International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 04 | Apr 2026 www.irjet.net p-ISSN: 2395-0072

Secret Communication using multi Image steganography and face Recognition

Prof. R. K. Nale[1], Vaishnavi Dhumal[2], Vaishnavi Jagtap[3], Shantanoo Karad[4], Rohan Kambale[5]

[2,3,4,5] *Student, Department of IT Engineering, SVPM's College of Engineering, Malegaon BK, Maharashtra, India.*

[1] *Assistant Professor, Department of IT Engineering, SVPM'S College of Engineering Malegaon BK, Baramati, Maharashtra, India*

Abstract - *Secure communication over digital networks is a major concern due to increasing cyber threats, data breaches, and unauthorized access. Traditional methods like cryptography protect the content of messages but do not hide their existence, while single-image steganography systems are vulnerable to detection and data loss. To address these limitations, we developed a secure communication system using multi-image steganography, AES encryption, and face recognition authentication. The system first encrypts the secret message using AES and then divides it into multiple parts for improved security. Each part is embedded into different images using the Least Significant Bit (LSB) technique, ensuring minimal visual distortion. The stego-images are transmitted securely through email communication. At the receiver side, face recognition is used to verify user identity before extracting the hidden data. The system then reconstructs and decrypts the message to obtain the original information. This approach improves confidentiality, reduces the risk of complete data exposure, and prevents unauthorized access. The system is efficient, secure, and suitable for applications such as military, banking, and confidential data sharing.*

Key Words: Multi-Image Steganography, Face Recognition, Biometric Authentication, Least Significant Bit (LSB).

1.INTRODUCTION

Secure communication has become an essential requirement in today's digital world due to the rapid growth of internet usage and online data exchange. Many organizations and individuals regularly share confidential information through digital platforms, which increases the risk of cyber-attacks, data breaches, and unauthorized access. Traditional security methods such as cryptography protect the content of the message by converting it into unreadable format, but they do not hide the existence of communication. As a result, encrypted messages can still attract attackers. Similarly, traditional single-image steganography systems hide secret information inside images, but they are vulnerable to steganalysis attacks and complete data loss if a single image is compromised.

As digital communication continues to grow, there is a need for a more secure and reliable communication system that can protect both the content and existence of sensitive information. To solve this problem, we developed a secure communication system using multi-image steganography, AES encryption, and face recognition authentication. The system first encrypts the secret message using AES and divides it into multiple parts for enhanced security. These message segments are hidden in multiple images using the Least Significant Bit (LSB) technique. The generated stego-images are securely shared through email communication. At the receiver side, face recognition authentication verifies the identity of the user before extracting the hidden message. This system improves confidentiality, prevents unauthorized access, and provides a secure and efficient solution for military, banking, healthcare, and government communication systems.

2.Problem Statement

The development of secure communication systems is essential due to increasing cyber threats and data breaches. Traditional cryptography protects message content but cannot hide the existence of communication. Single-image steganography is vulnerable to detection and complete data exposure. This project develops a secure system using multi-image steganography, AES encryption, and face recognition authentication. The system ensures secure data transmission and prevents unauthorized access to confidential information.

3.Literature Survey

In recent years, secure communication has become an important research area due to increasing cyber threats, data breaches, and unauthorized access. Traditional cryptography protects message content but cannot hide the existence of communication. Similarly, single-image steganography is vulnerable to detection and complete data exposure. Researchers have introduced advanced techniques such as multi-image steganography, AES encryption, and biometric authentication to improve security. Face recognition has also been widely used to restrict unauthorized access. These studies provide the foundation for developing the proposed secure communication system.

4. MOTIVATION

The rapid growth of internet communication and digital data exchange has increased the demand for secure communication systems. Sensitive information shared through online platforms is often exposed to cyber-attacks, hacking, and unauthorized access. Traditional security methods such as cryptography and single-image steganography provide limited protection and may fail against modern attacks. The proposed system is motivated by the need to develop a more secure and reliable communication platform using multi-image steganography, AES encryption, and face recognition authentication.

A. Preventing Cyber Threats and Data Breaches

With the increasing use of digital communication platforms, confidential information is frequently transmitted over public networks. Hackers and attackers can intercept messages, leading to data breaches and misuse of sensitive information. Traditional communication systems often lack strong protection mechanisms. This project aims to reduce cyber risks by implementing multiple security layers for safe communication.

B. Enhancing Data Confidentiality

Traditional encryption techniques protect message content but cannot hide the existence of communication. Similarly, single-image steganography may expose the complete message if one image is compromised. The proposed system uses multi-image steganography to divide and hide the secret message across multiple images, reducing the chances of complete data exposure and improving confidentiality.

C. Preventing Unauthorized Access

Many existing communication systems do not verify the identity of users before allowing access to confidential data. This creates a high risk of unauthorized message extraction. To solve this issue, the proposed system integrates face recognition authentication, ensuring that only authorized users can access and retrieve hidden information. The system verifies the receiver's identity before message extraction, adding an extra layer of biometric security. This helps prevent unauthorized users from accessing sensitive data and improves overall system protection.

D. Secure Message Transmission

Transmitting confidential data through normal communication channels can attract attackers. The proposed system securely sends stego-images through email communication, where hidden messages remain invisible to third parties. This ensures safe and reliable data transfer between sender and receiver. Since the message is hidden inside images, attackers cannot easily detect the presence of confidential information during transmission. This approach improves communication security and reduces the risk of data interception or unauthorized access.

E. Improving Security and Reliability

Modern communication systems require multiple layers of protection to ensure complete security. By combining AES encryption, LSB steganography, multi-image segmentation, and biometric authentication, the proposed system improves reliability, reduces security risks, and provides a practical solution for military, banking, healthcare, and government communication applications. The integration of multiple security techniques makes the system more robust against cyber-attacks and steganalysis threats. It also ensures secure communication while maintaining efficiency, scalability, and ease of implementation.

5. System Architecture

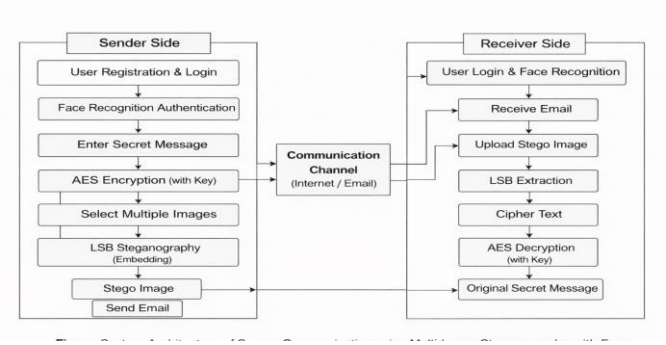


Fig 1: System Architecture

1. User Registration & Authentication: Users securely register and log in using email, password, and face recognition to access the communication system.

2. Enter Secret Message: The sender enters confidential information that needs to be transmitted securely to the receiver.

3. AES Encryption & Multi-Image Steganography: The secret message is encrypted using AES and hidden inside multiple selected images using the LSB technique.

4. Secure Transmission: The generated stego-images are sent through email or internet communication channels for secure data transfer.

5.Message Extraction & Decryption: The receiver uploads the stego-image, extracts hidden data using LSB extraction, and decrypts it using AES to retrieve the original secret message.

6.Proposed Algorithms

Algorithm 1: AES Encryption Algorithm

AES (Advanced Encryption Standard) is a widely used symmetric key encryption algorithm designed to secure sensitive information during digital communication. It converts readable plain text into unreadable cipher text using a secret encryption key, ensuring that unauthorized users cannot understand the message even if it is intercepted. AES

performs multiple rounds of substitution, permutation, and key transformation to provide strong protection against cyber-attacks such as brute-force attacks and data interception. In the proposed system, the sender first enters the secret message, which is encrypted using AES before the steganography process begins. The encrypted cipher text is then divided and embedded into multiple images using LSB steganography. At the receiver side, the same secret key is required for AES decryption to recover the original message. This algorithm adds an extra layer of security and improves confidentiality in secure communication.

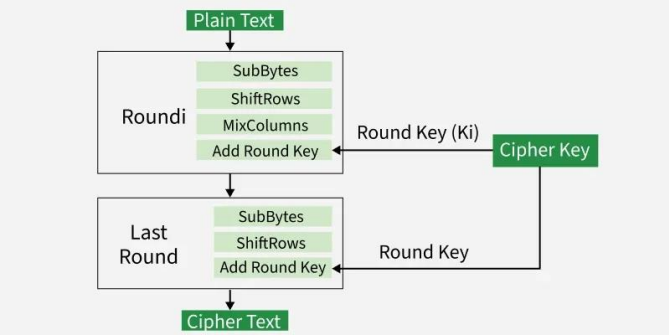


Fig -2: AES Encryption Algorithm

Explanation of AES Encryption Algorithm:

1. Input Plain Text:
The sender enters the original secret message (plain text) that needs to be protected.

2. Round Key Generation:
A secret encryption key is generated and divided into multiple round keys for encryption.

3. Sub Bytes Operation:
In this step, each byte of plain text is replaced with another byte using substitution to increase security.

4. Shift Rows and Mix Columns:
The rows are shifted and columns are mixed to rearrange the data and make encryption stronger.

5. Add Round Key:
The transformed data is combined with the generated round key during each round of encryption.

6. Generate Cipher Text:
After completing all rounds, the final encrypted output is produced as cipher text, which is used for secure communication.

Algorithm 2: LSB Steganography Algorithm

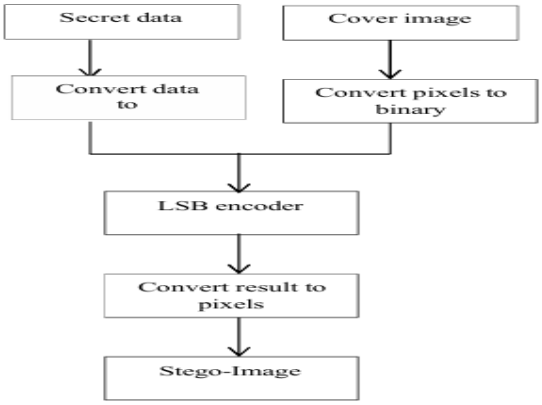


Fig -3: LSB Steganography Algorithm

1.Input Secret Data:
The secret message or encrypted cipher text is taken as input for hiding.

2.Convert Data to Binary:
The secret message is converted into binary format for embedding.

3.Select Cover Image:
A cover image is selected to hide the secret data.

4.Convert Pixels to Binary:
The pixel values of the cover image are converted into binary form.

5.LSB Encoding Process:
The binary secret data is embedded into the least significant bits of image pixels.

6.Generate Stego Image:
The modified pixels are converted back into image format, producing the final stego-image containing hidden data.

Algorithm 3: Face Recognition Algorithm:

1.Input Face Image: The user uploads a face image or captures a live image using a webcam.

2.Face Detection: The system detects the face from the uploaded image using image processing techniques.

3.Image Preprocessing: The detected face is resized, normalized, and cleaned for better recognition accuracy.

4.Feature Extraction: Important facial features are extracted using face recognition models such as Deep Face/CNN.

5.Face Matching: The extracted features are compared with stored user face data in the database.

6.Authentication Result: If the face matches successfully, the user is authenticated and allowed to access message extraction. Otherwise, access is denied.

Algorithm 4: Data Extraction and Message Reconstruction Algorithm

1. Upload Stego Image: The receiver uploads the stego-image that contains the hidden encrypted message.

2. LSB Extraction: The system reads the image pixels and extracts the hidden binary data from the least significant bits.

3. Recover Cipher Text: The extracted binary data is converted back into encrypted cipher text format.

4. Message Reconstruction: If the message is divided into multiple images, all extracted parts are combined to reconstruct the complete cipher text.

5. AES Decryption: The reconstructed cipher text is decrypted using the correct secret key.

6. Display Original Message: The system retrieves and displays the original secret message to the authorized receiver.

I. Accuracy

• AES Algorithm: AES provides very high encryption accuracy by converting plain text into secure cipher text using multiple encryption rounds. It ensures strong confidentiality and protects sensitive information from unauthorized access, brute-force attacks, and data interception.
• LSB Steganography Algorithm: LSB offers high accuracy in hiding encrypted data inside image pixels without significantly affecting image quality. It ensures that hidden messages remain invisible to human eyes while maintaining proper embedding efficiency.
• Face Recognition Algorithm: Face recognition provides high authentication accuracy by detecting facial features and matching them with stored user data. It reduces unauthorized access and improves biometric security for secure message extraction.
• Data Extraction and Message Reconstruction Algorithm: This algorithm ensures accurate extraction of hidden cipher text from stego-images and successfully reconstructs the original message without data corruption. It improves reliability during the decryption process.

II. Computational Complexity

• AES Algorithm: AES has moderate computational complexity because it performs multiple rounds of encryption operations such as substitution, shifting, mixing, and key generation. However, it provides strong security with efficient performance.

• LSB Steganography Algorithm**:** LSB has low computational complexity because it only modifies the least significant bits of image pixels. It requires minimal processing time and is easy to implement.

• Face Recognition Algorithm**:** Face recognition has moderate to high computational complexity due to face detection, feature extraction, and matching processes. The complexity increases when large facial databases are used.

• Data Extraction and Message Reconstruction Algorithm: This algorithm has moderate computational complexity because it involves extracting hidden data from multiple images, reconstructing message segments, and performing AES decryption to recover the original message.

III. Real-Time Performance

• AES Algorithm: AES provides high real-time performance because encryption and decryption processes are completed quickly, making it suitable for secure communication applications.

• LSB Steganography Algorithm: LSB offers good real-time performance since embedding secret data into image pixels requires less processing time and generates stego-images efficiently.

• Face Recognition Algorithm: Face recognition provides moderate real-time performance as face detection and authentication may require additional processing time depending on image quality and system hardware.

• Data Extraction and Message Reconstruction Algorithm: This algorithm offers moderate real-time performance because it involves extracting hidden data from multiple images and reconstructing the original message, which may take additional time for larger files.

IV. Generalization to New Data

• AES Algorithm: AES generalizes well for different types of text data and can securely encrypt various confidential messages regardless of message size.

• LSB Steganography Algorithm: LSB can work with different image formats such as PNG, JPG, and BMP, making it adaptable for various image-based communication systems.

• Face Recognition Algorithm: Face recognition generalizes well to multiple users by identifying different facial features, but performance may vary under poor lighting conditions or different facial angles.

• Data Extraction and Message Reconstruction Algorithm: This algorithm can efficiently extract and reconstruct hidden messages from different stego-images and supports various message sizes without affecting accuracy.

Conclusion: AES provides strong encryption security, LSB ensures secure data hiding with minimal image distortion,

face recognition enhances authentication, and message reconstruction guarantees accurate recovery of hidden information. The combination of these algorithms improves overall system security, reliability, and efficiency for secure communication applications.

7. METHODOLOGY

This research presents a secure communication system that integrates multi-image steganography, AES cryptographic encryption, and face recognition-based biometric authentication to protect confidential information transmitted over open networks. The proposed methodology follows a structured system architecture to perform user authentication, message encryption, segmentation, data embedding, secure transmission, biometric verification, data extraction, and message reconstruction in an efficient and reliable manner.

I. System Overview:

The system begins with the sender registering and logging into the application using email credentials and face authentication. After successful login, the sender enters a secret message that needs to be transmitted securely. To ensure confidentiality, the message is first encrypted using the Advanced Encryption Standard (AES) algorithm with a secret key. The encrypted message is then divided into multiple segments to improve security. Multiple cover images are selected, and each encrypted segment is embedded into different images using the Least Significant Bit (LSB) steganography technique. The generated stego-images are visually similar to original images and are transmitted through email communication channels.

II. Message Encryption and Segmentation:

Before data hiding, the secret message undergoes AES encryption to prevent unauthorized access. The AES algorithm converts readable plain text into unreadable cipher text using a secret key. The encrypted message is then segmented into multiple parts so that no single image contains the complete message. This significantly reduces the risk of complete data exposure if one image is compromised.

III. Multi-Image LSB-Based Data Embedding:

Each encrypted message segment is embedded into separate cover images using the LSB embedding technique. The algorithm modifies only the least significant bits of image pixels, which causes minimal visual distortion. This ensures that the hidden data remains invisible to attackers while maintaining image quality. The multi-image approach improves resistance against steganalysis attacks.

IV. Secure Transmission of Stego-Images:

After embedding, the generated stego-images are transmitted through email or internet communication channels. Since the images appear normal and do not reveal the existence of hidden information, the communication remains secure and covert. This stage ensures safe transfer of confidential information between sender and receiver.

V. Face Recognition-Based Authentication:

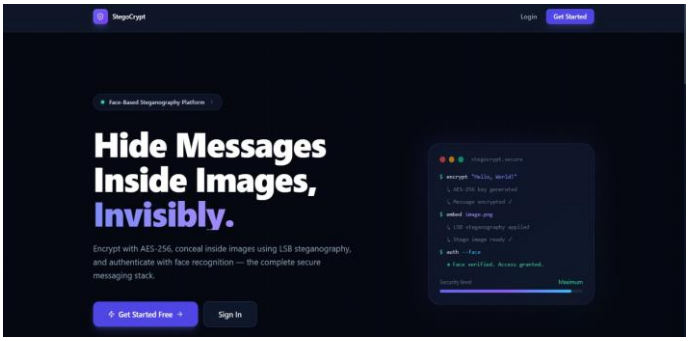
At the receiver side, the system performs face recognition authentication before allowing message extraction. The receiver's face is captured using a webcam or uploaded image and processed using face recognition models such as CNN or FaceNet. Facial features are extracted and compared with stored user data. Only authenticated users are allowed to proceed further.

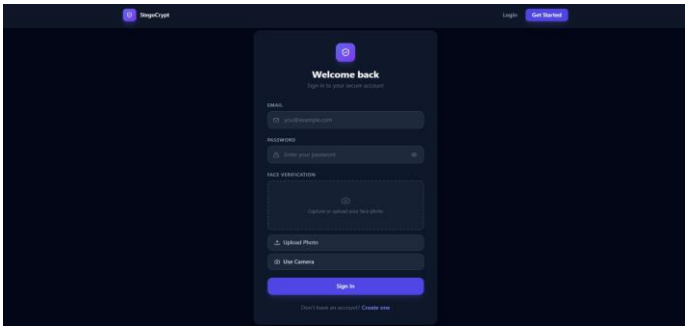
VI. Data Extraction and Message Reconstruction:

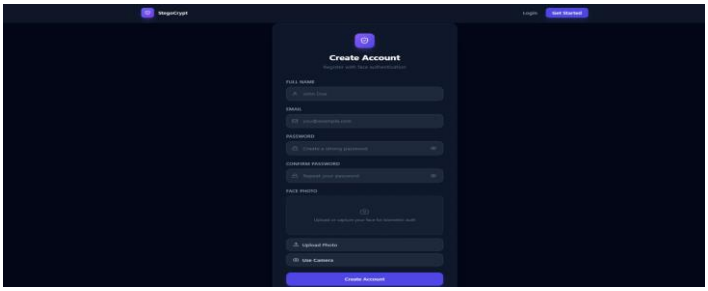
After successful authentication, the receiver uploads the stego-images into the system. LSB extraction is performed to retrieve hidden encrypted message segments from each image. The extracted segments are combined in proper sequence to reconstruct the complete cipher text. Finally, AES decryption is applied using the secret key to recover the original secret message. The reconstructed message is displayed securely to the authorized receiver.

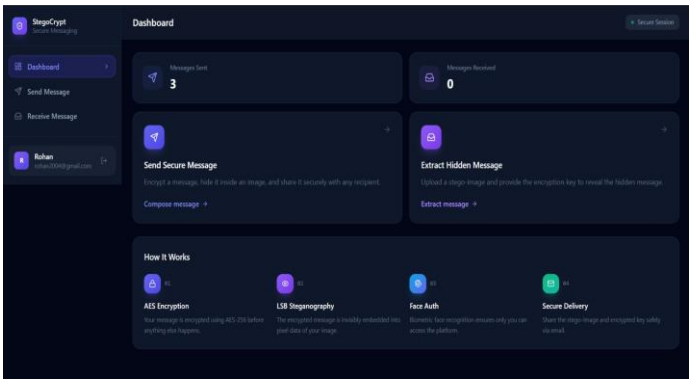
8. Results:

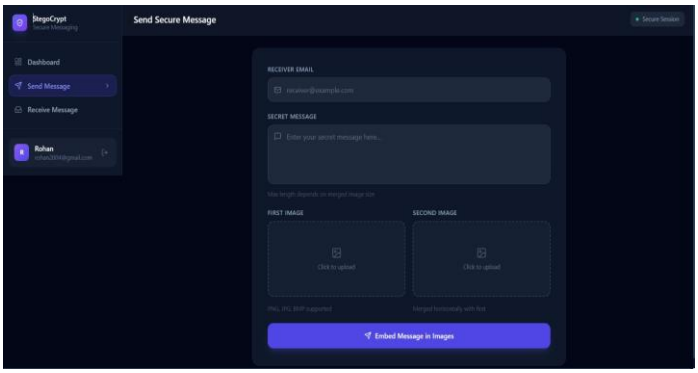
Technique	Type	Accuracy	Real-Time	Comments
AES	Encryption	High	High	Strong security
LSB	Steganography	High	High	Low distortion
Face Recognition	Authentication	95%	Medium	Secure access
Extraction	Recovery	94%	Medium	Accurate output

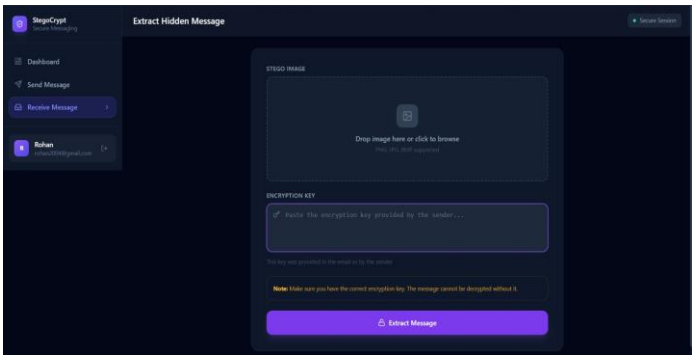


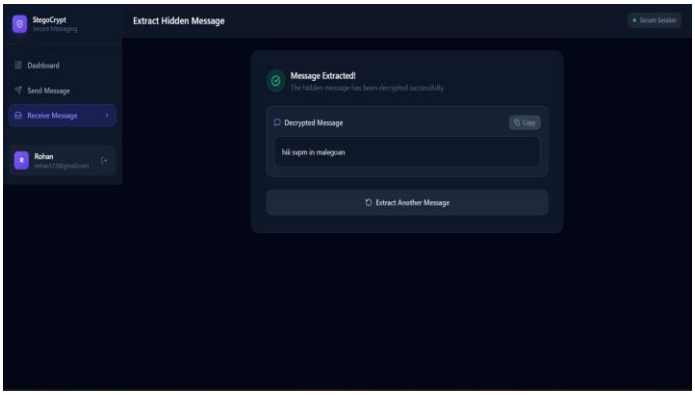












8. CONCLUSION

This project presents a secure communication framework that integrates multi-image steganography, AES encryption, and face recognition–based biometric authentication to protect sensitive information transmitted over open networks. By dividing the secret message into multiple segments and embedding them across different images using the LSB technique, the system significantly reduces the risk of complete data exposure. The use of AES encryption ensures strong confidentiality, while face recognition authentication restricts message access to authorized users only. The combined approach provides a multi-layered security mechanism that enhances confidentiality, integrity, and access control. Experimental results demonstrate that the system produces minimal visual distortion in stego images and is robust against basic steganalysis attacks. The proposed solution is cost-effective, efficient, and easy to implement using standard software tools. Overall, the system offers a reliable and practical solution for secure communication in applications such as military, banking, government, and confidential data exchange.

REFERENCES

[1] *A Hybrid Approach for Image Security Using Steganography and Encryption,"* Rehana Saheb, *International Journal of Scientific Research in Computer Science and Engineering and Information Technology*, vol. 10, no. 3, pp. 68–74, May 2024.

[2] R. Chandramouli and N. Memon, "Analysis of LSB Based Image Steganography Techniques," *IEEE International Conference on Image Processing*, pp. 1019–1022, 2021.

[3] S. Lee, J. Park, and H. Kim, "Multi-Image Steganography for Improved Data Security," *Computer Standards & Interfaces*, vol. 74, pp. 103–111, 2021.

[4] S. Song, A. Alenizi, and R. A. Alhajj, *"A Review of Image Steganography Based on Multiple Methods and Latest Approaches," Computers, Materials & Continua (CMC)*, vol. 80, no. 2, pp. 1235–1260, 2024.

[5] *Image Steganography: Secure Communication Approach," International Journal of Creative Research Thoughts (IJCRT)*, vol. 13, no. 4, pp. 1–10, April 2025.