Blockchain Based Image Encryption and Authenticity Verification System

Aapeksha Ray[1], Deeksha G[2], Deekshitha K[3], Gowri P Gowda[4], Prof. Kavitha S[5]
[1,2,3,4,5]*Computer Science Engineering Nagarjuna College of Engineering and Technology, Devanahalli, Bengaluru*

***Abstract*—In the digital age, image misuse, manipulation, and intellectual property theft have become significant concerns. This project introduces a secure image verification system that combines AES encryption, SHA-256 hashing, and blockchain technology to protect digital content. When an image is uploaded, it is first encrypted for confidentiality, then hashed to generate a unique digital fingerprint. This hash is recorded on a decentralized blockchain, creating a tamper-proof and timestamped record of ownership. Any alteration to the image changes the hash, allowing immediate detection of tampering. The system empowers creators to prove originality, prevent unauthorized use, and safeguard their work in professional settings. While challenges such as blockchain scalability, network delays, user accessibility, and energy consumption exist, the solution remains a powerful and transparent method for securing digital images in an evolving online environment.**

I. INTRODUCTION

In today's digital world, millions of images are uploaded and shared every single day across social media, online marketplaces, and content-sharing platforms. While this has made it easier for creators, photographers, and businesses to reach a wider audience, it has also opened the door to problems like image theft, copying, misuse, tampering, and false ownership claims. As images continue to spread quickly online, it becomes increasingly difficult to prove who originally created them or whether they have been altered.

To address these challenges, this project introduces a simple yet powerful web-based image verification system that uses blockchain technology and SHA-256 hashing to protect image authenticity. The idea is straightforward: whenever a user uploads an image, the system instantly generates a unique digital fingerprint, known as a hash. This hash is then stored securely on a blockchain ledger, which cannot be edited or identify applicable funding agency here. If none, delete this.

Tampered with. Even the smallest modification to the im-age—such as changing a pixel, adjusting brightness, or adding a watermark—will generate a completely different hash. This makes it easy to detect manipulation and verify whether an image is original or altered.

Traditional verification methods like metadata or centralized storage are not reliable because they can be easily changed, deleted, or hacked. In contrast, blockchain provides a de-centralized and transparent solution that guarantees long-term protection. Once the hash is stored on the blockchain, no one can modify it—not even the system administrators—making it a trustworthy digital record of the image's originality.

This system has practical applications across many fields. Digital artists can use it to prove ownership of their work. Journalists can verify the authenticity of photographs used in news reporting. Online sellers can protect product images from unauthorized reuse. In every case, the system acts as a digital shield, giving creators confidence that their images are protected and traceable.

Ultimately, the goal of this project is to empower users with a secure and dependable platform for verifying image authenticity. By combining blockchain with SHA-256 hashing, the system ensures that originality can be proven, manipulation can be detected, and ownership can be protected in an increasingly visual and fast-moving online world.

II. LITERATURE REVIEW

1. Chaos-Based Image Encryption Techniques.

Chaos-based image encryption techniques draw inspiration from the mathematical behavior of chaotic systems, which exhibit random-ness, sensitivity, and nonlinearity. These properties closely match the requirements of secure cryptographic design. Popular chaotic models such as the Logistic Map, Henon Map, Lorenz Systems, Tent Map, and Baker Map generate pseudo-random sequences used to shuffle pixel positions (permutation) and alter pixel values (substitution). This dual process significantly increases confusion and diffusion, making the encrypted image highly resistant to classical attacks. In these methods, even a minimal change in the initial key or parameter produces a completely different cipher image due to extreme sensitivity. This ensures a large key space and strong resistance against brute-force attacks.

2. Traditional vs Image-Specific Encryption Algorithms

Traditional encryption algorithms such as AES, DES, 3DES, and RSA were originally designed for text and binary data, not for large multimedia files. These algorithms treat data as uniform blocks or streams, which makes them secure but often inefficient for images due to high computational cost, larger file size, and the strong correlation between neighboring pixels in natural images. When applied directly, traditional methods can produce slow performance during encryption/decryption, especially for high-resolution images, and may not fully re-move pixel correlation, making images vulnerable to statis-tical analysis if not properly configured. In contrast, image-specific encryption algorithms are specially crafted to address the unique characteristics of images. These methods lever-age spatial redundancy, pixel intensity distribution, and two-dimensional structure. Common approaches include chaos-based encryption, bit-plane scrambling, DNA-based encoding, wavelet-based encryption, and permutation–substitution net-works (PSN).

3. AES-Based Image Encryption Approaches

Researchers have widely used the Advanced Encryption Standard (AES) for securing digital images because of its strong mathematical foundation and well-established resistance to brute-force at-tacks. Literature shows that AES significantly increases the entropy of images and ensures uniform pixel distribution in the encrypted output. However, studies also highlight challenges when AES is used for large, high-resolution images because it treats image data the same as text or binary blocks. This leads to higher computational overhead and slower processing speed. Some research proposes optimized or reduced-round AES versions to improve speed, while hybrid systems combine AES with pixel scrambling techniques to enhance correlation reduction. Several studies identify performance bottlenecks when AES is applied to real-time multimedia systems or large datasets. To address this, researchers propose reduced-round AES variants, parallel hardware implementations, or GPU-based acceleration to increase processing speed. These hybrid systems achieve enhanced security, reduce statistical weak-nesses, and significantly improve resistance to cryptanalytic attacks while maintaining acceptable performance for image-specific applications.

4. DES and 3DES for Secure Image Transfer

DES and 3DES were among the earliest cryptographic algorithms applied to image security. Literature indicates that DES provides a reasonable level of randomness but is now considered insecure due to its small key size. 3DES offers stronger protection but at the cost of significant processing time, making it inefficient for large image files. Researchers found that while DES-based encryption increases confusion at the pixel level, it does not effectively break image redundancy. As a result, many studies classify DES/3DES as outdated for modern image encryption needs and recommend using them only for lightweight or low-sensitivity environments. To improve security, researchers adopted 3DES, which applies DES three times in an encrypt–decrypt–encrypt sequence.

III. PROBLEM STATEMENT

With the rapid growth of digital communication, sensitive images such as medical scans, biometric data, financial documents, and surveillance footage are frequently transmitted and stored across untrusted networks. Traditional text-based encryption algorithms like DES, 3DES, and AES treat images as

generic binary data and fail to address inherent image characteristics such as high pixel correlation and large file size. As a result, encrypted images may still reveal statistical patterns and suffer from high computational cost, making them unsuitable for real-time applications. Furthermore, existing authenticity verification methods, including hashing and watermarking, are vulnerable to noise, compression, geometric transformations, and AI-based tampering techniques. These limitations create security gaps, making it difficult to ensure both confidentiality and integrity of images in practical environments. Therefore, there is a need for a more efficient, robust, and scalable system that ensures strong image encryption along with reliable authenticity verification.

IV. CHALLENGES / GAPS IDENTIFIED

- Dependency on External API

Most encryption algorithms like AES and 3DES perform operations block-by-block, which increases processing time for high-resolution medical, satellite, or biometric images. This limits real-time performance in applications like surveillance, video streaming, and IoT.

- Inefficient Handling of Image Redundancy

Traditional text-based ciphers do not consider high pixel correlation present in images. As a result, encrypted images may still retain patterns, making them partially vulnerable to statistical attacks.

- Poor Scalability for Real-Time Systems

Many algorithms fail to scale when image sizes increase or when multiple images must be encrypted simultaneously (e.g., cloud storage, CCTV networks). Delays affect usability and real-time decision-making.

- Lack of Standardization in Image Authentication Techniques

Different systems use different hashing, watermarking, and signature methods. The universal benchmark, making it hard to compare the accuracy and robustness of different authentication techniques.

- Sensitivity to Noise and Compression

Authentication systems that use fragile watermarking or pixel-based hashing break This leads to false alarms and poor reliability in practical environments

V. OBJECTIVES

- Secure Image Encryption

Design a system that protects images by reducing pixel correlation and increasing randomness, ensuring confidentiality against attacks like brute-force or statistical analysis.

- Customizable Authenticity Verification

Implement mechanisms such as hashing, watermarking, or blockchain to detect tampering and verify the originality of images.

- Efficiency and Real-Time Performance

Optimize encryption and verification algorithms to handle high-resolution images quickly, making the system suitable for real-time or cloud-based application.

- Robustness Against Manipulations

Ensure the system can detect or resist common modifications like compression, cropping, or geometric transformations while maintaining accuracy and reliability.

VI. RESULTS

Fig. 1. Image Verification Interface (Verification Page)

This figure shows the verification interface of the proposed blockchain-based image authentication system. The interface allows users to upload an image or provide an existing hash to initiate the verification process. The system displays the verification features available, including blockchain registration status, ownership details, timestamp verification, tamper detection, and SHA-256 hash comparison.

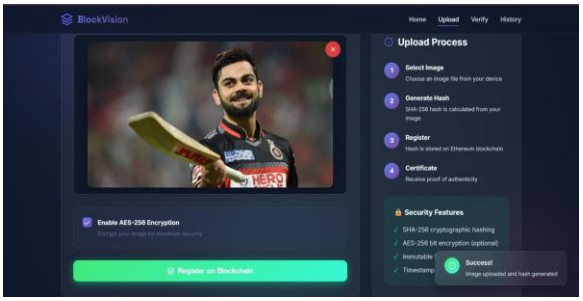

Fig. 2. Image Upload and Registration Interface

This figure illustrates the upload workflow within the sys-tem, where a selected image is processed to generate its SHA-256 hash. The interface guides the user through image selec-tion, hash generation, blockchain registration, and certificate retrieval. Optional AES-256 encryption is also provided before blockchain storage.

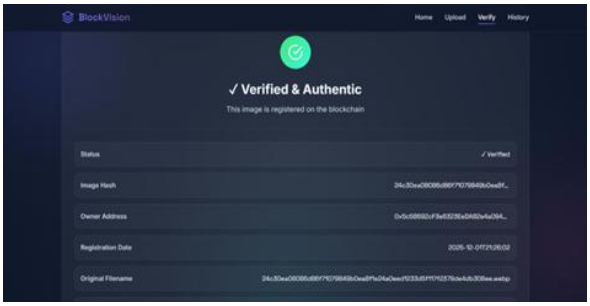

Fig. 3. Verified Image Details on Blockchain

This figure presents the verification results after successful blockchain validation. The system returns metadata including verification status, computed image hash, owner address, reg-istration date, and filename — demonstrating tamper-proof, immutable proof of authenticity.

Fig. 4. Blockchain Verification Certificate

This figure shows the auto-generated certificate issued upon successful verification or registration. It includes details such as the image hash, filename, timestamp, and encryption status, serving as formal documentation of authenticity and owner-ship.

REFERENCES

[1] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-Preserving Image Retrieval for Medical IoT Systems: A Blockchain-Based Approach," *IEEE Network*, vol. 33, no. 5, pp. 82–88, Sep./Oct. 2019.

[2] R. Mehta, N. Kapoor, S. Sourav, and R. Shorey, "Decentralised Image Sharing and Copyright Protection using Blockchain and Perceptual Hashes," in *Proc. 2019 11th Int. Conf. Communication Systems & Networks (COMSNETS)*, Bengaluru, India, 2019, pp. 311–318.

[3] C. J. Andi, R. Robet, O. Pribadi, and R. Wijaya, "Image Authentication Application with Blockchain to Prevent and Detect Image Plagiarism," in *Proc. 2021 Sixth Int. Conf. Informatics and Computing (ICIC)*, Jayapura, Indonesia, 2021, pp. 1–6.

[4] J. Pei, J. Dang, and Y. Wang, "Encryption Method of Privacy Information in Student Archives Based on Blockchain Technology," in *Proc. 2021 6th Int. Conf. Smart Grid and Electrical Automation (ICSGEA)*, Chongqing, China, 2021, pp. 215–219.

[5] F. Safwat, A. Akter, and N. Aman, "A Comparison of Chaotic Key Sequence and Blockchain Hasher for the Privacy Protection of the Internet of Things Image Data," in *Proc. 2021 IEEE Int. Conf. Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON)*, Dhaka, Bangladesh, 2021, pp. 124–129.

[6] B. Zhang, Y. Li, G. Chen, and H. Li, "Designing an Efficient Image Encryption-Then-Compression System by Using Interweaving Permutation and Blockchain-Watermarking," in *Proc. 2022 4th Int. Conf. Communications, Information System and Computer Engineering (CISCE)*, Beijing, China, 2022, pp. 239–243.

[7] R. C. Barik, G. Panda, A. Ratha, S. Padhan, and S. Changder, "Cyber Secure Remote Sensing Image Encryption Scheme using Blockchain and Dual Chaotic Map," in *Proc. 2023 3rd Int. Conf. Range Technology (ICORT)*, Chandipur, India, 2023, pp. 1–6.

[8] F. Yu, J. Peng, X. Li, C. Li, and B. Qu, "A Copyright-Preserving and Fair Image Trading

Scheme Based on Blockchain," *Tsinghua Science and Technology*, vol. 28, no. 5, pp. 963–974, Oct. 2023.

[9] S. Kanwal, U. Shahid, and M. Bano, "Blockchain Driven Medical Image Encryption Employing Chaotic Tent Map in Cloud Computing," *Scientific Reports*, vol. 15, 2025.

[10] T. Liu *et al*., "Color Image Authentication and Encryption Algorithm Based on Enhanced Dual-Chaos and Double-Random Phase Encoding," *Journal Name*, 2025.

[11] Z. Zhou and Q. Cui, "Blockchain-Based Secure and Efficient Secret Image Sharing for Wireless Networks," 2023.

[12] G. Archana *et al*., "Blockchain-driven Optimized Chaotic Encryption Scheme for Medical Image Transmission in IoT-Edge Environment," 2025.

[13] R. J. Cintra, V. S. Dimitrov, H. M. de Oliveira, and R. M. Campello de Souza, "Fragile Watermarking Using Finite Field Trigonometrical Transforms," 2015.

[14] Abrar, W. Abdul, and S. Ghouzali, "Secure Image Authentication Using Watermarking and Blockchain," *Intelligent Automation & Soft Computing*, vol. 28, no. 2, pp. 577–591, 2021.

[15] F. Ahmed, M. Ur Rehman, J. Ahmad, *et al*., "A DNA-Based Colour Image Encryption Scheme Using a Convolutional Autoencoder," 2022.

[16] G. A. Sathishkumar, K. Bhoopathy Bagan, and N. Sriraam, "Image Encryption Based on Diffusion and Multiple Chaotic Maps," 2011.

[17] S. Patel, B. K. P., and R. K. Muthu, "Image Encryption and Decryption Using Chaotic Logistic Mapping and DNA Encoding," 2020.

[18] "Image Encryption Using Blockchain and Chaos for Secure Communication," 2023.

[19] C. Li, Y. Zhang, and E. Y. Xie, "When an Attacker Meets a Cipher-Image in 2018: A Year in Review," 2019.

[20] "A Study on Secure Image Encryption Based on Blockchain," *Iraqi Journal of Intelligent Computing and Informatics (IJICI)*, 2025.

[21] W. Ding, Y. Ming, Z. Cao, and C. T. Lin, "A Novel Blockchain-Watermarking Mechanism Utilizing InterPlanetary File System and Fast Walsh-Hadamard Transform," *iScience*, vol. 27, no. 9, Art. no. 105394, 2024.

[22] S. K. Padhi, A. Tiwari, and Sk. Subidh Ali, "Deep Learning–Based Dual Watermarking for Image Copyright Protection and Authentication," 2025.

[23] "Secure Cryptographic Watermarking for Image Authentication: Algorithm, Methodology, and Experimental Analysis," *Journal of Propulsion Technology*, vol. 46, no. 04, pp. 112–124, 2025.

[24] "Secure and Flexible Image Watermarking Using IWT, SVD, and Chaos Models for Robustness and Imperceptibility," *Scientific Reports*, 2025.