eSystems Engineering Society EST. 2007

International Journal of Data Science and Advanced Analytics

Journal homepage: www.ijdsaa.com

Hybrid Crime Scene Policing in the Digital Evidence Era: A Conceptual Framework for Artificial Intelligence and Immersive Training

Saleh Mansour[1], Jamila Bukar Gana[2], Evans Kiprop[3], Mira Mansour[4], Wadih Gerges[5]
[1&5]Lebanese University, Institute of Social Sciences, Beirut-Lebanon
[2] Border Monitoring Officer, Nigeria Immigration Service, Abuja-Nigeria
[3] Virginia Association of Criminal Justice Educators, Virginia-USA
[4] Lebanese American University, Beirut-Lebanon
[1]salehm68@hotmail.com; [2] jamilag241@gmail.com; [3] evanskiprop97@gmail.com; [4] mira.mansour@lau.edu; [5]wadih.g1@hotmail.com;

Corresponding author email: salehm68@hotmail.com

Abstract- Hybrid crime scene policing in the digital evidence era increasingly involves the integration of physical and digital evidence, creating new operational, legal, and training challenges for law enforcement. This paper presents a conceptually framed, practice-informed analytical synthesis of selected literature and documented international use cases examining the role of artificial intelligence (AI) and immersive technologies in crime scene training and investigation. It proposes a tiered conceptual framework for AI and immersive training that integrates immersive simulation, AI-facilitated performance analysis, and hybrid physical–digital training, and discusses the associated legal, ethical, and operational considerations necessary for responsible implementation.

Keywords—Immersive Training; AI-Augmented Policing; Hybrid Crime Scenes; Digital Evidence Management; Virtual Reality Simulation

1. Introduction

Police are undergoing a paradigm shift as digital evidence becomes central to nearly every investigation. Research shows that such evidence features in over 90% of crimes, from homicide to financial fraud [1]. Mobile phones, CCTV footage, and internet histories frequently yield leads that may surpass traditional physical traces [2]. Concurrently, virtual reality (VR) and artificial intelligence (AI) are redefining the policing landscape. AI systems can process vast volumes of social media, communications, and video at superhuman speeds [2]; while VR simulators recreate crime scenes in immersive, risk-free environments [3]. Together, these technologies extend investigative capabilities beyond physical boundaries, fostering a hybrid space for digital-physical policing.

Yet this transformation introduces critical challenges. The line between physical and digital crime is increasingly blurred [4], producing hybrid crime scenes where material and virtual evidence converge. A burglary may now involve both fingerprint recovery and analysis of GPS logs or social media content. Training officers to operate effectively in such environments is essential. Recognizing this, the International Association of Chiefs of Police (IACP) established a Digital Evidence Task Force [1], while INTERPOL launched the first global police metaverse for immersive forensic training [5]. These initiatives reflect a consensus: police must adapt their methods to the data-intensive, digitally saturated context of modern crime.

This paper explores how experiential, AI-supported training is equipping police to manage hybrid crime scenes in the digital forensics' era [6]. The paper, therefore, adopts a practitioner-informed academic lens in synthesizing use cases around the world across

https://doi.org/10.69511/ijdsaa.v7i1.292
Received 03 March 2025; Received in revised form 15 July 2025; Accepted 01 August 2025.
Available online 01 August 2025.

continents. It investigates what is being done as actual applications of VR and AI in crime scene management. The subsequent sections of the paper review the benefits, limitations, and legal, ethical, and evidentiary considerations of these tools; hence, ensuring fairness, transparency, and admissibility. Lastly, the paper provides actionable recommendations to police agencies and academies and concludes with a roadmap toward responsible integration within legal frameworks and ethical considerations. Therefore, this paper adopts a conceptual, practice-informed analytical approach based on existing literature and case studies.

Despite the increasing number of literature publications related to artificial intelligence for digital forensics and immersive technology for police training, existing literature mainly focuses on these topics independently, with fewer considerations for their combination for hybrid physical and digital crime scenes. Furthermore, there is relatively scant literature related to these types of technology with regard to their relationship with evidence criteria, legal acceptability, and ethics for their operational implementations. Hence, this condition provides a motivation for conducting this research, which aims to integrate separated knowledge derived from literature and existing practices related to this issue for developing a conceptual framework for training for hybrid crime scenes in the context of digital evidence.

2. Conceptual Framework and Review Approach

This section outlines the conceptual framework and analytical approach used to synthesize selected literature and documented practice, rather than reporting an original empirical study.

The present study employs a three-level conceptual training framework, proposed as a recommended design for immersive, AI-augmented policing training, rather than a fully implemented or empirically evaluated intervention, that combines virtual scenario simulation, artificially intelligent performance feedback, and mixed physical-digital training exercises. Table 1 provides a conceptual overview of the three-level framework and its governance layers within hybrid physical–digital crime scene policing. Each level progressively enhances decision-making, evidence-handling, and digital forensics skills. At level one, illustrative examples describe how trainees engage in VR-based crime scene simulations of a scene with interactive evidence such as blood spatter, mobile phones, and virtual witnesses. Using handheld controllers, trainees collect evidence, and conduct interviews, while documented practice indicates that the system tracks all actions, flags overlooked objects or incorrect procedures, and dynamically introduces high-stress cues -such as an uncooperative suspect reappearing or a fire- to test real-time decision-making skills [3], [7].

The evidence and case examples cited in this paper have been selected by a targeted search of peer-reviewed literature, official publications issued by global law enforcement bodies such as INTERPOL, the International Association of Chiefs of Police, Europol, and documented within pilot initiatives by government or institutional entities. Cases were selected as illustrative examples that specifically have proven the application of artificial intelligence or immersive technology within policing training, digital forensics, or hybrid contexts, and where sufficient technical or procedural detail was available for analysis; hypothetical, commercial, or unproven examples were excluded. The review was limited to publications from 2012–2025 reflecting the period which immersive policing technologies have been sustained operational application.

Table 1 Conceptual framework illustrating the integration of immersive simulation and AI-driven analytics in hybrid physical–digital crime scene policing.

HYBRID CRIME SCENE CONTEXT Physical Evidence + Digital Evidence Streams
LEVEL 1: IMMERSIVE SCENE SIMULATION • VR-based reconstruction • Interactive physical & digital evidence • Procedural decision-making
LEVEL 2: AI-DRIVEN PERFORMANCE ANALYTICS • Action logging & traceability • Pattern & bias detection • NLP-assisted assessment
LEVEL 3: HYBRID PHYSICAL–DIGITAL TRAINING • Mixed-reality transfer • Chain-of-custody awareness • Skills integration
GOVERNANCE & SAFEGUARDS (CROSS-CUTTING) • Legal admissibility • Ethics & privacy • Auditability

At the second level, AI-driven analytics examine detailed training data, object search histories, tagging behavior, action timestamps, and conversation logs. These are employed to generate quantitative, individualized evaluation of performance [8], Pattern detection models may signal habitual oversights (often missed digital evidence like USB drives) [4], while natural language processing (NLP) identifies prejudiced or incoherent phrases in virtual witness statements [5]. Advanced systems will have reinforcement learning agents that adjust the complexity of scenarios dynamically in response to real-time performance, so students are continually challenged[9]. The following key metrics are generally drawn and offered in defined performance metrics:

- Accuracy of Evidence Collection (%)
- Time to Respond (seconds)
- Score on Protocol Adherence (out of 10)
- Detection of Interview Bias (through NLP)

These metrics are presented as illustrative indicators within a conceptual training framework; no empirical measurement, baseline comparison, or statistical testing

is conducted in this study, though feasible evaluation designs (e.g., pre/post training or matched cohorts) are discussed as implementation guidance for future studies. Accordingly, these quantitative measures provide actionable comments (e.g., "You missed a CCTV camera whose footage could radically redefine the case timeline"), minimizing reliance on instructor recall or subjective interpretation [1]. This computer-based evaluation loop enhances the accuracy, fairness, and instructional effectiveness of forensic training simulations.
The third tier includes hybrid mock scenes with integrated digital cues. FARO 3D scanners and augmented reality (AR) overlays, such as those supplied by Operator XR or comparable software, are used to simulate forensic challenges like network traces, encrypted devices, and surveillance feeds [8],[10]. Trainees are required to log and synchronize a single chain-of-custody log throughout digital and physical evidence [1]. According to Halford et al, AR-supported training modules significantly improved officer performance on key measures of evidence collection, procedure adherence, and comprehension of the crime scene. In parallel, the UAE VR pilot emphasized reduced cognitive load and improved decision-making in digitally enhanced scenarios [8].
These outcomes suggest that immersive AR training fosters faster, more complete scene processing with greater compliance to investigative protocols, consistent with findings from both international cohorts and UAE field pilots [8], [10], [11].
Current peer-reviewed studies show that VR police training delivers realism and stress responses equivalent to live training. Kleygrewe et al. (2024) tested 237 officers from the Netherlands and showed that VR delivered equal heart rate, effort, and perceived stress to real situations, attesting to its ecological validity. This implies that VR can simulate true pressures without exposing the trainees to field risks [7].
Moreover, Halford et al. (2024) reported high use of a VR system for arson investigation, and Hussain et al. (2023) illustrated Abu Dhabi Police's implementation of a self-sustaining VR Training Centre. Such findings highlight the applicability of VR to maintain forensic competencies and build capacity. Rather than superficial performance measures, the literature confirms VR as an efficient, scalable solution for training officers within hybrid digital-physical environments [10].
Building on this evidence, the immersive, AI-augmented model is increasingly embraced by technologically forward law enforcement institutions, including INTERPOL's Metaverse Training Initiative [5], and forms the operational basis for the case studies analysed in the following section. Rather than presenting a fixed system diagram, the framework is intentionally described conceptually to allow adaptation across legal, operational, and institutional policing contexts.
The subsequent sections are structured to progress from conceptual design to illustrative international use cases, and finally to analytical discussion and governance implications.

3. Applied Models of Tech-Enhanced Policing in Practice

This section presents applied models demonstrating how AI and immersive technologies are integrated into policing. Drawing on case studies from the UAE, INTERPOL, the United States, and Nigeria, it highlights practical uses of VR and AI across training, evidence analysis, reporting, and border security.

3.1 Virtual Reality Crime Scene Training – Abu Dhabi Police (UAE)

Abu Dhabi Police was among the first in the Middle East to introduce a Virtual Reality Arson Investigation Simulation in cooperation with academic institutions to enhance investigators' skills in hi-tech fire scenes. The VR simulates a burning building scenario with multiple ignition sources and debris, where trainees collect evidence and interview a suspect in timed, low-visibility environments. The goal is improved handling of arson cases involving careful chemical and physical evidence examination [8].
Research by Journal of Policy and Practice found VR participants to recognize fire signals and enhance information in the environment in comparison to lecture-trained controls [3].These results guarantee the safe utilisation of VR in stress-centred training in a bid to build decision-making resilience [4]. This success has resulted in diversification into such areas as traffic accidents, criminal photography, and forensics as part of UAE's policing vision in the future.
This section describes simulated crime scene analysis skill practice in virtual environments aimed at supporting real-world performance. Immersive VR technology enables unconstrained interaction in virtual worlds [11], forces real data through digital twins, and enables data-driven decision-making [12]. Examination of these tools, capabilities, scalability, and data management is crucial in determining "what works, what doesn't, and what's promising" in policing [8]. Effectiveness also depends on officers' adjustment and familiarity with technology, which increases engagement with VR as a training tool [6], [13].

3.2 AI-Driven Evidence Analysis - INTERPOL

As digital evidence grows exponentially, law enforcement agencies now employ AI as a supportive solution in managing investigations. Across North America and Europe, police use Magnet Axiom, a digital forensic software enhanced with AI. During a recent INTERPOL-led cybercrime sweep, officers used it to analyse seized devices, automatically sorting hundreds of thousands of images, transcribing hours of suspect calls, and clustering chat messages to expose conspiracies [5], [14]. Notably, a key feature was a large language model assistant: investigators asked queries such as “Find bank transfer discussions in 2019,” and the AI retrieved relevant

passages across devices, saving weeks of manual review [2].

At the same time, findings were carefully validated, AI outputs were double-checked by human analysts, with forensic reports documenting procedures for court. INTERPOL leads in capacity building for international policing: through its Global Academy and Metaverse, Police officers worldwide can access digital forensics courses and collaborate in shared virtual environments [5]. For instance, in 2023, 20 countries jointly tackled a virtual cybercrime case using an AI-enabled evidence system [15].

Overall, this example highlights the transnational nature of modern crime, suspects and data cross borders, as do training and investigative tools [13]. When properly applied, AI helps maintain investigative rigor under data overload, while initiatives like INTERPOL's ensure global access, preventing gaps between resource-rich and resource-poor agencies [15]. In addition, integrating AI and VR methodologies strengthens evidence management and risk assessment.

3.3 AI Reporting and Decision Support – Axon's Body Camera Transcription Pilot (USA).

Police work generates not only evidence but also extensive documentation, and AI is now being applied to streamline this process. A leading example is the Axon "Draft One" pilot program in California, where Axon, a major supplier of body-worn cameras, integrated an AI service (based on OpenAI technology) to automatically transcribe footage and draft incident reports [16]. Beginning in 2024, the Fresno Police Department and others tested the system: bodycam video is uploaded to a secure cloud, the AI produces a draft narrative, and the officer edits for accuracy. Consequently, this reduces hours spent on paperwork, allowing more time for community patrols [16].

Moreover, initial feedback has been positive: Fresno police reported significant time savings with minimal transcription error [16]. For instance, an officer demonstrated that AI correctly recorded a heated exchange during a traffic stop, which would have taken a long time to report by hand. To meet evidentiary standards, the District Attorney's office provided training, so officers understand that AI versions have to be validated [16].

Nevertheless, the pilot has also introduced ethical and legal implications, though. Civil rights groups such as the ACLU issue a warning that AI could introduce unconscious bias or misread situations, seeding errors into official reports in turn [17]. Defence lawyers also caution that AI use will impair officers' recall memory, long a component of accurate reporting [17]. Fresno PD responded in kind: AI reports are prominently marked, require human review, and are restricted to small cases to minimize the risk [16].

Equally important, the Axon Draft One case illustrates how AI is encroaching on frontline police procedures. While it achieves productivity benefits and improved documentation, it is also subject to transparency, training, and oversight for its integrity. Moreover, it shows how public–private collaboration between police agencies and tech firms is driving innovation, requiring clear regulatory requirements for AI implementation in policing responsibly [8].

3.4 Border Intelligence and AI Threat Interception – Nigeria Immigration Service (NIS)

At the Nigeria Immigration Service Command and Control Centre (C3), AI systems are applied at international airports to identify hybrid threats in real time. The eGates module integrates multiple layers of information: INTERPOL notices, country watch lists, biometric screening, and API/PNR data, to apprehend suspicious travellers at the border [10], [12], [18]. In one case where it was demonstrated, there was a foreign guest with no apparent signs of criminality, but who was identified on clearance due to a cyber-match against an open INTERPOL case involving the investigation of identity fraud. The experience demonstrated how the border checkpoint clearance can be the catalyst for further wider transnational investigation where cyber-travel data and biometric feeds are used to generate the first trail of evidence [10], [12].

Operational observations of the C3 are that AI is currently at the centre of hybrid threat management, yet experiential training for border control officials remains underdeveloped compared to policing agencies. Tools like the Migration Information and Data Analysis System (MIDAS) have proved their value, one biometric alert resulted in the identification of a trafficking suspect and facilitated international collaboration to the level of an arrest [13], [19]. The integration of AI within normal operations supports the need for enhanced immersive training programs between agencies. This will create combined responses against digital-physical crimes. The case example situates border intelligence units at the center of the evolving context of hybrid crime scene management.

4. Results and Discussion

The above models attest to the potentially transformative utility of immersive and AI technologies for policing, as well as the difficulties involved. Across disparate use-cases – training investigators in VR, applying AI to digital evidence analysis, automating reporting – several consistent themes emerge in the discourse of outcomes and lessons learned:

4.1 Enhanced Preparedness and Accuracy

Agencies leveraging these tools report perceived improvements in operational preparedness and investigative accuracy [7]. VR-trained officers usually outperform traditionally trained officers in scenario-based assessments, with greater retention of tactics and

forensic procedures [20]. The Abu Dhabi arson VR training, for example, not only enhanced factual knowledge but also conditioned officers to deal with stress and sensory overload, something that would have been impossible to replicate in a classroom [10]. In the same way, AI-driven analysis has enabled examiners to identify crucial evidence that might have been missed [6], [21], for example, uncovering a hidden pattern in transactional data or spotting a suspect face in hours of CCTV footage within seconds.

Equally important, as a complement to human ability, AI is capable to leverage an extra pair of "eyes" and "ears" that tenaciously go through information and therefore increase completeness. A tangible outcome is in digital forensic units, where AI tools have reduced backlogs; police labs are typically thousands of devices behind analysis [19], and automating triage can bring the most relevant devices/files to the front of the queue first, speeding up the delivery of justice.

4.2 Challenges and Limitations

Despite notable successes, practitioners face technical and human-factor challenges. Indeed, VR simulations, though realistic remain approximations; no program replicates the variability of real crime scenes. Thus, trainees must avoid “tunnel vision,” since real incidents often combine unexpected elements. Moreover, technical issues such as VR motion sickness, equipment costs, and the need for frequent content updates persist in several departments.

On the AI side, verification and trust are the primary challenge. Scientists are understandably cautious, because blind faith in algorithms poses the risk of automation bias, where users trust AI too much against opposing context [17], [22]. To illustrate, if AI indicates a suspect in social network data, investigators must corroborate through good old-fashioned detective work. Correspondingly, pilot deployments in California tested Axon’s ‘Draft One’ to transcribe and draft reports from body-cam footage; officers then edited outputs for accuracy. Agencies required human validation, clear labelling of AI-assisted text, and prosecutor training on evidentiary use [15].

Furthermore, reliance on third-party AI vendors raises transparency concerns, since proprietary “black box” algorithms limit explanation in court. Consequently, some agencies restrict AI to investigative phases or require vendor cooperation to ensure courtroom admissibility. To address this, companies promote explainable solutions such as Magnet Verify [14].

4.3 Ethical risks and human factors

The discussion around AI in policing inevitably turns to ethics. The predictive policing debacle is a cautionary tale good-faith efforts to improve policing ended in programming institutional biases and eroding trust in the community [17], [22], [23]. Since algorithms based on historical arrest data recreated over-policing in minority communities, some departments such as Los Angeles and Chicago went as far as to cancel or suspend their programs under public outcry and reports of bias [22].

Hence, transparency and fairness must be built in from the outset. Because policing is founded on community trust, and public safety is lost if this is undermined. Consequently, there is growing pressure for independent audits and stakeholder involvement in AI use.

Comfortingly, technologies like human-robot interaction, if used narrowly on processes like automatically sorting evidence or interviewing on record, portend less ethical peril, provided privacy and data security are maintained. In addition, VR can also be beneficial for both tactics and empathy training through the replication of civilian perspectives [7],[21]; however, there are reservations. A 2024 paper in Police Practice and Research Journal confirmed that enhanced activity in VR elevates stress levels in officers, necessitating technical and human-factor measures to offset the detrimental effects of VR [7].

4.4 International Collaboration and information Sharing

Greater collaboration among jurisdictions is one comforting trend considering that digital evidence has tendency to border-hop. The INTERPOL Metaverse, for example, enables investigators from around the world to train together in virtual classrooms and learn standardized methods for hybrid crime scenes [5], [24]. However, this technological harmonization is not accompanied by lasting legal uncertainty because many countries still lack any laws on crimes in virtual worlds and creating charges and penal uncertainty. Resolving this requires intimate global collaboration between law enforcers, policymakers, and jurists to create an early frontier legal system [24].

Such standardization is required for crimes such as cyber-fraud, wherein evidence must be examined collaboratively, and it allows emerging countries to bypass and leapfrog by advanced training. Inequality of resources remains an issue, yet interagency support and grants by Europol and UNODC are bridging the gap. International forums now emphasize that AI and immersive training need to establish professionalism and accuracy, and that knowledge transfer should take center stage.

Overall, immersive, AI-enhanced methods are consistently reported in the literature as beneficial for policing since they create realism in training, speed in analysis, and consistency in process. Adoption must, however, remain discerning, with technical dependability, legal defensibility, and ethical integrity remaining the make-or-break aspects.

To improve transparency and align the narrative discussion with its supporting sources, Table 2 summarizes the key analytical claims made in this paper and the types of evidence on which they are based.

Table 2 Summary Evidence Supporting Key Analytical Claims

Key Analytical Claim	Type of Supporting Evidence	Illustrative Sources
Immersive VR training enhances preparedness and procedural accuracy	Peer-reviewed training studies; institutional pilot evaluations	Kleygrewe et al. (2024); Halford et al. (2024); Hussain et al. (2023)
AI-assisted tools improve efficiency in digital evidence triage and analysis	Documented operational deployments; practitioner reports	INTERPOL (2022, 2023); Magnet Forensics
AI-supported reporting reduces administrative burden while requiring oversight	Government pilot programs; agency evaluations	Axon Draft One (2024); Fresno Police Department
Hybrid crime scene training raises legal and ethical challenges	Legal scholarship; policy guidance; regulatory analysis	Europol (2024); Brennan Center; Daubert standards
International collaboration mitigates capability and resource gaps	Multilateral initiatives; international training programs	INTERPOL Metaverse; UNODC

5. Regulatory Frameworks and Legal Safeguards

Application of AI and immersive technology in policing comes with the utmost ethical and legal concerns that should not be overlooked [6]. To ensure these technologies do more to strengthen justice and not undermine it, police departments must grapple with issues of bias, transparency, privacy, accountability, and admissibility.

5.1 Algorithmic Bias and Fairness

As identified, AI systems learn from historical data, and if biased, the AI unwillingly recreates the same. This is particularly problematic in those technologies that direct policing behaviour (e.g., suspect identification or predictive policing). For reasons of equality and fairness, law enforcement owes equal protection; applying an unfair algorithm could be at odds with that duty. Mitigation includes using diverse and representative data, using bias correction techniques, and subjecting algorithms to independent audits by impartial experts.

Other jurisdictions are moving towards making such audits mandatory or even certifying law enforcement AI tools as bias-free. In practice, police forces should also have a human screening process for AI outputs – treating them as advisory, not absolute. For instance, if an AI for crime analysis rates an individual as high risk, then a human analyst or officer has to confirm on his own grounds of such identification before taking an action. This multi-level process will ensnare bias or mistake injected by a machine.

5.2 Transparency and Explainability

Most countries' legal standards (e.g., the U.S. Daubert rule) require scientific evidence presented to a court to be valid and explainable to jurors [25]. AI violates this in that complex models are "black boxes" which are hard to explain. As a defence, lawyers must be able to challenge evidence, but cross-examining a program remains difficult. If an AI claims 98% certainty that the mark is from a gun, the defence can question on what grounds, basis, and error rate. That's why judges are now demanding source code or verification studies disclosure before accepting AI forensic evidence. This has driven the need for Explainable AI (xAI) that provides human-readable explanations, for example, face recognition informing us which features matched and what resolution the image was [14], [25] .

Consistent with this, police using AI need to document its accuracy and maintain detailed logs, tracking each time AI eliminates evidence or alters images. These logs form the digital chain of custody, showing evidence was handled methodically [21],[25]. Equally crucial as transparency in training is insuring that officers understand not only how to use AI tools but also their failure modes and limitations, e.g., recognizing that license plate readers often misread characters under poor lighting conditions, thus requiring manual double-checks are required [6], [22], [23].

5.3 Privacy and Data Protection

Use of AI and digital technology often involves the collection and processing of high amounts of data, some of which will be personal or sensitive. That creates privacy concerns and guaranteeing compliance with data protection law (e.g., GDPR in the EU, with tough controls on dealing with personal data) [17]. When creating AI models, law enforcement agencies must be able to have confidence they're operating on legally acquired data that are appropriate for policing [13]. For instance, in the case of using bodycam video to train models, there would need to be a consideration of whether those people in the video agreed or were told their faces would be used to train artificial intelligence – they usually did not, and therefore in applying legal representation, it might be illegal or require anonymization. Used operationally, AI could enable mass surveillance possibilities that push the boundaries of reasonable expectations of privacy. Facial recognition in real-time by CCTV or AI scanning social media messages would be incompatible with freedom of expression and privacy rights except where regulated. On moral grounds, the police should have advance warrants or judicial warrants when they use AI to search areas traditionally encompassing such authorization (e.g., what is being sent in private messages) [13], [17].

The answer is also robust cybersecurity: these advanced systems themselves become victims of abuse or hacking. An intruder compromising a police AI system could send investigation information or even enable evidence tampering (imagine an intruder changing the result of an

AI to deceive investigators). Agencies need to have robust access controls, encryption, and ongoing security auditing on their web-enabled tools [17], [26].

5.4 Authenticity and Deepfakes

The latest challenge is the rise of AI-faked content, or deepfakes. AI is now capable of producing highly realistic images, video, or sound, potentially fabricating evidence that never existed.

Verifying multimedia evidence has become crucial, with some means like blockchain timestamping and digital signatures on bodycams being investigated [25],[24]. The judicial system is concerned that deepfakes can "taint a trial" [16], [25] by throwing suspicion on all digital evidence. To counter this, the agencies must create AI forensics capacity to detect forgeries, utilising algorithms that scan pixel artifacts or lighting irregularities. The prosecutors must familiarise juries in a timely fashion with deepfakes, and the police must refrain from wrongful use of the same (e.g., bogus profiles utilising AI-generated images), since the latter dilutes credibility and overall violates legal prohibitions.

5.5 Accountability and Oversight

With increasing AI power in policing there is an equal demand for accountability. When something goes wrong, either a VR session teaches incorrect procedures or an AI program generates a bad lead, departments must answer to them with the same criticism that would be applied to human decisions. All significant AI-directed actions must be logged, audited, and under review, particularly if they have lawful or moral significance. Hence, experts advocate expansion of ethics or force-use boards to include AI management so that systematic analysis of false positives, complaints, or performance trends can be carried out. Additionally, accountability extends to vendors as well: contractual language should ensure their participation in court explanations and timely defect repairs. At the same time, some jurisdictions mandate algorithmic impact assessments, i.e., agencies must declare an AI system's purpose, data usage, risks, and mitigation options [17], [21]. Ultimately, AI deployment in law enforcement needs a fine balance between innovation and ethical vigilance. Preservation of fundamental principles of transparency, fairness, and integrity ensures that technological advancements serve to enhance, rather than undermine, justice.

6. Recommendations

Based on the above arguments and conclusions, the following recommendations are suggested to policymakers, training institutions, and law enforcement agencies to ensure the effective use of immersive, AI-based approaches in managing crime scenes while mitigating associated risks.

The following recommendations are directly derived from the analytical findings and case studies discussed in the preceding sections.

6.1 Holistic Training in Physical & Digital Forensics

Building on the training gaps identified in the analysis of hybrid crime scenes, Police Academies and schools of continuing education should customise curricula to embrace handling digital evidence as a crucial skill for all investigators (not just specialists). Weave in hybrid VR/AR crime scenes and where the trainees must collect digital evidence as well as physical evidence under simulated environments. Ensure that every traditional drill crime scene has a digital aspect (e.g., an online transaction, or a suspect phone), hence making it the new norm to integrate digital footprints into investigations. Periodically update scenario material to include developing technologies (e.g., IoT devices within scenes or new digital crime strategies). Employ outcome-based assessments in these training exercises: e.g., have trainees create both a typical scene report and a digital evidence report, simulating what will be expected in real cases.

6.2 AI Tools with Human Oversight

Integrating AI into policing workflows demands the establishment of robust Standard Operating Procedures (SOPs) that clearly define how officers interact with algorithmic outputs. These SOPs must state that AI-generated results serve as investigative leads, not final conclusions, neither evidence with high evidentiary value, and thus require documentation of each instance, including who used the tool and how the output was validated. Officers and analysts should be trained on the functionality and limitations of the tools to reduce misuse and overreliance. To reinforce accountability, major decisions such as arrests or warrants based on AI input should be reviewed and validated by a designated senior officer or independent authority. Agencies should also use multiple AI systems or human expert cross-validation to prevent single-source risk dependency and make decisions more dependable.

6.3 Authenticity and Deepfakes

Collaboration between law and judicial enforcement is essential to establishing clear admissibility standards for AI-generated evidence. Law enforcement can participate in mock trials to practice bringing AI tools into court and learn from legal experts. Investment in explainability, such as audit trails or interpretability modules integrated, should be met with training investigators to integrate these outputs properly into case files. Maintaining a roster of qualified forensic professionals to validate tool functionality will also reduce court concerns and satisfy evidentiary disclosure requirements. Backing up established credentials, such as from NIST, also adds weight to credibility. Finally, policies must be re-examined on a regular basis based on evolving case law to ensure court preparedness as well as continuously for legal compliance.

6.4 Ethical Oversight and Community Engagement in Tech Adoption

Prior to adopting immersive or AI technologies, agencies should conduct participatory ethical impact assessments with technical experts, community stakeholders, and regulatory authorities. Such a participatory approach addresses concerns like surveillance and privacy and supports proactive policy change. Agencies should also release transparency reports and involve the public in town halls or demonstrations. Ethical regulations internally must exclude misuse, especially non-law enforcement surveillance, with disciplinary action. To provide accountability, ethics and bias training needs to go along with deployments so that the officers are aware of how algorithms can perpetuate systemic bias and how they can counteract it. Table 3 outlines the most important legal and ethical aspects being debated in policing.

Table 3 Legal & Ethical Challenges in AI-Driven Policing

Dimension	Challenge	Implication
Explainability	AI decisions are opaque	Hinders courtroom admissibility
Bias & Discrimination	NLP errors in suspect/witness analysis	May reinforce systemic bias
Chain of Custody	Digital logs hard to verify without standardization	Legal exclusion of key evidence
Data Governance	Cloud-based systems storing sensitive evidence	Cross-jurisdictional data protection issues

6.5 Resource Allocation and Improvement

AI and virtual reality systems need to be continually invested in, not only in hardware but also in training staff and maintaining the systems up to date. Budgeting must account for regular VR scenario updates by subject-matter experts and periodic refresher training to maintain operational readiness. Agencies should track performance metrics, such as the actionable output of AI technology or street performance of VR-trained officers, to guide cost-benefit analysis. Technologies that don't perform, e.g., predictive tools with no measurable crime impact, need to be revisited or phased out. Beyond that, best practices need to be shared across the law enforcement community to enable mutual improvement, particularly for smaller agencies that can apply proven models at minimal or no development expense.

6.6 Plan for interoperability and scalability

Evidence management systems must be open standards-based, so that data can flow freely between agencies and any of a vast number of analysis tools can be applied. By such means, police forces will be well positioned to achieve the complete potential of AI and immersive training. The objective is to produce a virtuous circle: highly skilled officers leveraging better technologies more effectively, leading to more effective investigations and greater public trust. These gains, in turn, reinforce the commitment to continued innovation in technology and in training. Concurrently, this progress ensures that while policing embraces AI, it is founded firmly on the steadfast principles of justice, accountability, and public service.

7. Conclusion and future directions

The framework is intended as a transferable blueprint for training design rather than a report of an executed empirical study. As the digital world increasingly intrudes on policing, advanced models of investigation and training must be developed. This study illustrates how virtual reality, and artificial intelligence can transform crime scene investigation into dynamic engagement with physical and digital evidence. Case studies in the UAE, U.S., Europe, and Africa all confirm that such technologies improve readiness, situational awareness, and accuracy of evidence. Integration correctly maximizes cognitive and procedural capacity, while insufficient protection impairs prospects of bias, legal concerns, and loss of public trust.

In sum, hybrid crime scenes necessitate hybrid capacities and innovative skills. Aligning AI and immersive technologies within the framework of justice not only enhances policing effectiveness but also strengthens its legitimacy, signalling the dawn of an era of technology-enabled, rights-upholding law enforcement.

References

[1] IBM/IACP Study – STAX Inc., “Rising Digital Evidence and Data Breaches Boost Demand for Digital Forensics,” STAX, Jan. 2023. [Online]. Available: https://www.stax.com/insights/rising-digital-evidence-and-data-breaches-boost-demand-for-digital-forensics. Accessed: Jul. 22, 2025.

[2] B. Montgomery, “AI in Law Enforcement and the Future of Digital Forensics,” Police1, Nov. 2024. [Online]. Available: https://www.police1.com. Accessed: Jul. 24, 2025.

[3] Operator XR, “Virtual Reality Transforming Police Readiness,” Feb. 2023. [Online]. Available: https://operatorxr.com. Accessed: Jul. 27, 2025.

[4] K. Vlachopoulos, E. Magkos, and V. Chrissikopoulos, “A Model for Hybrid Evidence Investigation,” Int. J. Digit. Crime Forensics, 2012, doi: 10.4018/jdcf.2012100104.

[5] INTERPOL, “INTERPOL Launches First Global Police Metaverse,” Oct. 2022. [Online]. Available: https://www.interpol.int. Accessed: Jul. 30, 2025.

[6] S. Mansour and D. Rajput, “Enhancing Judicial Efficiency through Artificial Intelligence: Analyzing Federal Justice Systems from an Organizational Behaviour Perspective—A Data-Driven Study,” IJDSAA, vol. 6, no. 7, pp. 403–410, Apr. 2025, doi: https://doi.org/10.69511/ijdsaa.v6i7.262.

[7] L. Kleygrewe, R. I. V. Hutter, M. Koedijk, and R. R. D. Oudejans, “Virtual reality training for police officers: a

comparison of training responses in VR and real-life training," Police Pract. Res., vol. 25, no. 1, pp. 18–37, Jan. 2024, doi: 10.1080/15614263.2023.2176307.
[8] E. Halford, P. Keningale, A. Taleb Hussain, and C. Condon, "Assessing the utility of a virtual reality arson crime scene investigation simulation," Policing: A J. Policy Pract., vol. 18, p. paae122, Jan. 2024, doi: 10.1093/police/paae122.
[9] A. T. Hussain, E. Halford, and F. AlKaabi, "The Abu Dhabi Police Virtual Training Centre: A case study for building a virtual reality development capacity and capability," Policing: A J. Policy Pract., vol. 17, p. paad028, Jan. 2023, doi: 10.1093/police/paad028.
[10] Rabdan Academy, "Rabdan Academy Enhances Security and Innovation in Abu Dhabi through Pioneering Research Publications," Mar. 2025. [Online]. Available: https://ra.ac.ae. Accessed: Aug. 02, 2025.
[11] C. Pletz, "Which Factors Promote and Inhibit the Technology Acceptance of Immersive Virtual Reality Technology in Teaching-Learning Contexts? Results of an Expert Survey," Int. J. Emerg. Technol. Learn., vol. 16, no. 13, p. 248, Jul. 2021, doi: 10.3991/ijet.v16i13.20521.
[12] INTERPOL, "INTERPOL Artificial Intelligence." [Online]. Available: https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit. Accessed: Aug. 05, 2025.
[13] Magnet Forensics, "Magnet Verify." [Online]. Available: https://www.magnetforensics.com/products/magnet-verify. Accessed: Aug. 07, 2025.
[14] T. J. Cowper and M. E. Buerger, "Police and Augmented Reality Technology," FBI.gov Publications. [Online]. Available: https://www.fbi.gov. Accessed: Aug. 09, 2025.
[15] AXON, "AXON Draft One." [Online]. Available: https://www.axon.com/products/draft-one. Accessed: Aug. 11, 2025.
[16] European Union Agency for Law Enforcement Cooperation, AI and policing: the benefits and challenges of artificial intelligence for law enforcement. LU: Publications Office, 2024. [Online]. Available: https://data.europa.eu/doi/10.2813/0321023. Accessed: Aug. 13, 2025.
[17] M. Groer et al., "Salivary measures of stress and immunity in police officers engaged in simulated critical incident scenarios," J. Occup. Environ. Med., vol. 52, no. 6, pp. 595–602, Jun. 2010, doi: 10.1097/JOM.0b013e3181e129da.
[18] P. Martina, "Human trafficking: The gender dimension," in Human Trafficking Studies. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766265/EPRS_BRI%282024%29766265_EN.pdf?. Accessed: Aug. 15, 2025.
[19] "2023 MIDAS Brochure Updated." [Online]. Available: https://www.iom.int/resources/policy-brief-gender-dimension-trafficking-person? Accessed: Aug. 17, 2025.
[20] United Nations Office on Drugs and Crime (UNODC), Global Report on Trafficking in Persons 2024. United Nations, 2025.
[21] M. Z. I. Kalanauri, "AI Approaches to Predictive Justice: A Critical Assessment." [Online]. Available: https://humanitiesandrights.com/journal/index.php/har/article/download/118/74/? Accessed: Aug. 19, 2025.
[22] M. Tiwari, Y. Zhou, A. Childs, L. Y. C. Chang, and J. Ferrill, "Metaverse policing: A systematic literature review of challenges and recommendations," Comput. Human Behav., vol. 166, p. 108591, May 2025, doi: 10.1016/j.chb.2025.108591.
[23] E. Gentry, "The Challenges of Integrating AI-Generated Evidence into the Legal System," Akerman, Jun. 2024. [Online]. Available: https://www.akerman.com. Accessed: Aug. 22, 2025.
[24] HM Inspectorate of Constabulary and Fire & Rescue Services, an inspection into how well the police and other agencies use digital forensics in their investigations, London, UK, Dec. 2022. [Online]. Available:https://www.justiceinspectorates.gov.uk/hmicfrs. Accessed: Aug. 24, 2025.
[25] T. Lau, "Predictive Policing Explained," Brennan Center for Justice, Apr. 1, 2020. [Online]. Available: https://www.brennancenter.org. Accessed: Aug. 26, 2025.
[26] INTERPOL, "INTERPOL Biometric Hub." [Online]. Available: https://www.interpol.int/en/How-we-work/Forensics/Biometric-Hub. Accessed: Aug. 28, 2025.