IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511178

An Blockchain-Enabled AI Framework for Digital Evidence Management and Report Generation

Govindraj B. Chittapur[1], Bhavana K. Kotyal[2], Geeta H. Talawar[3], Gangabai S. Nedalagi[4], Aishwarya R. Rathod[5]

Department of Computer Science and Engineering, Basaveshwar Engineering College, Bagalkote, Karnataka, India[1-5]

Abstract: Digital evidence has grown significantly in volume and complexity, making manual examination increasingly time-consuming, costly, and susceptible to manipulation. At the same time, judicial and investigative processes require a verifiable chain of custody that documents every interaction with digital evidence through its entire lifecycle. Although existing work has addressed these problems, most solutions focus on individual aspects such as content analysis, blockchain-based evidence integrity, or automated report generation. This paper presents an integrated, image-oriented framework that unifies these capabilities within a secure, admission-controlled evidence management pipeline. Upon upload, each image undergoes cryptographic hashing, integrity validation, and metadata extraction before being analyzed using multiple artificial intelligence models, including a YOLOv8 detector with COCO pretrained weights, a custom-trained YOLOv11 model for detecting shotguns, handguns, and knives, CLIP-based scene classification, and BLIP-based image captioning. The outputs from these components are consolidated through a validator-score aggregation mechanism to classify evidence as ACCEPT, REVIEW, or REJECT. Accepted evidence is securely stored in a Supabase cloud storage bucket, while its integrity and custody records are maintained using a hash-linked blockchain ledger. Based exclusively on validated findings, an OpenAI language model generates a structured forensic report, which investigators review and approve before finalization. Experimental evaluation of the custom YOLOv11 detector achieved an AP@[0.50:0.95] of 0.682, AP50 of 0.860, AP75 of 0.775, and AR100 of 0.793, demonstrating strong performance for large objects (AP_{large} = 0.691) while revealing shortcomings in detecting small and medium-sized objects (AP_{small} = 0.000, AP_{medium} = 0.157). The current implementation is designed exclusively for still-image evidence and establishes a consolidated framework for secure digital evidence analysis, integrity preservation, and automated forensic report generation.

Keywords: digital forensics, chain of custody, blockchain, object detection, evidence admission, explainable reporting, image evidence, human-in-the-loop.

I. INTRODUCTION

Digital evidence has become an essential factor of modern criminal investigations; however, its increasing volume, diversity, and susceptibility to manipulation create significant challenges for forensic analysis. The evidential value of a digital item depends not only on the information it contains but also on the ability to demonstrate that it has remained authentic and unaltered throughout its lifecycle. Recent studies highlight the growing complexity of digital forensic investigations due to increasing data volumes, heterogeneous evidence sources, and rapidly evolving technologies [1]. Furthermore, improper handling and interpretation of digital evidence can affect judicial fairness and the presumption of innocence, emphasizing the need for reliable evidence management practices [2]. Although artificial intelligence techniques have improved the efficiency of digital evidence analysis, challenges related to evaluation, standardization, and authenticity verification remain important research concerns [3], [4]. The increasing availability of manipulated and AI-generated digital content has further strengthened the need for reliable authenticity assessment mechanisms [5].

Existing research has mainly developed along two separate directions. The first focuses on artificial intelligence-based approaches for multimedia forensic analysis, including image classification, manipulation detection, deepfake identification, and automated evidence interpretation [15]–[19]. The second focuses on blockchain-based mechanisms for preserving evidence integrity through immutable storage and transparent chain-of-custody management [6]–[10], [20]. Although recent studies have explored combining artificial intelligence and blockchain technologies for applications such as forensic evidence authentication, deepfake analysis, and evidence management [7], [11], [12], most approaches address only specific stages of the forensic workflow. However, an integrated framework that establishes a verifiable

 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026
DOI: 10.17148/IJARCCE.2026.1511178

connection between evidence validation, AI-generated findings, custody preservation, and forensic report generation remains insufficiently explored.

This paper proposes an AI- and blockchain-enabled framework for secure digital evidence management and automated forensic report generation. The proposed system validates uploaded image evidence through cryptographic hashing, perceptual hashing, metadata extraction, and integrity verification before performing AI-based analysis using a COCO-trained YOLOv8 detector, a custom YOLOv11 weapon detector, CLIP-based scene classification, and BLIP-based image captioning. The system processes the generated analytical results through an admission engine that classifies evidence as ACCEPT, REVIEW, or REJECT based on validation outcomes. Accepted evidence is securely stored in a Supabase cloud repository, while its integrity and chain of custody are preserved using a tamper-evident hash-linked chain-of-custody ledger. A constrained OpenAI-based report generation module produces structured forensic reports only from verified findings, with mandatory investigator approval before finalisation. By integrating evidence validation, AI-assisted image analysis, blockchain-enabled custody management, secure storage, and automated reporting, the proposed framework establishes a complete forensic workflow. The custom YOLOv11 detector is further evaluated using standard COCO Average Precision (AP) and Average Recall (AR) metrics to assess its effectiveness and limitations for forensic image analysis.

The paper is proceeds as follows. Section II presents the related work on AI-based digital evidence analysis and blockchain-enabled evidence management. Section III describes the proposed framework and overall system architecture. Section IV explains the algorithms and mathematical formulation used in the framework. Section V presents the implementation details and experimental setup, while Section VI discusses the results and evaluation. Section VII highlights the limitations and future research directions, and Section VIII concludes the paper.

II. RELATED WORK

Digital forensics and the evidential setting. A review of reviews identifies evidence volume, tool diversity and emerging data sources as persistent challenges [1]. Stoykova argues that unaddressed weaknesses in digital evidence handling threaten fairness and the presumption of innocence [2]. Together these works frame the problem as procedural as much as technical: an analytic tool that cannot document its own role in the evidence trail is difficult to defend. Our framework therefore treats provenance records and analysis outputs as one artefact.

AI for evidence analysis. Solanke and Biasiotti discuss evaluating, standardizing and optimizing AI-based evidence mining [3], and Nayerifard et al. survey machine learning across digital-forensics tasks [4]. Application-level studies address classification of heterogeneous evidence with multi-modal ensembles [15], tampered-image classification using deep and classical learners [17], manipulation detection in images and video [18], and detection of computer-generated imagery to support investigations [19]. A deep-learning and hybrid-optimization approach to tamper detection explicitly connects detection to legal reliability and chain of custody [21]. These studies mainly focus on the classifier. They say less about how a classifier's output should be stored, versioned and tied to the exact bytes it analysed, which is the point where our admission and custody stages operate.

Blockchain chain of custody. Ledger-based preservation has been proposed for classified forensic images [6], custody management combined with AI [7], cybercrime reporting and evidence management [9], asset custody in a decentralized setting [10], and an evidence-management system released as a software artefact [20]. Han couples smart contracts with electronic-evidence authentication in an arbitration setting [8]. The common contribution is tamper evidence for custody events. In most of these systems, the ledger records that an item exists and who touched it; the content-level findings that justified acceptance are less prominent. We extend the recorded payload to include the analysis digest and the admission decision.

Deepfake and synthetic-media detection. A systematic review of deepfake detection documents the breadth of detector families and their dependence on training conditions [5]. Forensic-oriented tools build on these detectors for multi-modal authentication and evidence reporting [11], blockchain-anchored evidence management [12], and AI-based identification of fake videos and images [13], [16]. Our present implementation does not include a synthetic-media detector; we mention this line of work because the validation engine is designed to accept an authenticity validator, and Section 9 identifies the integration as future work.

Explainable AI. Bharati et al. propose a multi-model deepfake detector that produces human-interpretable rationales specifically for legal investigation [14]. Their motivation, that an investigator or court needs reasons rather than only scores, is shared by our design. Rather than explaining a single network, we generate explanations at the pipeline level:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511178

a rule-based reasoner correlates detections, scene labels, and captions, and reports the correlation together with a confidence value.

Evidence management and reporting. Systems for cybercrime reporting [9], blockchain-backed evidence management [12], [20] and forensic tooling with report output [11] show that management and reporting are being combined with analysis. A gap that remains is a controlled path from machine output to a written report. Free-form generation can introduce statements that no analysis step ever produced. We address this by constraining report generation to a structured record of verified findings and placing investigator approval before finalization.

Research gaps. Reading across these themes, we identify four gaps. (G1) Analysis outputs are rarely cryptographically bound to the evidence item they describe. (G2) Admission of an item into custody is seldom an explicit, score-based decision with a human fallback. (G3) Chain-of-custody systems and AI analysers are often separate, so the custody record does not capture why an item was accepted. (G4) Report drafting, where present, is not clearly bounded by the verified findings. Table I compares the scope of representative works with the proposed framework.

TABLE I SCOPE COMPARISON WITH REPRESENTATIVE LITERATURE (ASSESSED FROM THE STATED SCOPE OF EACH CITED WORK; "—" MEANS NOT INDICATED IN THAT SCOPE).

Work	AI content analysis	Blockchain custody	Evidence management	Report output	Explicit admission gate	Human review before final report
[6]	—	✓	✓	—	—	—
[7]	✓	✓	✓	—	—	—
[9]	—	✓	✓	—	—	—
[11]	✓	—	—	✓	—	—
[12]	✓	✓	✓	—	—	—
[14]	✓	—	—	—	—	✓ (rationales for investigators)
[20]	—	✓	✓	—	—	—
[21]	✓	✓ (discussed)	—	—	—	—
Proposed	✓	✓	✓	✓	✓	✓

III. PROPOSED AI-BLOCKCHAIN FRAMEWORK

The framework processes one evidence image at a time through nine stages (Fig. 2): input evidence; AI detection and scene understanding; metadata extraction; AI evidence analysis; blockchain-based chain of custody; secure storage; report generation; investigator review; and the final investigation report. Two features distinguish the flow from a linear pipeline. First, a validation and admission step sits between analysis and custody, so that custody is a consequence of a decision rather than an automatic side effect of upload. Second, the human investigator appears twice: on items the admission engine does not accept, and on the generated report.

Evidence identity first. On upload, the system fixes the identity of the item by computing a SHA-256 digest and a perceptual hash, detecting the MIME type, and verifying any digital signature. The perceptual hash supports near-duplicate detection; the cryptographic digest supports exact integrity verification at every later stage. No model output is produced before the item has an identity.

Detection and scene understanding. Two detectors run on the preprocessed image. A YOLOv8 model with COCO weights provides general object context (people, vehicles, everyday objects). A custom YOLOv11 model, trained on a crime-scene object dataset from Roboflow Universe, targets three weapon classes: shotgun, handgun and knife. Gamma correction and CLAHE are applied before detection to reduce the effect of under-exposed or low-contrast scenes. CLIP assigns a scene label and BLIP produces a natural-language caption. OCR is applied to extract visible text. The two

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511178

detectors are complementary by design: the COCO model supplies breadth, while the custom model supplies the forensic categories that COCO does not contain.

Metadata extraction. Embedded metadata is extracted and compared with file-system and upload information. Disagreement, such as a timestamp inconsistent with upload time, becomes input to the timeline and metadata validators rather than being discarded.

AI evidence analysis. A rule-based reasoner correlates detected objects, scene label, caption and OCR text, and produces a short explanation with a confidence score. We use rules here deliberately: every inference can be traced to specific inputs, which is consistent with the interpretability concern raised in [14] and with the need for reliability in legal use [21].

Validation and admission. A set of validators (Section 4) produces per-aspect scores. The admission engine aggregates them, assesses risk, and outputs ACCEPT, REVIEW, or REJECT. ACCEPT leads directly to custody recording. REVIEW and REJECT are routed to a human investigator, who may confirm the decision or admit the item.

Chain of custody and storage. Each admitted item yields a custody block holding the evidence digest, an analysis digest, the admission decision, the actor and a timestamp, linked to the previous block by hash. The original image is stored in Supabase cloud storage. Verification re-computes the digest of the stored object and re-walks the ledger.

Report generation and review. A OpenAI model receives a structured record of the verified findings and returns a draft report. The investigator inspects the draft against the evidence viewer and AI findings, edits it where necessary, and approves it. Only the approved version is rendered as the final PDF report.

IV. SYSTEM ARCHITECTURE

Fig. 1 shows the layered architecture, which mirrors the evidence lifecycle. The layers are described below in the order in which an item traverses them.

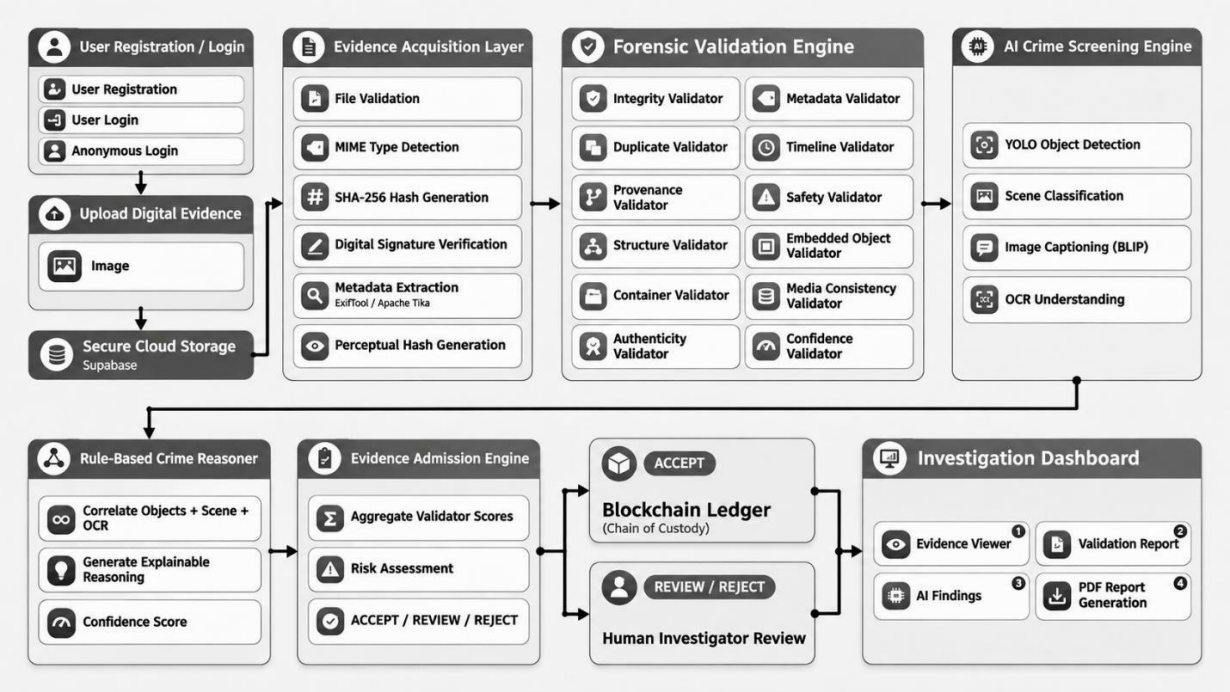


Fig. 1 Layered system architecture

User and upload layer. The layer supports registration, login and anonymous login, followed by evidence upload. Anonymous login allows a contributor to submit an image without a persistent identity; the submission is still hashed and validated like any other. Uploaded files are placed in Supabase secure cloud storage and passed to the acquisition layer.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511178

Evidence acquisition layer. This layer performs file validation, MIME-type detection, SHA-256 generation, digital-signature verification, metadata extraction (ExifTool and Apache Tika) and perceptual-hash generation. Its outputs are the identity record and the raw metadata used by later stages.

Forensic validation engine. Twelve validators examine the item from complementary angles: integrity, metadata, duplicate, timeline, provenance, safety, structure, embedded object, container, media consistency, authenticity and confidence. Each produces a bounded score and, where it fails, a reason. Keeping the validators separate allows individual checks to be added or replaced, for example the authenticity validator could host a deepfake or tamper detector of the kind surveyed in [5], [17], [18].

AI crime screening engine. This engine runs YOLO object detection, scene classification (CLIP), image captioning (BLIP) and OCR. The detection stage is the only component for which we report quantitative evaluation in this paper (Section 8).

Rule-based crime reasoner. The reasoner correlates objects, scene and OCR output, generates explainable reasoning and computes a confidence score. For example, a handgun detection in an indoor scene whose caption and OCR text are unrelated to weapons receives a lower correlation score than one supported by two other signals.

Evidence admission engine. It aggregates validator scores, performs risk assessment and returns ACCEPT, REVIEW or REJECT. ACCEPT forwards the item to the blockchain ledger. REVIEW and REJECT forward it to human investigator review.

Blockchain ledger and investigation dashboard. The ledger stores the custody chain. The dashboard exposes four views: the evidence viewer, the validation report, the AI findings and PDF report generation. These correspond to the material an investigator needs in order to verify a generated report against its sources.

Design rationale. Three choices follow from the gaps identified in Section 2. Hashing precedes analysis (G1). The admission engine separates custody from upload (G2). The ledger payload includes the analysis digest and decision so that the record explains acceptance (G3). The report generator reads only the recorded findings (G4).

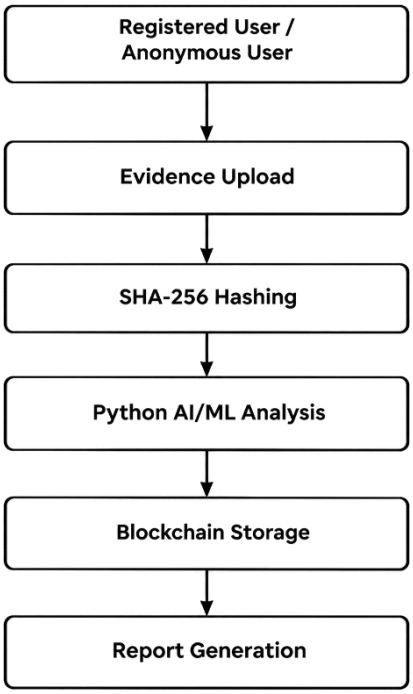


Fig. 2 End-to-end workflow diagram — Input Evidence → Secure Storage ->AI Detection and Scene Understanding → Metadata Extraction → AI Evidence Analysis → Validation/Admission → Blockchain Chain of Custody→ Report Generation → Investigator Review.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511178

V. PROPOSED ALGORITHMS

Four procedures define the framework. They operate on the integrated workflow and deliberately omit the internals of the hashing function, the detectors and the language model, which are used as given components. Notation is introduced in Section 6.

Algorithm 1. Overall framework procedure

Input : evidence image e, submitting user u (registered or anonymous)
Output: approved report R*, or a recorded non-admission outcome

```
(rec, A) ← EvidenceProcessing(e, u)  // Algorithm 2
if A = ACCEPT then
    blk ← AppendCustody(rec, actor = system)  // Algorithm 3
else  // REVIEW or REJECT
    queue rec for investigator review
    d ← investigator decision on rec
    if d = admit then
        blk ← AppendCustody(rec, actor = investigator)
    else
        retain rec with decision d; stop
store e in secure cloud storage under key h_e
draft ← GenerateReport(rec, blk)  // Algorithm 4
R* ← investigator review and approval of draft
render R* as the final investigation report
return R*
```

Algorithm 2. Evidence processing

Input : evidence image e, submitting user u
Output: evidence record rec, admission decision A

```
if not FileValid(e) or MIME(e) ∉ allowed then return (null, REJECT)
h_e ← SHA256(e);  p_e ← PerceptualHash(e)
sig ← VerifySignature(e)  // where a signature exists
M ← ExtractMetadata(e)  // ExifTool, Apache Tika
ẽ ← CLAHE(Gamma(e))  // preprocessing for detectors
D_coco ← YOLOv8(ẽ);  D_wpn ← YOLOv11(ẽ)
D* ← FilterDetections(D_coco ∪ D_wpn)  // Eq. (4)
s* ← CLIP(e);  cap ← BLIP(e);  T ← OCR(e)
(expl, C_AI) ← Reason(D*, s*, cap, T, M)  // rule-based, Eq. (5)
for each validator j in {1..12} do
    v_j ← Validate_j(e, h_e, p_e, sig, M, D*, C_AI)
S ← Σ_j α_j v_j;  F ← hard-failure flag  // Eqs. (6), (7)
A ← Admit(S, F, θ_a, θ_r)
η ← SHA256(Canon(D*, s*, cap, T, M, C_AI, S))  // analysis digest
rec ← (h_e, p_e, M, D*, s*, cap, T, expl, C_AI, S, A, η, u)
return (rec, A)
```

The order of steps 2 to 9 is intentional. The identity record (h_e, p_e) is created before any model runs, so that every later artefact can be tied to a specific byte sequence. Step 14 produces a digest of the canonical serialisation of the analysis so that the analysis, and not only the image, is fixed at the time of admission.

Algorithm 3. Blockchain chain-of-custody

```
Procedure AppendCustody(rec, actor)
1    prev ← head of ledger  // genesis if empty
```

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511178

```
2   blk ← (index = prev.index + 1, t = now(), actor,
3   h_e = rec.h_e, η = rec.η, A = rec.A, H_prev = prev.H)
4   blk.H ← SHA256(Serialise(blk without H))
5   append blk to ledger
6   return blk
```

```
Procedure VerifyCustody(e_stored, rec)
1   ok ← true;  H_prev ← genesis hash
2   for i = 1 to n do  // walk the ledger
3       if blk_i.H_prev ≠ H_prev then ok ← false
4       if blk_i.H ≠ SHA256(Serialise(blk_i without H)) then ok ← false
5       H_prev ← blk_i.H
6   blk_e ← block with h_e = rec.h_e
7   if blk_e does not exist then ok ← false
8   if SHA256(e_stored) ≠ blk_e.h_e then ok ← false
9   return ok
```

Verification therefore covers two separate failure modes: alteration of the ledger (steps 2–5) and alteration or substitution of the stored object (steps 6–8). Recomputing the analysis digest from the stored record and comparing it with η extends the check to the AI findings.

Algorithm 4. AI report generation with investigator verification

```
Input : evidence record rec, custody block blk
Output: approved report R*
```

```
1   Φ ← {h_e, blk.index, blk.t, M_subset, D*, s*, cap, T,
        expl, C_AI, validator scores, decision A}  // structured findings
2   prompt ← Template(Φ)  // instruct: use only fields of Φ; mark missing
        // items "not available"; no legal conclusions
3   draft ← Openai(prompt)
4   for each class label, count, score or hash quoted in draft do
5       if value ∉ Φ then flag the statement
6   if flagged statements exist then regenerate once; flag again if persistent
7   present draft, flags, evidence viewer and AI findings to investigator
8   repeat
9       investigator edits, removes or confirms statements
10  until investigator approves
11  R* ← approved text with report identifier and approval time
12  return R*
```

The language model never sees the raw image in this procedure; it sees only the recorded findings. Step 4 is a mechanical consistency check rather than a semantic guarantee, and the investigator remains the authority on content.

VI. IMPLEMENTATION AND EXPERIMENTAL SETUP

A. System Implementation

1) Overall Implementation:

The proposed HCEAF framework was implemented as a prototype for secure image-based digital evidence management. The system accepts uploaded image evidence and processes it through a sequence of validation, AI-based analysis, evidence preservation, and report generation stages. Each uploaded image is associated with a unique Case ID and Evidence ID to maintain traceability throughout the processing workflow.

2) Evidence Processing:

After evidence is uploaded through the system interface, the uploaded image undergoes evidence validation, including

 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026
DOI: 10.17148/IJARCCE.2026.1511178

file type verification, MIME type validation, file signature verification, SHA-256 hash generation, and metadata extraction. The validated evidence and its associated metadata are securely stored in Supabase cloud storage, with links to the generated evidence identifiers.

3) AI Analysis:

The AI crime screening module analyses the uploaded image using multiple complementary models. Object and weapon detection identify relevant objects in the scene, while scene classification from the Hugging Face model CLIP (Contrastive Language-Image Pre-training), image captioning from the AI model BLIP (Bootstrapping Language-Image Pre-training), and OCR provide contextual information. The evidence fusion engine consolidates outputs from these models to generate a unified interpretation of the uploaded evidence.

4) Final Processing:

After evidence admission and validation, the system records the processed evidence using a blockchain-based chain-of-custody mechanism to preserve integrity and traceability. Finally, the system generates an AI-assisted forensic report together with a preliminary FIR to support investigator review while preserving human oversight during decision-making.

B. Experimental Setup

1) Dataset:

The proposed prototype was evaluated using the publicly available Crime Scene Object Detection dataset from Roboflow Universe. The dataset contains crime-scene images annotated with thirteen object classes, including Handgun, Knife, Shotgun, Rope, Glass, Blood, Fingerprint, Human Body, Human Hair, Human Hand, Shoe Print, and Victim. The dataset comprises 4,463 annotated images distributed across training, validation, and test subsets.

For this work, a custom YOLOv11 object detection model was trained on selected classes relevant to digital forensic investigations: Handgun, Knife, Gun, and Person. Prior to training, image preprocessing techniques including gamma correction and Contrast Limited Adaptive Histogram Equalisation (CLAHE) were applied to improve image illumination and local contrast, thereby enhancing object visibility under varying lighting conditions. In addition to the custom detector, a pretrained YOLOv8 model trained on the Microsoft COCO dataset was incorporated to identify general objects present within the uploaded evidence images. The combination of the custom-trained and pretrained models enabled the system to detect both forensic-specific objects and common scene entities for subsequent evidence analysis.

2) Technology Used:

Component	**Technology**	**Purpose**
User Interface	Streamlit	Upload and visualize image evidence
Database	SQLite	Store evidence metadata and processing records
Cloud Storage	Supabase	Secure storage of validated evidence
Object Detection	YOLOv8 (COCO)	Detection of general objects
Weapon Detection	Custom YOLOv11	Detection of handgun, knife, gun and person
Scene Classification	CLIP	Classification of crime-scene context
Image Captioning	BLIP	Automatic scene description
OCR	EasyOCR	Extraction of textual information
Metadata Extraction	ExifTool, Apache Tika	Metadata and MIME type extraction
Integrity Verification	SHA-256	Evidence integrity verification
Blockchain	Ethereum	Chain-of-custody preservation
Report Generation	OpenAI GPT	AI-assisted forensic report generation

3) Experimental Protocol:

The implemented prototype was evaluated using the image dataset described in Section 6.2.1. Each uploaded image was processed through the complete evidence management pipeline, beginning with evidence registration, validation, metadata extraction, and secure cloud storage. The validated evidence was subsequently analysed using the AI crime

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511178

screening module, followed by evidence fusion, evidence admission, blockchain-based chain-of-custody recording, and AI-assisted forensic report generation. The performance of the AI models was evaluated using standard classification metrics, while the overall system efficiency was assessed by measuring the execution time of individual pipeline stages and the complete processing workflow.

XV. RESULTS AND EVALUATION

A. AI Model Performance

1) YOLOv11 (Custom Model):

AP @ [0.50:0.95]	**0.682**	**AR @ 1 detection**	**0.521**
AP50	0.860	AR @ 10 detections	0.753
AP75	0.775	AR @ 100 detections	0.793
AP small	0.000	AR small	0.000
AP medium	0.157	AR medium	0.410
AP large	0.691	AR large	0.798
AR50	0.959	AR75	0.879

2) YOLOv8 (COCO):

The pretrained YOLOv8 model was incorporated to identify general scene objects that complement the forensic-specific detections obtained from the custom YOLOv11 model. Since the model was used without retraining, its outputs were evaluated qualitatively as part of the integrated pipeline rather than through standalone training metrics.

B. End-to-End Pipeline Performance

Pipeline Stage	**Execution Time (s)**
Image Evidence Upload	30
Evidence Acquisition	10
Secure Cloud Upload	8
AI Crime Screening	28
Evidence Admission & Validation	7
Blockchain Registration	17
AI-Assisted Report Generation	20
Total Pipeline Execution Time	120

The end-to-end pipeline was evaluated by processing representative image evidence through the implemented prototype. We measured the execution time of each major processing stage from the system logs and user interface progress updates.

C. Prototype Result

Localisation quality. The model reaches AP50 = 0.860 and AP75 = 0.775, a drop of 0.085 when the IoU requirement rises from 0.50 to 0.75. The further drop to AP@[0.50:0.95] = 0.682 shows that precision degrades mainly at the strictest thresholds (above 0.75). Most correct detections are therefore well localised, which matters for the evidence viewer, where bounding boxes are displayed to the investigator as visual support for a finding.

Recall and detections per image. AR rises from 0.521 at one detection per image to 0.753 at ten, and only to 0.793 at one hundred. The large first increment is consistent with images containing more than one annotated object, since AR1 cannot exceed what a single detection can recover; the small second increment indicates that recall is nearly saturated by ten detections. AR50 = 0.959 and AR75 = 0.879 show that, at a permissive overlap threshold, about 96% of annotated objects are recovered. For a screening stage whose output is advisory and subject to review, this recall-oriented behaviour is preferable to a precision-oriented one, motivating the lower class-specific thresholds in Eq. (4).

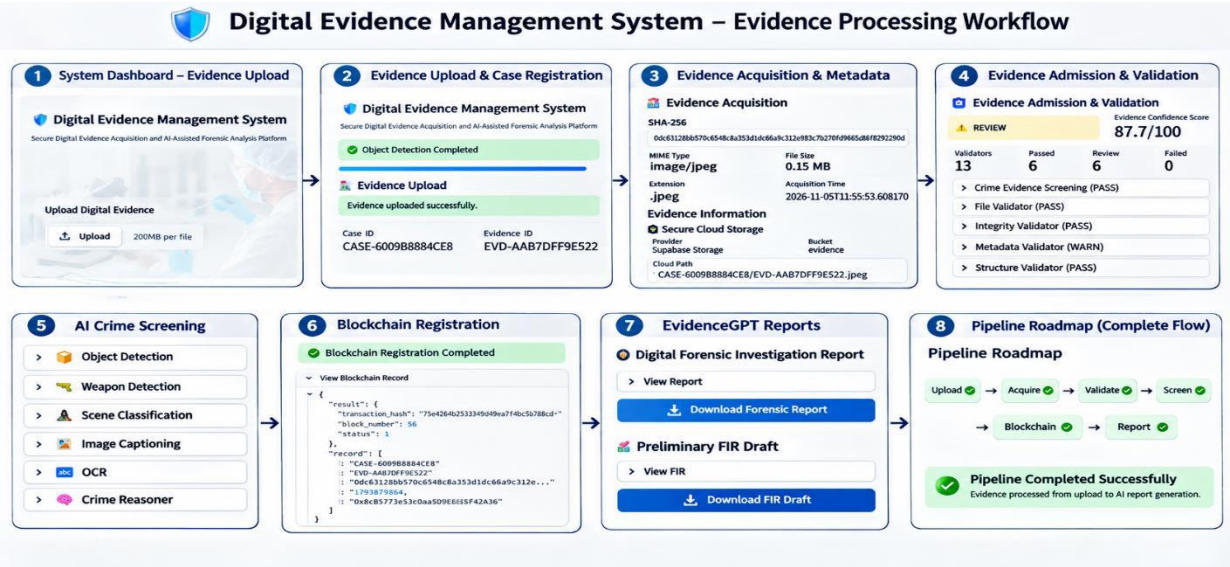
 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.1511178



Dependence on object size. The aggregate figure is dominated by large objects: $AP_{large} = 0.691$ is close to the overall AP, and $AR_{large} = 0.798$ is close to AR100. Performance falls sharply for medium objects ($AP_{medium} = 0.157$, $AR_{medium} = 0.410$), where recall is considerably higher than precision, suggesting that such objects are often found but with low-quality boxes or ranking. Both AP_{small} and AR_{small} are 0.000. Under the standard COCO evaluation convention, a value of -1 would signal that no ground-truth objects exist in a bucket, so 0.000 indicates that small objects were present but not recovered. If that convention was applied in our evaluation, small weapons in wide or distant frames should be treated as outside the reliable operating range of the current model. We have not examined the size distribution of the dataset and do not infer a cause beyond this.

Position relative to the literature. The surveyed deepfake and tamper-detection works focus on authenticity classification [13], [16]–[18], while ledger-based systems focus on custody [6], [9], [10], [20]. The framework combines weapon-oriented content screening with an admission decision and a custody record, placing the AI findings under the same integrity protection as the evidence itself. A numerical comparison with those works is not possible, since they address different tasks and datasets and we do not reproduce their results here.

XIII. LIMITATIONS AND FUTURE WORK

Limitations. (i) The implementation handles still images only; video, audio, documents and disk images are outside the present scope. (ii) The detector evaluation is aggregate. Per-class AP, a confusion matrix and an ablation of gamma correction and CLAHE are not available, and the small-object result ($AP_{small} = AR_{small} = 0.000$) shows a clear operating limit. (iii) The framework is evaluated at the component level; an end-to-end study with investigators, including measurements of review time and error rates, has not been carried out. (iv) The validator weights, reasoning-rule weights and admission thresholds are fixed design parameters and have not been calibrated against labelled admission outcomes. (v) The rule-based reasoner is interpretable but limited to the correlations it encodes, and CLIP and BLIP outputs are used as pretrained models without forensic fine-tuning. (vi) The report generator relies on an external language model; the consistency check in Algorithm 4 detects values absent from the findings record but cannot detect misleading phrasing, so investigator review remains essential. (vii) The ledger is a custody and integrity mechanism; it does not by itself establish that an image was truthful when captured, which is the concern of the authenticity and deepfake literature [5], [13], [16]–[18].

Future work. First, the authenticity validator can be populated with a tamper or synthetic-media detector in the manner of [11], [12], [14], [17], [18], with evaluation on a dedicated dataset. Second, small-object performance can be addressed by examining the dataset's size distribution and by testing higher-resolution or tiled inference, with the evaluation repeated for the size buckets reported here. Third, per-class metrics and a preprocessing ablation should be added. Fourth, the framework can be extended to video and multimodal evidence, following the direction of [15]. Fifth, extending the ledger record to include the digest of the approved report would bring the final report itself under the same verification as Eq. (9). Finally, a structured user study with practising investigators would test whether the admission decision and the constrained report draft reduce review effort without reducing accuracy, and would allow the weights and thresholds to be calibrated.

 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026
DOI: 10.17148/IJARCCE.2026.1511178

IX. CONCLUSION

This paper presented an image-oriented framework in which AI analysis, admission control, a hash-linked chain of custody, cloud storage and report drafting form one verifiable workflow with an investigator at the decision points. Its principal design choices are to fix an item's identity before analysis, to bind the analysis digest and the admission decision to the custody record, and to confine report generation to recorded findings subject to human approval. On the custom weapon detector, AP50 = 0.860, AP75 = 0.775 and AR100 = 0.793 indicate reliable localisation and recall for medium-to-large objects, while AP_{small} = 0.000 and AP_{medium} = 0.157 identify small and medium objects as the main weakness. The results justify the detector's role as an advisory screening component but do not constitute a system-level evaluation. The remaining work concerns authenticity validation, small-object detection, broader modalities and a user study.

REFERENCES

[1]. F. Casino, T. K. Dasaklis, G. P. Spathoulas, M. Anagnostopoulos, A. Ghosal, I. Borocz, A. Solanas, M. Conti, and C. Patsakis, "Research trends, challenges, and emerging topics in digital forensics: A review of reviews," *IEEE Access*, vol. 10, pp. 25464–25493, 2022, doi: 10.1109/ACCESS.2022.3154059.

[2]. A. Stoykova, "Digital evidence: Unaddressed threats to fairness and the presumption of innocence," *Comput. Law Secur. Rev.*, vol. 42, Art. no. 105575, 2021, doi: 10.1016/j.clsr.2021.105575.

[3]. A. A. Solanke and M. A. Biasiotti, "Digital forensics AI: Evaluating, standardising and optimising digital evidence mining techniques," *Künstliche Intelligenz*, vol. 36, pp. 143–161, 2022, doi: 10.1007/s13218-022-00763-9.

[4]. T. Nayerifard, H. Amintoosi, A. G. Bafghi, and A. Dehghantanha, "Machine learning in digital forensics: A systematic literature review", *arXiv*:2306.04965, 2023.

[5]. M. S. Rana, M. N. Nobi, B. Murali, and A. H. Sung, "Deepfake detection: A systematic literature review," *IEEE Access*, vol. 10, pp. 25494–25516, 2022, doi: 10.1109/ACCESS.2022.3154404.

[6]. M. M. Ali, M. S. Islam, M. N. Uddin, M. A. Uddin, and K. S. Kushal, "A blockchain-based digital classified forensic image preservation framework", preprint, 2024, doi: 10.22541/au.171575721.19694510/v1.

[7]. Adewumi, Engr. Idowu. (2025). Blockchain and Artificial Intelligence for Forensic Evidence Chain-of-Custody Management: Towards Transparent and Tamper-Proof Judicial Systems Aligned with SDG 16 and SDG 9. 10.21203/rs.3.rs-7926866/v1.

[8]. P. Han, "AI-powered digital arbitration framework leveraging smart contracts and electronic evidence authentication," *Sci. Rep.*, vol. 15, Art. no. 37327, 2025, doi: 10.1038/s41598-025-21313-x.

[9]. S. Akkala, S. Gupta, and P. V. Sai, "Secure and tamper-proof blockchain-enabled cybercrime reporting and evidence management system," *ITM Web Conf.*, vol. 81, Art. no. 01007, 2026, doi: 10.1051/itmconf/20268101007.

[10]. R. P. Santosh, B. Rohith, B. S. Abhiram, and S. G. Kaushik, "SecureXChain: A decentralised blockchain-based chain of custody system for secure and transparent asset management," in *Emerging Technologies, AI, Computing, Communication and Cybersecurity*, 2025, pp. 249–256, doi: 10.1201/9781003739791-47.

[11]. A. Bhondave, A. A. Utikar, A. Pund, and S. Shinde, "Deepfake forensics tool: AI-driven multi-modal media authentication with forensic evidence reporting," *Indian Sci. J. Res. Eng. Manage.*, 2026, doi: 10.55041/ijsrem57455.

[12]. Minnah, N. (2026). DeepFake Forensics AI: "A Multi-Modal Detection and Blockchain-Anchored Evidence Management Platform". *arXiv e-prints* (arXiv:2605.29353). https://doi.org/10.48550/arXiv.2605.29353

[13]. Shivangi Tiwari and Bharti Kumari, Trans., "Development of Digital Forensics Technique Based in AI to Identify Deepfake Video and Image", *International Journal of Scientific Research in Science and Technology*, vol. 13, no. 3, pp. 01–05, May 2026, doi: 10.32628/IJSRST26133116.

[14]. Nitu Bharati, Patrick Wong, Soraya Kouadri Mostéfaoui, Dhouha Kbaier, Jan Collie, "Explainable deepfake detection: A multi-model framework with human-interpretable rationales for legal investigation purposes", *Machine Learning with Applications*, Volume 23, 2026, 100819, ISSN 2666-8270, https://doi.org/10.1016/j.mlwa.2025.100819.

[15]. S, Ujjain & Jaiswal, Yuvaraj & Palanichamy, Tamilselvi. (2025). A Multi-Modal Ensemble Framework for Automated Digital Forensics Evidence Classification and Investigation. 1-5. 10.1109/IConSCEPT66142.2025.11436876.

[16]. Pal, Manoj & Soni, Hemant & Dey, Saswata & Polagani, Sai Santhosh & Gandhi, Amita & Lakhina, Upasana. (2025). "A Digital Forensic Model for Identifying Deepfake Multimedia in The Cyber-Social Space". 230-235. 10.1109/ICOCO67189.2025.11334094.

 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026
DOI: 10.17148/IJARCCE.2026.1511178

[17]. Chitti, Praveen & Prabhushetty, K. (2022). A Deep Learning and Machine Learning Approach for Image Classification of Tempered Images in Digital Forensic Analysis. *International Journal of Advanced Computer Science and Applications*, 13. 10.14569/IJACSA.2022.0131069.

[18]. Waqas, Muhammad & Alam, Aftab & Khan, Sara. (2024).” ADVANCING FORENSIC APPLICATIONS: THE ROLE OF ARTIFICIAL INTELLIGENCE IN DETECTING AND MITIGATING IMAGE AND VIDEO MANIPULATION”. *Computers and Education Letters*. 1. 32-41. 10.64038/cel.01202428.

[19]. R. K. Roy, N. Pandey, S. Ghatak, and R. Sharma, "Enhancing criminal investigations through an AI-based photographic memory for CGI detection”, in *Proc. ICICNIS*, 2025, doi: 10.1109/icicnis66685.2025.11315796.

[20]. G. Dandimeni, “EVID-DGC – Blockchain-based evidence management system,” *Zenodo*, 2026, doi: 10.5281/zenodo.18397132.

[21]. S. N. V. J. D. Kosuru and B. Unhelkar, “A deep learning and hybrid optimisation framework for digital evidence tamper detection: Legal reliability, chain of custody, and cyber forensics,” *Restitution Law Rev.*, vol. 34, no. 2, pp. 55–69, 2026.

 This work is licensed under a Creative Commons Attribution 4.0 International License