WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Provenance and Authentication of Digital Content

***Prof. R. T. Waghmode[1], Dnyaneshwari Bodake[2], Purvesh Chaudhari[3], Sanskruti Dol[4], Rutuja Gejage[5]***

[12345]Department of Computer Engineering Sinhgad Institute of Technology and Science, Pune

**ABSTRACT:**

This project is a multimedia authentication system built on the blockchain. For every image or audio file, it creates a distinct digital fingerprint and uses steganography to encode a secret cryptographic key inside the file. A tamper-proof record of authenticity and ownership is subsequently created by registering this key and file hash on the Ethereum blockchain. Additionally, the system facilitates ownership transfers and content updates, with all modifications being recorded in a local database. In the current fast growing life as the internet grows, we observe that digital content authors face a wide range of challenges, including content authoring. This research presents a revolutionary steganographic method for digital information provenance and authentication. We guarantee the authenticity and integrity of digital media throughout its existence by integrating cryptographic hashes and keys into it. Blockchain technology is also incorporated into the system to safely store and validate content data. By mapping the encoded keys, the dual-key system and steganography make it possible to readily verify the authenticity and origin of content, even when it has been distributed or altered.

**Keywords**: Duel-Key Verification, Tamper-proof, Metadata, Cryptographic hash, Content Security, Top-wise preparation

## INTRODUCTION :

In the current digital era, confirming the legitimacy of multimedia material is a major difficulty. It is possible to modify or avoid using conventional techniques for digital watermarking or metadata tagging. ledger that keeps track of content registration, and steganography makes it possible to place digital fingerprints that are buried inside audio and picture files. Together, they provide a strong system for identifying tampering and guaranteeing the integrity of the content. Verifying the validity of multimedia content has become more difficult due to the quick growth of digital media and the simplicity of file alteration. Conventional techniques, including visible watermarks or standard information tags, are frequently prone to alteration or deletion. Our proposal offers a novel answer to these problems by fusing steganography and blockchain, two potent technologies cryptography and blockchain. A decentralized, impenetrable ledger that securely and permanently records transactions is provided by blockchain technology. Our approach ensures that any further modifications may be recognized instantly after material is validated by recording digital fingerprints and hidden keys on the Ethereum blockchain. The art of encrypting digital files is known as steganography. In our project, we conceal cryptographic keys within the actual media files. This two-layered method, which stores a key in the image's metadata as well as its pixels or audio frames, adds an extra layer of protection against unwanted changes. This paper describes the design, implementation, and assessment of our system, demonstrating how it provides a scalable framework for future improvements while guaranteeing the ownership and integrity of digital property.

## LITERATURE SURVEY:

The Four Papers are studied [1] In the paper A Comprehensive Study of Digital Image Steganographic Techniques, the authors explore various methods for data hiding using cover mediums like images, audio, and video. Techniques discussed include LSB (Least Significant Bit) replacement, edge-based embedding, provenance authentication, and pixel pointer-based methods. Mahdi et al. proposed an improved LSB-based technique where secret keys and pseudo-random number generation are used to select pixel regions, enhancing security. However, while the method strengthens secrecy, it lacks detailed evaluation regarding the perceptual invisibility of the hidden data within the images. [2] The paper Combining Steganography with Data Obfuscation: A Study on Advanced Security Measures for Confidential Data Transmission focuses on audio signal security through multiple encryption and scrambling steps. The authors use different pseudo-random sequences and keys to scramble and multiply the original audio signal, making it resemble random noise and hiding its actual content. By cutting the signal into frames and applying multiple operations, they enhance encryption robustness. This technique ensures that without the appropriate decryption key, the original audio cannot be retrieved, thus providing a strong layer of security during data transmission. [3] In the paper Chaos-Based Encryption Technique for Compressed H264/AVC Videos, the focus is on secure encryption of H.264/AVC compressed videos while maintaining syntax compliance and efficient performance. The authors emphasize that conventional encryption methods like DES or AES are unsuitable because they add too much computational load. Instead, lightweight encryption is integrated directly into the video encoding process, allowing the resulting encrypted videos to remain standard-compliant and playable. This ensures high-level security without sacrificing compression efficiency or introducing significant computational burdens. [4] The paper A Novel Digital Audio Encryption and Forensics Watermarking

Scheme addresses the challenges of audio copyright protection and forensic authentication through digital watermarking. Two techniques are discussed: Hu and Lu's semi-fragile watermarking based on compressed sensing, which embeds watermarks into high and low-frequency regions of the audio using DWT, and Lai et al.'s fragile watermarking approach using homomorphic encryption in the encrypted wavelet domain. While these schemes effectively verify tampering and maintain audio quality, they show varying robustness, particularly withstanding different signal processing attacks.

## III. PROPOSED SYSTEM:

The proposed system aims to address the limitations of the existing systems by offering an integrated platform for medication reminders and disease predictions. By leveraging modern technologies such as ReactJS, Node.js, and machine learning models, the system provides users with accurate predictions for diseases like pneumonia, obesity, and diabetes. The inclusion of features like email reminders, personalized reports, and secure authentication enhances the user experience and promotes proactive healthcare management.

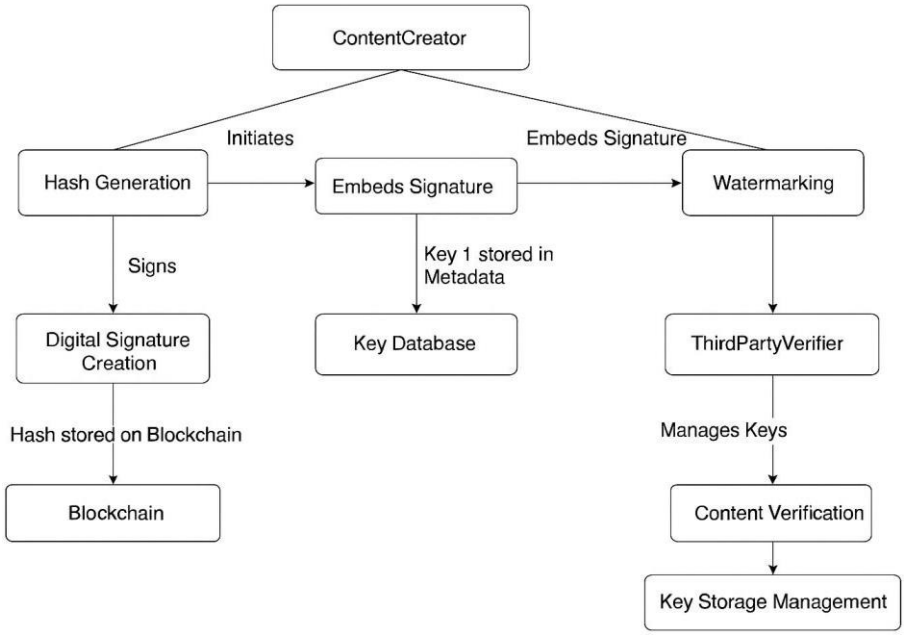



**Figure 1: System Architecture of the proposed system**

### *3.1 IMPLEMENTATION*

**1.** ***User Authentication and Profile Management***

This module manages user registration, login, and authentication to ensure secure access. Users can create accounts, log in using email and password, and manage their profiles. The system maintains role-based access (e.g., admin, verifier, contributor) and protects user data using secure hashing and session handling techniques. All activities and uploaded content are linked to the user's account for traceability.

**2.** ***Content Upload and Steganographic Embedding***

In this module, users upload digital content (such as images or documents) for authentication. The system generates a unique SHA-256 hash of the content and embeds it invisibly into the file using LSB or DWT-based steganography. This ensures the content carries a tamper-proof signature that can be verified later. The modified (stego) content is saved for future comparison.

**3.** ***Content Verification and Provenance Check***

This module handles the verification process. When a user submits content for authentication, the system extracts the embedded hash and compares it with the stored original hash. If both match, the content is marked as authentic; if not, it is flagged as modified. This process helps identify unauthorized changes and ensures content integrity.

**4.** ***Key Mapping and Storage***

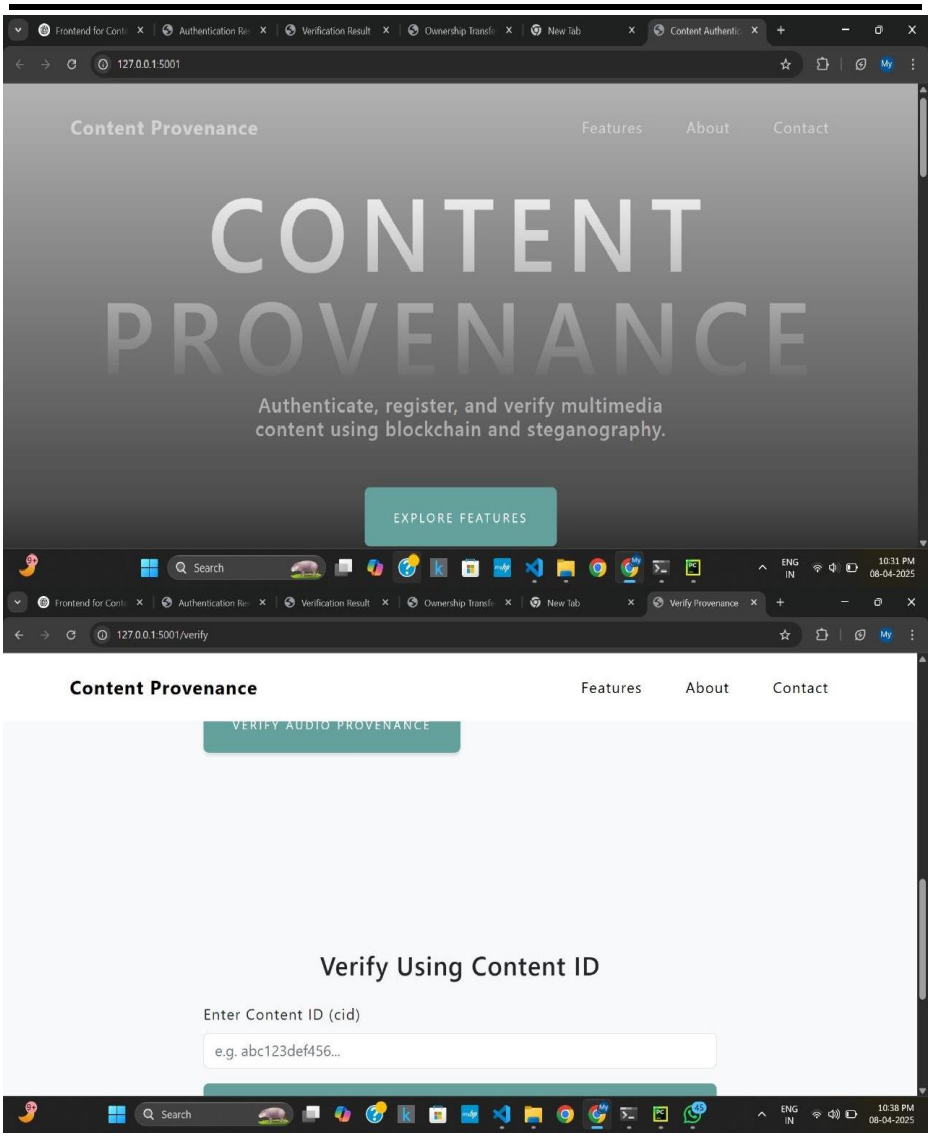
This module maps two keys (one stored in metadata and one embedded via steganography) to a unique entry in the database. These keys are linked to the original content's hash and the user ID. During verification, the system checks if both extracted keys point to the same record. This two-key mechanism improves verification reliability and supports provenance tracking.

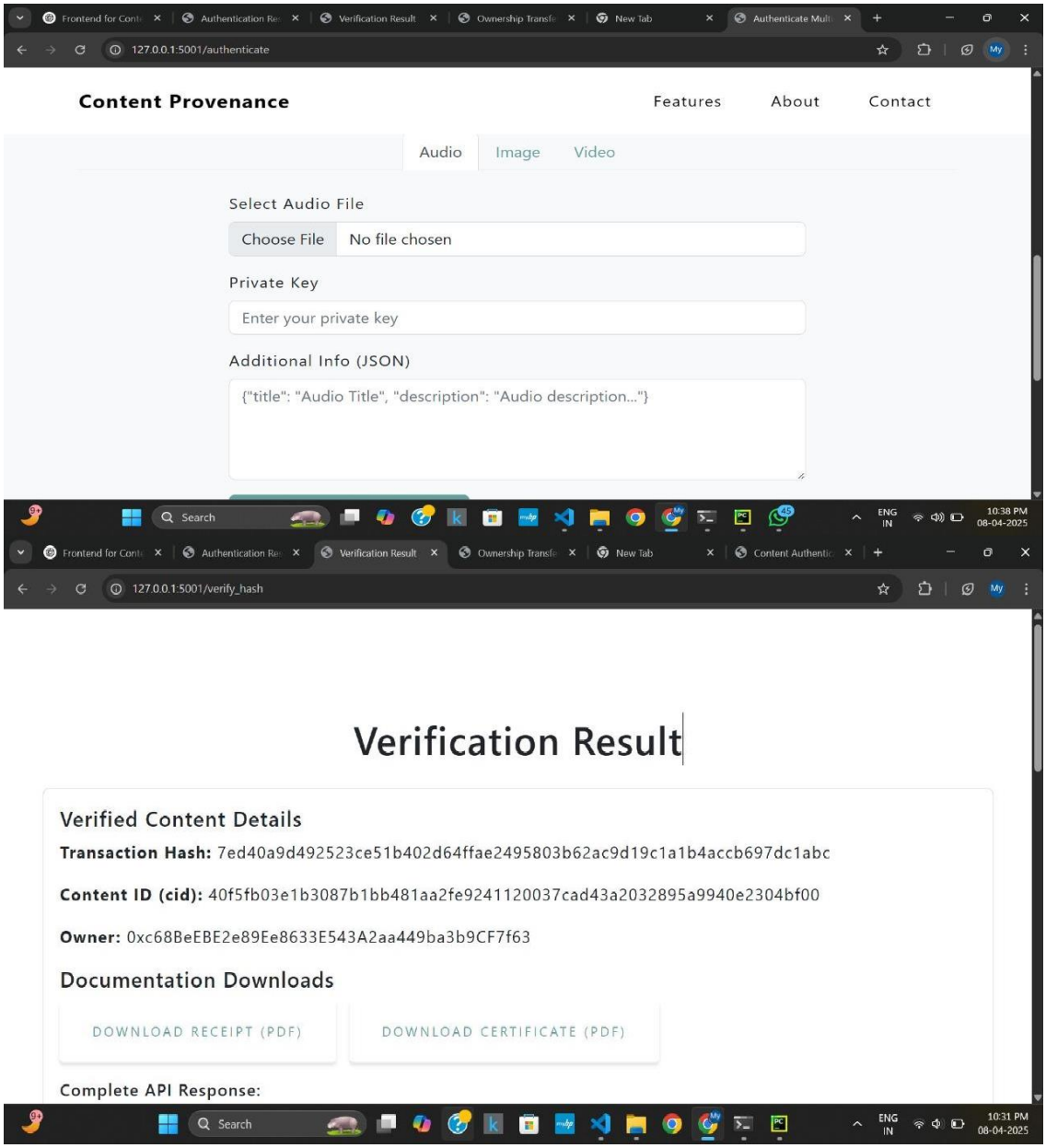
**5. *Database Management***

This module handles the structured storage and retrieval of user data, hashes, stego-content, verification logs, and key mappings. CRUD operations manage user profiles, content details, authentication keys, and timestamps. The database also supports historical tracking, enabling audits and validation of content over time.

## RESULTS AND DISCUSSION:

The system was rigorously tested with a variety of multimedia files under controlled conditions, demonstrating strong performance across multiple criteria. Authenticity verification showed that hidden keys extracted from both images and audio files consistently matched blockchain records, with even minor modifications leading to mismatched keys—highlighting the system's effectiveness in tamper detection. Ownership transfers were executed seamlessly, with accurate transaction logging on both the blockchain and the local database, while update logs offered clear traceability and accountability. Performance metrics indicated practical efficiency in file processing tasks such as hashing, key embedding, and extraction, with minimal latency even under high verification loads. Additionally, the integration of blockchain and steganography proved robust against common tampering methods, and scalability tests suggested the system could effectively handle increased data volumes, confirming its viability for real-world, high-volume applications.






## CONCLUSION:

The study shows that a very safe way to authenticate multimedia content is to combine blockchain technology with sophisticated steganography techniques. By using both digital fingerprinting and concealed key embedding, the dual-layer security strategy makes sure that any unauthorized changes are quickly identified. Furthermore, the solution offers a clear chain of ownership and history in addition to preserving content integrity by keeping an immutable record on the blockchain and a thorough update log in a local database. In order to increase adoption in digital copyright protection and forensic investigations, future work will concentrate on improving the user interface, investigating decentralized storage options, and maximizing processing efficiency. Test findings show that the system successfully identifies unauthorized changes, guaranteeing that only authenticated content is original and confirmed.Performance assessments also show that the system can effectively manage requests for real-time authentication and verification, which qualifies it for widespread use in media security applications. All things considered, this project offers a scalable, decentralized, and safe multimedia authentication solution. Digital files are kept safe, verifiable, and tamper-proof by integrating steganographic security, blockchain immutability, and sophisticated cryptographic algorithms. Future improvements could include support for more multimedia formats, AI-based tamper detection, and interaction with decentralized storage systems (IPFS), which would increase its efficacy in thwarting digital fraud and guaranteeing content authenticity in a world that is becoming more and more digital.

## REFERENCE:

1. S. P. Jakhar, A. Nandal, A. Dhaka, B. Jiang, L. Zhou, and V. N. Mishra, “Fractal feature based image resolution enhancement using wavelet– fractal transformation in gradient domain,” J. Circuits, Syst. Comput., vol. 32, no. 2, Jan. 2023, Art. no.

2350035.

**2.** A. Dhaka, A. Nandal, H. G. Rosales, H. Malik, F. E. L. Monteagudo,2021.

**3.** M. I. Martinez-Acuna, and S. Singh, "Likelihood estimation and wavelet transformation based optimization for minimization of noisy pixels," IEEE Access, vol. 9, pp. 132168–132190, 2021.

**4.** H.T. Hu, H.H. Chou, and T.T. Lee, "Robust blind speech watermark-ing via FFTbased perceptual vector norm modulation with frame self synchronization," IEEE Access, vol. 9, pp. 9916–9925.

**5.** Z. Liu, Y. Huang, and J. Huang, "Patchwork-based audio watermark- ing robust against de-synchronization and recapturing attacks," IEEE Trans. Inf. Forensics Security, vol. 14, no. 5, pp. 1171–1180, May 2019.

**6.** G. Zhang, L. Zheng, Z. Su, Y. Zeng, and G. Wang, "M-sequences and sliding window based audio watermarking robust against largescale cropping attacks," IEEE Trans. Inf. Forensics Security, vol. 18, pp.

**7.** H. Liu, "Audio block encryption using 3D chaotic system with adap- tive parameter perturbation," Multimedia Tools Appl., vol. 82, no. 18, pp. 27973–27987, Jul. 2023.

**8.** A. Kumar and M. Dua, "Audio encryption using two chaotic map based dynamic diffusion and double DNA encoding," Appl. Acoust., vol. 203, Feb. 2023, Art. no. 109196.