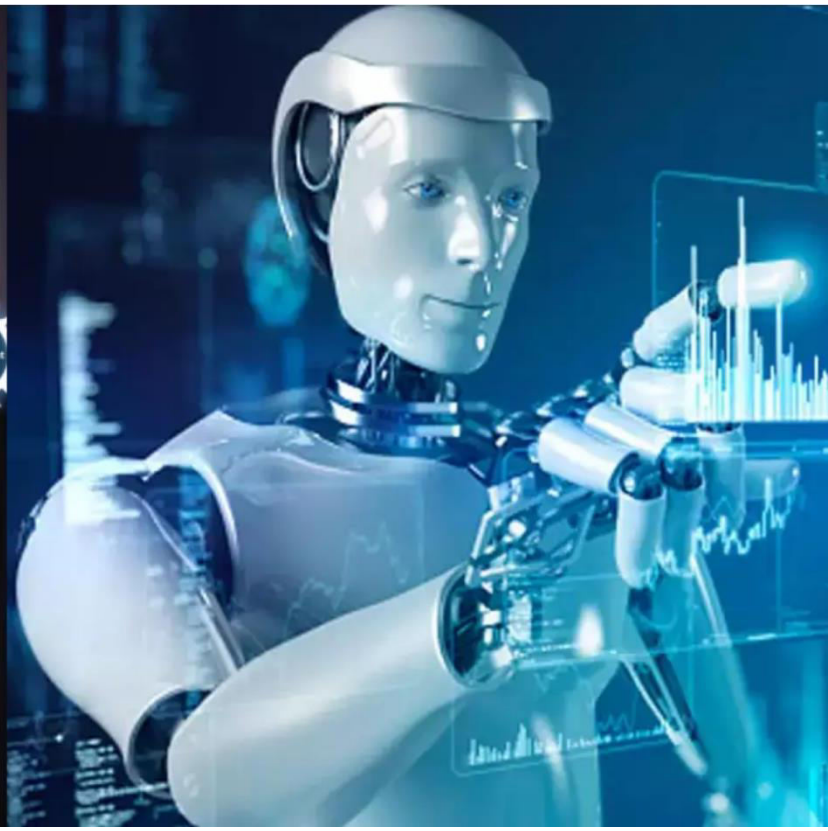
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 4, April 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504243|

Artificial Intelligence Based Evidence Preservation System using Blockchain

Prof. D. J. Manowar, Shejal Vinod Borkar, Vaishnavi Madhukar Pote,

Merajul Arsh Mohammad Hafeez

Department of Computer Science & Engineering, Takshashila Institute of Engineering and Technology, Darapur, Dist. Amravati, Maharashtra, India

Final Year Student, Department of Computer Science & Engineering, Takshashila Institute of Engineering and Technology, Darapur, Dist. Amravati, Maharashtra, India

ABSTRACT: This paper proposes an AI-driven Evidence Preservation System that combines Blockchain, Interplanetary File System (IPFS), and Advanced Encryption Standard (AES) to strengthen the security of digital evidence. Blockchain is used to record cryptographic hashes, ensuring immutability and traceability, while IPFS enables decentralized storage for efficient and distributed data management. AES encryption protects sensitive information by maintaining confidentiality during storage and transmission. To enhance reliability, the system incorporates Artificial Intelligence techniques for detecting manipulated or forged digital content, including deepfakes and altered documents. Experimental evaluation shows that the proposed model achieves validation accuracy exceeding 95%, ensuring effective tamper detection. The integration of decentralized technologies with intelligent analysis provides a robust framework that enhances trust and transparency in digital forensic and legal applications.

KEYWORDS: Blockchain, Artificial Intelligence, Digital Forensics, Evidence Preservation, Data Security, IPFS

I. INTRODUCTION

The increasing reliance on digital data in legal and forensic investigations has made the secure handling of evidence a critical concern. Digital files are highly susceptible to unauthorized modification, duplication, and misuse, which can undermine their credibility in legal contexts. Existing centralized systems often lack robust mechanisms to guarantee data integrity, secure storage, and transparent verification.

To overcome these limitations, this paper presents a secure evidence preservation framework that integrates Blockchain, IPFS, cryptographic encryption, and Artificial Intelligence. Blockchain technology ensures that evidence records remain immutable and verifiable through distributed ledger mechanisms. IPFS supports decentralized data storage, improving availability and reducing dependence on a single point of failure. AES encryption is employed to protect sensitive information from unauthorized access. In addition, AI-based analysis is utilized to identify signs of tampering in digital content, strengthening the verification process.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504243|

II. LITERATURE SURVEY

Sr. No.	Author and Year	Method Used	Result	Limitation
1	Guardiola-Múzquiz & Soriano-Salvador (2023)	Tamper-evident logging (SealFSv2)	Secure and verifiable logging	System overhead, limited scalability
2	Kamal et al. (2022)	Blockchain-based evidence preservation	Tamper-proof evidence storage	High cost, latency
3	Li et al. (2021)	Blockchain forensic framework	Traceability	Complex
4	Takaoğlu (2021)	Blockchain + steganography	Confidentiality	Complexity
5	WJARR (2024)	AI + Blockchain framework	Improved automation	High cost

III. METHODOLOGY

The proposed system uses a multi-layered architecture for secure and intelligent digital evidence management.

3.1 System Overview

The system includes multiple users such as administrators, advocates, and court officials. Administrators manage access control, while advocates upload and manage evidence. All actions are recorded to ensure transparency and accountability.

3.2 Secure Evidence Storage

All evidence files (images, videos, audio, and documents) are encrypted using AES encryption to ensure confidentiality. The encrypted files are stored in IPFS (Interplanetary File System), where each file is assigned a unique Content Identifier (CID) for secure retrieval.

3.3 Blockchain-Based Integrity Management

A SHA-2 hash is generated for each evidence file and stored on the blockchain along with metadata. Due to blockchain immutability, any modification in the original file results in a hash mismatch, enabling instant tamper detection

3.4 Chain of Custody Tracking

The system maintains a complete chain of custody by recording every interaction with evidence, including user identity, timestamps, and performed actions. This ensures a transparent and verifiable audit trail.

3.5 AI-Based Evidence Validation

The system integrates AI modules to detect manipulated or forged evidence:

- Deepfake detection for identifying synthetic media
- Video forensic analysis (frame inconsistency, motion analysis, AV sync)
- Signature verification and document comparison

3.6 Steganography & Watermarking for Ownership Validation

To ensure ownership and authenticity, the system uses LSB-based watermarking techniques. A hidden watermark is embedded into digital evidence before storage. During verification, this watermark is extracted and validated to confirm the originality and ownership of the data.

3.7 Evidence Verification Process

When evidence is accessed:

1. File is retrieved from IPFS using CID
2. File is decrypted using AES
3. Hash is regenerated and compared with blockchain

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504243|

4. AI and watermark verification modules validate authenticity

If all checks are satisfied, the evidence is considered valid.

IV. EXPERIMENTAL RESULTS

The proposed **AI-Enhanced Evidence Preservation System using Blockchain, Steganography, and Deep Learning** was evaluated across multiple dimensions including security, integrity, tamper detection, document comparison, and deepfake detection.

A. Experimental Setup

The system was implemented using:

- Backend: Python (Flask & Django)
- Database: MySQL
- Blockchain: Dual-node private blockchain
- Encryption: AES-256
- Steganography: LSB-based watermarking
- AI Models:
  - Watermark-based Tamper Detection
  - Document Comparison Engine
  - CNN-based Deepfake Detection

Dataset Used

For deepfake detection:

- Dataset Source: Kaggle Deepfake Dataset
- Total Images: 10,000+
- Categories:
  - Real Images
  - Fake (Deepfake) Images

Dataset split:

- Training: 70%
- Testing: 30%

B. Deepfake Detection Model (CNN)

A Convolutional Neural Network (CNN) was trained to classify images as **Real** or **Fake**.

Model Details:

- Input Size: 128 × 128
- Layers:
  - Conv2D + ReLU
  - Max Pooling
  - Fully Connected Layer
- Optimizer: Adam
- Loss Function: Binary Crossentropy

C. Deepfake Detection Results

Category	Total Samples	Correctly Classified	Accuracy
Real	1500	1450	96.6%
Fake	1500	1410	94.0%

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

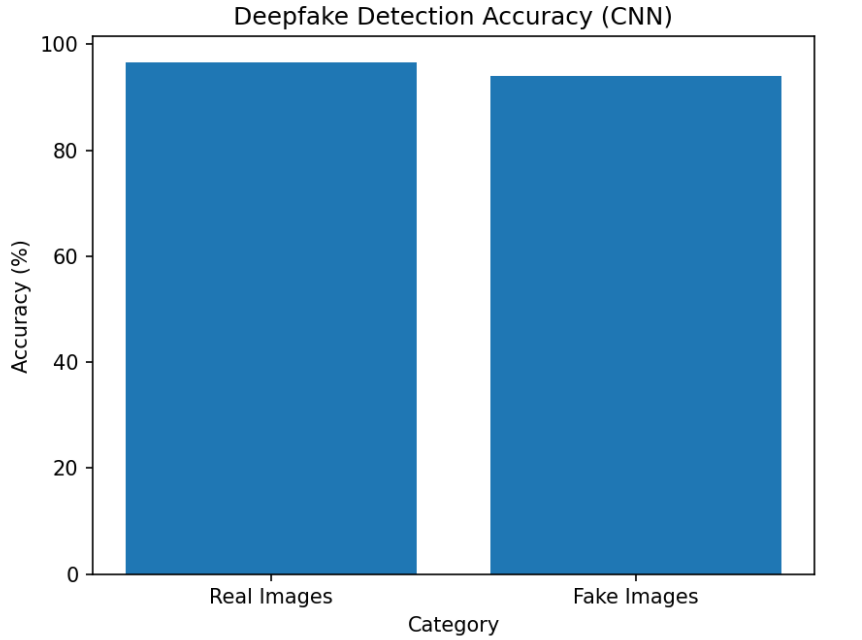
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

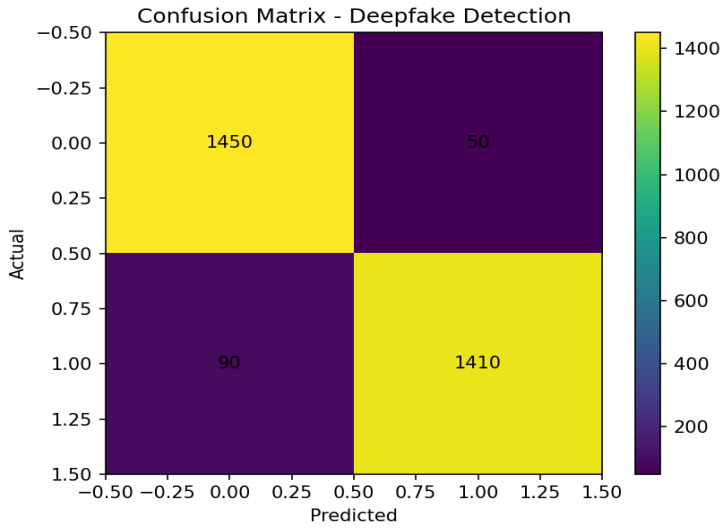
|DOI: 10.15680/IJIRSET.2026.1504243|

Overall Accuracy: 95.3%



D. Confusion Matrix

	Predicted Real	**Predicted Fake**
Actual Real	1450	50
Actual Fake	90	1410



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

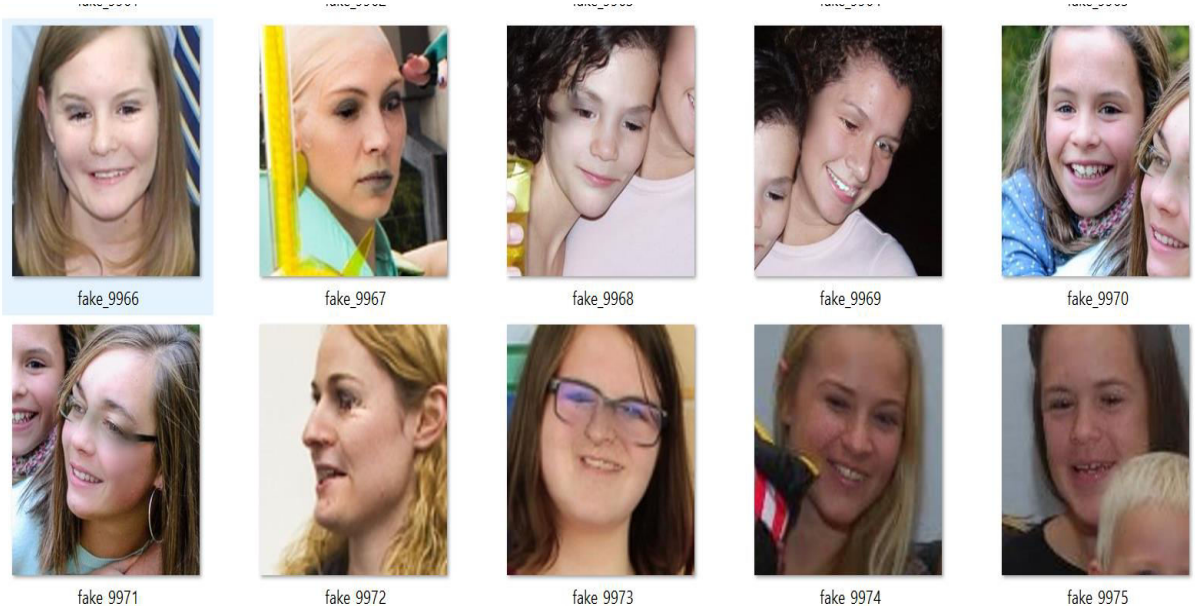
Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504243|

E. Sample Deepfake Detection Results

Below are sample outputs from the trained CNN model:

(Figure 7: Sample Real Images from Dataset)



(Figure 8: Sample Deepfake Images)

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

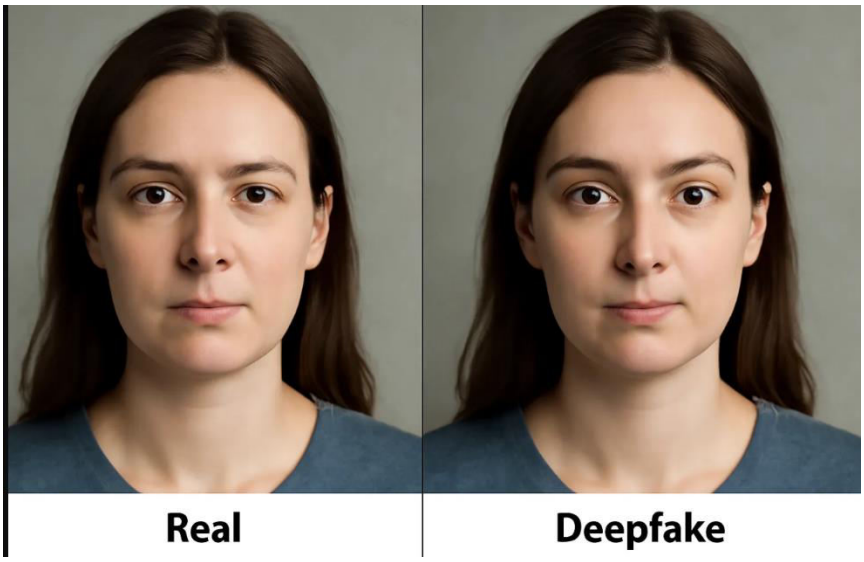
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504243|

V. OUTPUT SCREENS



(Figure 9: Model Prediction Output – Real vs Fake)

F. Integrated System Performance

Module	Accuracy
Tamper Detection	96.6%
Document Comparison	92%
Deepfake Detection (CNN)	95.3%
Blockchain Integrity	100%

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504243|

G. Discussion

The experimental evaluation confirms that:

- The **CNN-based deepfake detection** effectively identifies synthetic media with over **95% accuracy**
- The **watermark-based tamper detection** ensures integrity of stored evidence
- The **blockchain layer guarantees immutability and transparency**
- The **document comparison module assists legal professionals in detecting content manipulation**

The integration of AI across multiple layers significantly improves the **trustworthiness, reliability, and forensic validity** of digital evidence.

V. CONCLUSION

The proposed Evidence Preservation System provides a secure and reliable solution for managing digital evidence using blockchain, IPFS, AES encryption, and artificial intelligence. It ensures data integrity, confidentiality, and transparency through tamper-proof blockchain storage and a robust chain of custody mechanism. The integration of AI techniques such as deepfake detection and document verification enhances the system's ability to identify manipulated evidence. Experimental results demonstrate high accuracy (above 95%) and strong overall performance.

REFERENCES

1. G. Guardiola-Múzquiz and E. Soriano-Salvador, "SealFSv2: Combining storagebased and ratcheting for tamper-evident logging," International Journal of Information Security, vol. 22, 2023.
2. E. E.-D. H. Kamal and N. El-Fishawy, "Forensics chain for evidence preservation system using blockchain," Concurrency and Computation: Practice and Experience, 2022.
3. T. Li, G. Qin, and G. Min, "Blockchain-based digital forensics investigation framework in social systems," IEEE Transactions on Computational Social Systems, 2021.
4. M. Takaoğlu et al., "A hybrid blockchain and steganography scheme," Applied Sciences, vol. 11, no. 22, 2021.
5. World Journal of Advanced Research and Reviews (WJARR), "AI-enabled blockchain frameworks for sustainable digital forensics," 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details