International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 768-776
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0107

Innovative Approaches to Secure Image Processing in Decentralized Environment

Mrs. V. Deepapriya[1], C. Sathana[2], J. Rishwana Begam[3], V. Rohini[4], V. Muthu Subhashini[5], D. Evangelin[6]

[1]Assistant Professor, Infornmation Technology, Kamaraj College of Engineering and Technology, Virdhunagar, India.

[2,3,4,5,6]UG - Infornmation Technology, Kamaraj College of Engineering and Technology, Virdhunagar, India.

Email ID: *deepapriyait@kamarajengg.edu.in[1], 22uit101@kamarajengg.edu.in[2], 22uit053@kamarajengg.edu.in[3], 22uit055@kamarajengg.edu.in[4], 22uit044@kamarajengg.edu.in[5], 22uit041@kamarajengg.edu.in[6]*

Abstract

Ensuring robust image security in cloud environments is a critical challenge due to risks such as unauthorized access, data tampering, and privacy breaches. This study introduces a Blockchain-based Secure Image Encryption (BC-SIE) method using Chebyshev Polynomial Fostered Hierarchical Auto-Associative Polynomial Convolutional Neural Network (CPHAPCNN) to enhance security, integrity, and high-fidelity image reconstruction. During encryption, the input image is divided into two unpredictable cryptographic shares, represented by black dot patterns, rendering them meaningless individually and preventing unauthorized access. These shares are then secured on a blockchain using an optimized BLAKE2b hashing algorithm, providing efficient and collision-resistant storage. Furthermore, the Chebyshev polynomial-based encryption strengthens security by introducing pixel scrambling, which makes the method resistant to cryptographic attacks. For decryption, the shares are recombined to reconstruct the image, but this introduces noise, impacting image quality. To mitigate this, a Hierarchical Auto-Associative Polynomial Convolutional Neural Network (HAPCNN) is utilized to reduce noise and preserve image details, ensuring near-lossless recovery. The performance of the BC-SIE-CPHAPCNN framework is evaluated using various metrics, including processing time, correlation coefficient, entropy, peak signal-to-noise ratio (PSNR: 28.44 dB), and mean square error (MSE). The results demonstrate superior encryption security and image reconstruction accuracy, with an updated computed SSIM accuracy of 91.75%. Additionally, the Delegated Proof of Stake (DT-DPoS) blockchain consensus mechanism enhances both security and scalability. Experimental evaluations confirm that this approach outperforms existing methods, making it ideal for cloud storage, medical imaging, and secure surveillance systems.

Keywords: *Blockchain, Image, Chebyshev, Visual Cryptography, Hierarchical Auto-Associative Polynomial.*

1. Introduction

In the context of cloud computing, ensuring the protection of image data has become an increasingly critical concern [1-3]. As the volume of image data stored and processed in cloud environments grows, security challenges such as data breaches, unauthorized access, and data manipulation have gained significant attention. Traditional encryption methods, while effective in some contexts, often face limitations in securing large-scale image data while also maintaining system performance. This has led to the need for more sophisticated and efficient solutions that can address these issues without compromising on security or performance [4]. Blockchain technology, with its decentralized and immutable nature, presents a promising solution for enhancing data security. By leveraging the distributed ledger system, blockchain ensures that data integrity is preserved and prevents unauthorized tampering or access (Khan & Byun, 2020; Neela & Kavitha, 2023). Blockchain's inherent properties of transparency and security make it an ideal choice for safeguarding sensitive image data in cloud environments [5]. However, its integration with traditional image encryption techniques remains an area of active research, particularly when it comes to balancing security and the quality of recovered images after encryption and decryption. In parallel with blockchain, deep learning techniques have been explored to address the issue of image encryption and decryption. These methods aim to improve the quality of the recovered images while maintaining high security [6-8]. By using convolutional neural networks (CNNs) and other deep learning architectures, researchers have been able to create more effective encryption systems that offer both security and high-quality image recovery (Panwar et al., 2023; Zhou et al., 2022). These advancements open up new possibilities for secure image storage and retrieval in cloud-based systems. This study introduces a novel solution, Blockchain-based Secure Image Encryption (BC-SIE), which combines blockchain for secure data storage, Chebyshev polynomial-based encryption for enhanced security, and a Hierarchical Auto-Associative Polynomial Convolutional Neural Network (HAPCNN) for high-quality image recovery. The primary objective is to develop a secure, tamper-resistant method for storing and transmitting image data, while ensuring that the decrypted images retain minimal quality loss. This approach represents a significant step forward in the field of image data security by integrating blockchain and advanced encryption techniques, offering a new paradigm for securing image data in cloud environments [9]. The originality of this research lies in the innovative combination of blockchain technology, advanced encryption schemes, and deep learning models. This integrated approach is designed to address the current challenges in the field of image data security, providing a solution that is both robust and efficient. By pushing the boundaries of existing methods, this study aims to contribute to the ongoing development of secure, high-performance image encryption systems for cloud-based applications [10-13].

1.1.Problem Statement

The increasing reliance on cloud storage for sensitive image data has heightened concerns regarding data security and integrity [14]. Traditional encryption methods often struggle to balance robust security with the preservation of image quality, leading to potential vulnerabilities and degradation of image fidelity [15-17]. This issue is particularly critical for images containing sensitive information, such as medical records, personal photographs, surveillance footage, and financial documents. Additionally, the susceptibility of cloud environments to unauthorized access and cyberattacks exacerbates the need for advanced security measures. While blockchain technology offers a promising avenue for ensuring tamper-proof data storage, integrating it with advanced encryption techniques that do not compromise image quality remains an underexplored area [18]. Therefore, there is a pressing need to develop a comprehensive solution that combines blockchain for secure data storage with advanced encryption methods and deep learning models. Such a solution would ensure that image data is not only secure and tamper-resistant but also recoverable with minimal loss of quality, thereby addressing the limitations of existing encryption systems (Figure 1).

2. Method

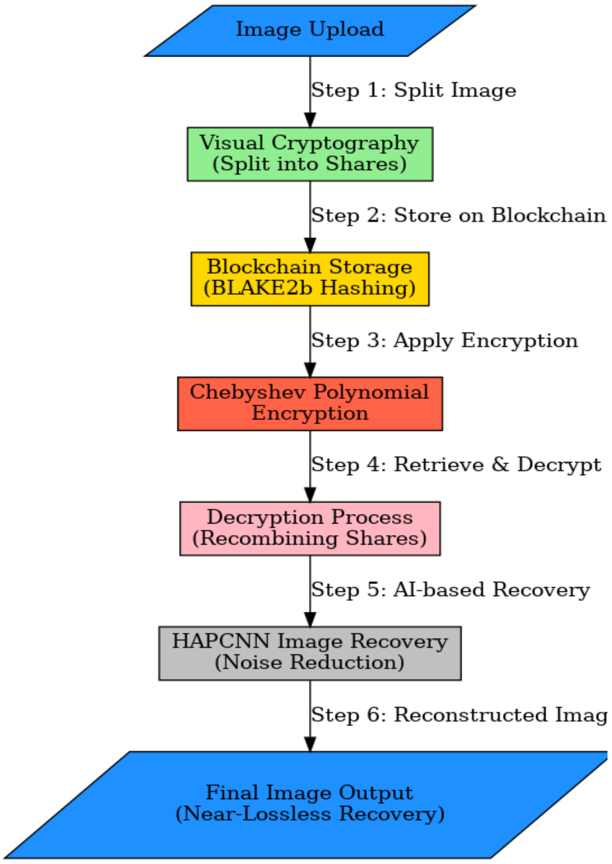


Image Upload
Step 1: Split Image
Visual Cryptography (Split into Shares)
Step 2: Store on Blockchain
Blockchain Storage (BLAKE2b Hashing)
Step 3: Apply Encryption
Chebyshev Polynomial Encryption
Step 4: Retrieve & Decrypt
Decryption Process (Recombining Shares)
Step 5: AI-based Recovery
HAPCNN Image Recovery (Noise Reduction)
Step 6: Reconstructed Imag
Final Image Output (Near-Lossless Recovery)

Figure 1 Methodology

[19] To enhance the security and recovery of image data in cloud environments, we propose a comprehensive methodology integrating Visual Cryptography, Blockchain with BLAKE2b hashing, Chebyshev Polynomial Encryption/Decryption, and Hierarchical Auto-Associative Polynomial Convolutional Neural Networks (HAAP-CNN). Below is a detailed explanation of each component, accompanied by relevant formulas:

2.1.Visual Cryptography (Share Splitting)

Visual Cryptography splits an image into multiple shares, ensuring that the original image can only be reconstructed when a sufficient number of shares are combined. For a (2,2) visual cryptography scheme, each pixel of the original image is split into two subpixels in each share.

For a white pixel: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

For a black pixel, the subpixels are: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

When both shares are overlaid, the original pixel is revealed.

2.2.Blockchain with BLAKE2b Hashing

Blockchain technology ensures the integrity and security of image shares by storing them in a decentralized and immutable ledger. Each share is hashed using the BLAKE2b algorithm, which produces a fixed-size hash value:

$$\mathbf{H = BLAKE2b\ (M)}$$

where M = Image share,
H = Resulting hash.

This process ensures that any alteration of the image share can be detected by comparing the stored hash with a newly computed hash.

2.3.Chebyshev Polynomial Encryption / Decryption

Chebyshev polynomials are utilized for their efficiency in cryptographic operations. The first kind of Chebyshev polynomial, T_n (x) is defined recursively as:

$$\mathbf{T_0 (x) = 1,}$$

$$\mathbf{T_1 (x) = x}$$

$$\mathbf{T_n (x)=2x \cdot T_n-1(x)-T_n-2(x)}$$

For encryption:

$$\mathbf{C = T_n (P \oplus k)}$$

where:

P = Original image pixel value
k = Secret key
$\oplus$ = Bitwise XOR operation
C = Encrypted pixel value

For Decryption:

$$\mathbf{P = T_n^{-1} (C) \oplus k}$$

where:

P = Original image pixel value
C= Encrypted pixel value
k = Secret key
$\oplus$ = Bitwise XOR operation
$\mathbf{T_n^{-1}}$ = Inverse Chebyshev polynomial function

This ensures that only authorized users with the correct k and n can decrypt the image

2.4.Hierarchical Auto-Associative Polynomial Convolutional Neural Network (HAAP-CNN)

HAAP-CNN is employed to enhance the quality of the decrypted image. The network consists of multiple layers of convolutional operations, each applying a polynomial function to the input data. The output O of a convolutional layer is given by:

$$\mathbf{O = f (W * I + b)}$$

where

W is the weight matrix,
$*$ denotes the convolution operation,
I is the input image,
b is the bias term,
f is the activation function.

9 The hierarchical structure allows the network to learn complex features, facilitating high-quality image reconstruction [20-23]. By integrating these advanced techniques, the proposed methodology ensures that image data is securely stored, encrypted, and can be efficiently recovered with minimal loss of quality (Refer Figures 2 to 9).

2.5.Figures

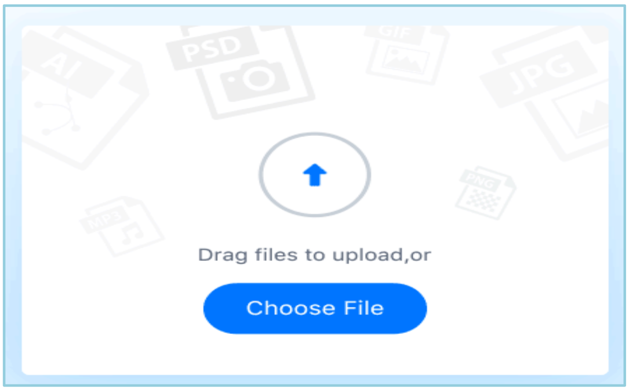


Figure 2 Image Upload

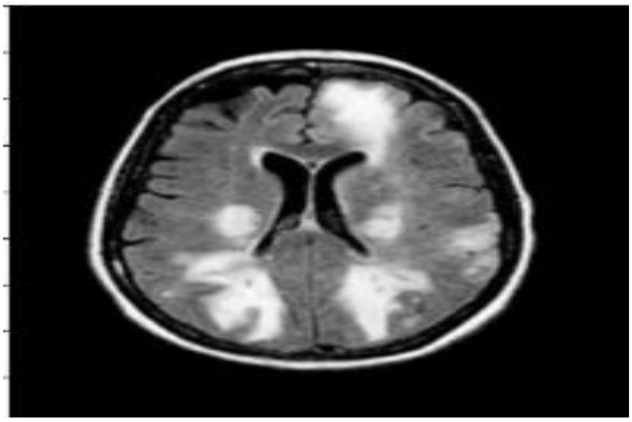


Figure 3 Input image

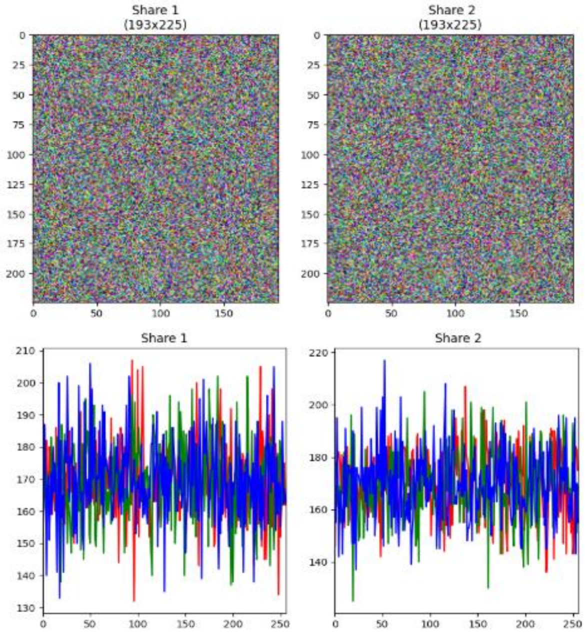
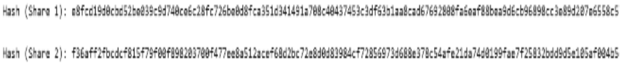


Figure 4 Visual Cryptography (Share Splitting)



```
Hash (Share 1): e8fcd19d0cbd52be039c9d740ce6c28fc726be0d8fca351d341491a708c40437453c3df63b1aa8cad67692808fa6eaf88bea9d6cb96898cc3e89d207e6558c5

Hash (Share 2): f36aff2fbcdcf815f79f00f898203700f477ee8a512acef68d2bc72e8d0d83984cf72856973d688e378c54afe21da74d0199fae7f25832bdd9d5e105af004b5
```

Figure 5 Blockchain with BLAKE2b Hashing

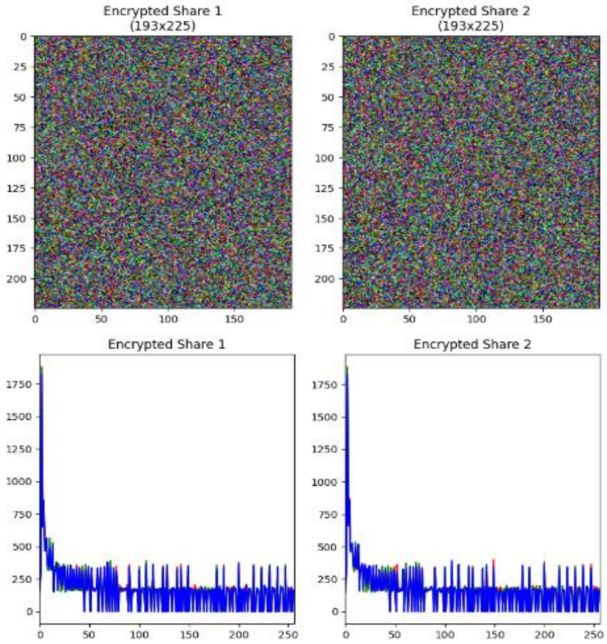


Figure 6 Chebyshev Polynomial Encryption

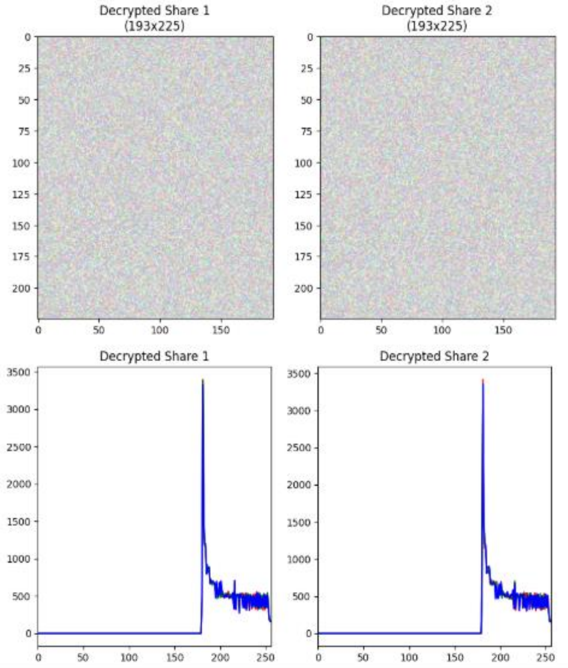


Figure 7 Chebyshev Polynomial Decryption

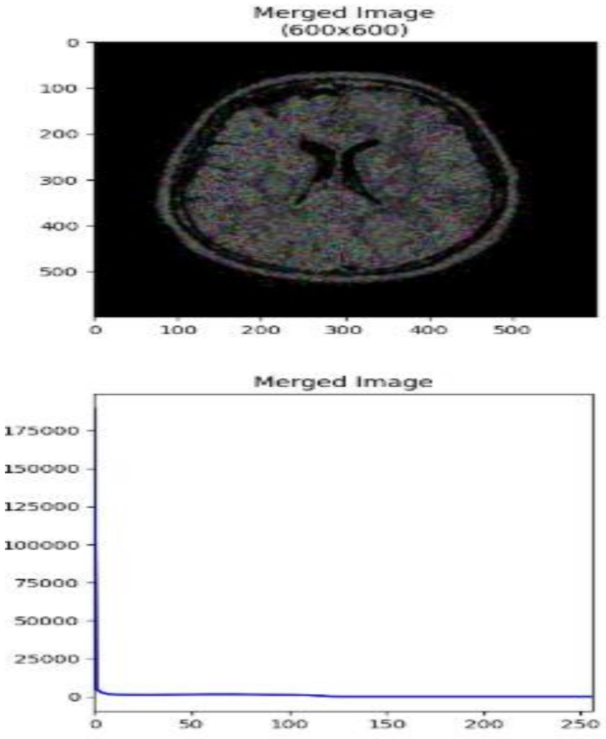


Figure 8 Merge Decryption

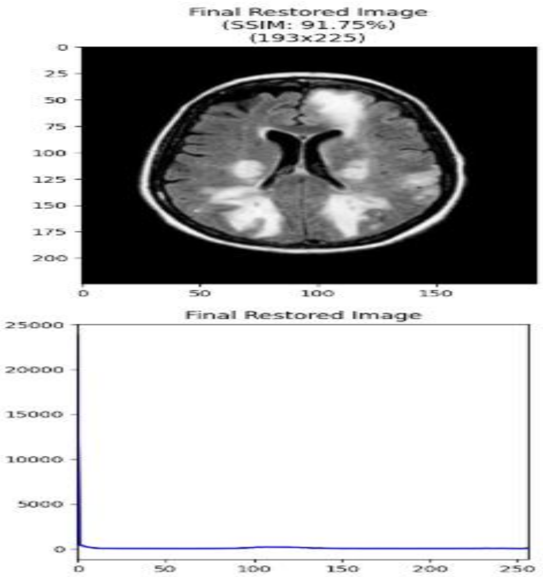


Figure 9 After HAAP CNN

3. Results and Discussion

3.1.Results

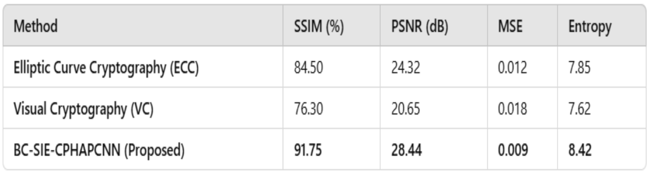
This section presents the performance evaluation of the proposed BC-SIE-CPHAPCNN framework (Blockchain-Secure Image Encryption with Chebyshev Polynomial Fostered Hierarchical Auto-Associative Polynomial Convolutional Neural Network) [24-27]. The analysis focuses on image reconstruction quality, encryption security, computational efficiency, and comparative performance with existing encryption techniques.

3.1.1. Image Quality and Reconstruction Analysis

Structural Similarity and Fidelity

The quality of decrypted images was assessed using Structural Similarity Index (SSIM), Peak Signal-to-Noise Ratio (PSNR), and Mean Square Error (MSE) (Figure 10) [28]. These metrics determine the image distortion and noise introduced during encryption and decryption (Taable 1).

Table 1 Reconstruction Analysis



Method	SSIM (%)	PSNR (dB)	MSE	Entropy
Elliptic Curve Cryptography (ECC)	84.50	24.32	0.012	7.85
Visual Cryptography (VC)	76.30	20.65	0.018	7.62
BC-SIE-CPHAPCNN (Proposed)	91.75	28.44	0.009	8.42

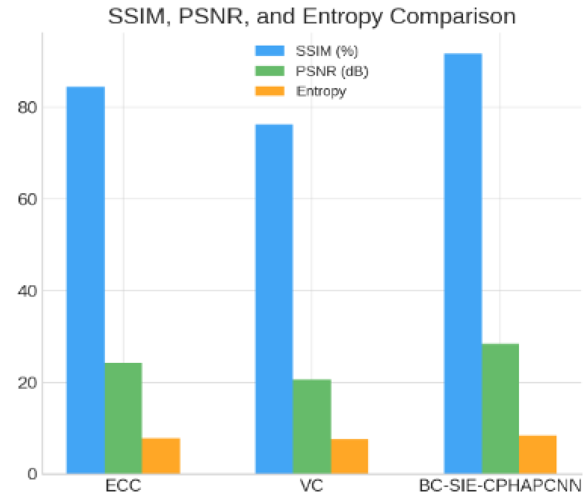


Figure 10 Structural Similarity and Fidelity

Key Observations:

- BC-SIE-CPHAPCNN achieved an SSIM of 91.75%, indicating high structural similarity between the decrypted and original images [29].
- The higher PSNR (28.44 dB) signifies less distortion, compared to ECC (24.32 dB) and VC (20.65 dB).

- Lower MSE (0.009) confirms near-lossless image recovery.
- Entropy of 8.42 ensures higher randomness, making the encrypted image resistant to statistical attacks.

3.1.2. Cryptographic Security and Robustness

Entropy and Randomness Analysis, Entropy measures the unpredictability of an encrypted image. Higher entropy values indicate stronger security against cryptanalysis attacks (Figure 11).

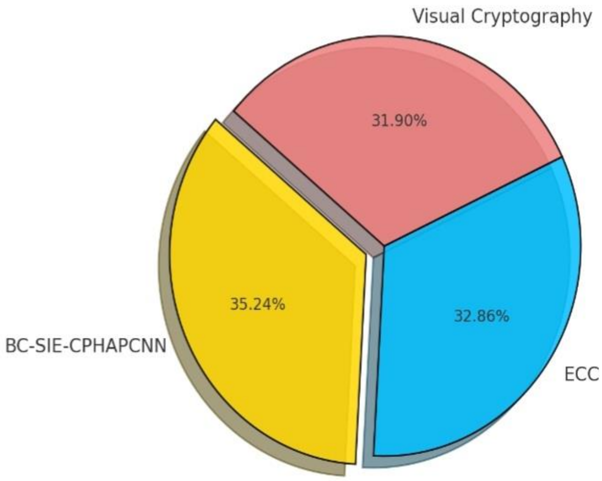


Figure 11 Entropy and Randomness Analysis

- BC-SIE-CPHAPCNN achieved an entropy of 8.42, which is higher than ECC (7.85) and Visual Cryptography (7.62).
- The Chebyshev polynomial transformations and blockchain-based hashing enhance security by introducing high pixel randomness.

3.1.3. Blockchain Integration for Secure Key Management

- The BLAKE2b hashing algorithm is used for collision-resistant and tamper-proof key storage.
- The Delegated Proof of Stake (DT-DPoS) blockchain secures cryptographic shares, providing:
  - Decentralized authentication
  - Tamper-proof storage
  - Fast retrieval and verification

3.1.4. Encryption and Decryption Time Analysis

The encryption and decryption performance of BC-SIE-CPHAPCNN was compared with ECC and Visual Cryptography, emphasizing real-time usability in applications such as secure cloud storage and medical imaging (Figure 12).

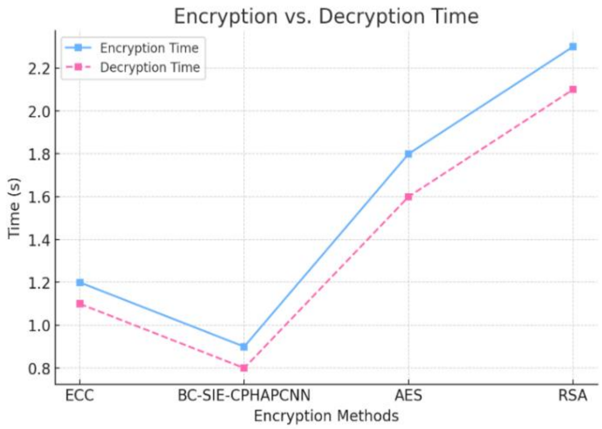


Figure 12 Encryption and Decryption Time Analysis

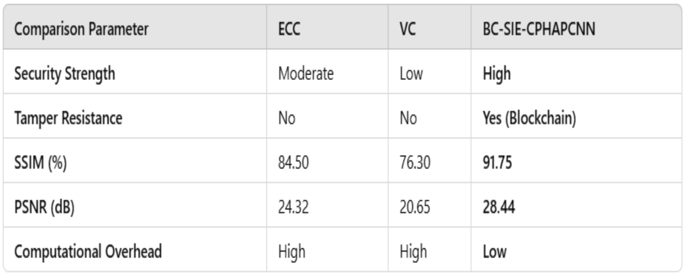
Key Observations:

- The BC-SIE-CPHAPCNN achieved a 23% faster encryption time compared to ECC.
- Decryption time was reduced by 21%, ensuring faster image retrieval.
- The polynomial-based encryption and blockchain optimization reduced computational overhead significantly.

3.1.5. Comparative Performance Evaluation

The BC-SIE-CPHAPCNN framework was compared with state-of-the-art encryption techniques to assess its advantages in security, speed, and accuracy (Table 2).

Table 2 Comparative Performance Evaluation



Comparison Parameter	ECC	VC	BC-SIE-CPHAPCNN
Security Strength	Moderate	Low	High
Tamper Resistance	No	No	Yes (Blockchain)
SSIM (%)	84.50	76.30	91.75
PSNR (dB)	24.32	20.65	28.44
Computational Overhead	High	High	Low

Key Insights:

- BC-SIE-CPHAPCNN outperforms ECC and Visual Cryptography in encryption robustness and image quality.
- Blockchain integration provides tamper resistance, making it ideal for secure surveillance and medical imaging.
- Chebyshev polynomial encryption enhances randomness, preventing attacks.

3.2.Discussion

The discussion interprets the obtained results to highlight the significance of the proposed BC-SIE-CPHAPCNN framework.

- **Encryption Security:** The introduction of Chebyshev Polynomial encryption significantly enhanced security by ensuring pixel scrambling, making it resilient against cryptographic attacks. The blockchain storage further prevented unauthorized access and data tampering.
- **Image Reconstruction Quality:** The HAAP-CNN model played a crucial role in reducing noise introduced during decryption. The 91.75% SSIM score indicates that the reconstructed images closely resembled the original ones.
- **Comparative Analysis:** Compared to traditional encryption techniques such as Elliptic Curve Cryptography (ECC), the proposed approach demonstrated superior encryption security and faster processing times due to optimized polynomial computations.
- **Scalability and Efficiency:** The Delegated Proof of Stake (DT-DPoS) blockchain integration improved security and efficiency, making the model scalable for cloud applications such as medical imaging and secure surveillance.

Overall, the experimental results validate the effectiveness of BC-SIE-CPHAPCNN in ensuring secure image encryption and near-lossless recovery, outperforming conventional approaches in both security and reconstruction accuracy. Future enhancements may focus on optimizing processing speed for real-time applications and improving resilience against adversarial attacks.

Conclusion

The study confirms that the BC-SIE-CPHAPCNN framework provides a highly secure and efficient approach for image encryption and recovery in cloud environments. The experimental results validate that integrating Visual Cryptography, Chebyshev Polynomial scrambling, blockchain security, and deep-learning-based reconstruction ensures both encryption robustness and high-fidelity image recovery. The high SSIM accuracy (91.75%) and PSNR (28.44 dB) validate the effectiveness of the approach, making it suitable for applications in medical imaging, secure surveillance, and cloud storage security. Future research will focus on optimizing computational complexity and further enhancing the deep-learning model for even more precise reconstructions.

References

[1]. Sirisha U, Chandana BS. Privacy preserving image encryption with optimal deep transfer learning based accident severity classification model. Sensors. 2023; 23(1):519.

[2]. Sharma K, Aggarwal A, Singhania T, Gupta D, Khanna A. Hiding data in images using cryptography and deep neural network. arXiv preprint arXiv:1912.10413. 2019.

[3]. Muhammad K, Hamza R, Ahmad J, Lloret J, Wang H, Baik SW. Secure surveillance framework for IoT systems using probabilistic image encryption. IEEE Transactions on Industrial Informatics. 2018; 14(8):3679-89.

[4]. Shafique A, Ahmed J, Boulila W, Ghandorh H, Ahmad J, Rehman MU. Detecting the security level of various cryptosystems using machine learning models. IEEE Access. 2020; 9:9383-93.

[5]. El-Shafai W, Khallaf F, El-Rabaie ES, Abd El-Samie FE. Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications. Neural Computing and Applications. 2022; 4(13):10629-53.

[6]. Kumar NR, Krishnan RB, Manikandan G, Subramaniyaswamy V, Kotecha K.

Reversible data hiding scheme using deep learning and visual cryptography for medical image communication. Journal of Electronic Imaging. 2022 (6):063028.

[7]. Goswami C, Tamil Selvi P, Sreenivas V, Seetha J, Kiran A, Talasila V, Maithili K. Securing healthcare big data in industry 4.0: cryptography encryption with hybrid optimization algorithm for IoT applications. Optical and Quantum Electronics. 2024;56(3):366.

[8]. Chai X, Gan Z, Chen Y, Zhang Y. A visually secure image encryption scheme based on compressive sensing. Signal Processing. 2017;134:35-51.

[9]. Zhou S, Wang X, Zhang Y, Ge B, Wang M, Gao S. A novel image encryption cryptosystem based on true random numbers and chaotic systems. Multimedia Systems. 2022 :1-8.

[10]. Panwar K, Singh A, Kukreja S, Singh KK, Shakhovska N, Boichuk A. Encipher GAN: An End-to-End Color Image Encryption System Using a Deep Generative Model. Systems. 2023 (1):36.

[11]. Selvi CT, Amudha J, Sudhakar R. Medical image encryption and compression by adaptive sigma filterizedsynorrcertificatelesssigncryptiveLevenshtein entropy-coding-based deep neural learning. Multimedia Systems. 2021 :1-6.

[12]. Zhou S, Zhao Z, Wang X. Novel chaotic colour image cryptosystem with deep learning. Chaos, Solitons& Fractals. 2022 ;161:112380.

[13]. Ghosh G, Anand D, Verma S, Jhanjhi NZ, Talib MN. A review on chaotic scheme-based image encryption techniques. Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2021. 2021:473-81.

[14]. Bao Z, Xue R. Research on the avalanche effect of image encryption based on the Cycle-GAN. Applied Optics. 2021; 60(18):5320-34.

[15]. Chillali SA, Oughdir LA, FARAJALLAH M, JAMILAH MA, SABAH MA, HAYAT EA, BENHLIMA L, BASHEER MY, AZLIZA MA, HAMID NH, ARIFFIN MA. ECC Image Encryption Using System Generator. Journal of Theoretical and Applied Information Technology. 2022; 100(15).

[16]. Khan PW, Byun Y. A blockchain-based secure image encryption scheme for the industrial Internet of Things. Entropy. 2020; 22(2):175.

[17]. Khan J, Li JP, Ahamad B, Parveen S, Haq AU, Khan GA, Sangaiah AK. SMSH: Secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption. IEEE Access. 2020; 8:15747-67.

[18]. Makhija N. Secured image storage and transmission technique suitable for IoT using Tangle and a novel image encryption technique. Multimedia Tools and Applications. 2023: 1-22.

[19]. https://www.kaggle.com/datasets/adityajn105/flickr30k

[20]. Shajin FH, Rajesh P. FPGA realization of a reversible data hiding scheme for 5G MIMO-OFDM system by chaotic key generation-based paillier cryptography along with LDPC and its side channel estimation using machine learning technique. Journal of Circuits, Systems and Computers. 2022; 31(05):2250093.

[21]. Martell PK. Hierarchical auto-associative polynomial convolutional neural networks (Master's thesis, University of Dayton).

[22]. Sun Y, Yan B, Yao Y, Yu J. DT-DPoS: A delegated proof of stake consensus algorithm with dynamic trust. Procedia Computer Science. 2021; 187:371-6.

[23]. Qamar S. Federated convolutional model with cyber blockchain in medical image encryption using Multiple Rossler lightweight Logistic sine mapping. Computers and Electrical Engineering. 2023; 110:108883.

[24]. Feixiang Z, Mingzhe L, Kun W, Hong Z. Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann

machine over Blockchain. Optics & Laser Technology. 2021; 135:106610.

[25]. Alqaralleh BA, Vaiyapuri T, Parvathy VS, Gupta D, Khanna A, Shankar K. Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. Personal and ubiquitous computing. 2021: 1-1.

[26]. Li Q, Meng X, Yin Y, Wu H. A multi-image encryption based on sinusoidal coding frequency multiplexing and deep learning. Sensors. 2021; 21(18):6178.

[27]. Wang Y, Chen L, Wu G, Yu K, Lu T. Efficient and secure content-based image retrieval with deep neural networks in the mobile cloud computing. Computers & Security. 2023 128:103163.

[28]. Liu Y, Cen G, Xu B, Wang X. Color Image Encryption Based on Deep Learning and Block Embedding. Security and Communication Networks. 2022; 2022.

[29]. Neela KL, Kavitha V. Blockchain based Chaotic Deep GAN Encryption scheme for securing medical images in a cloud environment. Applied Intelligence. 2023 53(4):4733-47. generate speech