reproducible evidentiary procedures if inputs, system versions, prompts, parameters, and logs are preserved. The legal issue is therefore not variability alone but whether the process is sufficiently documented, testable, and challengeable.

Authors revised the manuscript and uploaded the document.

1.2. Reviewer 2

Reviewer:

In the paragraph stating that "AI-enabled financial crime detection can improve the identification of abnormal transactions, relational patterns, and behavioral anomalies," the discussion should distinguish between anomaly detection and criminal detection. An anomalous financial transaction is not necessarily unlawful, and a statistically unusual pattern cannot itself establish mens rea, participation, or criminal provenance. The manuscript would benefit from explicitly describing the evidentiary progression from algorithmic flagging to investigative corroboration, documentary verification, forensic financial analysis, and ultimately legally admissible proof. This distinction is central to preventing the article from overstating what AI systems actually "detect."

The paragraph beginning "Artificial intelligence also changes the relationship between criminal investigation and surveillance technologies" requires a more precise distinction between identification, verification, and surveillance. For example, facial recognition used to compare a known suspect against stored images is methodologically different from real-time facial recognition across public spaces. The sentence "A system capable of rapidly identifying a person of interest can significantly accelerate an urgent investigation" should therefore be qualified by explaining that facial recognition normally produces similarity scores or candidate matches rather than certain identification. The legal and evidentiary consequences of one-to-one verification and one-to-many identification should also be differentiated.

In the paragraph on predictive applications, especially the sentence “By analyzing historical crime records, geographical information, temporal patterns, and other variables, AI systems may estimate where certain forms of crime are more likely to occur,” the manuscript shifts from scientific crime detection toward crime prevention and resource deployment. The authors should justify the inclusion of predictive policing within the conceptual scope of “crime detection.” A useful revision would distinguish retrospective detection, real-time detection, prospective risk forecasting, and preventive deployment as analytically separate uses of AI. Without this clarification, the manuscript risks conceptual stretching.

The paragraph discussing criminal profiling, beginning “A further transformation concerns criminal profiling,” should more explicitly distinguish investigative profiling from individualized prediction of criminality. These are scientifically and legally different practices. Case-based profiling may organize behavioral characteristics from an already committed offense, whereas prediction of future criminal conduct often relies on population-level statistical associations. The manuscript correctly warns against equating profiling with proof, but it should additionally explain the risk of base-rate error, overgeneralization, and false-positive classification when probabilistic models are applied to individuals.

Authors revised the manuscript and uploaded the document.

2. Revised

Editor’s decision: Accepted.
Editor in Chief’s decision: Accepted.