Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 7 | July-2026
ISSN (O) 3107-6696

Secure Digital Evidence Verification System Using Digital Signatures

Mogga Dileep
Department of computer science(M.sc)
Co author: V. Satish
Assistant professor in Dr.Lankapalli Bullayya college

Abstract - The increasing use of digital images as evidence in legal, forensic, and organizational applications has raised significant concerns regarding image authenticity and integrity. Modern image editing tools make it easy to manipulate digital evidence, creating the need for a secure and reliable verification system. This paper presents a Secure Digital Evidence Verification System using Digital Signature, a web-based platform designed to ensure the authenticity, integrity, and traceability of digital image evidence throughout its lifecycle.

The proposed system integrates Digital Signatures, Discrete Wavelet Transform (DWT)-based invisible watermarking, and SHA-256 cryptographic hashing to provide a multi-layered security framework. During the image sealing process, a unique Submission ID is invisibly embedded into the image using DWT watermarking, while a digital signature is generated and securely stored in both the image metadata and the centralized database. A SHA-256 hash of the sealed image is also generated and stored to detect any unauthorized modifications. The system implements role-based access control, enabling General Public users to submit evidence, Public Authorities to verify authenticity, and Administrators to manage users, approvals, and audit logs.

The proposed framework effectively detects image tampering, preserves evidence authenticity, and provides a secure workflow for digital evidence submission and verification. It offers a practical solution for digital forensic investigations, law enforcement agencies, and judicial systems requiring trustworthy digital evidence management.

I. Introduction

Digital images are increasingly used as evidence in legal investigations, law enforcement, insurance claims, and organizational documentation. However, the widespread availability of advanced image editing tools has made it easier to manipulate digital evidence, raising serious concerns about its authenticity and integrity. Conventional image verification methods often fail to provide a secure mechanism for proving ownership, detecting tampering, and maintaining the trustworthiness of digital evidence throughout its lifecycle.

This research presents a Secure Digital Evidence Verification System using Digital Signature, a web-based platform that ensures secure image submission and reliable authenticity verification. The proposed system integrates Digital Signatures, Discrete Wavelet Transform (DWT)-based invisible watermarking, and SHA-256 cryptographic hashing to establish a multi-layered security framework. During the image sealing process, a unique Submission ID is invisibly embedded into the image using DWT watermarking, while a digital signature is securely stored in both the image metadata and the centralized database. The SHA-256 hash of the sealed image is also maintained to detect unauthorized modifications. Furthermore, role-based access control enables General Public users, Public Authorities, and Administrators to securely manage evidence submission, verification, and monitoring, providing a practical and reliable solution for digital evidence management in forensic and judicial applications.

II. Problem Statement

The rapid growth of digital image usage in legal, forensic, and organizational applications has increased the need for secure evidence management. However, digital images can be easily manipulated using advanced editing software, making it difficult to verify their authenticity and integrity. Existing image verification methods often lack comprehensive mechanisms for secure submission, ownership validation, tamper detection, and traceability throughout the evidence lifecycle.

Major challenges include:

- Difficulty in verifying the authenticity of digital image evidence.
- Risk of unauthorized image tampering and forgery.
- Absence of a secure mechanism to associate evidence with its rightful owner.
- Limited traceability and monitoring of evidence submissions.

- Lack of an integrated framework for secure submission, verification, and administrative management.

Therefore, a Secure Digital Evidence Verification System using Digital Signature is required to ensure reliable image authentication, detect unauthorized modifications, and provide a secure, role-based platform for digital evidence submission, verification, and management.

III. Objectives

The primary objectives of the proposed Secure Digital Evidence Verification System using Digital Signature are:

- To develop a secure web-based platform for digital image evidence submission and verification.
- To implement Digital Signature technology for authenticating digital image evidence.
- To embed a unique Submission ID into images using Discrete Wavelet Transform (DWT)-based invisible watermarking.
- To generate and verify SHA-256 cryptographic hashes for reliable tamper detection and image integrity verification.
- To establish a role-based access control mechanism for General Public users, Public Authorities, and Administrators.
- To provide secure evidence tracking, centralized monitoring, and efficient verification for forensic, legal, and judicial applications.

This matches the structure and concise style of your friend's paper while being entirely specific to your project and suitable for an IEEE/Springer/Scopus research paper.

IV. Literature Survey

A. Traditional Digital Image Verification Systems

Traditional digital image verification methods primarily rely on manual inspection, visible watermarks, or metadata analysis to determine image authenticity. However, these approaches are vulnerable to image editing, metadata manipulation, and unauthorized modifications, making them insufficient for ensuring the integrity and traceability of digital evidence in forensic and legal applications.

B.Digital Signature-BasedAuthentication Systems

Digital Signature techniques have been widely adopted to verify the authenticity and ownership of digital content. These systems provide cryptographic proof of origin and help prevent unauthorized alterations. However, conventional implementations often focus solely on signature verification without integrating image watermarking or comprehensive evidence management workflows.

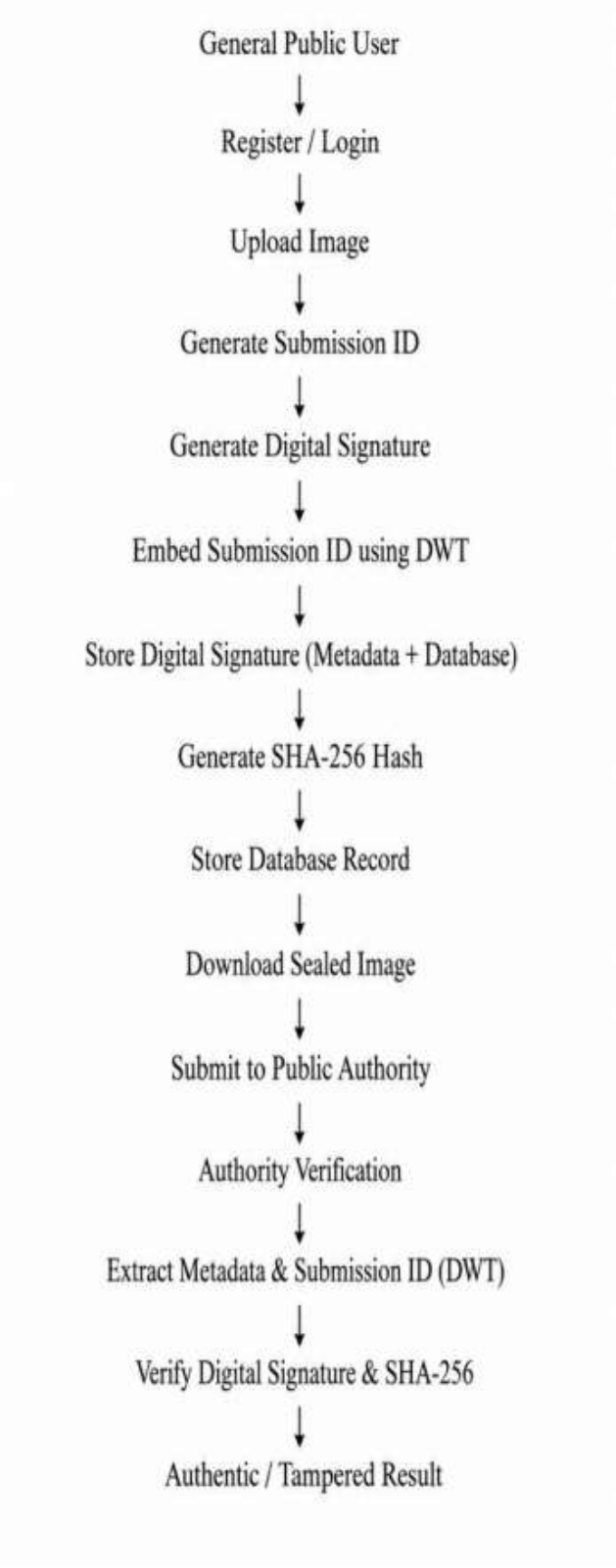
C. Digital Watermarking Techniques

Digital watermarking methods, particularly Discrete Wavelet Transform (DWT)-based invisible watermarking, have been extensively used to embed hidden information within digital images without significantly affecting visual quality. Invisible watermarking enhances traceability and enables secure identification of digital evidence while maintaining the original appearance of the image.

D. Cryptographic Integrity Verification

Cryptographic hash algorithms such as SHA-256 are widely employed to verify data integrity by generating a unique hash value for digital content. Any modification to an image results in a different hash value, enabling reliable tamper detection. Integrating cryptographic hashing with Digital Signatures and DWT watermarking provides a comprehensive security framework for secure digital evidence verification.

V. Proposed System Architecture



VI. Methodology

1. Image Sealing Process

The uploaded digital image undergoes a secure sealing process before submission. The process includes:

- Image upload and validation.
- Generation of a unique Submission ID.
- Digital Signature generation.
- DWT-based invisible watermark embedding.
- SHA-256 hash generation.

2. Digital Signature and Watermark Embedding

A Digital Signature is generated for every sealed image to establish authenticity and ownership. The signature is securely stored in both the image metadata and the centralized database. Simultaneously, the unique Submission ID is invisibly embedded into the image using the Discrete Wavelet Transform (DWT) technique, ensuring traceability without affecting the visual quality of the image.

3. Secure Database Storage

The system securely stores all verification-related information in the database.

Stored information includes:

- Submission ID
- Digital Signature
- SHA-256 Hash
- User and Authority Details
- Submission Records

This enables secure evidence management and efficient retrieval during verification.

4. Image Verification Process

When a Public Authority uploads a sealed image for verification:

1. The embedded Submission ID is extracted using DWT.
2. The Digital Signature is retrieved from the image metadata and validated against the database.
3. The SHA-256 hash of the uploaded image is generated and compared with the stored hash.
4. The system determines whether the image is Authentic or Tampered and displays the verification result.

VII. System Implementation

Technologies Used

Component	Technology
Programming Language	Python
Backend Framework	FastAPI
Frontend	HTML, CSS, JavaScript, Tailwind CSS
Image Processing	OpenCV, Pillow
Watermarking	PyWavelets (DWT)
Cryptographic Hashing	SHA-256 (hashlib)
Digital Signature	RSA Digital Signature (cryptography library)
Database	SQLite
ORM	SQLAlchemy
Authentication	Session-based Authentication

VIII. Results and Discussion

The developed Secure Digital Evidence Verification System successfully performs:

- Secure digital image sealing and submission.
- Digital Signature generation and authentication.
- Invisible DWT-based watermark embedding.
- SHA-256 hash generation for integrity verification.
- Detection of unauthorized image tampering.
- Role-based evidence submission and verification.

The system provides a secure and reliable approach for digital evidence management by combining Digital Signatures, DWT-based invisible watermarking, and SHA-256 cryptographic hashing. The integrated security framework ensures image authenticity, integrity, and traceability while enabling efficient verification by authorized entities, making it suitable for forensic, legal, and judicial applications.

IX. Advantages

- Ensures secure digital image authentication.
- Detects unauthorized image tampering effectively.
- Provides multi-layered security using Digital Signature, DWT, and SHA-256.
- Maintains evidence traceability through unique Submission IDs.
- Supports secure role-based access and verification.
- Improves the reliability of digital evidence management for forensic and judicial applications.

X. Limitations

- Performance depends on the robustness of the Digital Signature verification process.
- Image compression or severe distortion may affect DWT watermark extraction.
- Secure database management is essential for reliable verification.
- The system is currently designed to verify digital image evidence only.

XI. Future Scope

Future enhancements of the proposed system include:

- Blockchain integration for immutable evidence records.
- Support for multiple digital evidence formats such as PDF, video, and audio.
- AI-assisted image forgery detection using deep learning techniques.
- QR code–based secure evidence sharing and verification.
- Cloud-based deployment for large-scale evidence management.
- Mobile application support for real-time evidence submission and verification.

XII. Conclusion

This research presents a Secure Digital Evidence Verification System using Digital Signature for ensuring the authenticity, integrity, and traceability of digital image evidence. The proposed system integrates Digital Signatures, Discrete Wavelet Transform (DWT)-based invisible watermarking, and SHA-256 cryptographic hashing to establish a robust multi-

layered security framework. By embedding a unique Submission ID, securely storing Digital Signatures in image metadata and the database, and performing cryptographic integrity verification, the system effectively detects image tampering while preserving evidence authenticity. Furthermore, the role-based architecture enables secure evidence submission, verification, and administrative monitoring. The proposed solution provides a reliable and practical framework for digital evidence management, making it suitable for forensic investigations, law enforcement agencies, and judicial applications.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, 1978.

[2] National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHA-256)*, FIPS PUB 180-4, 2015.

[3] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, 2002.

[4] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, Pearson Education, 2018.