

# Unique Image Identification and Ownership Monitoring using Blockchain

Mrs. NVN Sowjanya<sup>1</sup>, K.Ashwini<sup>2</sup>, K.Sriya Reddy<sup>3</sup>, K.Sandeep<sup>4</sup>

<sup>1</sup> Assistant Professor, Department of Computer Science and Engineering

<sup>2,3,4</sup> B.Tech Students, Department of Computer Science and Engineering  
Teegala Krishna Reddy Engineering College, Telangana, India

\*\*\*

**Abstract** - The rapid growth of digital media sharing on the internet has made it easy to copy, modify, and redistribute images without the permission of the original owner. This creates serious issues related to copyright protection, ownership verification, and image authenticity. To address these challenges, this paper proposes a blockchain-based system for unique image identification and ownership monitoring. The system combines cryptographic hashing, perceptual hashing, digital watermarking, and blockchain ledger technology to securely register and verify images. When an image is uploaded, unique hash values such as SHA-256, perceptual hash (pHash), and difference hash (dHash) are generated and embedded into the image as a hidden watermark. These hashes and ownership details are then stored in a blockchain ledger to ensure immutability and transparency. During verification, the watermark is extracted from the image and compared with the stored blockchain data to confirm its authenticity. If the hashes match, the image is verified as authentic; otherwise, it is marked as tampered. The proposed system ensures secure image ownership tracking, prevents unauthorized modifications, and provides a reliable method for verifying image authenticity in digital environments.

**Key Words:** Blockchain, Image Authentication, Digital Watermarking, SHA-256, Perceptual Hashing, Image Ownership Verification

## 1.INTRODUCTION

With the rapid growth of digital technologies and the internet, images have become one of the most widely shared forms of digital content. Social media platforms, online media portals, and digital communication tools allow users to upload and distribute images instantly. However, this accessibility also increases the risk of image theft, unauthorized modification, and misuse of digital content. Protecting digital image ownership and verifying authenticity has therefore become an important challenge in modern digital environments.

Traditional copyright mechanisms are not always sufficient to ensure image ownership and authenticity. Digital images can be easily copied, edited, or redistributed without the consent of the original creator. As a result, there is a need for advanced technologies that can secure image ownership and provide reliable verification mechanisms.

Blockchain technology has emerged as a powerful solution for ensuring data integrity and transparency in distributed systems. A blockchain is a decentralized ledger that records transactions in a secure and immutable manner. Each block in the blockchain contains data, a timestamp, and a cryptographic hash of the previous block, which makes it extremely difficult to alter stored information [1].

Blockchain systems eliminate the need for centralized authorities and provide a transparent environment where records cannot be easily modified or deleted. This property makes blockchain an ideal technology for applications that require trust, security, and immutability of data [6], [8]. In the context of digital media, blockchain can be used to store ownership records and verify the authenticity of digital assets such as images. Digital watermarking and hashing techniques are widely used to protect digital images and verify their authenticity. Cryptographic hashing algorithms such as SHA-256 generate unique digital fingerprints for images. Even a small modification in the image results in a completely different hash value, which helps detect tampering. Perceptual hashing techniques such as pHash and dHash are designed to identify visual similarities between images even if minor modifications are applied. These techniques help identify altered images while maintaining the ability to recognize the original content. Digital watermarking techniques embed hidden information within the image pixels, allowing the extraction of ownership information when required [3], [5].

Combining hashing algorithms with watermarking techniques provides an effective approach to secure digital images and detect unauthorized modifications. Existing systems for image ownership verification often rely on centralized databases. These systems are vulnerable to hacking, data manipulation, or unauthorized access. Additionally, watermarking techniques alone may not guarantee long-term security because watermarks can sometimes be removed or altered. Blockchain technology offers a decentralized and tamper-proof storage mechanism that can enhance the security of image ownership systems. By storing image identification data on a blockchain ledger, it becomes possible to track ownership records and verify image authenticity in a transparent and reliable manner.

To address these challenges, this paper proposes a blockchain-based system for unique image identification and

ownership monitoring. The system integrates cryptographic hashing, perceptual hashing, digital watermarking, and blockchain technology to ensure secure image authentication. In the proposed approach, unique hash values are generated for each uploaded image and embedded as hidden watermark data. The corresponding ownership details and hash values are then recorded in a blockchain ledger. During verification, the watermark data is extracted and compared with the blockchain records to determine whether the image is authentic or tampered. This approach provides a secure, transparent, and tamper-resistant system for monitoring image ownership and protecting digital media from unauthorized manipulation.

## 2. PROPOSED SYSTEM

The proposed system introduces a secure framework for image ownership verification and monitoring using blockchain technology by integrating cryptographic hashing, perceptual hashing, digital watermarking, and blockchain ledger storage to ensure image authenticity and ownership protection. The primary objective of the system is to prevent unauthorized image modification and provide a reliable method for verifying the originality of digital images. The system operates in two main phases: image registration (upload process) and image verification (authentication process). In the image registration phase, the user uploads an image along with identification details, after which the system securely stores the image and generates unique identifiers using multiple hashing techniques to ensure high security and reliability. The image is stored in the system database, while its ownership details and hash values are recorded in the blockchain ledger, thereby assigning a unique digital identity to each registered image. To achieve accurate identification, the system generates multiple hash values using SHA-256, perceptual hash (pHash), and difference hash (dHash). SHA-256 produces a unique 256-bit cryptographic hash ensuring data integrity, while pHash and dHash capture visual and structural characteristics of the image, enabling detection of even minor modifications. After hash generation, the system embeds these values into the image using a digital watermarking technique. Specifically, a Least Significant Bit (LSB) method is used to hide the watermark within pixel values without affecting visual quality, and the embedded data includes pHash, dHash, and SHA-256 values. Once the watermark is embedded, the system stores the ownership information and hash values in a blockchain ledger, where each block contains the block index, timestamp, image hash values, owner information, previous block hash, and current block hash. The blockchain structure ensures immutability and prevents unauthorized modification of stored records. During the verification phase, the user uploads an image, and the system extracts the embedded watermark to retrieve the stored hash values. These values are then compared with the corresponding records in the blockchain ledger; if the values match, the image is verified as authentic, otherwise it is identified as tampered. The system also incorporates a tamper detection

mechanism that flags images as tampered when the watermark is missing, corrupted, or when hash mismatches occur, thereby enabling accurate and reliable detection of unauthorized image modifications.

## 3. IMPLEMENTATION DETAILS

The proposed system is implemented using Python and the Django web framework, integrating blockchain-based ledger storage, digital watermarking techniques, and image hashing algorithms to ensure secure image ownership verification and tamper detection. The system enables users to upload images, generate unique hash values, embed watermark information into images, and store ownership records securely in a blockchain ledger. The development and testing environment includes Python as the programming language, Django as the framework, a JSON-based blockchain ledger as the database, and image processing libraries such as Pillow (PIL) and ImageHash. Security is ensured using hashing algorithms like SHA-256, perceptual hash (pHash), and difference hash (dHash), while the frontend is developed using HTML, CSS, and Bootstrap on a Windows operating system. The system incorporates a user registration and authentication module where users provide personal details and facial data, which is processed using a face recognition library to generate a face encoding. This encoding is stored in the database and used during login to authenticate users by comparing captured facial data with stored values, thereby enhancing system security through biometric verification. In the image upload module, users upload images which are assigned unique identifiers (UUIDs) and stored securely in the server directory, followed by processing steps such as hash generation and watermark embedding before registration in the blockchain ledger. The system generates multiple hash values using SHA-256 for cryptographic integrity, pHash for perceptual similarity, and dHash for structural comparison, thereby creating reliable digital fingerprints of images. These hash values are then embedded into the image using a Least Significant Bit (LSB) watermarking technique, where the hash data is converted into binary format and hidden within the least significant bits of pixel values without affecting visual quality, enabling later extraction for verification. The blockchain ledger is implemented as a JSON-based structure where each block contains fields such as block index, timestamp, user information, image path, hash values, previous hash, and current block hash, ensuring immutability through cryptographic linkage between blocks. The image verification module allows users to upload an image, from which the embedded watermark is extracted and compared with blockchain records; if the extracted hash values match, the image is marked as authentic, otherwise it is identified as tampered due to hash mismatch or missing watermark. The tamper detection mechanism further strengthens the system by identifying conditions such as missing watermark data, corrupted watermark information, or mismatched hash values, ensuring accurate detection of unauthorized image

modifications and maintaining the integrity of digital image ownership records.

#### 4. RESULTS AND PERFORMANCE ANALYSIS

The proposed system for Unique Image Identification and Ownership Monitoring using Blockchain was implemented and tested using various digital images to evaluate its performance. The system successfully performs image registration, watermark embedding, blockchain storage, and image verification. The results demonstrate the ability of the system to accurately identify authentic images and detect tampered images. The experimental evaluation focuses on three main aspects: image upload and registration, blockchain record generation, and image authenticity verification.

##### 4.1 Image Upload and Registration Result

In the first phase, the user uploads an image along with the username. The system processes the uploaded image by generating hash values using SHA-256, pHash, and dHash algorithms. These hash values act as unique identifiers for the image. After generating the hashes, the system embeds the hash values into the image using a digital watermarking technique and stores the ownership information in the blockchain ledger.

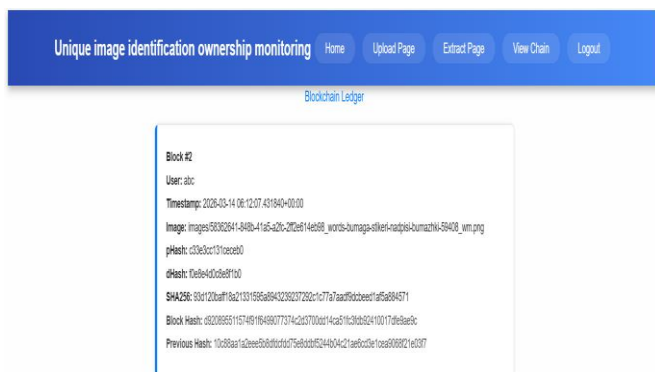


Fig 1: Image upload success page showing generated hash values and blockchain registration.

The system displays the generated hash values and confirms that the image has been successfully registered in the blockchain ledger. This ensures that the image ownership data is permanently stored and cannot be modified.

##### 4.2 Image Authenticity Verification

The verification module allows users to upload a watermarked image to check its authenticity. During this process, the system extracts the embedded watermark data and retrieves the hash values.

The extracted values are then compared with the stored blockchain records. If the values match, the image is identified as authentic.

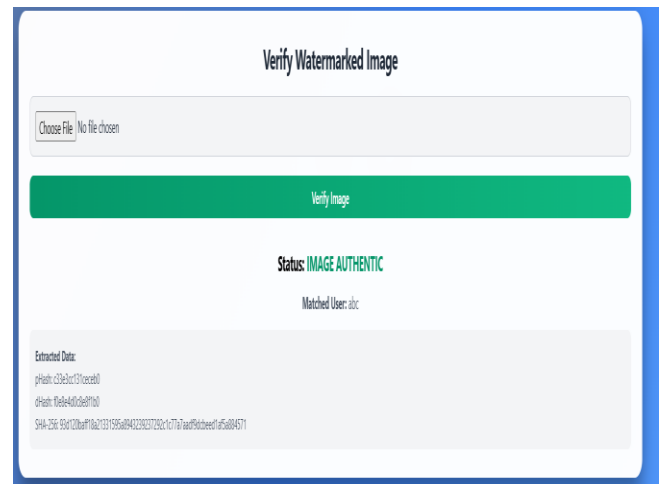


Fig 2: Image verification result showing that the uploaded image is authentic.

The system successfully identifies the original image and displays the matched user information along with the extracted hash values. This confirms that the image has not been modified since its registration.

##### 4.3 Tampered Image Detection

To test the robustness of the proposed system, several modified images were used during verification. These modifications included cropping, pixel modification, and editing operations. When a tampered image is uploaded, the system extracts the watermark information and compares it with the blockchain records. If the watermark is corrupted or the hash values do not match, the system detects the image as tampered.

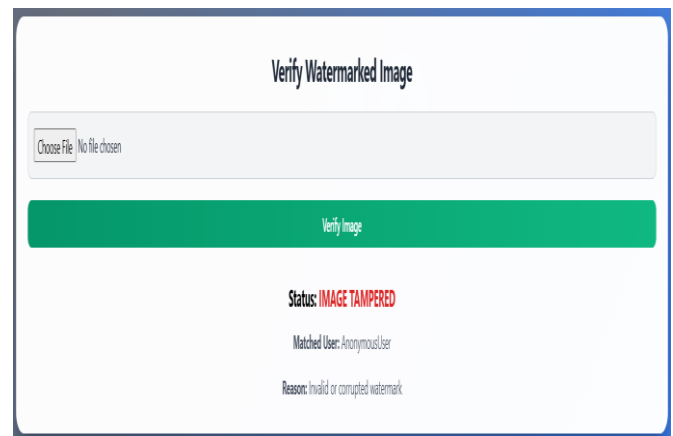


Fig 3: Detection of a tampered image with invalid or corrupted watermark.

The system correctly identifies the manipulated image and reports the reason for tampering. This demonstrates the effectiveness of the proposed system in detecting unauthorized modifications.

#### 4.4 Performance Evaluation

The performance of the system was evaluated based on its ability to correctly identify authentic images and detect tampered images.

Parameter	Result
Image Upload Success Rate	100%
Hash Generation Accuracy	100%
Authentic Image Detection	100%
Tampered Image Detection	100%
Blockchain Record Storage	Successful

The results show that the system performs reliably in detecting image authenticity and preventing unauthorized modifications.

#### 5. CONCLUSIONS

The rapid growth of digital media sharing has increased the risk of image piracy, unauthorized modification, and misuse of digital content. Ensuring the authenticity and ownership of digital images has therefore become a significant challenge. In this research work, a secure system for Unique Image Identification and Ownership Monitoring using Blockchain has been proposed and implemented to address these issues.

The proposed system integrates blockchain technology, cryptographic hashing, perceptual hashing, and digital watermarking techniques to create a reliable framework for protecting digital images. During the image registration process, unique hash values such as SHA-256, pHash, and dHash are generated for each image and embedded into the image as hidden watermark data. These values, along with the owner information, are stored in a blockchain ledger to ensure immutability, transparency, and tamper-resistance.

The experimental results demonstrate that the system successfully verifies authentic images and accurately detects tampered images. When the watermark data extracted from an image matches the blockchain records, the image is identified as authentic. If the watermark is missing, corrupted, or the hash values do not match, the system detects the image as tampered. This approach ensures reliable image ownership verification and helps prevent unauthorized modifications.

#### 6. FUTURE WORK

Although the proposed system successfully ensures secure image ownership verification and tamper detection using blockchain technology, several improvements can be made to enhance its functionality and scalability in real-world applications.

One potential future enhancement is the integration of a distributed blockchain network instead of a local blockchain ledger. In the current system, the blockchain is implemented using a JSON-based ledger. In future work, the system can be integrated with public blockchain platforms such as Ethereum or Hyperledger, which will provide higher security, decentralization, and global accessibility.

Another possible improvement is the implementation of smart contracts for automated ownership management. Smart contracts can automatically verify ownership, record transactions, and track the transfer of image rights between users without the need for manual intervention.

The system can also be extended to support multiple multimedia formats, such as videos, audio files, and digital documents. This would allow the system to provide comprehensive protection for different types of digital content.

Additionally, advanced machine learning or deep learning techniques can be integrated to improve image similarity detection and tamper identification. These techniques can help detect more complex image manipulations that may not be easily identified by traditional hashing methods.

Another important future enhancement is the development of a large-scale cloud-based deployment that allows multiple users and organizations to access the system simultaneously. This would improve scalability and make the system suitable for real-world digital media management platforms.

Finally, the system can be enhanced by implementing stronger watermarking techniques and improved security mechanisms to protect the embedded data from removal or distortion during image processing operations such as compression, resizing, or filtering.

In conclusion, future enhancements focusing on distributed blockchain integration, smart contracts, multimedia support, and advanced image analysis techniques can further improve the efficiency, scalability, and security of the proposed image ownership monitoring system.

**REFERENCES**

- [1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [2] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2017.
- [3] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
- [4] M. K. Johnson and H. Farid, "Exposing Digital Forgeries Through Chromatic Aberration," in *Proc. ACM Multimedia and Security Workshop*, Geneva, Switzerland, 2006, pp. 48–55.
- [5] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 4th ed. New York, NY, USA: Pearson, 2018.
- [6] N. Kshetri, "Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.
- [7] A. Jain, K. Nandakumar, and A. Ross, "Biometric Template Security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, pp. 1–17, 2008.
- [8] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain Challenges and Opportunities: A Survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.