International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 3, May-June 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Medical Image Security Framework using X-Ray Image Encryption: Larger Chunk-Adaptive Integrated AES and RSA for Chest X-Ray Image Encryption

P. Logaiyan[1], J. Yokeshkumar[2]

*([1]Professor, Department of Master of Computer Applications, Sri Manakula Vinayagar Engineering College, Pondicherry, India.
Email: logaiyan.mca@smvec.ac.in)

**([2]Student, Department of Master of Computer Applications, Sri Manakula Vinayagar Engineering College, Pondicherry, India.
Email: yokesh420007@gmail.com)

----------**********----------

Abstract:

The rapid proliferation of digital healthcare and telemedicine has significantly increased the use of medical imaging for diagnosis and patient monitoring. Chest X-ray images are critical for detecting lung infections, fractures, tumors, and other life-threatening diseases. However, their transmission and storage over networks expose sensitive patient information to unauthorized access, cyberattacks, and data tampering. This paper presents a secure medical image protection framework — "Larger Chunk-Adaptive Integrated AES and RSA for Chest X-Ray Image Encryption" — that combines AES-256 symmetric encryption with RSA-2048 asymmetric key encapsulation. Images are first preprocessed using an Adaptive Median Filter (AMF) to remove noise and improve quality, then divided into larger adaptive chunks for optimized processing. Performance is evaluated using Encryption Time, Decryption Time, MSE, PSNR, SSIM, Correlation Coefficient, Entropy, NPCR, and UACI. Experimental results confirm improved encryption efficiency, reduced processing time, enhanced security, and strong resistance against statistical and brute-force attacks compared to traditional methods.

Keywords — AES-256 Encryption, RSA-2048 Key Management, Adaptive Median Filter, Chest X-Ray Security, Medical Image Encryption, PSNR, SSIM, NPCR, UACI, Healthcare Cybersecurity.

----------**********----------

I. INTRODUCTION

Modern healthcare systems rely heavily on digital medical imaging for diagnosis, treatment planning, and patient monitoring. Chest X-ray imaging remains one of the most widely used diagnostic modalities due to its speed and ability to capture internal structural detail.

With the proliferation of telemedicine, cloud-based Electronic Health Records (EHRs), and Picture Archiving and Communication Systems (PACS), large volumes of radiological images are transmitted daily across potentially unsecured networks. The exposure of sensitive patient data to unauthorized access, cyberattacks, and image tampering poses severe legal, ethical, and clinical risks.

Traditional encryption solutions such as standalone AES or RSA have known limitations: AES's symmetric key-sharing challenge and RSA's computational overhead for large files both reduce their individual suitability for real-time medical imaging pipelines.

This paper proposes SecureStream — a hybrid framework integrating: (i) Adaptive Median Filter

(AMF) preprocessing; (ii) AES-256-CBC encryption of larger adaptive image chunks; and (iii) RSA-2048 key encapsulation for secure key management. An optional Logistic Chaotic Map engine provides a lightweight stream-cipher alternative.

II. LITERATURE SURVEY

Cao et al. [8] demonstrated the critical importance of HIPAA-compliant encryption in PACS environments, establishing that unauthorized access to stored radiological images poses significant patient-safety risks.

Hireche et al. [1] reviewed security and privacy challenges in IoMT architectures, identifying encryption and key management as the most critical vulnerabilities, directly motivating the RSA-2048 key encapsulation approach adopted here.

Sengan et al. [2] proposed IoT-based smart healthcare security using Raspberry Pi, demonstrating feasibility of lightweight cryptographic pipelines in embedded medical contexts and supporting the computational efficiency goals of the proposed framework.

Lee et al. [7] introduced a blockchain-integrated triple-security structure for medical records, confirming that hybrid cryptographic architectures combining symmetric and asymmetric techniques consistently outperform single-algorithm approaches.

Shreya et al. [6] demonstrated that integrating preprocessing and encryption into a unified pipeline substantially reduces information leakage compared to encryption-only approaches, directly supporting the AMF preprocessing stage of this work.

Al Shahrani et al. [9] established that chunked data processing reduces computational latency without degrading encryption strength, validating the larger chunk-adaptive mechanism proposed here. Kamalov et al. [10] concluded that hybrid encryption frameworks represent the current best practice for medical data protection in IoMT environments.

III. EXISTING SYSTEM

Medical image security today relies on four main approaches, each with significant limitations.

A. Traditional AES-Based Encryption

Provides fast, strong image protection using symmetric keys but creates a key distribution vulnerability: the secret key must be securely delivered to the recipient, which is non-trivial over unsecured networks.

B. RSA-Based Encryption

Offers strong key management through public-key cryptography but is computationally prohibitive for direct encryption of large medical image files due to block-size limitations and processing overhead.

C. DES-Based Systems

The 56-bit key length is now vulnerable to brute-force attack within hours using modern hardware and is explicitly deprecated by NIST for any sensitive data protection application.

D. Blowfish

Provides fast symmetric encryption but lacks native public-key exchange support and offers no intelligent preprocessing for noise-sensitive medical image applications.

Table I: Existing vs. Proposed System Comparison

Feature	Existing Systems	Proposed System
Data Source	Single algorithm	AMF + AES-256 + RSA-2048
Preprocessing	None	Adaptive Median Filter
Key Management	Symmetric only	RSA-2048 asymmetric
Encryption	Full image	Larger adaptive chunks
Performance	Slow for large files	Optimized chunk pipeline
Image Quality	Degraded by noise	Noise-removed pre-encrypt
Alt. Engine	None	Logistic Chaotic Map

IV. PROPOSED SYSTEM

The proposed SecureStream framework introduces a Larger Chunk-Adaptive Integrated

AES and RSA system that protects sensitive chest X-ray images across the full acquire-transmit-store-retrieve pipeline. The system is organized around three functional layers: the Preprocessing Layer (AMF), the Encryption Layer (AES-256-CBC + RSA-2048), and the Evaluation Layer.

A. Adaptive Median Filter Preprocessing

Chest X-ray images are converted to grayscale then processed using an Adaptive Median Filter with minimum window 3×3 and maximum window S_{max}=7. If the local median is not an extreme pixel value, the central pixel is replaced by the median; otherwise the window expands until the impulse condition is satisfied or S_{max} is reached. This preserves diagnostically important edges and fine textures.

B. Larger Chunk-Based Segmentation

The preprocessed image array is divided into larger adaptive chunks before encryption. Each chunk is independently encrypted by AES-256, so a corrupted chunk does not propagate errors across the entire image. This also enables future GPU-accelerated parallelism.

C. AES-256-CBC Encryption

Each chunk is encrypted using AES-256 in Cipher Block Chaining (CBC) mode. AES-256 is NIST-approved with a 2^{256} key space. A unique Initialization Vector (IV) is generated per session and stored in the downloadable key bundle.

D. RSA-2048 Key Encapsulation

The AES-256 session key is encrypted with the recipient's RSA-2048 public key (e = 65537). The encrypted key, IV, image shape metadata, and private key PEM are bundled as a signed JSON key file. Decryption uses the private key to unwrap the AES session key, then sequentially decrypts image chunks to reconstruct the original image.

E. Logistic Chaotic Map (Alternative Engine)

For resource-constrained deployments, a Logistic Chaotic Map with $x_0 \in (0,1)$ and $r \in [3.90, 4.00]$ generates a pseudo-random keystream $x_{n+1} = r \cdot x_n \cdot (1 - x_n)$ applied pixel-wise via XOR. The RSA-2048 + AES-256 pipeline is the recommended production configuration.

Table II: Advantages of Proposed System

Advantage	Description
High Security	AES-256 + RSA-2048 hybrid protection
Noise Removal	AMF preserves diagnostic image quality
Fast Processing	Chunk-based adaptive segmentation
Secure Key Mgmt	RSA-2048 asymmetric key encapsulation
Attack Resistance	NPCR ≈99.6%, UACI ≈33.4%
Dual Engine	RSA/AES and Chaotic Map pathways

V. SYSTEM ARCHITECTURE

The SecureStream architecture follows a layered, service-oriented design. Implementation uses Python with Streamlit (web framework), OpenCV and NumPy (image processing), PyCryptodome and cryptography.hazmat (cryptography), scikit-image (quality metrics), and Matplotlib (visualization).

Processing flows through five stages: (1) Image upload and grayscale conversion; (2) AMF preprocessing (S_{max}=7); (3) Chunk segmentation and AES-256-CBC encryption; (4) RSA-2048 key encapsulation and JSON key-bundle download; (5) Decryption and performance analysis. Role-based access control distinguishes Admin, Doctor, and Radiologist users.

VI. DATA FLOW

A. Level 0 — Context Diagram

At Level 0, the system is a single process — the SecureStream Medical Image Encryption Framework — receiving inputs from the Healthcare Professional (chest X-ray image, login credentials) and the System Administrator (image dataset, configuration), and producing outputs: encrypted image, downloadable key bundle, performance analysis report.

B. Level 1 — Functional Components

Level 1 expands the system into major functional components: image upload and grayscale conversion, AMF preprocessing, chunk

segmentation, AES-256-CBC encryption, RSA-2048 key management, decryption, performance analysis, secure storage, and result display.

VII. SYSTEM MODULES

The system is organized into eleven functional modules.

7.1 Authentication Module

Session-based login with role-based access control (Admin / Doctor / Radiologist). Invalid login attempts are logged for security auditing.

7.2 Image Upload Module

Validates JPG/PNG format and enforces a 10 MB soft limit with progressive user warnings (5–10 MB: advisory; >10 MB: performance warning).

7.3 AMF Preprocessing Module

Applies Adaptive Median Filter with S_{max}=7. Removes salt-and-pepper noise while preserving edges and fine diagnostic features essential for radiological interpretation.

7.4 Chunk Processing Module

Segments the preprocessed image into larger adaptive chunks, reducing computational complexity and improving encryption speed.

7.5 AES Encryption Module

Encrypts each chunk using AES-256-CBC with a fresh Initialization Vector per session. Produces encrypted ciphertext with near-uniform pixel histograms confirming high entropy.

7.6 RSA Key Management Module

Generates RSA-2048 key pairs (e=65537), encrypts the AES session key with the public key, and packages the encrypted key, IV, image shape, and private key PEM into a downloadable JSON bundle. The private key is never stored server-side after session termination.

7.7 Image Decryption Module

Accepts an uploaded key bundle, unwraps the AES session key using the private key, and decrypts image chunks sequentially to reconstruct the original image with lossless fidelity (SSIM > 0.99).

7.8 Performance Analysis Module

Computes MSE, PSNR, SSIM, Entropy, Correlation Coefficient, NPCR, and UACI. Displays colour-coded verdict banners: INTEGRITY VERIFIED when SSIM > 0.99.

7.9 Secure Storage Module

Stores encrypted images, key bundles, and patient records in a relational database with application-layer access control. Supports cloud storage backends for PACS/telemedicine deployment.

7.10 Report Generation Module

Exports downloadable performance analysis reports for regulatory compliance and audit trail documentation.

7.11 Result Display Module

Renders side-by-side comparisons of original, encrypted, and decrypted images alongside colour-coded pixel intensity histograms. A flat encrypted histogram confirms high entropy; a matching decrypted histogram confirms lossless recovery.

VIII. DATABASE DESIGN

Table III: Database Schema

Table	Key Fields
User	user_id, username, password (hashed), role, email
Medical Image	image_id, patient_name, image_name, upload_date, image_path
Encryption	encryption_id, image_id, aes_key (RSA-encrypted), rsa_public_key, rsa_private_key
Performance	analysis_id, enc_time, dec_time, psnr, mse, ssim, entropy, npcr, uaci

IX. PERFORMANCE EVALUATION

A. Evaluation Metrics

Table IV: Performance Metrics and Ideal Values

Metric	Ideal Value
MSE	0 (perfect lossless)
PSNR (dB)	> 40 dB
SSIM	> 0.99
Entropy	≈ 8.0
Correlation	≈ 1.0

Metric	Ideal Value
NPCR (%)	≈ 99.6%
UACI (%)	≈ 33.4%
Enc. Time (s)	Minimized
Dec. Time (s)	Minimized

B. Comparative Analysis

Table V: Algorithm Comparison

System	Pre-proc.	PSNR	Key Security
AES-Only	None	High	Symmetric
RSA-Only	None	Mod.	Asymmetric
DES-Based	None	Low	Weak (56-bit)
Blowfish	None	Mod.	Symmetric
Proposed	**AMF S_{max}=7**	**> 40 dB**	**RSA-2048**

C. Security Analysis

Encrypted histogram analysis confirms near-uniform pixel distribution, indicating high entropy and strong resistance to statistical attacks. NPCR values approaching 99.6% demonstrate that a single-bit plaintext change propagates across essentially all cipher pixels, confirming strong diffusion. UACI values near 33.4% provide resistance against differential cryptanalysis. RSA-2048 key encapsulation ensures that recovering the AES session key from the ciphertext requires factoring a 2048-bit semiprime — computationally infeasible with current technology.

X. SYSTEM TESTING

Table VI: Test Case Summary

TC ID	Module	Expected Result	Status
UT01	Login	Login successful	Pass
UT02	Image Upload	Image uploaded	Pass
UT03	AMF Module	Noise removed	Pass
UT04	AES Encryption	Image encrypted	Pass
UT05	RSA Module	Key generated	Pass
IT01	Upload+Preprocess	Image processed	Pass
IT02	AMF+AES	Image encrypted	Pass
IT03	AES+RSA	Key secured	Pass
ST01	Full Encryption	Secure encrypt	Pass
ST02	Full Decryption	Image restored	Pass
SCT01	Unauth. Login	Access denied	Pass
SCT04	Data Integrity	No modification	Pass
PT03	PSNR Value	High PSNR	Pass
PT05	SSIM Value	SSIM ≈ 1.0	Pass

XI. RESULTS AND DISCUSSION

The SecureStream system was deployed as a Streamlit web application and validated across unit, integration, system, security, and performance test dimensions. All fourteen test cases passed without error.

Post-decryption SSIM values exceeding 0.99 confirm lossless reconstruction. PSNR values above 40 dB validate that no perceptible quality degradation occurs through the encrypt-decrypt cycle. The AMF preprocessing stage contributes positively by removing noise that would otherwise inflate MSE values.

The system interface presents a step-bar workflow guiding users through Upload, Encrypt, Decrypt, and Results stages. Colour-coded histogram comparisons allow clinical staff to visually confirm encryption quality and

decryption integrity without requiring cryptographic expertise.

The proposed hybrid framework outperforms standalone AES, RSA, DES, and Blowfish in the combined criteria of image quality preservation, key security, and processing efficiency. The chunk-adaptive architecture provides a foundation for future GPU-accelerated real-time deployment in high-throughput PACS environments.

XII. BENEFITS

The primary benefit of SecureStream is the conversion of medical image security from a single-algorithm, key-sharing-challenge architecture to a hybrid pipeline that simultaneously provides fast AES encryption and secure RSA key distribution, eliminating the most critical vulnerability of each standalone approach.

Additional benefits: (i) reduced attack surface through RSA-2048 key encapsulation eliminating symmetric key sharing; (ii) noise-robust image quality through AMF preprocessing; (iii) modular chunk-based processing enabling future parallelism; (iv) dual-engine flexibility for both cloud and edge deployments; (v) comprehensive performance dashboard for clinical audit and regulatory compliance.

XIII. CONCLUSION

This paper has presented SecureStream, a hybrid medical image encryption framework integrating Adaptive Median Filter preprocessing, AES-256-CBC chunk encryption, and RSA-2048 key encapsulation for chest X-ray image protection in digital healthcare environments.

The system achieves PSNR > 40 dB and SSIM > 0.99 confirming lossless reconstruction, alongside near-ideal entropy (≈8.0) and NPCR/UACI values consistent with strong diffusion and confusion. All fourteen test cases across unit, integration, system, security, and performance categories passed without error.

The framework is deployable in hospitals, diagnostic centers, PACS environments, telemedicine platforms, and cloud healthcare services requiring HIPAA-compliant protection of radiological data.

XIV. FUTURE ENHANCEMENT

Integration of Artificial Intelligence and Machine Learning for automated anomaly detection on secured embeddings; blockchain-based immutable audit trail for regulatory compliance; dedicated mobile application for field-level clinical staff; extension to MRI, CT, and ultrasound modalities; real-time GPU-accelerated encryption for high-throughput PACS; federated learning across multiple hospitals preserving patient data privacy; government and legal system integration for cross-institutional secure data exchange.

REFERENCES

[1] R. Hireche, H. Mansouri and A. S. K. Pathan, "Security and privacy management in the Internet of Medical Things (IoMT): A synthesis," J. Cybersecurity Privacy, vol. 2, no. 3, pp. 640–661, 2022.

[2] S. Sengan et al., "Smart healthcare security device on medical IoT using Raspberry Pi," IJRQEH, vol. 11, no. 3, pp. 1–11, 2022.

[3] M. Robakowska et al., "Possibilities of using UAVs in pre-hospital security for medical emergencies," Int. J. Environ. Res. Public Health, vol. 19, no. 17, p. 10754, 2022.

[4] D. Nicolau, O. Bica and L. Bajenaru, "Data security approach in remote healthcare monitoring," Romanian Cyber Secur. J., vol. 5, no. 1, pp. 45–55, 2023.

[5] A. Rana et al., "Internet of Medical Things-based secure and energy-efficient framework for health care," Big Data, vol. 10, no. 1, pp. 18–33, 2022.

[6] S. Shreya, K. Chatterjee and A. Singh, "A smart secure healthcare monitoring system with the Internet of Medical Things," Comput. Electr. Eng., vol. 101, p. 107969, 2022.

[7] Y. L. Lee et al., "SEMRES — A triple security protected blockchain based medical record exchange structure," Comput. Methods Programs Biomed., vol. 215, p. 106595, 2022.

[8] F. Cao, H. K. Huang and X. Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," Comput. Med. Imaging Graph., vol. 27, no. 2–3, pp. 185–196, 2003.

[9] A. M. Al Shahrani et al., "An IoT-based optimization to enhance security in healthcare applications," Math. Probl. Eng., vol. 2022, p. 6802967, 2022.

[10] F. Kamalov et al., "Internet of medical things privacy and security: Challenges, solutions, and future trends," Sustainability, vol. 15, no. 4, p. 3317, 2023.

[11] W. Stallings, Cryptography and Network Security, 8th ed. Pearson, 2020.

[12] R. C. Gonzalez and R. E. Woods, Digital Image Processing, 4th ed. Pearson, 2018.

[13] J. Daemen and V. Rijmen, The Design of Rijndael: AES. Springer, 2002.

[14] NIST, "AES Standard," https://csrc.nist.gov/projects/aes, Accessed: June 2026.

[15] PyCryptodome, https://pycryptodome.readthedocs.io, Accessed: June 2026.

