From Centralization To Decentralization: Blockchain's Role In Transforming Social Media Platform Page mr.

Nishanth.R[1], Santhosh .J[2], Saravanan. E[3], Aravindhan. M[4], Dhamodharan. V[5]
[1, 2, 3, 4] Dept of Artificial Intelligence and Data Science
[5]Assist prof, Dept of Artificial Intelligence and Data Science
[1, 2, 3, 4, 5] M.A.M College of Engineering and Technology, Trichy, Tamil Nadu, India

Abstract- *The growing dependence on social media platforms for day-to-day communication has made digital privacy a serious concern. Platforms such as Instagram, Twitter, and Facebook host vast amounts of user-generated content, including images, text, and metadata, much of which can unintentionally expose personal details. Despite the available privacy controls, these tools often fall short of preventing the misuse or unauthorized distribution of sensitive content. This study presents a secure image-sharing framework that combines wavelet-SVD-based watermarking, steganography, and blockchain technology to address these vulnerabilities. The system supports image categorization, invisible watermark embedding, and screen-shot prevention. Blockchain ledgers ensure tamper-proof storage of image ownership records, whereas the dual-layered security approach makes the unauthorized extraction of hidden content extremely difficult.*

Keywords: Steganography, Watermarking, Blockchain, Image Privacy, Social Networks, Discrete Wavelet Transform, Screenshot Protection

I. INTRODUCTION

The rapid expansion of social media usage has fundamentally transformed how people communicate, share memories and express themselves online. Platforms that host user images are increasingly becoming targets for privacy violations, including unauthorized downloads, redistribution, and screenshot-based copying of images. Despite existing privacy settings, the protection offered remains superficial and fails to address deeper security concerns.

This project addresses this challenge by building a multilayered image protection framework that incorporates digital watermarking using wavelet-SVD decomposition, steganographic data embedding, and blockchain-backed integrity verification. Together, these layers ensure that image ownership is established, hidden data remain secure, and all transactions are transparently logged. Users can classify their uploaded images as sensitive or non-sensitive, triggering appropriate security measures. Anti-screenshot controls and download restrictions make it significantly more difficult for unauthorized users to misuse protected content.

1.1 Image Watermarking

Digital watermarking has emerged as a key technique in the field of multimedia security. At its core, watermarking involves embedding a small, invisible signal into digital media in a way that survives common processing operations, while remaining imperceptible to casual viewers. The wavelet-SVD approach exploits the frequency decomposition properties of wavelets combined with the algebraic stability of Singular Value Decomposition to produce highly robust watermarks.

1.2 Applications of Network Security

Network security is the foundation of modern digital infrastructure. It safeguards personal and financial data during transmission, protects health records in medical systems, and prevents unauthorized intrusion into government and corporate networks. In social media contexts, it ensures that user interactions, content uploads, and account credentials are protected against interception and misuse.

Fig. 1: Network Security Components

1.3 Privacy Protection in Images

Image-based privacy violations are a growing threat to social platforms. Users are often unaware of how much personal information their photos can reveal, from GPS coordinates in EXIF metadata to identifiable faces and surroundings. Key challenges include:

- Lack of ownership control once images are publicly shared or forwarded
- Exposure of sensitive metadata such as GPS coordinates and device information
- Unauthorized commercial use of personal photographs
- Inadequate and confusing platform privacy policies
- Risks of cyberbullying and identity theft through misappropriated images

II. LITERATURE SURVEY

2.1 Existing System

Current social networking platforms rely primarily on binary privacy toggles — public or private — to protect user images. These blunt tools fail to prevent misuse by individuals who already have access, cannot stop screenshots, and offer no mechanism for verifying the authenticity of images after sharing. The net result is a fragile privacy ecosystem in which sensitive images are routinely copied, forwarded, and repurposed without the original owner's knowledge or consent.

2.1.1 Disadvantages

- Rigid privacy settings with no contextual or granular control options
- No protection against misuse by trusted connections or followers
- Inability to prevent screenshots or screen recording of sensitive content
- Absence of tamper-detection mechanisms after image publication

[1] Hideme: Privacy-Preserving Photo Sharing on Social Networks

Authors: Li, Fenghua Year: 2019

Hidemeintroduced a cryptographic framework for selective image access on social networks. It decouples image storage from access control so that even intercepted data cannot be viewed without proper authorization. The system supports user-defined access policies and provides metadata protection.

Limitations: Heavy computational requirements, complex access policy management,and scalability constraints in large networks.

[2] ML-Based Social Media Bot Detection

Authors: Aljabri, Malak Year: 2023

This survey evaluates supervised, unsupervised, and deep-learning methods for detecting bot accounts on social platforms. Feature engineering is critical to the model performance.

Limitations: Large labeled datasets are required; sophisticated bots evade current detectors; high false-positive rates.

[3] Rumor Detection via Graph Neural Networks

Authors: Xu, Shouzhi, et al. Year: 2023

A GNN-based hierarchical feature aggregation model for identifying misinformation. The system captures both the content and propagation dynamics, outperforming traditional classifiers.

Limitations: High model complexity,challenging real-time inference,and large training corpora are required.

[4] Image Metadata Privacy and Forensic Balance

Authors: Golam &Albalawi Year: 2024

This study examines the tension between protecting image metadata for privacy and preserving it for forensic investigation, and proposes selective metadata masking techniques.

Limitations: Non-trivial balance between forensic utility and privacy; metadata management overhead; limited frameworks.

[5] Online Social Network Security Challenges

Authors: Zhang, Chi Year: 2010

A foundational survey mapped social network threat categories (data leakage, identity theft, and inference attacks) to corresponding mitigation strategies.

Limitations: Techniques are outdated relative to AI-driven threats,and multimedia content security is not adequately addressed.

[6] Privacy Protection Strategies on Social Media

Authors: Zulfahmi et al. Year: 2023

A dual-lens analysis of privacy protection that combines technical mechanisms and behavioral interventions advocates for automated privacy recommendation systems.

Limitations: Strong dependence on user compliance and limited image-specific coverage.

[7] LSTM-Attention POI Recommendation with Privacy

Authors: Wang, Kun Year: 2023

LSTM-based sequential modeling with attention mechanisms to recommend points of interest while applying differential-privacy techniques to limit data exposure.

Limitations: Significant computing demands; applicability limited to the LBSN domain; accuracy may be reduced by privacy constraints.

[8] Visual Privacy in Assisted Living Environments

Authors: Ravi, Siddharth, et al. Year: 2024

A review of visual anonymization techniques — blurring, pixelation, masking, and differential privacy — applied to smart homes and care environments.

Limitations: The quality vs. privacy trade-off persists,and advanced methods incur high processing costs.

[9] Security and Privacy in the Metaverse

Authors: Huang, Yan Year: 2023

This study maps the security landscape of the emerging metaverse andexplores blockchain and decentralized identity frameworks to enhance trust in virtual spaces.

Limitations: Low field maturity, no standardized security frameworks,and minimal real-world deployment experience.

[10] Privacy-Preserving AI in Healthcare

Authors: Khalid, Nazish, et al. Year: 2023

Survey of federated learning, differential privacy, and secure aggregation for training AI models on sensitive medical data without centralizing patient records.

Limitations: Privacy constraints reduce model accuracy, communication overhead is significant,and clinical deployment remains complex.

III. PROPOSED SYSTEM

The proposed framework overcomes the shortcomings of existing image-sharing platforms by incorporating multiple complementary protection mechanisms. Rather than relying on a single control, the system integrates watermarking, steganography, and blockchain technology into a cohesive pipeline that simultaneously addresses ownership, secrecy, and auditability.

When a user uploads an image, it is first classified as sensitive or non-sensitive. Sensitive images triggered the full-protection pipeline. The image passes through a wavelet-SVD watermarking module that embeds invisible ownership metadata. Steganographic techniques hide additional confidential information within image data, creating a two-layer barrier.

3.1 Advantages

- Multi-layer security combining watermarking, steganography, and blockchain
- Ownership metadata embedded invisibly, surviving common image processing
- Blockchain records provide tamper-proof, time-stamped audit trails
- Anti-screenshot and download-restriction mechanisms prevent physical-layer copying
- Flexible privacy settings allow per-image protection level customization

3.2 Proposed Architecture

The architecture organizes functionality into three principal entity types — image owners, image users, and image servers — that communicate through a web application layer. The owner's upload request triggers the classification and preprocessing modules before watermark embedding via the Discrete Wavelet Transform. After embedding, the image and its blockchain record are stored. Access requests are evaluated against privacy policies prior to delivery.

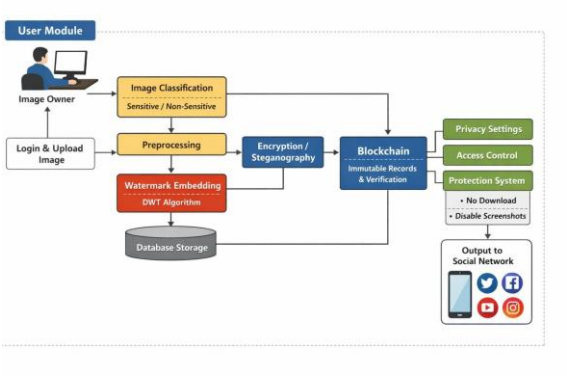

Fig. 2: Proposed Architecture Diagram

3.3 Proposed Block Diagram

The block diagram traces the workflow from login to final storage. After user authentication, the uploaded image is entered into the classification block. Depending on its sensitivity label, it proceeds to preprocessing, watermark embedding, and an optional steganographic overlay. The secured image is stored on the server side, while the blockchain module simultaneously logs the transaction details.

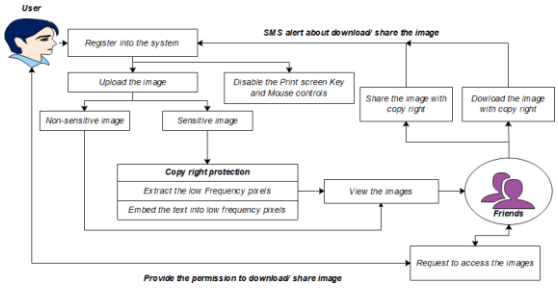

Fig. 3: Proposed Block Diagram

IV. SYSTEM REQUIREMENTS

4.1 Hardware Specifications

- Processor: Intel Core i3 / 2.6 GHz or higher
- RAM: Minimum 1 GB (4 GB recommended)
- Hard Disk: 160 GB storage capacity
- Optical Drive: 650 MB CD/DVD drive
- Input Device: Standard keyboard and mouse
- Display: 15-inch color monitor

4.2 Software Specifications

- Operating System: Windows 10 / 11
- Front-End: ASP.NET (C#)
- Back-End Database: Microsoft SQL Server
- Development IDE: Visual Studio 2019 / 2022
- Application Type: Web Application

4.3 Technology Description

ASP.NET Framework: ASP.NET is a server-side web application framework built on the. NET platform. It supports component-based development through a rich library of controls and provides built-in session management, authentication, and state management. The Common Language Runtime (CLR) enforces memory safety and handles exceptions uniformly across modules, making it well-suited for enterprise-grade web applications that demand both reliability and security.

Microsoft SQL Server: SQL Server is a relational database management system that underpins the application's persistent-storage layer. It uses a page-based storage engine with 8 KB pages that supports B-tree indexed access for fast retrieval. The platform provides comprehensive concurrency control via lock management and supports both pessimistic and optimistic concurrency models. Its Transact-SQL dialect enables the execution of complex business logic close to the data.

V. SYSTEM IMPLEMENTATION

5.1 UML Diagrams

The Unified Modeling Language (UML) provides a standardized notation for modeling software architectures. The project employs structural diagrams (class and component diagrams) to document static relationships and behavioral diagrams (use case, sequence, and activity diagrams) to capture dynamic interactions. Data Flow Diagrams complement these by illustrating information movement at progressive levels of detail.

5.2 Use Case Diagram

The use case diagram identifies three primary actors: the Image Owner, Image User, and System Server. The Image Owner initiates the upload, classification, and watermark embedding. Image Users interact through view, download request, and share request use cases. The Server mediates all transactions and enforces privacy policies through include and extend associations between use cases.

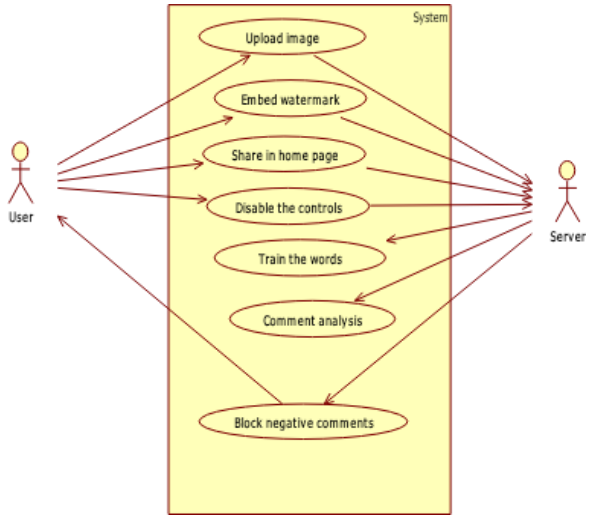

Fig. 4: Use Case Diagram

5.3 Class Diagram

The class diagram exposes five core classes: User, Image, Watermark, StegoLayer, and BlockchainRecord. Users aggregate both owner and consumer roles through inheritance. An image is associated with one watermark and optionally one stego layer. Methods such as embedWatermark(), extractWatermark(), and verifyIntegrity() encapsulate core algorithmic logic.

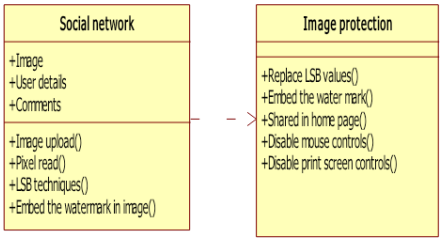

Fig. 5: Class Diagram

5.4 Sequence Diagram

The sequence diagram for the image upload flow shows the owner authenticating with the web server, which calls the Classification Service. Depending on the returned label, the Watermark Service is invoked to embed the owner signature. The server persists the result to the Image Database and simultaneously sends a record to the Blockchain Node. The confirmation is returned to the owner upon a successful block commit.

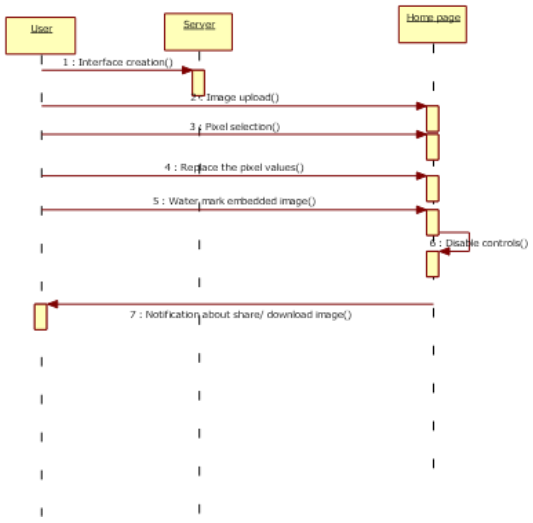

Fig. 6: Sequence Diagram

5.5 Activity Diagram

The activity diagram models the branching logic of the privacy-enforcement workflow. After uploading, the system evaluates the sensitivity label at the decision node. Sensitive images flow through watermark embedding, steganographic overlays, and screenshot protection before storage. Non-sensitive images bypass the advanced layers but still receive blockchain registration.

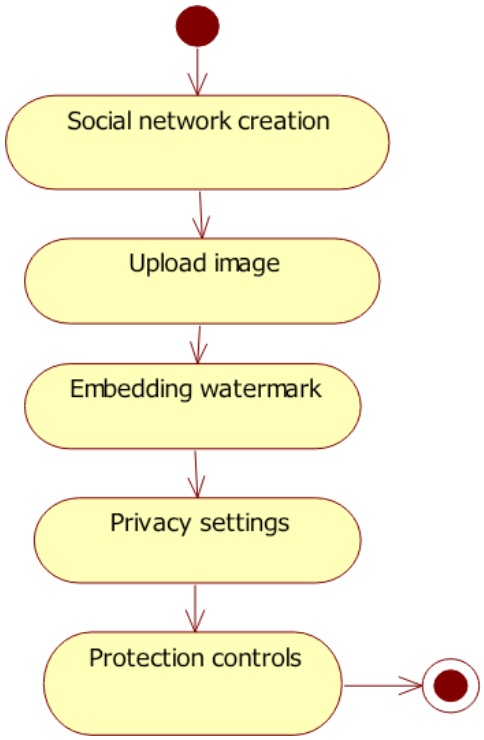

Fig. 7: Activity Diagram

5.6 Data Flow Diagram

The Level-0 DFD presents the system as a single process that receives image uploads from users and returns secured, blockchain-verified images. The Level-1 DFD decomposes this into five subprocesses: Authentication, Image Classification, Watermark Processing, Steganography, and Blockchain Logging. Level-2 DFDs further decompose Watermark Processing into DWT Analysis, SVD Embedding, and Inverse Transform Recovery stages.

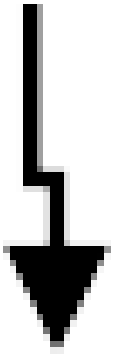

Fig. 8: DFD Level 0

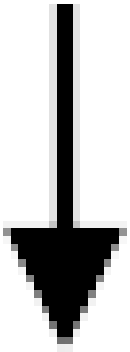

Fig. 9: DFD Level 1

VI. MODULE DESCRIPTION

6.1 Modules

- Social Network Creation – establishes user roles and connection management
- Image Upload – handles acquisition and sensitivity classification
- Watermark Embedding – applies Wavelet-SVD ownership marking
- Privacy Settings – manages per-image access control policies
- Protection System – enforces download restrictions and screenshot blocking

6.2.1 Social Network Creation

The social network module establishes a platform infrastructure that supports three distinct user roles: Image Owner, Image User, and Image Server. Owners upload and manage their content, and users browse and request access. The server mediates all transactions and enforces the privacy policies. The front end was implemented as an ASP.NET web application, enabling cross-browser accessibility without requiring client-side installation.

6.2.2 Image Upload

Upon uploading, each image is analyzed and tagged as either sensitive or non-sensitive. Sensitive images include personal photographs or documents that warrant full protection. Non-sensitive images may follow a lighter security approach. The classification step determines which downstream modules are activated, ensuring that the computational overhead is proportional to the protection required.

6.2.3 Watermark Embedding

Watermarking is performed in the wavelet domain using Singular Value Decomposition. The host image is decomposed into frequency sub-bands using Discrete Wavelet Transform. The SVD of a selected subband is computed, and the watermark signal is embedded by modifying the singular values. The inverse DWT was used to reconstruct the watermarked image. This approach ensures robustness against JPEG compression, cropping, and image rotation attacks.

6.2.4 Privacy Settings

The privacy module implements a two-stage policy classification. In the first stage, a classifier determines whether an image requires privacy protection based on its content and the owner preferences. In the second stage, if protection is required, the system generates an access whitelist from trusted contacts. Users outside this list receive only a watermarked preview rather than the original.

6.2.5 Protection System

The protection module deploys browser-based hooks to prevent the unauthorized duplication of data. Screenshot capture APIs at the OS level are intercepted and blocked for the protected content. Download attempts by unauthorized users only return a watermarked derivative. These controls are implemented across all major browser environments using CSS pointer-event restrictions, JavaScript event listeners, and server-side file delivery logic.

VII. VERIFICATION AND VALIDATION

7.1 Verification

Verification activities confirmed that each module conformed to its design specifications. Unit tests were conducted on the DWT-SVD watermarking algorithm to verify that the embedded marks could be reliably extracted after common image transformations. Integration tests validated the end-to-end data flow from upload to blockchain commit. The access control logic was tested against the boundary conditions, confirming that unauthorized access attempts were consistently denied.

7.2 Validation

Validation was performed through user scenario testing. Simulated privacy breach attempts, including screenshot capture, unauthorized downloads, and image tampering, were executed against the protected images. In each scenario, the system either blocked the action or detected the tampering through watermark verification. Blockchain integrity checks confirmed that no committed records could be altered retroactively.

VIII. RESULTS AND SCREENSHOTS

The following screenshots demonstrate the working prototype of the secure image-sharing system deployed on a local development server. The application was tested across multiple browsers and for different user roles.

Fig. 10: Home Page – Social Network Interface

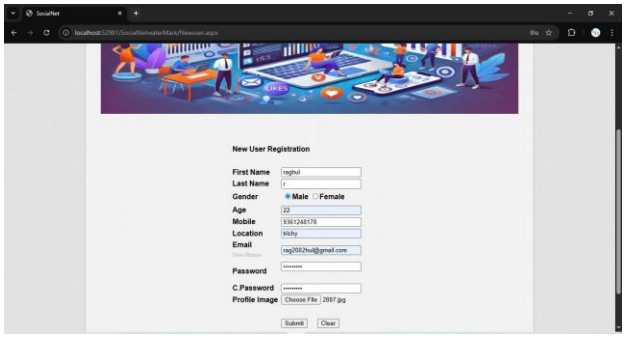

Fig. 11: User Registration / Login Page

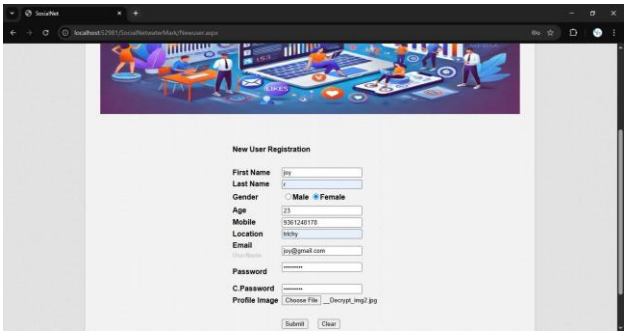

Fig. 12: Image Upload and Classification Module

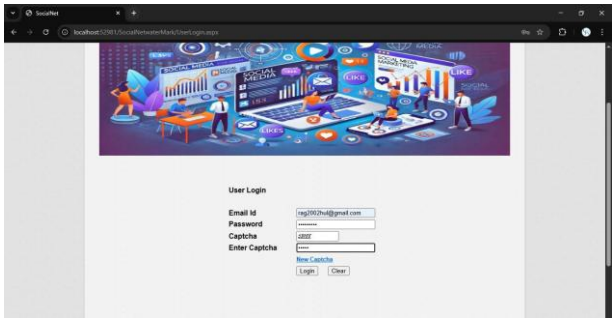

Fig. 13: Watermark Embedding Process

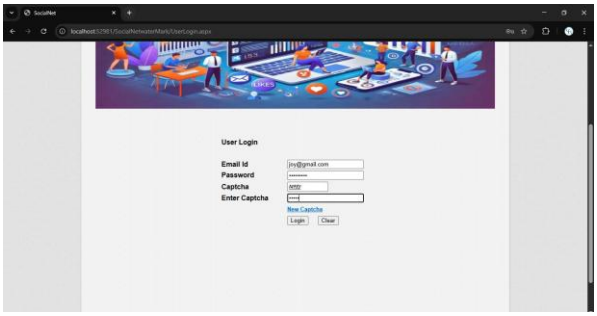

Fig. 14: Privacy Settings Configuration

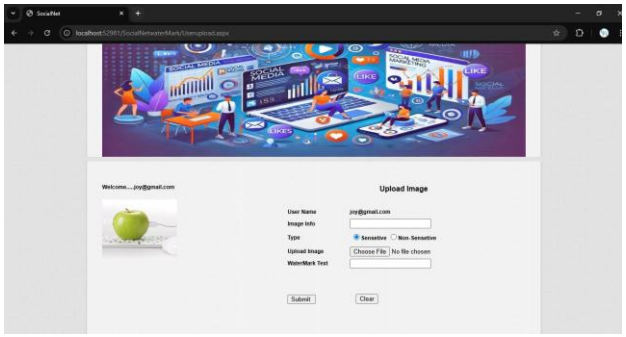

Fig. 15: Image Sharing with Copyright

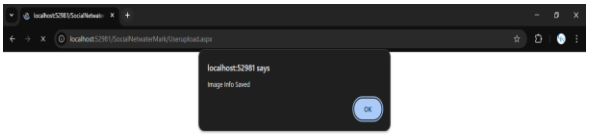

Fig. 16: Friend Request and Access Control

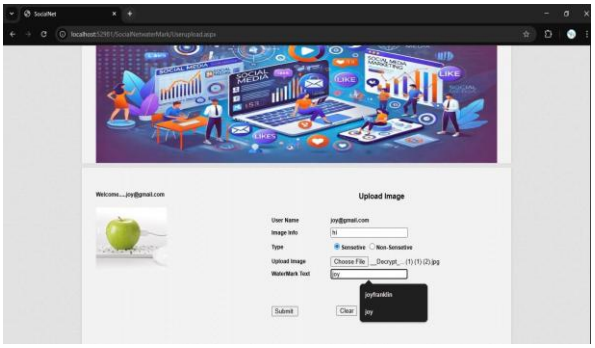

Fig. 17: Notification / Alert System

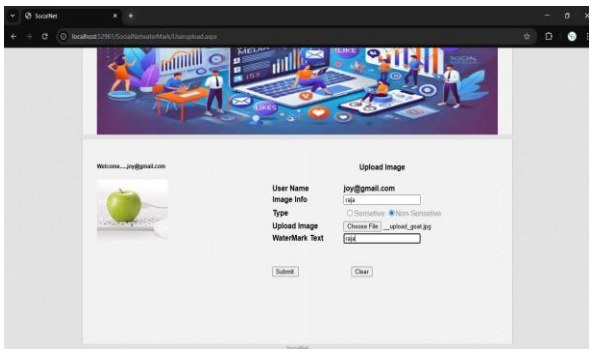

Fig. 18: Download Protection – Watermarked Output

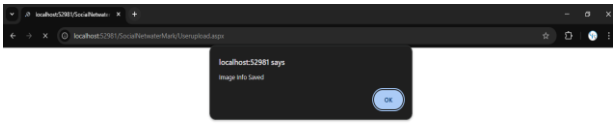

Fig. 19: Screenshot Blocking in Action

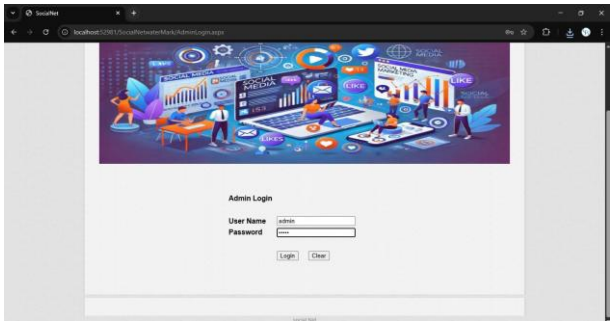

Fig. 20: Admin Dashboard – Upload Info

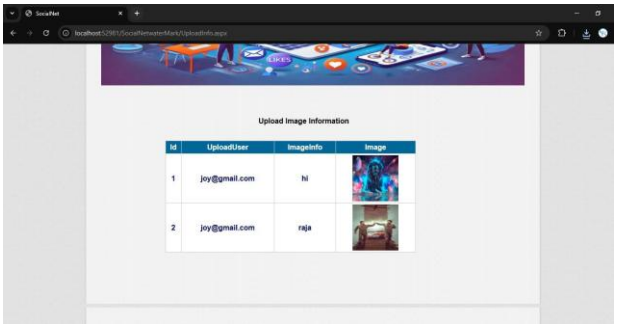

Fig. 21: Blockchain Record Verification

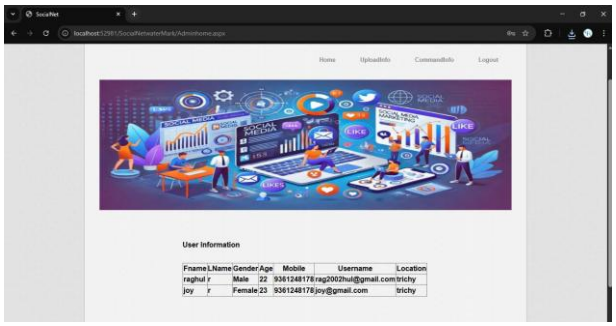

Fig. 22: Comment Analysis and Negative Block Module

IX. CONCLUSION

This study presents a holistic approach to image privacy on social networks, addressing both the technical and practical dimensions of the problem. By combining wavelet-SVD watermarking, steganographic embedding, and blockchain-based audit trails, the system delivers ownership verification, content secrecy, and transaction immutability within a single integrated platform.

The multilayer architecture ensures that no single point of failure can compromise the overall security of the protected image. Anti-screenshot controls and download restrictions add a physical-layer dimension that is absent from existing platform solutions. Empirical testing confirmed the effectiveness of the proposed system against common attack scenarios while maintaining acceptable image quality and system responsiveness.

Looking ahead, the integration of AI-driven content classifiers, adaptive watermarking strength, and smart-contract-based licensing can further extend the framework's capabilities, enabling it to serve as a comprehensive digital rights management solution for the evolving social media landscape.

REFERENCES

[1] Li, Fenghua, et al. "Hideme: Privacy-preserving photo sharing on social networks." IEEE INFOCOM 2019. IEEE, 2019.
[2] Aljabri, Malak, et al. "Machine learning-based social media bot detection: a comprehensive literature review." Social Network Analysis and Mining 13.1 (2023): 20.
[3] Xu, Shouzhi, et al. "Rumor detection on social media using hierarchically aggregated feature via graph neural networks." Applied Intelligence 53.3 (2023): 3136–3149.
[4] Golam, Abdullah, and Umar Albalawi. "Invisible Boundaries: Balancing Image Metadata Privacy with Forensic Imperatives." International Journal on Information Technologies & Security 16.4 (2024).
[5] Zhang, Chi, et al. "Privacy and security for online social networks: challenges and opportunities." IEEE Network 24.4 (2010): 13–18.
[6] Zulfahmi, Muhammad, et al. "Privacy protection strategies on social media." Procedia Computer Science 216 (2023): 471–478.
[7] Wang, Kun, Xiaofeng Wang, and Xuan Lu. "POI recommendation method using LSTM-attention in LBSN considering privacy protection." Complex & Intelligent Systems 9.3 (2023): 2801–2812.
[8] Ravi, Siddharth, Pau Climent-Pérez, and Francisco Flórez-Revuelta. "A review on visual privacy preservation techniques for active and assisted living." MultimediaTools and Applications 83.5 (2024): 14715–14755.
[9] Huang, Yan, Yi Joy Li, and Zhipeng Cai. "Security and privacy in metaverse: A comprehensive survey." Big Data Mining and Analytics 6.2 (2023): 234–247.
[10] Khalid, Nazish, et al. "Privacy-preserving artificial intelligence in healthcare: Techniques and applications." Computers in Biology and Medicine 158 (2023): 106848.