



# Reversible Data Embedding in Encrypted Images Using for Secure Communication

V. Shalini<sup>1</sup>, S. Thamilmathi<sup>2</sup>, V. Dhavamani<sup>3</sup>, M. Mohamed Faisal<sup>4</sup>

U.G. Student, Department of Computer Science and Engineering, Sir Issac Newton College of Engineering and Technology, Nagappatinam, Tamilnadu, India<sup>1</sup>

Assistant Professor, Department of Computer Science and Engineering, Sir Issac Newton College of Engineering and Technology, Nagappatinam, Tamilnadu, India<sup>2,3</sup>

Assistant Professor and Head, Department of Computer Science and Engineering, Sir Issac Newton College of Engineering and Technology, Nagappatinam, Tamilnadu, India<sup>4</sup>

**ABSTRACT:** Reversible Data Hiding in Encrypted Images (RDHEI) plays a crucial role in protecting sensitive medical data while preserving the diagnostic quality of clinical images. This study proposes a secure framework for lung cancer diagnosis based on an  $(n, k)$  threshold secret sharing scheme. Original lung scan images are transformed into multiple encrypted shares using polynomial-based distribution, ensuring that individual shares do not reveal anatomical information. Patient metadata is securely embedded into the encrypted shares using optimized reference matrices to achieve high embedding capacity with low communication overhead. During reconstruction, a multivariate linear equation (MLE) solver enables perfect, bit-level recovery of the original image, ensuring diagnostic reliability. The reconstructed images are analyzed using deep learning models including MobileNetV2, ResNet50, and VGG16 to support automated lung cancer detection. The proposed framework effectively balances patient privacy.

**KEYWORDS:** Reversible Data hiding, Encrypting Images, Secret Sharing, Multivariate Linear Equation.

## I. INTRODUCTION

Reversible Data Hiding in Encrypted Images (RDHEI) has emerged as an important technique for securing sensitive medical information while preserving the original image quality. In medical imaging, especially lung cancer diagnosis, maintaining both data privacy and diagnostic accuracy is critical. Traditional encryption methods protect data but do not allow additional information embedding without distortion. RDHEI overcomes this limitation by enabling data embedding in encrypted images with perfect reversibility. In this project, an  $(n, k)$  threshold secret sharing scheme is applied to divide lung scan images into multiple secure shares. Patient medical information is embedded into encrypted shares without revealing anatomical details. A multivariate linear equation (MLE) solver ensures exact reconstruction of the original image. The reconstructed images are further analysed using deep learning models to support automated lung cancer detection.

## II. LITERATURE SURVEY

Several reversible data hiding in encrypted images (RDHEI) methods have been proposed to improve security, embedding capacity, and image recovery Cao et al. introduced a prediction error compression scheme with authentication to improve embedding efficiency and ensure data integrity, though this approach increases processing time [1]. Elhoseny et al. applied a  $(T, N)$  secret sharing method for secure IoT and cloud environments, but it suffers from higher storage and communication overhead [2]. Li et al. proposed interpolation techniques to expand embedding space, which enhances capacity but also raises memory and computation costs [3]. Saeidi and Mirzakuchaki employed LWE-based secret sharing to strengthen security against modern attacks, though it requires significant computational resources [4]. Tang et al. utilized adaptive edge detection with matrix-based secret sharing to boost embedding capacity, but this comes at the expense of increased computation [5]. Wu et al. developed a high-capacity method using multi-prediction and binary tree labelling, achieving better performance but with higher complexity [6]. Yu et al. introduced a scheme based on secret sharing and multivariate linear equations for accurate reconstruction, though it

suffers from high computational complexity and communication overhead [7]. Zhang and Tang proposed adaptive multisecret sharing for multi-user environments, which increases flexibility but also system complexity [8]. Zhang and Tang earlier designed a block-based secret sharing method with pixel correlation, though it offers limited embedding capacity [9]. Zhou et al. presented a multi-data hider approach enabling multiple users to embed data independently, but it introduces synchronization and key management challenges [10]. Overall, existing RDHEI methods improve security and reversibility but face challenges such as high computational complexity, increased overhead, and limited scalability, highlighting the need for more efficient and adaptable approaches.

### III. METHODOLOGY

The proposed system for Reversible Data Embedding in Encrypted Images for Secure Communication follows a multi-stage process to ensure both data security and perfect image recovery. Initially, the original image is encrypted using a suitable encryption algorithm to protect its content from unauthorized access. After encryption, the encrypted image is processed to identify suitable embedding locations based on pixel characteristics or available redundancy. Secret data is then embedded into the encrypted image using a reversible data hiding technique, ensuring that the embedding process does not permanently distort the image. To enhance security, optional secret sharing or key-based mechanisms can be applied so that only authorized users can extract the hidden information. At the receiver side, the embedded data is first extracted using the corresponding key, and then the decryption process is performed to recover the original image. The method ensures lossless recovery of the original image and accurate extraction of hidden data. Overall, the proposed methodology provides secure communication by combining encryption and reversible data hiding while maintaining high embedding capacity and data integrity.

### IV. EXPERIMENTAL RESULTS

Figure 1 shows the registration interface of the RDHEI system. Figure 2 shows the login page for user authentication. Figure 3 shows the overall overview of the RDHEI system. Figure 4 shows the interface for selecting or uploading lung scan images. Figure 5 shows the medical data entry and security setup. Figure 6 shows the secure decryption and data access process. Figure 7 shows the AI diagnosis and recovered result. Figure 8 shows the performance comparison of different algorithms. Figure 9 shows the confusion matrix of the VGG16 model. Figure 10 shows the confusion matrix of the ResNet50 model. Figure 11 shows the confusion matrix of the MobileNetV2 model. Figure 12 shows the ROC curve analysis of the models.



FIGURE 1 Registration RDHEI System



FIGURE 2 Login Page RDHEI System

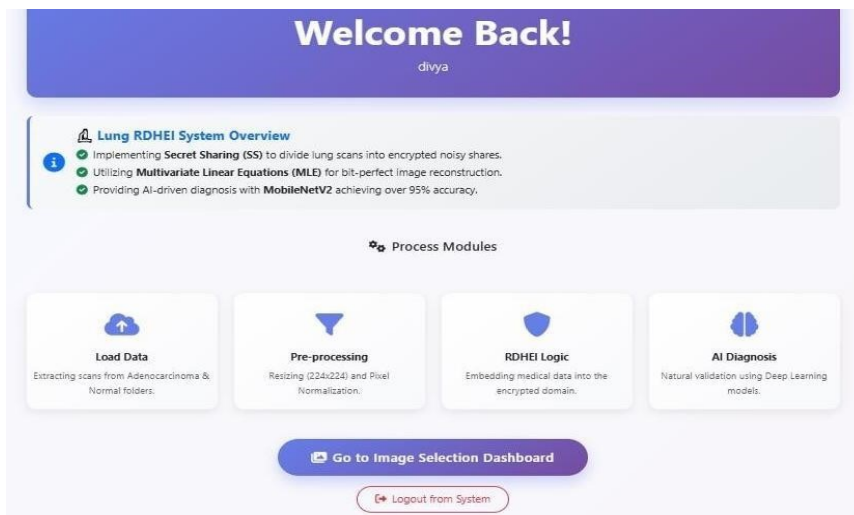


FIGURE 3 Lung RDHEI System Overview

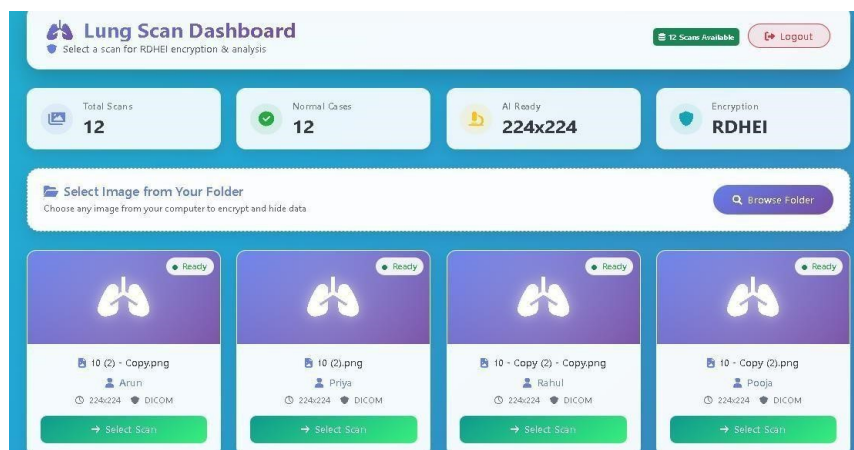
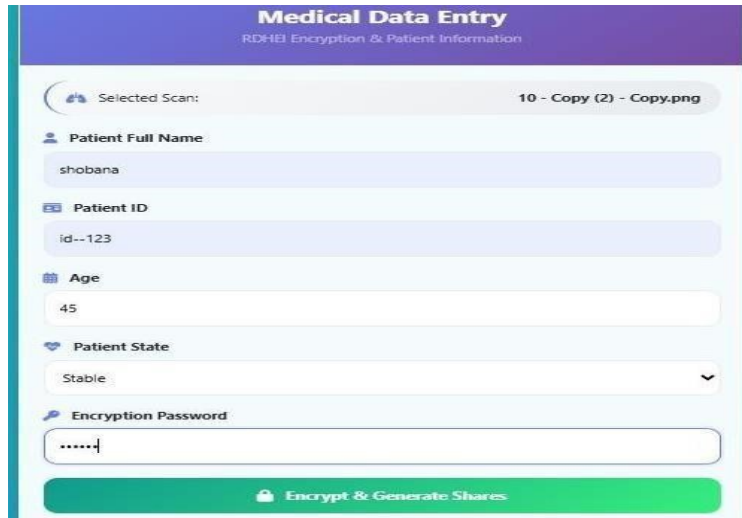


FIGURE 4 Lung Scan Dashboard and Image Selection



**Medical Data Entry**  
RDHEI Encryption & Patient Information

Selected Scan: 10 - Copy (2) - Copy.png

**Patient Full Name:** shobana

**Patient ID:** id--123

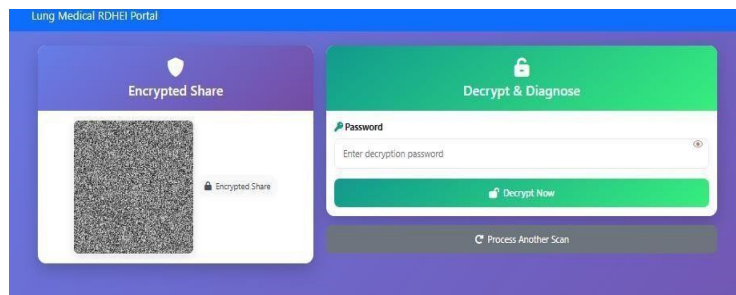
**Age:** 45

**Patient State:** Stable

**Encryption Password:** .....

**Encrypt & Generate Shares**

FIGURE5 Medical Data Entry and Security



Lung Medical RDHEI Portal

**Encrypted Share**

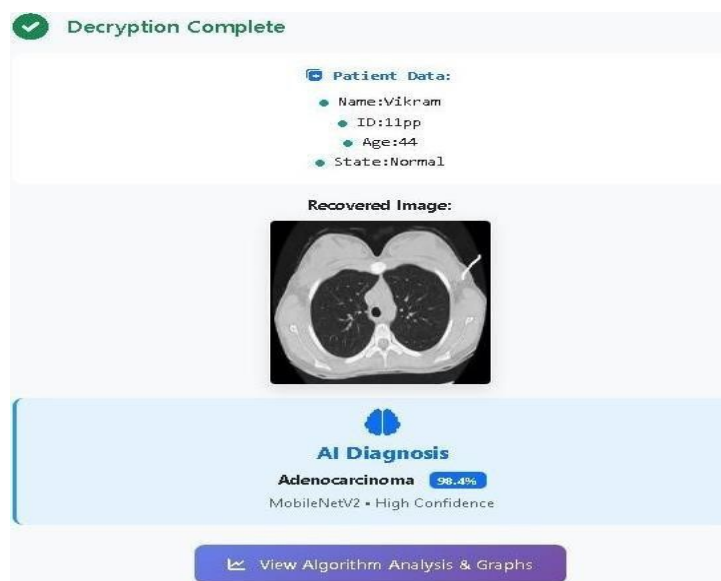
**Decrypt & Diagnose**

**Password:** Enter decryption password

**Decrypt Now**

**Process Another Scan**

FIGURE 6 Secure Decryption and Diagnostic Access



**Decryption Complete**

**Patient Data:**

- Name: Vikram
- ID: 11pp
- Age: 44
- State: Normal

**Recovered Image:**



**AI Diagnosis**

**Adenocarcinoma** 98.4%

MobileNetV2 • High Confidence

**View Algorithm Analysis & Graphs**

FIGURE 7 AI Diagnosis and Result Recovery

Volume 15, Issue 4, April 2026

DOI: 10.15680/IJIRSET.2026.1504058 |

### Algorithm Performance Analysis

VGG16: 91.2%    ResNet50: 93.8%    MobileNetV2: 98.4%

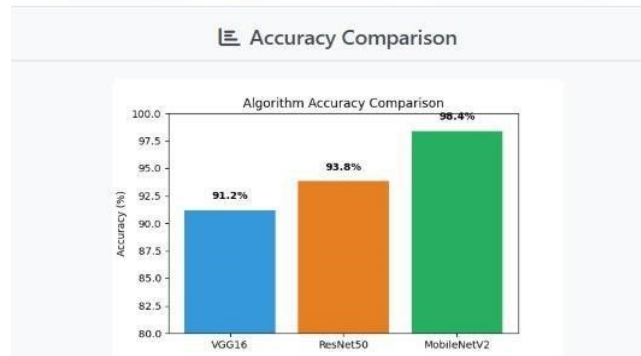


FIGURE 8 Algorithm Performance

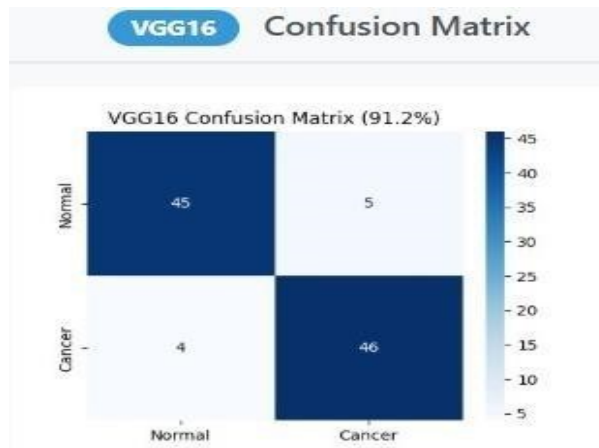


FIGURE 9 CM VGG16 MODEL

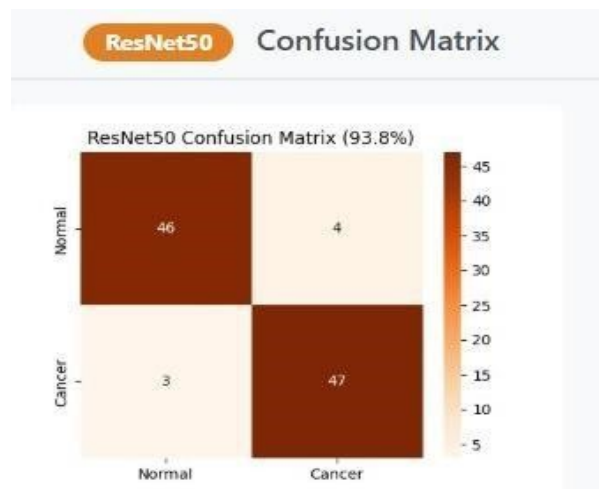


FIGURE 10 CM RESNET50 MODEL

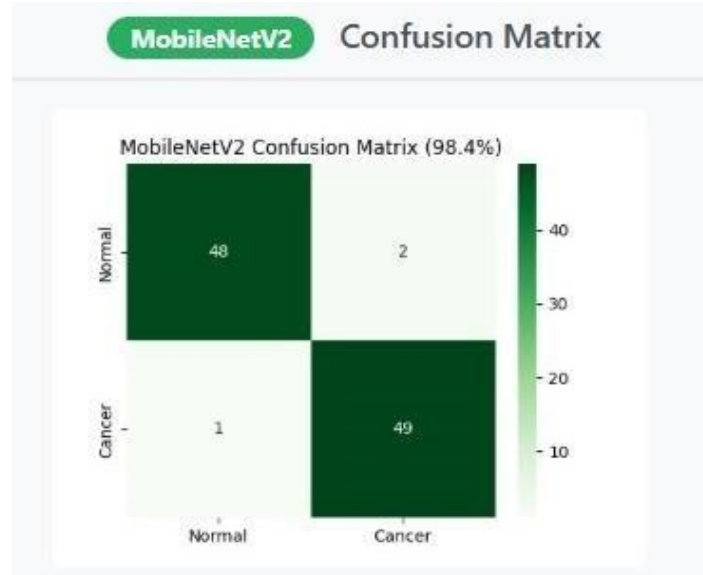
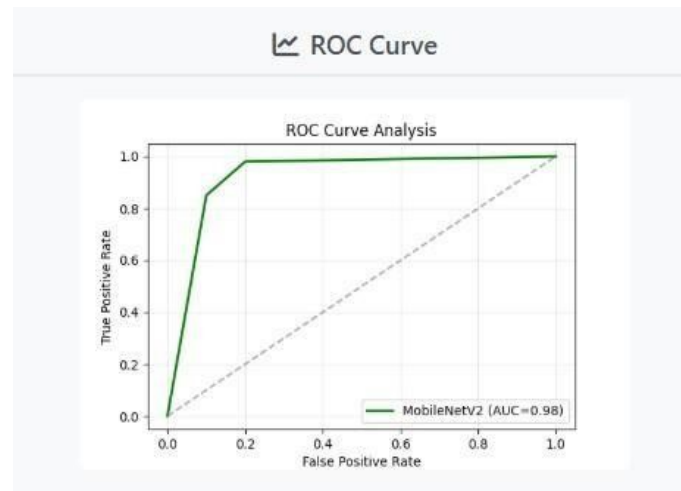


FIGURE 11 CM MOBILENETV2 MODEL



A2.12: ROC CURVE ANALYSIS

### V. CONCLUSION

The present research proposes a secure and reversible data hiding framework for encrypted lung images. The proposed framework integrates threshold secret sharing, reference matrices, and multivariate linear equation (MLE) solving techniques to achieve accurate and lossless image reconstruction. Patient metadata is securely embedded within the encrypted shares without degrading the visual quality of the medical image, thereby ensuring patient privacy and compliance with healthcare data protection standards. The framework also enables reliable transmission, extraction, and recovery of the original image even when some shares are missing or intercepted. The reconstructed images preserve full diagnostic quality and can be further analysed using deep learning models such as MobileNetV2, ResNet50, and VGG16 for automated lung cancer detection. Experimental evaluation demonstrates high embedding capacity, robustness, and perfect reversibility of the proposed method. Overall, the proposed framework effectively ensures secure medical data management while supporting AI-based clinical analysis, thereby validating the practical applicability of RDHEI in medical imaging systems.

**REFERENCES**

- [1] X. Cao et al., "Reversible data hiding and authentication scheme for encrypted images based on prediction error compression," *IEEE Trans. Information Forensics and Security*, vol. 14, no. 6, pp. 1520–1531, 2019
- [2] M. Elhoseny et al., "Hiding information in encrypted images with (T, N) secret sharing for IoT and cloud services," *IEEE Access*, vol. 8, Art. no. 113176, 2020.
- [3] J. Li et al., "Reversible data hiding in encrypted images based on two-round image interpolation," *IEEE Access*, vol. 9, Art. no. 87943, 2021.
- [4] Saeidi and Mirzakuchaki, "Reversible data hiding in encrypted images using LWE-based secret sharing," *IEEE Access*, vol. 13, Art. no. 102345, 2025.
- [5] Tang et al., "Reversible data hiding algorithm in encrypted images based on adaptive median edge detection and matrix-based secret sharing," *Multimedia Tools and Applications*, vol. 81, no. 10, pp. 14025–14044, 2022.
- [6] Y. Wu, Y. Xiang, and Y. Guo, "High-capacity reversible data hiding in encrypted images using multi-prediction and parametric binary tree labelling," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 30, no. 8, pp. 2659–2672, 2020.
- [7] Yu et al., "Reversible data hiding in encrypted images with secret sharing and multivariate linear equation," *IEEE Access*, vol. 13, Art. no. 104567, 2025.
- [8] Zhang and Tang, "Highly secure and adaptive multiset secret sharing for reversible data hiding in encrypted images," *IEEE Access*, vol. 9, Art. no. 126543, 2021.
- [9] Zhang and Tang, "Reversible data hiding over encrypted images via intrinsic correlation in block-based secret sharing," *IEEE Trans. Circuits and Systems for Video Technology*, vol. 28, no. 10, pp. 2600–2612, 2018.
- [10] Zhou, Zhang, and Yang, "Reversible data hiding in encrypted images using multiple data hiders sharing algorithm," *IEEE Access*, vol. 11, Art. no. 55678, 2023.



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details