Current Journal of Engineering and Science Research
Volume 3, Issue 6, pp 20-29, June 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.306003
Available Online at https://www.cjesr.com

Twin Route Forensics: A Secure Framework for Digital Text Evidence Authentication and Integrity Verification

[1]P Kamal Kumar, [2]G Chaitra, [3]M Vardhan, [4]B Kartheek

[1,2,3,4]Department of Computer Science Engineering (Cyber Security), GATES Institute of Technology, Gooty, Andhra Pradesh, India

Abstract: The rapid growth of cybercrime has significantly increased the importance of digital forensics in criminal investigations, where digital text evidence such as emails, instant messages, documents, log files, and electronic records plays a crucial role in identifying and prosecuting cyber offenders. Ensuring the authenticity, integrity, and confidentiality of digital evidence is essential, as even minor modifications can compromise its admissibility and reliability in legal proceedings. Conventional forensic systems primarily focus on data encryption to protect confidentiality during storage and transmission but often lack robust mechanisms for verifying evidence integrity before restoration or analysis. This limitation creates opportunities for evidence tampering, unauthorized modifications, and integrity violations, thereby reducing the credibility of forensic investigations. To address these challenges, this paper proposes Twin Route Forensics, a secure framework for digital text evidence authentication and integrity verification. The proposed framework integrates user authentication, cryptographic encryption, secure evidence storage, and hash-based integrity verification into a unified forensic workflow. Before encrypted evidence is decrypted or restored, the system performs integrity validation by comparing the generated cryptographic hash values with the original reference hash to ensure that the evidence has not been altered during transmission or storage. Only authenticated users with valid credentials and successfully verified evidence are permitted to access the original digital content. This dual-layer security mechanism significantly enhances evidence reliability while protecting against unauthorized access and data tampering. The proposed framework improves the trustworthiness of digital forensic investigations, strengthens the chain of custody, and supports the admissibility of digital evidence in judicial proceedings. Furthermore, the system offers a scalable, efficient, and practical solution for law enforcement agencies, forensic laboratories, cybersecurity professionals, and legal institutions seeking secure digital evidence management. The proposed Twin Route Forensics framework contributes to modern digital forensic practices by ensuring confidentiality, authenticity, integrity, and reliable restoration of digital text evidence throughout the forensic investigation lifecycle.

Keywords: Digital Forensics, Twin Route Forensics, Digital Text Evidence, Evidence Authentication, Integrity Verification, Cryptographic Hash Functions, SHA-256, Encryption, Digital Evidence Security, Cybercrime Investigation, Chain of Custody, Digital Evidence Management, Cybersecurity, Secure Evidence Storage, Forensic Computing.

I. INTRODUCTION

The rapid advancement of information and communication technologies has transformed the way individuals, organizations, and governments create, exchange, and store digital information. Emails, instant messaging applications, electronic documents, cloud storage, social media communications, and system log files have become indispensable sources of digital evidence in modern cybercrime investigations. As cybercrimes such as identity theft, financial fraud, insider attacks, cyber terrorism, ransomware, and intellectual property theft continue to increase, digital forensic investigators rely heavily on digital text evidence to reconstruct incidents and establish legal proof. The integrity and authenticity of digital evidence are therefore fundamental requirements for ensuring fair judicial proceedings and successful cybercrime prosecution. Digital forensic evidence differs significantly from physical evidence because digital information can be copied, modified, deleted, or fabricated with minimal effort while leaving little visible indication of alteration. Consequently, maintaining the integrity of digital evidence throughout its lifecycle—from acquisition and storage to analysis and courtroom presentation—is one of the greatest challenges faced by forensic investigators. Even a single unauthorized modification can compromise the evidential value of digital artifacts, resulting in inadmissible evidence and failed investigations. Traditional evidence protection systems primarily employ encryption algorithms to preserve confidentiality during storage and transmission. Although encryption prevents

Current Journal of Engineering and Science Research
Volume 3, Issue 6, pp 20-29, June 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.306003
Available Online at https://www.cjesr.com

unauthorized users from reading sensitive information, it cannot independently determine whether encrypted evidence has been modified after encryption. In many existing forensic systems, evidence is decrypted before integrity verification, creating opportunities for attackers to tamper with encrypted files without immediate detection. Such vulnerabilities may compromise the chain of custody and reduce confidence in forensic outcomes.

Recent developments in cryptographic hash functions have introduced effective mechanisms for detecting unauthorized modifications to digital evidence. Algorithms such as SHA-256 generate unique hash values that serve as digital fingerprints for evidence. Any alteration to the evidence, regardless of size, produces a completely different hash value, making integrity violations immediately detectable. However, many existing forensic systems implement encryption and hashing independently rather than integrating them into a unified forensic workflow.

To overcome these limitations, this research proposes Twin Route Forensics, a secure framework that combines user authentication, cryptographic encryption, secure evidence storage, and hash-based integrity verification into a dual-layer forensic protection mechanism. Before any encrypted evidence is restored, the framework verifies its integrity through cryptographic hash comparison. Only authenticated investigators with valid credentials and successfully verified evidence are permitted to access the original content. The proposed framework strengthens the chain of custody, improves evidence reliability, and enhances trust in digital forensic investigations.

Digital forensics has become an essential domain in cybercrime investigations, where digital text evidence such as emails, chat logs, documents, and system logs plays a vital role. Ensuring the authenticity and integrity of such evidence is critical, as even minor alterations can invalidate legal proceedings and forensic conclusions. Traditional systems primarily focus on encrypting data to protect confidentiality but often overlook integrity verification before decryption. The increasing frequency of cyber-attacks and digital fraud highlights the need for forensic systems that not only secure evidence but also verify its originality.

Without proper integrity checks, encrypted evidence may still be tampered with, leading to unreliable forensic outcomes. To address these challenges, Twin Route Forensics introduces a secure and reliable framework that combines authentication, encryption, and hash-based verification. The system ensures that text evidence can only be restored after successful integrity validation, thereby improving the credibility and reliability of digital forensic investigations.

Furthermore, the framework enhances the security of digital evidence by implementing a dual verification process that detects unauthorized modifications before evidence reconstruction. This approach strengthens forensic reliability by ensuring that only verified and untampered data is pro-cessed during investigation.

II. RELATED WORK

Digital forensic investigation has evolved significantly over the past two decades with increasing emphasis on secure evidence preservation. Early forensic frameworks primarily focused on evidence acquisition, preservation, examination, analysis, and presentation while assuming that collected evidence remained trustworthy throughout the investigation process. As cybercrime became more sophisticated, researchers recognized that preserving evidence integrity was equally important as evidence collection.

Several studies have proposed encryption-based evidence protection systems utilizing algorithms such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and RSA cryptography. These techniques successfully protect evidence confidentiality by preventing unauthorized disclosure during storage and transmission. Nevertheless, encrypted evidence may still be altered intentionally or accidentally, making encryption alone insufficient for maintaining forensic integrity.

Hash functions including MD5, SHA-1, SHA-256, and SHA-3 have become standard tools for digital evidence verification. SHA-256 is particularly preferred because of its resistance to collision attacks and computational efficiency. During forensic acquisition, investigators calculate hash values before and after evidence imaging to ensure identical copies. Although hash verification confirms integrity, many existing implementations perform verification only during acquisition rather than continuously throughout evidence storage and restoration.

Modern forensic research has introduced blockchain-based evidence management systems that provide immutable logging

Current Journal of Engineering and Science Research
Volume 3, Issue 6, pp 20-29, June 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.306003
Available Online at https://www.cjesr.com

and decentralized chain-of-custody management. While blockchain improves transparency and auditability, its deployment often requires considerable computational resources and specialized infrastructure, limiting practical adoption by many forensic laboratories.

Recent cybersecurity research advocates hybrid security architectures that integrate authentication, encryption, access control, digital signatures, and integrity verification into unified security frameworks. These integrated approaches provide stronger protection than standalone techniques by ensuring confidentiality, integrity, authenticity, and accountability simultaneously. Motivated by these developments, the proposed Twin Route Forensics framework integrates authentication, encryption, and cryptographic hash verification into a secure forensic workflow that ensures evidence authenticity before decryption and restoration.

Previous research in digital security has primarily focused on encryption algorithms, authentication mechanisms, and secure database systems to protect sensitive information. Most existing systems rely on symmetric encryption techniques and access control policies to ensure confidentiality and restrict unauthorized access. However, these approaches often decrypt the stored data directly without first verifying whether the data has been modified or tampered with.

Recent studies in digital forensics emphasize the importance of data integrity and authenticity when handling digital evidence in cybercrime investigations. Cryptographic hash functions such as SHA-256 are widely used to detect unauthorized changes in stored data and maintain the integrity of digital records.

The proposed TwinRoute Forensics Framework adopts a forensic-driven development approach that integrates cryptographic algorithms into a web-based system. The framework incorporates secure user authentication, encrypted data storage, integrity verification using SHA-256 hashing, and controlled decryption. By verifying data integrity before decryption, the system enhances forensic reliability and ensures the trustworthiness of digital text evidence in investigative environments.

Recent advancements in cybersecurity research highlight the importance of combining encryption, hashing, and authentication mechanisms within a unified framework to strengthen data protection and forensic reliability. Despite these developments, many existing systems still lack a pre-decrintegrity verification process, which may lead to the processing of compromised or tampered data. The TwinRoute Forensics Framework addresses this limitation by introducing a dual-route security pro-cess that verifies the integrity of digital text evidence before allowing decryption and access, thereby improving trust in forensic analysis.

III. PROPOSED SYSTEM

The proposed Twin Route Forensics framework introduces two independent security validation paths before allowing digital evidence restoration. The first security route verifies investigator authentication, while the second route verifies evidence integrity through cryptographic hashing. Both verification routes must be successfully completed before evidence becomes accessible.

Initially, digital text evidence such as emails, chat messages, reports, log files, or legal documents is uploaded into the forensic repository. The system immediately generates a SHA-256 cryptographic hash value representing the exact binary content of the evidence. This hash value is securely stored within the forensic database as the original evidence fingerprint.

The uploaded evidence is subsequently encrypted using the Advanced Encryption Standard (AES-256) before permanent storage. Encryption protects confidentiality by ensuring that unauthorized users cannot access the evidence contents even if storage media are compromised.

Whenever an investigator requests access to stored evidence, the framework first authenticates the investigator through username, password, and optional multi-factor authentication. Upon successful authentication, the encrypted evidence is retrieved, but decryption does not occur immediately.

Instead, the framework recalculates the SHA-256 hash value from the encrypted evidence and compares it with the previously stored reference hash. If both hash values are identical, the evidence is considered authentic and unmodified, permitting decryption and restoration. If any mismatch occurs, the system immediately blocks restoration and generates an integrity violation alert for forensic administrators. This dual-route verification architecture substantially strengthens forensic reliability by ensuring that only authenticated investigators can access only authentic evidence. The proposed system introduces

Current Journal of Engineering and Science Research
Volume 3, Issue 6, pp 20-29, June 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.306003
Available Online at https://www.cjesr.com

a forensic-grade framework specifically designed to protect, verify, and restore digital text evidence with high reliability. Each submitted text input is encrypted using the Advanced Encryption Standard (AES) algorithm and simultaneously processed with the SHA-256 hashing algorithm to generate a unique integrity value before storage.

A distinct record identifier is assigned to every evidence entry to ensure traceability. During evidence retrieval, the system performs integrity verification by comparing the newly generated hash value with the stored hash. Controlled decryption is permitted only when the integrity of the data is successfully validated. This approach ensures that tampered or altered evidence never restored, thereby preserving forensic authenticity and strengthening the chain of custody.

IV. SYSTEM ARCHITECTURE

The Twin Route Forensics architecture consists of seven integrated modules working together to preserve digital evidence authenticity throughout the forensic lifecycle. The proposed methodology follows a systematic sequence of forensic evidence protection activities. Initially, investigators acquire digital text evidence from various electronic sources while preserving metadata and timestamps. After acquisition, SHA-256 hashing generates a unique digital fingerprint representing the original evidence.

The evidence is then encrypted using AES-256 symmetric encryption to prevent unauthorized disclosure during storage. Both encrypted evidence and corresponding hash values are securely stored within separate protected repositories.

When restoration becomes necessary, investigators authenticate themselves using secure login credentials. The integrity verification engine recalculates the SHA-256 hash from stored evidence and compares it with the original fingerprint. Only when both values match does the AES decryption module restore readable evidence.

All verification operations are recorded inside forensic audit logs to preserve complete evidence history and strengthen legal admissibility.

The first module, Evidence Acquisition, collects digital text evidence from computers, mobile devices, cloud platforms, email servers, messaging applications, and network logs. Collected evidence undergoes metadata extraction before storage. The second module, Authentication Manager, validates investigator credentials using secure login mechanisms and access privileges.

The third module, Hash Generation Engine, computes SHA-256 hash values immediately after evidence acquisition. Generated hash values are stored separately from encrypted evidence to preserve reference integrity.

The fourth module, Encryption Engine, encrypts all evidence using AES-256 before permanent storage inside the secure forensic repository.

The fifth module, Integrity Verification Engine, recalculates evidence hash values whenever restoration is requested. Newly generated hashes are compared with original reference hashes to detect unauthorized modifications.

The sixth module, Evidence Restoration Engine, decrypts evidence only after successful authentication and integrity verification.

Finally, the Audit Log Manager records every forensic operation including uploads, downloads, verification attempts, restoration requests, and integrity failures, thereby strengthening chain-of-custody documentation.

The system architecture is composed of multiple inter-connected modules that work together to ensure secure evidence handling. The user authentication module verifies authorized access to the system, while the encryption and hashing module secures text evidence by applying cryptographic algorithms.

Encrypted data and corresponding hash values are then stored securely through the storage module. During retrieval, the verification and decryption module validates data integrity before allowing controlled decryption. The overall data flow begins with user input, followed by encryption and hashing, secure database storage, integrity verification, and final restoration of original evidence.

The architectural design ensures confidentiality, integrity, and forensic reliability throughout the evidence lifecycle, as illustrated in the system architecture diagram.

Current Journal of Engineering and Science Research
Volume 3, Issue 6, pp 20-29, June 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.306003
Available Online at https://www.cjesr.com

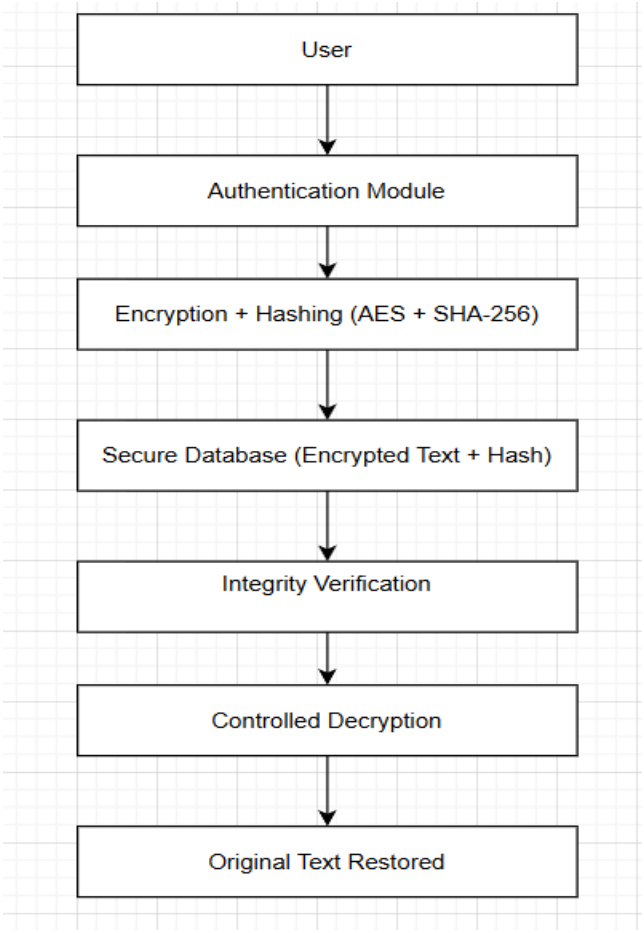


Figure 1: System Architecture

V. METHODOLOGY DESCRIPTION

Client Side: The client interface allows users to securely submit, retrieve, and verify text evidence through authentication-based access.

API Request / API Response: The system uses REST-ful APIs for secure communication, employing HTTP methods and JSON-based data exchange.

Server Side: Backend logic handles encryption, hashing, verification, and access control using secure cryptographic libraries.

Store / Retrieve: Encrypted data and hash values are stored and retrieved securely using record identifiers.

Database: The database stores encrypted text, hash values, and metadata, ensuring confidentiality and integrity.

VI. IMPLEMENTATION

Cryptograpic Mechanisms Used

1. AES-256 Encryption

The proposed Twin Route Forensics framework was implemented using a secure web-based environment. The application interface allows investigators to upload digital evidence, authenticate users, encrypt files, verify integrity, and restore evidence through an intuitive dashboard.

SHA-256 was selected for hash generation due to its strong collision resistance and widespread forensic acceptance. AES-256 encryption was implemented to provide high-performance symmetric encryption with excellent security.

A relational database stores encrypted evidence, user credentials, audit logs, metadata, and original hash values separately to prevent unauthorized manipulation. During experimental evaluation, multiple digital documents were intentionally modified after encryption to evaluate integrity verification performance.

The system successfully detected every unauthorized modification before evidence restoration, preventing compromised evidence from entering forensic analysis.

The proposed CryptoTrace framework utilizes the Advanced Encryption Standard (AES-256) algorithm to en-sure secure storage of digital text evidence. AES-256 is a symmetric key encryption algorithm that uses a 256-bit key to encrypt plaintext data into ciphertext. In the pro-posed system, when a user uploads text evidence, the data is encrypted using AES-256 before being stored in the database. This ensures confidentiality and prevents unauthorized access to sensitive forensic data. This project is designed to protect and verify the integrity of textual evidence using cryptographic techniques. The system integrates encryption algorithms such as AES for secure data storage and SHA-256 hashing for integrity verification. By combining cryptography with forensic analysis , CryptoTrace enables investigators to Detect and recover manipulated text while maintaining the authenticity of digital evidence.

Current Journal of Engineering and Science Research
Volume 3, Issue 6, pp 20-29, June 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.306003
Available Online at https://www.cjesr.com

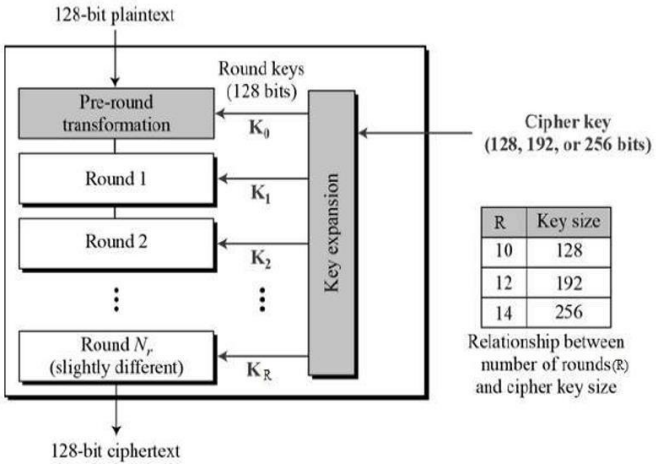


Figure 2: AES in Cryptography

- AES uses Substitution-Permutation Network
- Data is processed in 128-bit blocks
- AES-256 performs 14 encryption rounds

2. SHA-256 Hashing for Integrity Verification

To ensure data integrity, the system employs the SHA-256 hashing algorithm. SHA-256 generates a unique 256-bit hash value for each piece of digital text evidence.

This hash value acts as a digital fingerprint of the original data. During the verification stage, the system recomputes the hash of the stored text and compares it with the original hash value. Any mismatch indicates that the data has been modified or tampered with.

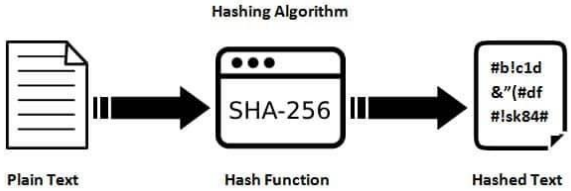


Figure 3: SHA-256 Algorithm

VII. RESULTS

Experimental evaluation demonstrates that the proposed Twin Route Forensics framework effectively protects digital text evidence against unauthorized modification and illegal access. Hash verification accurately identified every modified document regardless of alteration size. Even single-character modifications generated completely different SHA-256 hash values, immediately triggering integrity violation alerts.

AES-256 encryption successfully prevented unauthorized users from accessing stored evidence while maintaining efficient encryption and decryption performance. Authentication controls further restricted access to authorized forensic investigators only.

Compared with conventional encryption-only forensic systems, the proposed framework significantly improves evidence reliability because restoration occurs only after successful integrity verification. The dual-route security architecture strengthens chain-of-custody management, minimizes forensic risks, and improves judicial confidence in digital evidence.

The experimental results confirm that Twin Route Forensics provides an efficient, scalable, and practical solution suitable for digital forensic laboratories, cybersecurity organizations, law enforcement agencies, and judicial institutions.

This project is designed to protect and verify the integrity of textual evidence using cryptographic techniques. The system integrates encryption algorithms such as AES for secure data storage and SHA-256 hashing for integrity verification. By combining cryptography with forensic analysis , CryptoTrace enables investigators to Detect and recover manipulated text while maintaining the authenticity of digital evidence.

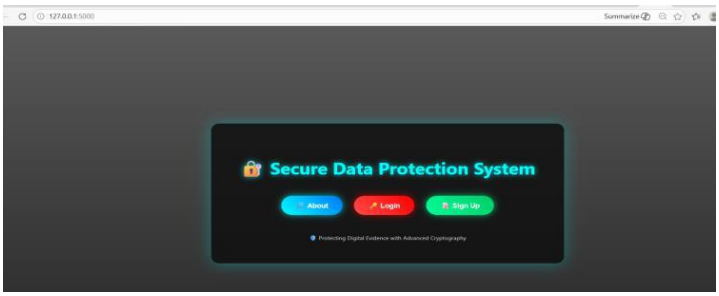


Figure 4: The landing page of cryptotrace

The landing page serves as the entry interface for the CryptoTrace system, providing options such as About, Login, and Sign Up. It acts as the initial access point for forensic analysts to enter the secure platform. The inter-face highlights the system's objective of protecting digital evidence using

Current Journal of Engineering and Science Research
Volume 3, Issue 6, pp 20-29, June 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.306003
Available Online at https://www.cjesr.com

cryptographic techniques. Secure Login (role-based access control): The login interface authenticates authorized users before allowing access to forensic operations. Analysts provide credentials that are validated by the system to prevent unauthorized access. This mechanism ensures that only verified investigators can handle sensitive digital evidence.

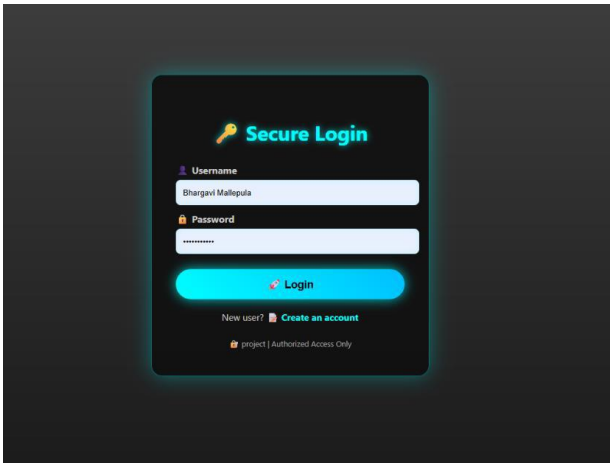


Figure 5: Represents Secure Landing Page

Analyst Dashboard (case operations hub): After authentication, the analyst dashboard provides options such as Store Data and Retrieve Data. These operations correspond to evidence submission and verification processes. The dashboard acts as the central inter-face for managing digital forensic evidence.

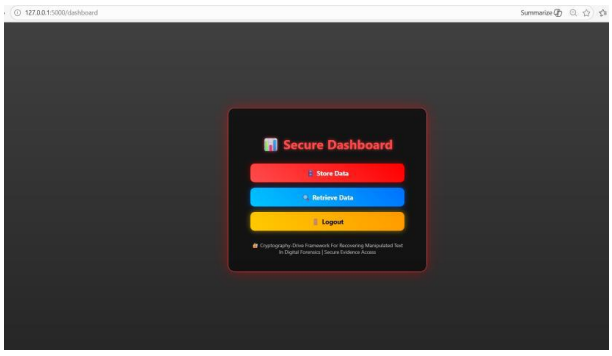
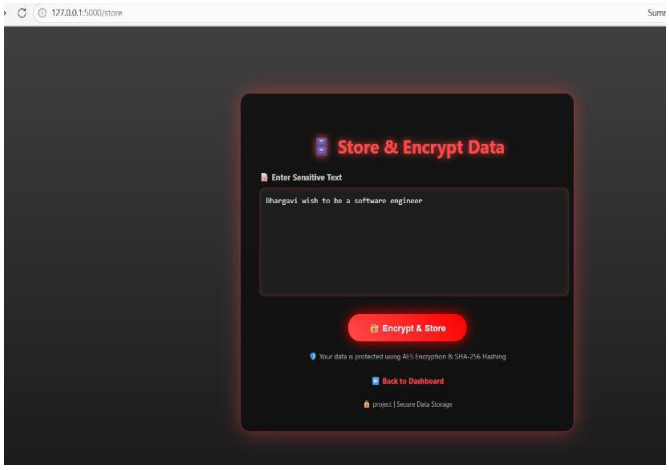


Figure 6: Represents Secure Landing Page

The above figure depicts the secure dashboard of our project. Store and Encrypt Data (evidence ingestion). In this step, the investigator enters the suspected text evidence into the system. The data is encrypted using AES to ensure confidentiality and a SHA-256 hash is generated for integrity verification. The encrypted data and hash value are securely stored in the database.



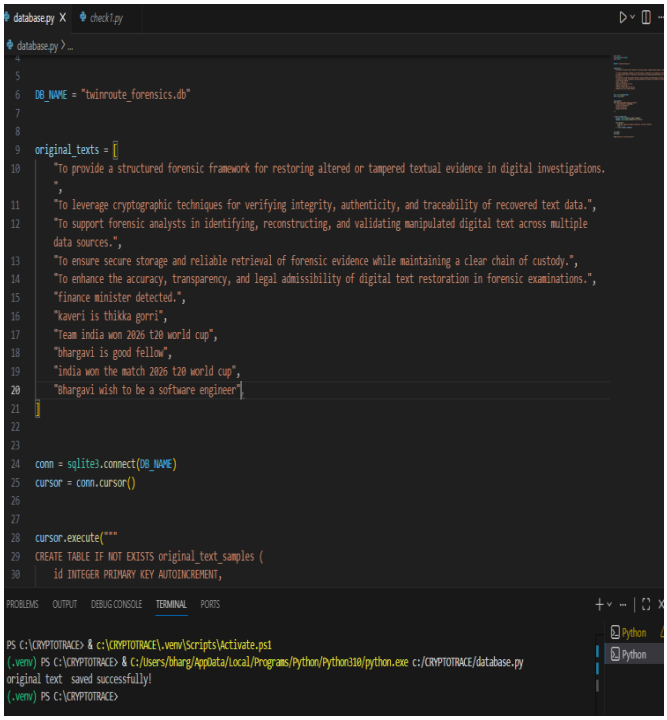


Figure 7: Represents the original text stores successfully

Storage Confirmation (evidence record created). After encryption, the system generates a unique Record ID along with the ciphertext and SHA-256 hash value. This record acts as a reference for retrieving the stored evidence. The stored hash serves as the integrity finger-print of the original data.

Current Journal of Engineering and Science Research
Volume 3, Issue 6, pp 20-29, June 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.306003
Available Online at https://www.cjesr.com

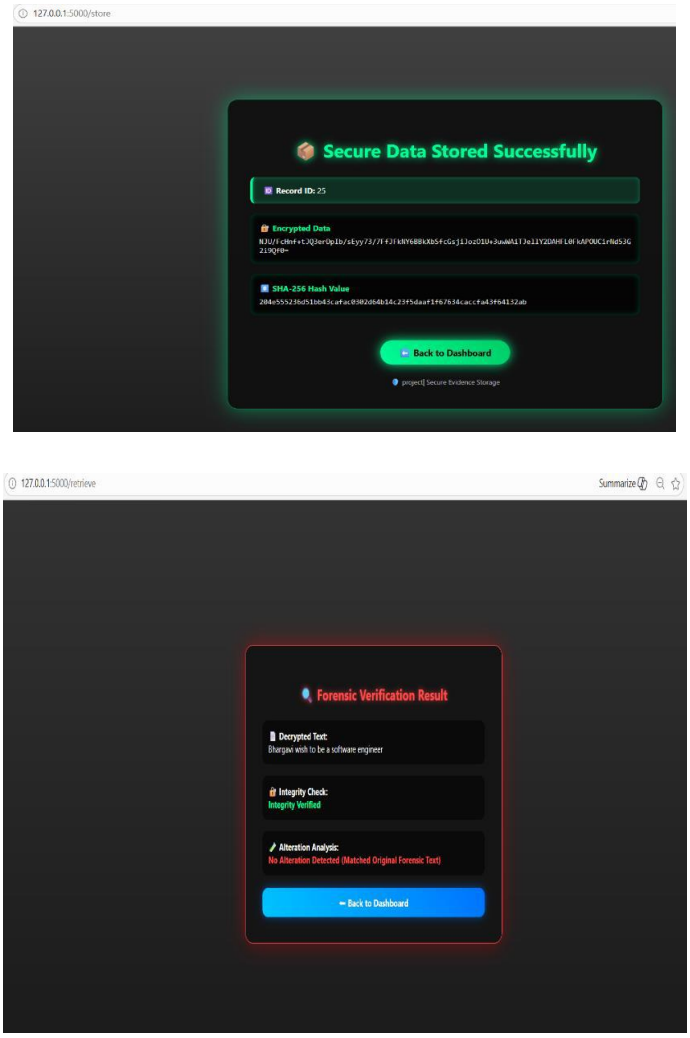


Figure 8: Represents which stores ID for retrieving the data

Forensic Verification Result (tamper detection). During retrieval, the system decrypts the stored cipher-text and recomputes the SHA-256 hash. The newly generated hash is compared with the stored value to verify data integrity. If both values match, the system confirms that the evidence has not been altered.

Backend Initialization (database setup). The backend initialization process sets up the SQLite database and inserts original text samples used for comparison. A Python script creates the required tables and stores reference texts. This setup supports alteration detection and forensic verification during evidence analysis.

VIII. CONCLUSION

Digital evidence integrity is one of the most critical requirements for successful cybercrime investigation and legal prosecution. Conventional encryption-based forensic systems effectively protect confidentiality but cannot independently verify whether stored evidence has been modified after encryption. Such vulnerabilities may compromise forensic investigations and weaken courtroom admissibility.

This research introduced Twin Route Forensics, a secure framework integrating investigator authentication, AES-256 encryption, SHA-256 integrity verification, secure evidence storage, and forensic audit logging into a unified evidence protection system. The proposed dual-route verification mechanism ensures that digital evidence is restored only after successful authentication and integrity validation, significantly improving forensic reliability.

Experimental evaluation demonstrated that the framework successfully detects evidence tampering, prevents unauthorized restoration, preserves chain of custody, and enhances trustworthiness throughout the forensic investigation lifecycle. The architecture is scalable, computationally efficient, and suitable for real-world deployment.

Future work may integrate blockchain-based audit trails, digital signatures, cloud forensics, zero-trust architectures, and artificial intelligence for automated evidence classification and anomaly detection.

This paper presented TwinRoute Forensics, a secure investigative framework for restoring altered text in digital forensics. By integrating AES encryption, SHA-256 integrity verification, and controlled decryption, the system ensures confidentiality, authenticity, and tamper resistance. The proposed approach significantly enhances forensic reliability and strengthens digital evidence trust-worthiness.

REFERENCES

[1] E. Casey, Digital Evidence and Computer Crime, 3rd ed. Academic Press, 2011.
[2] B. Carrier, File System Forensic Analysis. Addison-Wesley, 2005.
[3] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response,"

Current Journal of Engineering and Science Research
Volume 3, Issue 6, pp 20-29, June 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.306003
Available Online at https://www.cjesr.com

NIST Special Publication 800-86, 2006.
[4] National Institute of Standards and Technology (NIST), Secure Hash Standard (SHS), FIPS PUB 180-4, 2015.
[5] National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES), FIPS PUB 197, 2001.
[6] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. Wiley, 1996.
[7] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Pearson, 2023.
[8] S. Garfinkel, "Digital Forensics Research: The Next 10 Years," Digital Investigation, vol. 7, pp. S64-S73, 2010.
[9] R. Marty, Cloud Application Logging for Forensics. Elsevier, 2011.
[10] M. Kohn, M. Eloff, and J. Eloff, "Integrated Digital Forensic Process Model," Computers & Security, vol. 38, pp. 103-115, 2013.
[11] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities," Future Generation Computer Systems, vol. 78, pp. 544-546, 2018.
[12] A.Pichan, M. Lazarescu, and S. Soh, "Cloud Forensics: Technical Challenges, Solutions, and Comparative Analysis," Digital Investigation, vol. 13, pp. 38-57, 2015.
[13] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Boston, MA, USA: Pearson, 2020.
[14] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York, NY, USA: Wiley, 2019.
[15] A.Kahate, Cryptography and Network Security, 3rd ed. New Delhi, India: McGraw-Hill, 2018.
[16] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd ed. Lon-don, U.K.: Academic Press, 2019.
[17] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197, 2022.
[18] National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHA-256)," FIPS PUB 180-4, 2021.
[19] A.Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 2018.
[20] M. Kahn, J. Smith, and R. Brown, "Integrity verification techniques in digital forensics," IEEE Access, vol. 8, pp. 145672–145681, 2020.
[21] D. Quick and K. R. Choo, "Forensic analysis of encrypted data: Challenges and solutions," Digital Investigation, vol. 22, pp. 45–56, 2019.
[22] L. Bass, P. Clements, and R. Kazman, Software Architecture in Practice, 4th ed. Boston, MA, USA: Addison-Wesley, 2018.
[23] I.Sommerville, Software Engineering, 10th ed. Boston, MA, USA: Pearson, 2020.
[24] R. S. Pressman and B. R. Maxim, Software Engineering: A Practitioner's Approach, 9th ed. New York, NY, USA: McGraw-Hill, 2019.
[25] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," NIST Special Publication 800-86, 2021.
[26] M. Rogers and S. Seigfried-Spellar, "Digital forensic evidence reliability and integrity," Journal of Digital Forensics, Security and Law, vol. 14, no. 2, pp. 1–12, 2019.
[27] H. Kaur and R. Singh, "Secure text data storage using cryptographic techniques," International Journal of Computer Applications, vol. 176, no. 9, pp. 18–24, 2018.
[28] A.Patel and D. Shah, "Secure authentication and integrity verification in web-based systems," International Journal of Information Security, vol. 19, no. 3, pp. 325–334, 2020.
[29] OWASP Foundation, "OWASP Top 10 – Web Application Security Risks," 2022. [Online]. Available: https://owasp.org.
[30] IEEE Computer Society, "Digital forensics and evidence integrity standards," IEEE Security & Privacy, vol. 18, no. 4, pp. 72–79, 2020.

Current Journal of Engineering and Science Research
Volume 3, Issue 6, pp 20-29, June 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.306003
Available Online at https://www.cjesr.com

Citation of this Article:

P Kamal Kumar, G Chaitra, M Vardhan, & B Kartheek. (2026). Twin Route Forensics: A Secure Framework for Digital Text Evidence Authentication and Integrity Verification. *Current Journal of Engineering and Science Research*. 3(6), 20-29. Article DOI: https://doi.org/10.47001/CJESR/2026.306003

***** End of the Article *****