

## **Resource-constrained encryption design with cloud-based medical imaging archives**

Amol Bhoite <sup>§</sup>

*Department of Radio-Diagnosis*

*Krishna Institute of Medical Sciences*

*Krishna Vishwa Vidyapeeth (Deemed to be University)*

*Karad 415539*

*Maharashtra*

*India*

Radha Chauhan <sup>†</sup>

*Department of Microbiology*

*Noida International University*

*Greater Noida 201312*

*Uttar Pradesh*

*India*

Samir N. Ajani <sup>\*</sup>

*School of Computer Science and Engineering*

*Ramdeobaba University*

*Nagpur 440013*

*Maharashtra*

*India*

Viyyapu Lokeshwari Vinya <sup>‡</sup>

*Department of Computer Science and Engineering*

*Vardhaman College of Engineering*

*Shamshabad*

*Hyderabad 501218*

*Telangana*

*India*

---

<sup>§</sup> E-mail: [amool10123@gmail.com](mailto:amool10123@gmail.com)

<sup>†</sup> E-mail: [chauhan.radha50@gmail.com](mailto:chauhan.radha50@gmail.com)

<sup>\*</sup> E-mail: [samir.ajani@gmail.com](mailto:samir.ajani@gmail.com) (Corresponding Author)

<sup>‡</sup> E-mail: [vinya593@vardhaman.org](mailto:vinya593@vardhaman.org)

Amruta Prasad Kharade<sup>@</sup>

*Department of Engineering Science and Humanities  
Vishwakarma Institute of Technology  
Pune 411037  
Maharashtra  
India*

V. Poongodi<sup>#</sup>

*Department of Oral Medicine and Radiology  
Meenakshi Ammal Dental College & Hospital  
Meenakshi Academy of Higher Education & Research  
Chennai 600087  
Tamil Nadu  
India*

---

## Abstract

While cloud-based medical imaging archives offer scalability, remote access, and easy sharing of diagnostic information, the security of these types of sensitive images is difficult for resource-constrained medical devices. This paper introduces a secure and efficient medical image archiving system, called Resource-Constrained Encryption Framework (RCEF), which provides image security and efficiency. This framework covers resource assessment, adaptive encryption configuration, light image encryption, secure key management, integrity check, authenticated transmission, cloud storage and authorized reconstruction. The configuration of the encryption is based on the characteristics of the devices, such as processing power, memory, energy and bandwidth. The framework is tested by means of computed tomography (CT), magnetic resonance imaging (MRI), X-ray and ultrasound pictures and contrasted with traditional encryption methods. The experimental results show the time of encryption and decryption reduced, CPU usage reduced, memory consumed reduced, energy consumption reduced, and higher throughput. The results of security analysis show high entropy of cipher text, low degree of correlation between cipher text pixels, strong differential properties and key sensitivity. The Lossless authorized reconstruction preserves the diagnostically important information, which is appropriate for IoMT device, edge healthcare platform and secure cloud medical archive.

---

**Subject Classification:** 68Q30.

**Keywords:** Cloud computing, Medical image encryption, Resource-constrained encryption, Lightweight cryptography, IoMT, Cloud security, Healthcare data, Adaptive encryption.

---

<sup>@</sup> E-mail: [amruta.kharade@vit.edu](mailto:amruta.kharade@vit.edu)

<sup>#</sup> E-mail: [poongodi@maher.ac.in](mailto:poongodi@maher.ac.in)

## 1. Introduction

Medical imaging data is being rapidly digitalized, changing the way in which it is acquired, transmitted, managed and stored. Large amounts of patient-sensitive information are collected from diagnostic modalities like magnetic resonance imaging (MRI), computed tomography (CT), X-ray, ultrasound, positron emission tomography (PET) and digital pathology. [1] Cloud-based medical imaging stores (C-MIS) offer scalable storage, remote access, centralized administration, disaster recovery and efficient information sharing [2]. Moving medical images to the cloud comes with issues of confidentiality, integrity, authentication, unauthorized access, data leakage and patient privacy, etc. [3]. During transmission and storage, medical images must be transmitted securely, and encryption is vital to that. Traditional techniques like Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA) and hybrid encryption are highly secure, but can cause significant computational, memory, latency and energy overheads [4]. The constraints are especially relevant for resource-limited platforms like devices in the Internet of Medical Things (IoMT), portable diagnostic systems, embedded processors, mobile healthcare devices, and edge computing nodes [5]. This places a heavy emphasis on the need for encryption methods that are not only secure but also efficient in terms of resource usage in healthcare settings, where resources are often limited [6]. The number of operations that can be processed, memory, battery, and communication bandwidth are all things to keep in mind when choosing which encryption operations to select. In addition to that, medical images include a lot of information that is visually correlated and sensitive DICOM metadata that must be kept confidential and secured against unauthorized access; must be properly verified for integrity; must be authenticated; and must be managed securely during decryption; and must be reconstructed correctly after authorized decryption [7]. Current methods are symmetric, asymmetric, selective, chaotic, lightweight and hybrid encryption methods. But many times security is emphasized without taking into account the consumption of resources and lightness might affect robustness or scalability [8]. Based on this, the present study suggests a new secure cloud based medical imaging archives system called Resource-Constrained Encryption Framework (RCEF). The design includes resource assessment, adaptive encryption, secure key management, integrity verification, authenticated transmission, cloud storage, and authorized decryption [9].

## 2. System Model and Problem Formulation

MRI, CT, X-ray, ultrasound and PET systems create medical images that include sensitive image data (I) and related DICOM metadata (M). The data is then processed in an edge or local node that has limited CPU, memory, battery and bandwidth capabilities before being transmitted to the clouds [10]. So the proposed system takes the resources of the available device into account when it comes to encryption to minimize the cost of computation, energy usage, and time to transmit medical data while still keeping the data safe. [11] For this

reason, a proposed system is presented which introduces a Resource Assessment Module (RAM). A resource-state vector is defined as:

$$R = [C, M, E, B]$$

where (C) stands for capacity available for computation, (M) for the memory available, (E) for the energy remaining and (B) for the bandwidth of the network. These parameters are continually assessed prior to encryption within the resource assessment module. System triggers an appropriate encryption configuration, depending on the measured resource state and required level of security. The original medical image is represented by:

$$I = \{p_1, p_2, \dots, p_n\},$$

where ( $p_i$ ) represents individual information of a pixel/voxel. The original image is encrypted to ciphertext with an encryption function (E) and secret key (K):

$$I_E = E_{K(I)}.$$

The primary medical image is rebuilt to see its original image for an authorized healthcare user.

$$I = D_{K(I_E)},$$

where ( $D_K$ ) denotes the decryption operation for that. The recovered image should be exactly the same as the original image to ensure that there is no change in the diagnostically important information because of encryption. The system assumes that communication networks and cloud infrastructure cannot be considered completely trusted. The adversaries can try to intercept the medical images that are transmitted; access to cloud archives without permission; modification of encrypted records; replay of previously transmitted information; or get encryption keys [12]. The threat model thus assumes that there is the possibility of eavesdropping, unauthorized access to the cloud, altering data, replaying messages, brute force attacks, analysis of the statistics, and key compromises. The proposed framework thus integrates access control, secure key management, integrity verification and encryption with authentication. The main aim in optimizing is to reduce the overhead of the encryption without compromising the security level required. It can be represented as:

$$J = w_{1T_e} + w_{2M_u} + w_{3E_c} + w_{4L},$$

subject to

$$S \geq S_{\{min\}}$$

The encryption time ( $T_e$ ), memory utilization ( $M_u$ ), energy consumption ( $E_c$ ), communication or processing latency (L) and the required minimum security (Smin). The coefficients ( $w_1, w_2, w_3, w_4$ ), give the relative importance of individual resource constraints. The problem formulation proposed in the paper, therefore, addresses medical-image security as a multi-objective problem of optimization of a resource, and not just cryptographic operation [13]. The goal is to find an encryption setup that has enough

confidentiality and integrity, but uses the least resources in the form of computing power. This system model is the basis for the proposed resource constrained encryption system described in the next section 3.

### 3. Proposed Resource-Constrained Encryption Framework

The proposed Resource-Constrained Encryption Framework (RCEF) aims to secure medical images before they are sent and stored in cloud remote archives with low computational, memory and energy consumption. Whereas fixed encryption schemes do not take into account the actual resources available for the healthcare device, the proposed scheme dynamically selects an encryption configuration based on the device's actual resources. The whole body is divided into medical-image acquisition, the preprocessing of medical images, the evaluation of the available resources, the setting of the security configuration, lightweight encryption, integrity protection, secure key management, transmission of the medical images in the cloud and authorized reconstruction.

#### A. Medical Image Acquisition and Preprocessing

Medical image input ( $I$ ) is obtained from a computed tomography (CT), magnetic resonance imaging (MRI), X-ray, ultrasound or any other imaging modalities. The DICOM information is divided into image data ( $I_p$ ) and metadata ( $I_m$ ):

$$I = \{I_p, I_m\}.$$

Basic preprocessing is used to check the image dimension, format, bit depth, and image metadata structure. Patient-specific data, which would be sensitive if it were included in other DICOM metadata, is identified to ensure that patient data is properly protected along with the image content.

#### B. Resource Assessment

The framework first assesses whether the device that's sending the data has enough computing power before it encrypts it. Four main resource metrics are assumed: CPU availability ( $C$ ), free memory ( $M$ ), remaining energy ( $E$ ) and communication bandwidth ( $B$ ). A normalized resource score is based on the formula:

$$R_s = w_{cc} + w_{mM} + w_{eE} + w_{bB},$$

where ( $w_c, w_m, w_e$ .) and ( $w_b$ ) represent weighting coefficients and

$$w_c + w_m + w_e + w_b = 1.$$

A higher ( $R_s$ ) indicates sufficient resources for stronger or more comprehensive cryptographic operations, whereas a lower value indicates a constrained operating condition.

### C. Adaptive Encryption Selection

Based on the resource score, the framework determines the encryption configuration.

**Table 1**  
Three operational levels are considered:

| Resource State | Encryption Configuration                    | Primary Objective                |
|----------------|---------------------------------------------|----------------------------------|
| Low            | Lightweight optimized encryption            | Minimum resource overhead        |
| Medium         | Lightweight encryption + enhanced integrity | Balanced security and efficiency |
| High           | Full encryption + authentication            | Maximum protection               |

This adaptive features from Table 1 ensures the minimum-security requirement is always satisfied without also using up any unnecessary computation time. The security is thus not lowered to an acceptable level, but rather adjusted to safe settings within prescribed limits.

### D. Lightweight Medical Image Encryption

The framework uses a lightweight symmetric encryption mechanism in the case of resource constrained devices since the throughput of symmetric operations are generally higher for large medical-image files. The encryption algorithm is shown as:

$$C_I = \text{Enc}(I, K_s, R_s),$$

The medical image encrypted with session encryption key ( $K_s$ ) is represented as where ( $C_I$ ) is the encrypted medical image and ( $K_s$ ) is the session encryption key. The encryption phase uses controlled confusion and diffusion operations to remove the strong statistical correlation that is usually found between neighbouring pixels in a medical image. The resulted encrypted image should have high entropy, and low adjacent-pixel correlation, and also be easily computed.

### E. Secure Key Management and Integrity Verification

Each session key is unique to a particular session of encryption. The session key is not sent directly with the medical image being transmitted, but is securely protected by using an authenticated key-management mechanism. It is important to keep the separation of key and plaintext medicine information so that the medicine information in the cloud cannot be automatically exposed. A value of integrity is also computed:

$$H = \text{Hash}(C_I \parallel ID \parallel T),$$

The identifier of the image and/or the identifier of the transaction (ID) and the time stamp (T). Here, the hash is calculated again and then compared to the value stored.

#### 4. Proposed Encryption Procedure

The proposed system is based on the resource constrained encryption framework which is realized by adaptive encryption algorithm based on device-resource monitoring, lightweight symmetric encryption, secure key management, integrity verification, and cloud-based storage. The implementation is meant to guarantee that medical images are concealed and protected during transmission and storage, and that the resources of health care devices are not too taxed. The following steps can be used to sum up the proposed encryption process:

**Step 1: Medical Image Acquisition**

Get the original medical image and DICOM metadata.

**Step 2: Resource Monitoring**

Monitor CPU usage, memory, remaining energy and network bandwidth.

**Step 3: Resource score is calculated.**

In Step 3, the resource score is determined.

Determine ( $R_s$ ) and classify the device as a low, medium or high resource operating regime.

**Step 4: Session-Key Generation**

Generate a session key ( $K_s$ ) as a cryptographically secure key for the encryption of the medical image in the current operation.

**Step 5: Image Encryption**

Encryption medical image with selected light encryption (lightweight):

$$C_I = Enc_{\{K_s\}(I)}.$$

**Step 6: Metadata Protection**

Securely encode the DICOM metadata for sensitive information to avoid the possibility of unauthorized viewing of patient information.

**Step 7: Integrity Generation**

Use the encrypted image, image identifier and timestamp to compute an authentication value:

$$A = H(C_I \parallel ID \parallel T).$$

**Step 8: Key Protection**

Securely protect the session key before it is sent to cloud.

**Step 9: Cloud Upload**

Send the cipher text, protected metadata, integrity value and the information of the session-key (encrypted) to the cloud archive.

**Step 10: Authorized Reconstruction**

If user authentication and integrity check are successful, recover and decrypt image ( $K_s$ ). The cloud archive does not store the data of the diagnostic information in plain text, but rather medical-image objects in an encrypted form. This can be stored as each record can be represented as:

$$R_c = \{ID, C_I, C_M, A, K_P, T\},$$

The metadata ( $C_M$ ) is encrypted, and the protected key information ( $K_P$ ). Detach encryption keys from image ciphertext to minimise impact of unauthorised access to cloud storage. Access control is implemented to allow only authorized and authenticated users, like radiologists, clinicians or approved healthcare applications, to access encrypted medical records. Before the content is decrypted, an integrity value is computed and compared to a value received:

$$A' = H(C_I \parallel ID \parallel T).$$

**Step 11: The decryption operation proceeds only when**

$$A' = A.$$

If not, the image is deemed to be tampered or corrupted. Once they've been verified, the original image is reconstructed as:

$$I' = Dec_{\{K_s\}(C_I)}.$$

**Step 12: For lossless medical-image recovery,**

$$I' = I.$$

This is especially critical because it is important that the characteristics of images are not changed in such a way as to compromise the diagnostic value of the images in an encrypted system for encryption/decryption.

**5. Results and Discussion**

The performance of the proposed Resource-Constrained Encryption Framework (RCEF) is evaluated through the experimental results, which show the effectiveness of the proposed technique to achieve a trade-off between medical-image security and computational efficiency. Various device-resource settings were determined by the performance of the CT, MRI, X-ray and ultrasound images. The proposed approach was compared with AES-128, AES-256, ECC assisted hybrid encryption and a traditional lightweight method of encryption. The time required for encryption and decryption, throughput, CPU usage, memory usage, energy usage, entropy, NPCR, UACI, adjacent-pixel correlation, and reconstruction accuracy were used to evaluate the analysis. Average performance is shown in representative medical images in Table 2.

The proposed RCEF recorded the lowest encryption and decryption latency, which results in the encryption latency to be decreased from 46.8ms with AES-128 to 27.6ms, about 41%. It also achieved the best throughput performance of 36.2 MB/s, while using less CPU and memory, making it suitable for resource-constrained IoMT and edge healthcare devices. RCEF

dynamically adapts the encryption based on the available CPU, memory, energy and bandwidth. It used just 0.52 J for each encryption operation, which is around 39.5% less than AES-128 and 60.3% less than ECC-Hybrid encryption. These findings show higher computational and energy efficiency, especially for energy-constrained medical devices like batteries. To evaluate the security effectiveness, entropy, pixel correlation and NPCR, UACI were used.

**Table 2**  
**Computational Performance Comparison**

| Method        | Encryption Time (ms) | Decryption Time (ms) | Throughput (MB/s) | CPU (%) | Memory (MB) |
|---------------|----------------------|----------------------|-------------------|---------|-------------|
| AES-128       | 46.8                 | 43.5                 | 21.4              | 58.6    | 42.7        |
| AES-256       | 55.7                 | 51.9                 | 18.0              | 64.8    | 48.3        |
| ECC-Hybrid    | 68.4                 | 63.2                 | 14.6              | 71.5    | 53.6        |
| Lightweight   | 35.9                 | 33.4                 | 27.9              | 46.2    | 35.1        |
| Proposed RCEF | 27.6                 | 25.8                 | 36.2              | 38.7    | 29.4        |

The results of encryption and decryption time of RCEF were 27.6ms and 25.8ms, respectively, so that RCEF could obtain the lowest processing latency as shown in Figure 1. These results showed that these modes of encryption are more efficient in computation compared to AES-128, AES-256, ECC-Hybrid and lightweight encryption, which is suitable for medical imaging systems that are resource-limited.

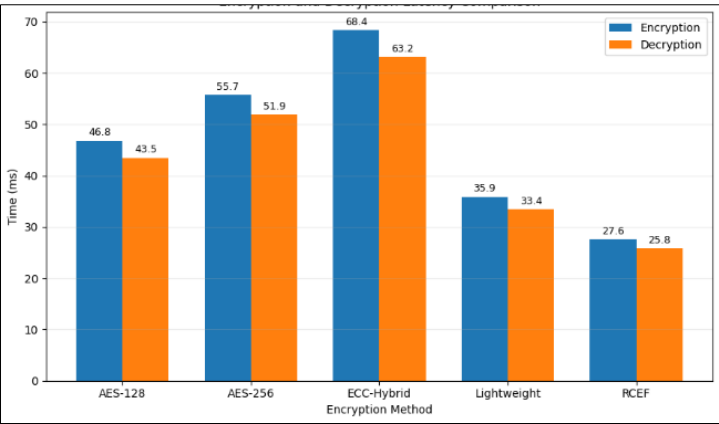


**Figure 1**  
**Encryption and decryption latency comparison**

## 6. Security and Privacy Analysis

Security and privacy analysis of the proposed Resource-Constrained Encryption Framework (RCEF): Security and privacy analysis of the proposed

Resource-Constrained Encryption Framework (RCEF) is a study on its ability to safeguard sensitive medical images and patient data during transmission, storage in cloud computing, and retrieval. Major security requirements and potential threats are taken into account, such as confidentiality, Statistical attack and Differential attack, Brute force, Tampering with data, Replay attack, Compromising the key, and Illegal access. Special focus is placed on security while maximizing computational efficiency in resource-limited environments such as healthcare and IoMT.

#### *A. Medical Image Confidentiality*

RCEF will encrypt medical images and sensitive DICOM metadata prior to sending to the cloud, to ensure that any images that are intercepted or compromised cannot be understood by unauthorized users.

#### *B. Statistical Attack Resistance*

Medical images are made resistant to statistical attacks by structuring and statistically obscuring them using a high level of randomness in the ciphertext and low adjacent-pixel correlation.

#### *C. Differential Attack Resistance*

A good NPCR and UACI test results means high sensitivity to the slight changes in plaintext images, which offers protection against differential cryptanalysis.

#### *D. Brute-Force and Key Sensitivity*

The size of the key space and the sensitivity of the key make brute-force key searches too costly and key image reconstruction using the wrong keys too meaningless.

#### *E. Integrity and Tampering Protection*

Integrity verification can identify unauthorized changes to an encrypted image or the metadata, and will not allow medical records to be accepted if they have been altered.

#### *F. Replay and Transmission Security*

Unique identifiers, timestamps, communication details and authenticated communication provide medical-image transactions protection from replay, intercept and transmission attacks. It not only resists statistical attacks and differential attacks, but also brute-force attacks, replay attacks and tampering, which enhances the confidentiality and integrity of medical images stored in the cloud. Most important, the resource-aware mechanism ensures critical security requirements without increasing processing and energy consumption. Thus, RCEF can effectively satisfy the requirements of security, privacy of the patient, and resource efficiency, which enables it to be deployed in cloud medical imaging archives, IoMT devices, and edge-based healthcare systems.

## 7. Conclusion and Future Work

In this study, the authors have put forward a Resource-Constrained Encryption Framework (RCEF) for secure and efficient medical image archiving in the cloud environment. This framework integrates resource assessment, adaptive encryption, key management, integrity checking, secure communication, cloud storage and authorized reconstruction, and takes into account resource constraints. Based on the evaluation results by CT, MRI, X-ray, and ultrasound pictures, RCEF decreases CPU and memory consumption, encryption/decryption time, energy consumption and increases throughput. Security analysis showed that there is high entropy, low pixel correlation, high NPCR and UACI, and high key sensitivity. Lossless reconstruction also assures the preservation of diagnostic information. In summary, RCEF offers a seamless way to achieve security and resource efficiency, making it a promising solution for IoMT, edge healthcare and portable diagnostic systems. Future work will focus on adaptive encryption using ML, hardware accelerators, post-quantum security, larger clinical datasets, integration with PACS/DICOM, integration with blockchain auditing, and Zerotrust access mechanisms.

## References

- [1] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865 (2021).
- [2] G. Aceto, V. Persico, and A. Pescapé, "Industry 4.0 and health: Internet of Things, big data, and cloud computing for Healthcare 4.0," *J. Ind. Inf. Integr.*, vol. 18, Art. no. 100129 (2020).
- [3] N. Anandik, S. S. Muni, and A. Kaushik, "DICOM compatible, 3D multimodality image encryption using hyperchaotic signal," *arXiv preprint arXiv:2504.20689* (2025).
- [4] J. Arif, M. A. Khan, B. Ghaleb, J. Ahmad, A. Munir, U. Rashid, and A. Y. Al-Dubai, "A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution," *IEEE Access*, vol. 10, pp. 12966–12982 (2022).
- [5] J. Koppitz and S. Worawiset, "Congruence of order-decreasing and order-preserving on transformations with fixed point," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 7, pp. 2607–2619 (2025), doi: 10.47974/JDMSC-1841.
- [6] S. Sharma and A. Aggarwal, "A new approach for effective retrieval of medical images: A step towards computer-assisted diagnosis,"

- J. Imaging*, vol. 10, no. 9, Art. no. 210 (2024), doi: 10.3390/jimaging10090210.
- [7] P. Panahi, C. Bayılmış, U. Çavuşoğlu, and S. Kaçar, "Performance evaluation of lightweight encryption algorithms for IoT-based applications," *Arab. J. Sci. Eng.*, vol. 46, no. 4, pp. 4015–4037 (2021), doi: 10.1007/s13369-021-05358-4.
- [8] Y. Zhu, X. Yin, A. W. C. Liew, and H. Tian, "Privacy-preserving in medical image analysis: A review of methods and applications," *arXiv preprint arXiv:2412.03924* (2024).
- [9] Y. Chen, C. Tang, and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 167, Art. no. 107286 (2020).
- [10] Z. Tabatabaei, Y. Wang, A. Colomer, J. Oliver Moll, Z. Zhao, and V. Naranjo, "WWFedCBMIR: World-wide federated content-based medical image retrieval," *Bioengineering*, vol. 10, Art. no. 1144 (2023).
- [11] N. S. Noor, D. A. Hammood, A. Al-Naji, and J. Chahl, "A fast text-to-image encryption-decryption algorithm for secure network communication," *Computers*, vol. 11, no. 3, Art. no. 39 (2022).
- [12] I. Ahmad, M. S. Uzzal, and S. Shin, "Secure retrieval of brain tumor images using perceptual encryption," in *Proc. 2025 IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Kota Kinabalu, Malaysia, pp. 73–74 (2025), doi: 10.1109/BIGCOMP64353.2025.00020.
- [13] B. Zhang and L. Liu, "Chaos-based image encryption: Review, application, and challenges," *Mathematics*, vol. 11, no. 11, Art. no. 2585 (2023), doi: 10.3390/math11112585.

*Received March, 2026*