International Journal of Electrical, Electronics and Computer Systems
ISSN: 2347-2820
Volume 15 Issue 01 (2026) | Pages: 86-90

Decentralized Evidence Management and AI-Assisted Forensic Sketch Generation System

Jalindar Nivrutti Ekatpure[1], Sonali Ekande[2], Mayur Kokare[3], Tabasum Mulani[4], Geeta Patil[5]

[1]S. B. Patil College of Engineering
[2,3,4,5]Department of Computer Engineering, Savitribai Phule Pune University
[1]*j.ekatpure@gmail.com* , [2]*sonaliekhande12@gmail.com* , [3]*mayurkokare4212@gmail.com,*
[4]*tabassummulani4@gmail.com,*[5]*Patilgeetagopal@gmail.com*

Peer Review Information

***Type**: Article*
***Received**: 22 March 2026*
***Revised**: 06 April 2026*
***Accepted**: 24 May 2026*
***Published**: 05 June 2026*

Abstract

The increasing reliance on digital evidence in criminal investigations necessitates secure and transparent management systems. Traditional forensic systems suffer from vulnerabilities such as data tampering, lack of traceability, and inefficient suspect identification. This paper proposes a decentralized system, ForensicChain, which integrates blockchain technology, InterPlanetary File System (IPFS), and artificial intelligence for secure evidence management and forensic sketch generation. Blockchain ensures immutability and transparent chain of custody, while IPFS provides decentralized storage.

Keywords: Blockchain; Digital Forensics; InterPlanetary File System (IPFS); AI Sketch Generation; Face Recognition; Evidence Management; Cybersecurity.

How to Cite This Article

Ekatpure, J. N., Ekande, S., Kokare, M., Mulani, T., & Patil, G. (2026). Decentralized evidence management and AI-assisted forensic sketch generation system. *International Journal of Electrical, Electronics and Computer Systems*, 15(1), 86–90.

Introduction

The increasing use of digital evidence in modern criminal investigations has introduced significant challenges in ensuring data integrity, security, and transparency. Traditional forensic systems rely on centralized architectures, which are vulnerable to tampering, unauthorized access, and lack of traceability. This study explores the application of decentralized technologies and artificial intelligence to address these limitations. By integrating blockchain for immutable evidence logging, IPFS for distributed storage, and AI for automated forensic sketch generation, the proposed system aims to enhance reliability and efficiency in forensic processes. Blockchain ensures a verifiable chain of custody, while AI techniques enable accurate suspect identification through sketch generation and face recognition. Through this research, we aim to improve the trustworthiness and effectiveness of forensic investigations. Ultimately, the goal is to support a more secure, transparent, and technology-driven approach to evidence management in the field of digital forensics.

Overview of the project objectives

- Develop Decentralized System: Design a blockchain-based framework to ensure secure and tamper-proof evidence management.
- Secure Evidence Storage: Utilize IPFS to store digital evidence in a decentralized and distributed manner, eliminating single points of failure.
- Ensure Data Integrity: Implement cryptographic hashing (SHA-256) and blockchain anchoring to maintain immutability and authenticity of evidence.
- Automate Sketch Generation: Use artificial intelligence to generate forensic sketches from textual descriptions provided by investigators or witnesses.
- Implement Face Recognition: Apply embedding-based similarity matching techniques to identify suspects from a criminal database.

Literature Survey

1. Blockchain-Based Digital Evidence Management System, Haya R. Hasan, Khaled Salah, 2019: In this paper, the challenge of evidence tampering and lack of transparency in centralized forensic systems is addressed. The authors proposed a blockchain-based framework for secure evidence logging. The solution ensures immutability and auditability of records. Future work focuses on improving scalability and legal integration. [1]

2. A Blockchain Framework for Chain of Custody in Digital Forensics, M. N. Islam, M. S. Hossain, 2020: This study highlights the absence of a verifiable chain of custody in digital investigations. Smart contracts were used to automate custody tracking and ensure authenticity. The system improves trust but requires cross-organizational adoption. Future work includes automation and broader integration. [2]

3. IPFS-Based Secure Storage for Digital Evidence, A. Singh, R. Kumar, 2021: The paper addresses the issue of centralized storage leading to data loss and single point failure. IPFS was used to provide decentralized and distributed storage. The solution improves availability and security of evidence. Future enhancements include faster retrieval mechanisms and hybrid storage models. [3]

4. Face Recognition Using 128D Embeddings for Identification, Davis E. King, 2018: This research focuses on improving suspect identification accuracy. It uses deep learning-based 128-dimensional embeddings for face recognition. The approach provides reliable biometric matching. Future work aims to improve performance on low-quality and distorted images. [4]

5. Generative AI for Forensic Sketch Generation, AI Research Surveys, 2022: This study addresses the limitations of manual forensic sketch generation, which is slow and inconsistent. Generative AI models were used to create sketches from textual descriptions. The solution reduces dependency on artists. Future work includes improving realism, reducing bias, and enhancing control over generated outputs. [5]

6. Blockchain for Secure Digital Forensics, M. Crosby et al., 2016: The paper explores blockchain technology beyond cryptocurrency applications. It highlights its potential in ensuring data integrity and security in digital systems. The approach supports tamper-proof record keeping. Future work includes applying blockchain to large-scale forensic systems. [6]

7. Ethereum-Based Smart Contract Systems, Gavin Wood, 2014: This work introduces Ethereum as a decentralized platform for executing smart contracts. It enables automated and transparent processes. The system provides a foundation for secure forensic applications. Future improvements include scalability and gas optimization. [7]

8. Decentralized Systems Using IPFS and Blockchain Integration, Various Authors, 2021: This study discusses integrating IPFS with blockchain for secure and efficient data storage. It solves issues related to centralization and data redundancy. The system enhances reliability and accessibility. Future work focuses on optimizing performance and reducing latency. [8]

Visualization

• *Evidence Verification Dashboard*
Graphical interface displaying evidence hash comparison and verification status. Helps investigators quickly confirm integrity and detect any tampering attempts.

• *Face Matching Results*
Visualization of similarity scores between generated sketch embeddings and stored criminal database profiles. Ranked output helps identify the most probable suspects efficiently.

Limitations Of Existing Work

- Centralized Systems: Traditional systems rely on centralized storage, making them vulnerable to tampering and single point of failure.
- Lack of Traceability: Absence of a proper chain of custody makes it difficult to verify evidence authenticity.
- Manual Sketch Generation: Depends on human artists, leading to delays and inconsistent results.

Future Work

Enhance blockchain scalability to handle large volumes of forensic data and improve transaction speed. Improve AI models for more realistic and accurate sketch generation with better attribute control. Develop cross-agency integration for secure data sharing between law enforcement departments. Deploy the system as a web and mobile application for real-time forensic analysis and investigation support.

Results And Interpretation

• *System Performance:*
The proposed system successfully ensures tamper-proof evidence storage using blockchain and secure decentralized storage through IPFS. AI-based sketch generation produces quick and consistent results, while face recognition using embedding similarity provides accurate suspect matching.

• *Insights:*
Blockchain significantly improves transparency and chain of custody verification. AI automation reduces manual effort and speeds up investigations. The integration of decentralized storage and intelligent matching enhances overall efficiency and reliability of forensic processes.

Evaluation Metrics:
The following metrics are commonly used to evaluate the performance of regression and deep learning models:

The following metrics are used to evaluate the performance of the proposed forensic system:

Metric	Definition	Purpose
Hash Integrity Verification	Validates whether the generated SHA-256 hash of evidence matches the stored blockchain hash.	Ensures evidence integrity and detects any tampering.
Similarity Score (Cosine Similarity)	Measures similarity between sketch embedding and stored criminal embeddings.	Helps in accurate suspect identification and ranking.
Accuracy	Ratio of correctly identified suspects to total cases tested.	Evaluates overall effectiveness of the identification system.
False Match Rate (FMR)	Probability of incorrectly matching a non-matching identity.	Measures system reliability and reduces false accusations.
False Non-Match Rate (FNMR)	Probability of failing to match a correct identity.	Ensures genuine suspects are not missed.
System Response Time	Time taken to process evidence, generate sketch, and return matching results.	Evaluates system efficiency and real-time performance.

Result/Output

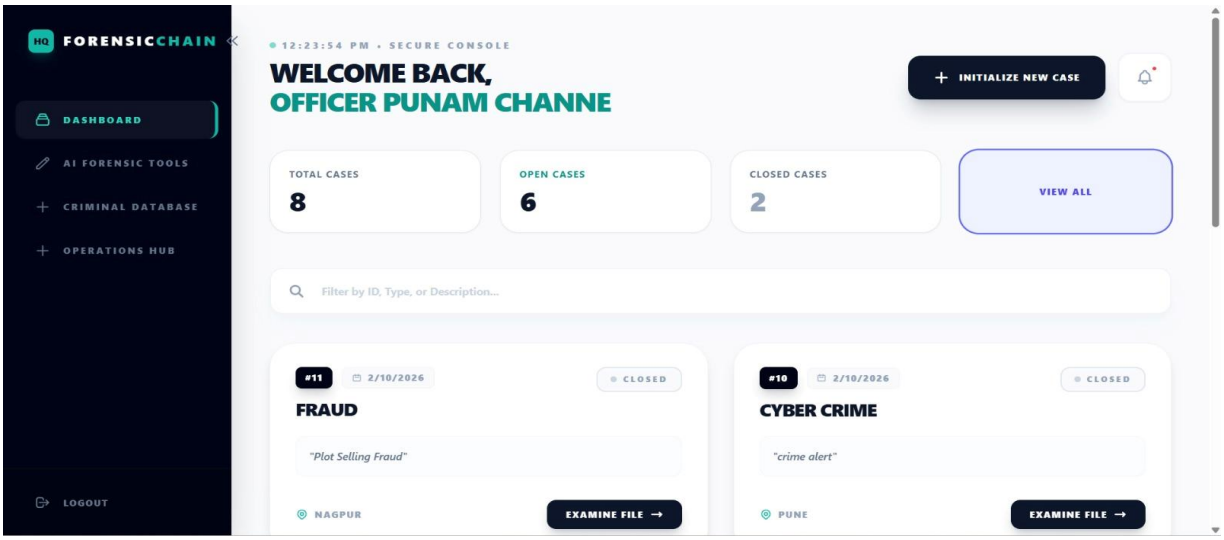

Fig. 1. *ForensicChain Dashboard Interface for Case Management*

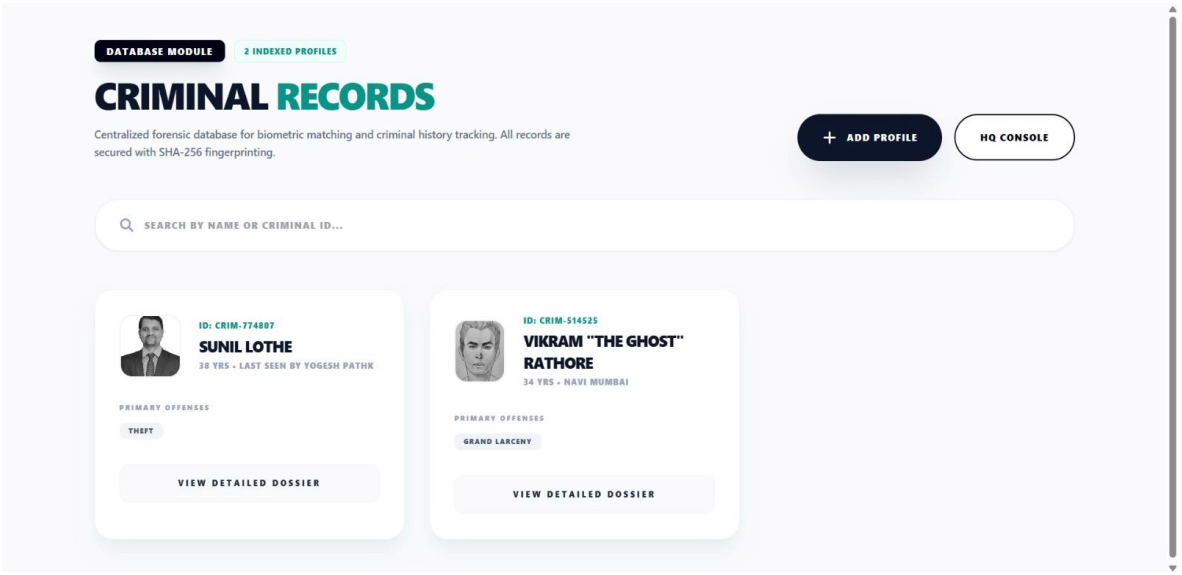

Fig. 2. *Criminal Records Database Module with Biometric Profiles*

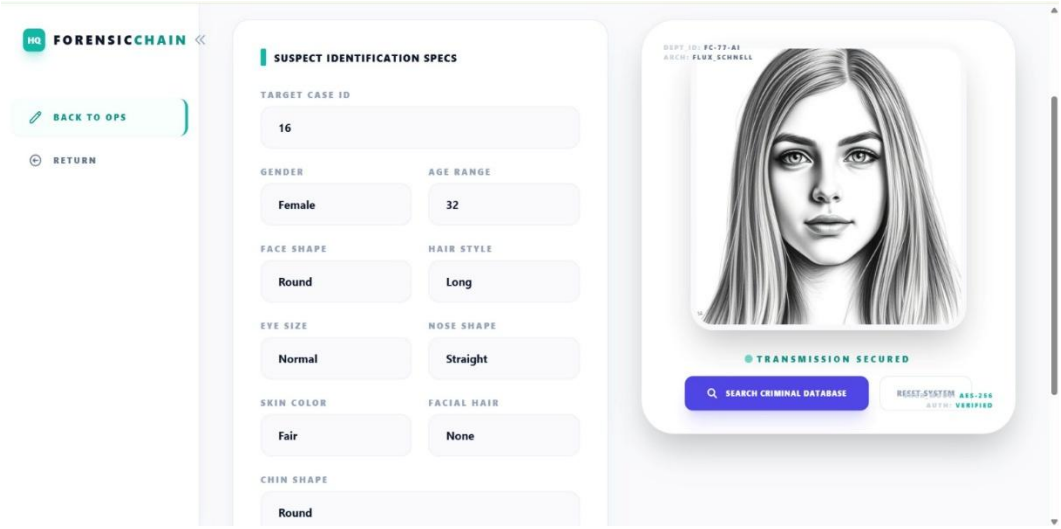

Fig. 3. *AI-Based Forensic Sketch Generation and Suspect Identification Interface*

Conclusion

This paper presents *ForensicChain*, a decentralized and AI-powered system designed to enhance the security, transparency, and efficiency of forensic evidence management. By integrating blockchain technology for immutable record keeping, IPFS for decentralized storage, and artificial intelligence for automated sketch generation and face recognition, the system effectively addresses the limitations of traditional forensic methods. The proposed approach ensures a verifiable chain of custody, protects evidence from tampering, and significantly improves suspect identification accuracy. Additionally, it reduces manual effort and enhances the speed of forensic investigations. Overall, the system provides a reliable and scalable solution for modern digital forensics, contributing to more trustworthy and technology-driven law enforcement processes. Furthermore, the system demonstrates strong potential for real-world deployment across law enforcement agencies by enabling secure data sharing, improved collaboration, and faster decision-making. With future enhancements in scalability, AI model accuracy, and cross-platform accessibility, the proposed solution can evolve into a comprehensive forensic ecosystem. This work lays a solid foundation for integrating advanced technologies into forensic science, ultimately strengthening the justice system and ensuring higher levels of accountability and trust.

References

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger (Yellow Paper),” Ethereum Foundation, 2014.
3. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain Technology: Beyond Bitcoin,” *Applied Innovation Review*, no. 2, pp. 6–19, 2016.
4. H. R. Hasan and K. Salah, “Blockchain-Based Framework for Secure and Reliable Digital Evidence Management,” *IEEE Access*, vol. 7, pp. 102–115, 2019.
5. M. N. Islam and M. S. Hossain, “A Blockchain Framework for Chain of Custody in Digital Forensics,” *IEEE Conference*, 2020.
6. A. Singh and R. Kumar, “IPFS-Based Secure Storage for Digital Evidence,” *International Journal of Computer Applications*, 2021.
7. J. Benet, “IPFS - Content Addressed, Versioned, P2P File System,” 2014.
8. D. E. King, “Dlib-ml: A Machine Learning Toolkit,” *Journal of Machine Learning Research*, vol. 10, pp. 1755–1758, 2009.
9. F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A Unified Embedding for Face Recognition and Clustering,” *IEEE CVPR*, 2015.
10. Goodfellow et al., “Generative Adversarial Nets,” *NeurIPS*, 2014.
11. A. Radford et al., “Unsupervised Representation Learning with Deep Convolutional GANs,” *ICLR*, 2016.
12. T. Karras et al., “A Style-Based Generator Architecture for Generative Adversarial Networks,” *IEEE CVPR*, 2019.
13. Y. LeCun, Y. Bengio, and G. Hinton, “Deep Learning,” *Nature*, vol. 521, pp. 436–444, 2015.
14. V. Buterin, “Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform,” 2014.
15. NIST, “Digital Evidence Guidelines,” National Institute of Standards and Technology, 2018.