PROJECT DOCUMENTATION

Title: AI-Based Digital Evidence Authentication System for Forensic Analysis

Tool Name: EvidenceHub Forensic Suite

Prepared for:
Manager, Proforce Intelligent System Ltd and entire Management

Prepared by:
Chimenka Goodluck Uchechi
(Digital Forensics Analyst)

Date: Monday, September 15, 2025

Executive Summary

The AI-Based Digital Evidence Authentication System is a forensic tool developed to authenticate and verify the integrity of digital images and documents. It uses artificial intelligence (AI), machine learning (ML), and metadata forensics to detect tampering, deepfake manipulations, and hidden inconsistencies.

This system enhances trust in digital evidence, ensuring it remains admissible in legal proceedings and reliable for law enforcement investigations. Proforce Intelligent System Ltd can advance this project to an industrial-grade solution, providing a competitive advantage in the field of cybersecurity and digital forensics.

Project Objectives

- Detect and prevent digital evidence manipulation.
- Authenticate both pictures, audio, video and documents.
- Provide deepfake and forgery detection capabilities.
- Reveals hidden malware, rootkits or any unwanted program.
- Improves and embeds other forensic tool capability to make detection reliable.
- Ensure chain of custody tracking for legal admissibility.
- Generate forensic reports with integrity verification.
- Deliver a user-friendly interface for investigators and analysts.

System Architecture & Modules

A. Input & Preprocessing
- Upload images, scanned documents, videos, audios or digital files.

- Extract metadata (timestamps, device info, authoring history).
- Normalize formats for analysis.

B. Image Authentication Module
- AI-powered analysis using PyTorch pre-trained CNNs (e.g., ResNet, EfficientNet).
- Detect pixel-level inconsistencies, compression artifacts, and possible deepfakes.
- Performs error level analysis and noise suppression to detect edited pictures
- Classify results as Authentic / Manipulated / Suspicious.

C. Document Authentication Module
- Supports PDF, DOCX, and scanned formats.
- Identifies metadata tampering, content modifications, or hidden edits.
- NLP-based detection for AI-generated vs. human-written text.
- Checks metadata inconsistency, and file level analysis to detect unwanted executions.

D. AI & Model Layer
- Built on PyTorch for flexibility.
- Models fine-tuned on forensic datasets.
- Supports integration of new models as threats evolve.

E. Chain of Custody & Integrity Module
- Hashing with SHA-256 for evidence integrity.
- Logs all actions (upload, verification, report generation) with timestamps.
- Maintains traceability for legal admissibility.

F. User Interface
- Simple dashboard for evidence verification.
- Upload, verify, and generate forensic reports.
- Results displayed with confidence scores.

G. Reporting Module
- Generates PDF/HTML forensic reports.
- Includes metadata, AI analysis, decision summary, and system confidence.

Current Features Implemented

- Image verification with AI models (PyTorch).
- Metadata extraction for documents and pictures.
- Basic deepfake detection.

- Chain of custody logging (local storage).
- Prototype forensic report generation.

Expansion Areas (Industrial Upgrade Needed)

1. Scalability – Deploy on cloud infrastructure with GPU acceleration.
2. Accuracy – Fine-tune models with larger forensic datasets.
3. Speed – Optimize for handling large volumes of evidence efficiently.
4. UI/UX – Develop a polished web interface for investigators and legal teams.
5. Integration – Provide APIs for law enforcement databases and court systems.
6. Security – Add encryption for uploads, results, and chain-of-custody logs.
7. Explainability – Incorporate AI explainers for legal justification of results.
8. Blockchain Module (Future) – Store custody logs on blockchain for immutability.
7. Use other forensic tool support to improve performance and accuracy

Technologies Used

- Programming Language: Python 3, JavaScript,
- Frameworks: Django, PyTorch, OpenCV, NLP toolkits
- Database: SQLite (upgrade path: PostgreSQL)
- Security: SHA-256 hashing, TLS/SSL encryption
- API: Hunging face API
- Platform: Parrot OS (Linux) with GPU support

Limitations of Current Prototype

- Limited dataset (requires expansion for higher accuracy).
- Heavy computation required for large files.
- Deepfake detection in early development stage.
- Chain of custody not yet cloud/distributed.

Future Improvements

- Multi-language forensic reports.
- Mobile application for field investigators.
- Distributed cloud-based forensic verification.
- Blockchain-based custody tracking.
- Continuous AI model retraining with new forensic data.

Conclusion & Recommendation

The developed system is functional at prototype level and demonstrates strong potential for industrial adoption. With further investment in infrastructure, dataset acquisition, and development resources, Proforce Intelligent System Ltd can transform this tool into a world-class forensic solution.

It is recommended to:
- Advance to industrial development phase.
- Allocate resources for model optimization and UI/UX development.
- Pilot the system with law enforcement or corporate clients.

In conclusion, I am available to present a live demonstration of the system and collaborate with the AI team to transition it into an industrial-grade solution.