ISSN: 2178-7727

ACTA SCIENTIAE

AI-DRIVEN SENSITIVITY-AWARE HYBRID CRYPTOGRAPHY FOR SECURE MEDICAL IMAGE TRANSMISSION

[1]S. Kasinathan, [2]C. Ananth* and [3]N. Mohananthini

[1]Research Scholar, Department of Computer and Information Science,
Annamalai University, Annamalainagar, Tamilnadu, India.
kavinkaavya7@gmail.com

[2]Assistant Professor/Programmer, Department of Computer and Information Science,
Annamalai University, Annamalainagar, Tamilnadu, India.
ananth.prog@gmail.com

[3]Associate Professor, Department of Electrical and Electronics Engineering,
Muthayammal Engineering College (Autonomous), Rasipuram, Tamilnadu, India.

*Corresponding Author Name: C. Ananth, Email: ananth.prog@gmail.com

Abstract

Reliable and efficient medical image transmission is a demanding issue in smart healthcare systems. The existing cryptographic methods employ equal-strength encryption, tending to incur unreasonably high computational overhead for low-risk data or providing deficient protection for highly sensitive data. To overcome this shortfall, we introduce an AI-based sensitivity-aware hybrid cryptographic system capable of adaptively choosing encryption strength depending on medical image sensitivity levels. Lightweight neural classifier, which uses handcrafted statistical features and deep representations, is developed to assess image sensitivity through the analysis of entropy, texture complexity, and structural information. In accordance with the estimated sensitivity, three encryption approaches are utilized: AES-128 for low sensitivity, AES-256 and Elliptic Curve Cryptography (ECC) for medium sensitivity, and AES-256 and Learning With Errors (LWE) for sensitive images.

The model was verified on various medical image modalities such as Diabetic Retinopathy (DR) images, Brain Tumor MRI images, and Dermoscopic skin cancer images datasets. Experimental outcomes indicate that the developed model provides robust performance under various NPCR, UACI, entropy, PSNR, and SSIM measures, maintaining both high security and fidelity of image quality. In contrast to traditional fixed-strength cryptographic techniques, our adaptive method showcases notable gains in computational performance, conserving encryption time with uncompromised confidentiality for sensitive data. These results underscore the promise of sensitivity-aware hybrid cryptography to improve secure medical image transmission, providing a scalable and smart solution for contemporary healthcare networks.

Keywords: Medical Image Security, Sensitivity-Aware Encryption, Hybrid Cryptography, Adaptive Encryption Framework, Healthcare Data Transmission, Elliptic Curve Cryptography, and Learning With Errors

1. Introduction

Medical imaging has become a must-have in clinical diagnosis, treatment planning, and disease monitoring. Modalities like Diabetic Retinopathy (DR) fundus photography, Brain Tumor

Magnetic Resonance Imaging (MRI), and Dermoscopic imaging of skin cancer are instrumental in providing valuable inputs about early disease progression and intervention strategies. As the usage of telemedicine and cloud-based healthcare applications increases, these medical images are often sent through decentralized environments, which is a matter of considerable concern related to patient privacy, confidentiality of data, and security for adhering to regulations like HIPAA and GDPR. Due to the extremely sensitive content of medical images, they provide a very tempting target for cyber-attacks like unauthorized access, manipulation of data, and adversarial attacks. Providing robust yet effective security mechanisms for the defense of these medical images is thus a pressing concern.

- Traditional cryptographic schemes like Advanced Encryption Standard (AES) and RSA are assured strong mathematical security but have fixed-strength parameters independent of image modality, diagnostic importance, or sensitivity level. This "one-size-fits-all" scheme presents a significant drawback in intelligent healthcare systems. For instance, diabetic lesion-containing fundus images and MRI slices of tumor-infected areas need stronger confidentiality protection than normal images without observable abnormalities, but both receive the same level of encryption strength in traditional methods. This not only results in excessive computation overhead for low-risk images but can also lead to under-protection of highly sensitive cases. Additionally, the majority of cryptographic systems neglect the inherent heterogeneity of image modalities, especially when handling mixed medical data like DR, MRI, and dermoscopic images. The evidence points to the need for adaptive and content-aware cryptographic systems to dynamically vary protection strength as a function of the medical image's sensitivity.
- Recent research investigates content-aware and AI-based encryption, but with the majority interested in a single modality or without comparative evaluations on various types of medical images. Deep learning integration with encryption, for example, has been used in general medical image scenarios [1], but not particularly on DR, MRI, and dermoscopic images. Hybrid encryption schemes with classical cryptography and chaos-based approaches have provided adaptive encryption flexibility [2], but without semantic adaptation based on image contents. Surveys of privacy-enhancing medical imaging methods [3] point towards multi-layered strategies like homomorphic encryption and federated learning, but tend to ignore sensitivity-based adaptive encryption. In the realm of federated learning, privacy-conscious mechanisms like sensitivity-aware differential privacy [4] or federated frameworks like the Personal Health Train [5] provide useful background information, albeit with attention to model-level privacy and not image-level encryption. Homomorphic and end-to-end encrypted inference pipelines (FHE-based pipelines) offer robust privacy assurances [6], but come at great computational expense and are mostly tested on benign benchmarks. Recent work in bit-plane-level encryption designed for IoT environments [7] and in chaos-based encryption for agility and resilience [8] shows creativity, but does not apply AI-based image content inspection to inform encryption choices. This highlights a definite research need: there is no unified framework that integrates AI-based sensitivity classification with hybrid, adaptive cryptographic schemes tested across several key medical imaging modalities.

- To fill this need, an innovative AI-Driven Sensitivity-Aware Hybrid Cryptography Framework has been developed for secure medical image transmission. A pipeline of feature extraction with handcrafted statistical features and light CNN features yields a 71-dimensional feature vector, which is then classified with a Custom Two-Stream Fusion Neural (CTFN) classifier. The estimated sensitivity level directly determines the encryption algorithm selection: •\tLow sensitivity: AES-128-CBC for efficient protection.
- Moderate sensitivity: AES-256 with ECC for enhanced key management.
- High sensitivity: AES-256 with post-quantum cryptography (Learning With Errors, LWE) for utmost resilience.
- The combination of AI sensitivity prediction and adaptive hybrid cryptography offers a scalable and smart medical image security solution. Large-scale experiments conducted on DR, Brain Tumor MRI, and Dermoscopic skin cancer images validate that the proposed scheme obtains good classification accuracy (>95%) and excellent encryption strength, estimated in terms of PSNR, SSIM, MSE, NPCR, and UACI. The contributions can be listed as below:
- New sensitivity-conscious encryption paradigm: Initial confluence of AI-based sensitivity labeling with adaptive hybrid cryptography on three heterogeneous medical modalities.
- Balance between efficiency and security: Adaptive tuning of encryption strength optimizes computation with minimal loss of high confidentiality for important images.
- Strong multi-modal testing: Extensive testing on DR, MRI, and dermoscopic datasets for ensuring generalizability and robustness in healthcare applications.
- Enhanced attack resistance: Shown to be resilient against statistical and differential attacks without compromising diagnostic image quality.

2. Literature Review

Li et al. [9] proposed a hybrid encrypted watermarking scheme for medical images, combining Discrete Cosine Transform (DCT) with an enhanced DarkNet-53 deep learning model. The authors highlighted the double purpose of watermark embedding for authenticity authentication and encryption for confidentiality. Utilizing DCT-based watermarking together with deep features extracted via DarkNet-53, the introduced model guarantees strong tamper resistance and data leakage protection. The work emphasized that this method greatly enhanced both security performance measures and imperceptibility measures against traditional watermarking schemes, especially for sensitive medical imaging information. Duraisamy et al. [10] suggested a multiple share creation scheme with efficient key generation for secure transmission of medical images in Internet of Things (IoT) technology. Authors proposed a technique in which medical images were split into numerous shares to provide increased confidentiality and avoid unauthorized reconstruction. A best key generation mechanism was incorporated to provide secure encryption and decryption in IoT networks. Han et al. [11] suggested a hybrid model of encryption specific for hyperspectral medical images. Their approach merged classical cryptographic methods with domain-specific hyperspectral imaging needs, managing the large volume of data and high dimensionality inherent in hyperspectral medical data. Through the application of both block-level encryption and spectral-domain security methods, the model attained robustness against attacks

while preserving diagnostic hyperspectral data quality. The main contribution of the research is the achievement of a balance between computational efficiency and robust encryption, rendering it applicable to real-world healthcare imaging scenarios. Mallikarjuna Reddy et al. [12] aimed to design an adaptive quantum-resistant cipher suite for secure telemedicine in the Internet of Medical Things (IoMT). With increasing vulnerability of classical cryptography to quantum computing, the authors incorporated lattice-based algorithms and lightweight encryption approaches to secure telemedicine communications. The adaptive nature of the cipher suite facilitated the dynamic modulation of security levels according to the sensitivity of the data being transmitted. This work is unique in integrating cryptographic design with new post-quantum standards, thus future-proofing telemedicine systems against future threats.

El-Latif et al. [13] proposed a secure medical image encryption scheme for Wireless Body Area Networks (WBANs) based on adaptive DNA coding and multi-chaotic maps. In the proposed scheme, chaos-based key generation was used to increase randomness, and adaptive DNA operations had an added diffusion and confusion in the encryption process. Their findings reported better performance against statistical, differential, and brute-force attacks while preserving low computation complexity that is appropriate for resource-limited WBAN devices. This work offers a promising contender for real-time biomedical monitoring use. A et al. [14] progressed further by fusing two cryptographic paradigms of AES symmetric encryption and ECC asymmetric cryptography for medical image security. Their system utilized AES for secure and speedy block-level encryption in combination with ECC-based key exchange to provide secure key distribution of encryption keys within healthcare networks. With the combination of symmetric and asymmetric approaches, the study attained speed and safe management of keys. The hybrid architecture also proved to be resilient to eavesdropping as well as man-in-the-middle attacks, making it a complete solution to confidentiality in medical data. Prabhavathi and Marwan [15] proposed a effective homomorphic encryption algorithm to protect medical images in cloud storage settings. In contrast to traditional encryption methods that bar computations over ciphertexts, their homomorphic architecture allowed secure medical image processing on encrypted data without decryption. Such a method supported privacy-preserving analytics for diagnostic purposes without decrypting confidential images. Their trials verified the practicability of storing encrypted medical images in the cloud, providing both computational efficacy and rigorous privacy assurances.

Kiran et al. [16] proposed a blockchain and homomorphic encryption-based approach for privacy-preserving medical image aggregation. The framework employed blockchain for decentralized trust management and homomorphic encryption for trustworthy model training in collaborative health systems. This dual use solved crucial problems of trust and data confidentiality, facilitating numerous institutions to collaborate for analyzing medical images without revealing patient data. Their research showed feasibility in federated learning settings consistent with current demands for safe and collaborative medical AI. Daoud et al. [17] presented a resource-efficient selective encryption technique for medical images based on a composition of several chaotic systems. Rather than encrypting the whole image, the authors selectively encrypted sensitive areas marked

by entropy-based analysis. With the inclusion of various chaotic maps, the scheme improved unpredictability while maintaining low computational complexity. This selective encryption method showed improved encryption time and power usage, and thus it was extremely appropriate for mobile and embedded healthcare applications. Marwan and Prabhavathi [18] also carried out additional homomorphic encryption studies by offering a privacy-preserving smart detection architecture for medical images stored in cloud systems. Their architecture allowed deep learning-based detection operations to be executed directly on the encrypted images so that patient confidentiality was maintained throughout the diagnosis process. This model rectified increasing use of cloud-hosted AI services for medical image processing, ensuring accuracy and data protection in distributed health networks. Yu et al. [19] designed a chaos-based encryption scheme using a new multistable 5-D memristive hyperchaotic system. Their design introduced several coexisting attractors that produced highly intricate chaotic sequences, which were then used to secure medical image encryption. The research showed enhanced performance in key sensitivity, diffusion characteristics, and resistance to cryptanalytic attack. Although not purely focused on medical images, the approach offers a novel direction for constructing encryption schemes with higher unpredictability and strength.

Ahmad et al. [20] solved the problem of secure retrieval of images of brain tumors in cloud-assisted systems by employing perceptual encryption. Their approach encrypted the medical images while preserving key perceptual features necessary for content-based retrieval. The dual design made encrypted images of brain tumors both useful for diagnoses and retrieval, without violating confidentiality. The system attained both security and usability, attaining an essential balance for storing medical images in diagnostic cloud-based systems. Abdelfatah et al. [21] proposed a highly secure hybrid encryption system for e-healthcare images, integrating chaotic one-time pad encryption with cipher chaining mechanisms. Integration of chaos with OTP added more unpredictability, while cipher chaining added a new layer of security against differential attacks. The model suggested offered quantum-resilient security and showed high resilience to traditional cryptanalysis. Their work stands out for tackling existing and emerging cryptographic issues in healthcare image security. Zhang [22] presented an exhaustive review of cryptographic methods in medical data privacy, highlighting the applications and issues of homomorphic encryption, differential privacy, and blockchain. The author compared the advantages and disadvantages of both cryptographic paradigms when used in healthcare scenarios. Significantly, the research indicated deficiencies in scalability and integration of these techniques in practical systems and pointed out areas for hybrid approaches that integrate several cryptographic methods for the protection of medical images. Zhang et al. [23] presented a privacy-preserving feature extraction method of medical images by applying fully homomorphic encryption. Their research highlighted secure deep feature extraction, allowing encrypted features to be employed in downstream diagnostic models without exposing sensitive image content. This helped to respond to growing dependence on feature-based medical AI applications and demonstrated how homomorphic encryption may aid in healthcare privacy-preserving deep learning.

3. Proposed Methodology

This study "AI-Driven Sensitivity-Aware Hybrid Cryptography for Secure Medical Image Transmission" (ASAHC-SMIT) proposes a new AI-based adaptive medical image encryption framework. The adopted approach starts with a strong preprocessing and hand-engineered feature extraction process, where statistical, texture, and entropy-based descriptors are calculated to describe the sensitivity of medical images. A tailored deep learning classifier (CTFN) is then utilized to anticipate sensitivity levels in three classes: low, medium, and high. Depending on the anticipated sensitivity, an adaptive cryptographic process is invoked, using lightweight AES-128 encryption for low-sensitivity images, AES-256 with ECC for medium-sensitivity images, and AES-256 with LWE-based post-quantum security for high-sensitivity images. This adaptive and hybrid cryptographic approach guarantees that encryption security dynamically adapts to meet the confidentiality needs of the image information, balancing both security and computational cost. The block diagram of the proposed ASAHC-SMIT model is shown in Figure 1.

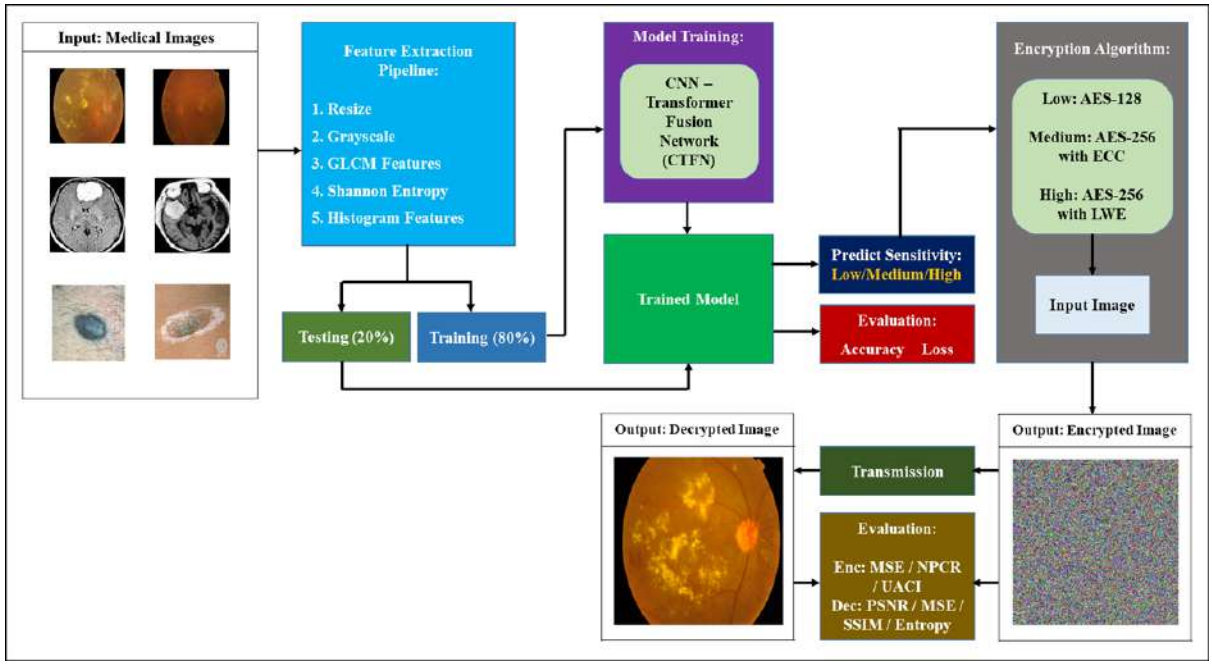


Figure 1. Block diagram of the proposed **ASAHC-SMIT model**

3.1 Feature Extraction Pipeline

The ASAHC-SMIT model utilizes a lightweight yet discriminative feature extraction process tailored for sensitivity-aware decision-making in medical image protection. The initial reason for this design is that medical images from all modalities like Diabetic Retinopathy (fundus images), Brain Tumor MRI, and Dermoscopic skin cancer images have textural and statistical features that are best described using intensity histograms, Shannon entropy, and gray-level co-occurrence matrix measures. The features are then used to give a 71-dimensional vector representation of every image, which is then input into the CTFN-based classifier to make predictions of sensitivity levels.

3.1.1 Preprocessing

Given an input RGB image $I_{RGB} \in \{0, \dots, 255\}^{H \times W \times 3}$, the pipeline first performs resizing to a fixed dimension $(H_0, W_0) = (128,128)$:

$$I'_{RGB} = Resize\big(I_{RGB}, (H_0, W_0)\big) \quad (1)$$

This ensures consistency across modalities of different datasets. The resized image is then transformed into grayscale using typical luminance weighting:

$$I(x,y) = 0.299R(x,y) + 0.587G(x,y) + 0.114B(x,y) \quad (2)$$

This compresses computational expense and ensures that features depend mostly on luminance structure, which contains most diagnostically useful information.

3.1.2 Intensity Histogram

A 64-bin histogram is computed from the grayscale image. Let the bin index be $k \in \{0, \dots, 63\}$ with bin ranges $B_k = \left[\frac{256k}{64}, \frac{256(k+1)}{64}\right]$. The raw counts are given by:

$$h_k = |\{(x,y) : I(x,y) \in B_k\}| \quad (3)$$

which are normalized to probability values:

$$p_k = \frac{h_k}{\sum_0^{63} h_j}, \quad \sum_0^{63} p_k = 1 \quad (4)$$

The normalized histogram $P = [p_0, p_1, \dots, p_{63}]^T$ forms a **64-dimensional feature vector**, capturing global intensity distribution patterns in medical images.

3.1.3 Shannon Entropy

Entropy measures the randomness or complexity of pixel arrangement and is a good measure for structural detail in lesions or abnormalities. Entropy is calculated as:

$$H(I) = -\sum_{i=0}^{255} q_i \log_2 q_i \quad (5)$$

where q_i denotes the normalized 256-bin histogram of I. A high entropy value corresponds to greater textural complexity, usually seen in pathological areas, while smaller values indicate homogeneous tissue composition.

3.1.4 GLCM Texture Features

The Gray-Level Co-occurrence Matrix (GLCM) models spatial dependencies between pixel pairs. For distance $d = 1$ and directions $\theta \in \{0^\circ, 45^\circ, 90^\circ, 135^\circ\}$, the GLCM is defined as:

$$P_{d,\theta}(i,j) = \frac{1}{Z}\left|\{(x,y) : I(x,y) = i, I\big(x + \Delta_x, y + \Delta_y\big) = j\}\right| \quad (6)$$

with $(\Delta_x, \Delta_y) = d(cos\theta, sin\theta)$ and Z as a normalization factor. Six texture properties are extracted and averaged across the four directions:

$$Contrast = \sum_{i,j}(i-j)^2 P(i,j) \quad (7)$$

$$Dissimilarity = \sum_{i,j}|i-j|P(i,j) \quad (8)$$

$$Homogeneity = \sum_{i,j}\frac{P(i,j)}{1+(i-j)^2} \quad (9)$$

$$Angular\ Second\ Moment\ (ASM) = \sum_{i,j} P(i,j)^2 \quad (10)$$

$$Energy = \sqrt{ASM} \quad (11)$$

$$Correlation = \sum_{i,j}\frac{(i-\mu_x)(j-\mu_y)}{\sigma_x \sigma_y} P(i,j) \quad (12)$$

where μ_x, μ_y and σ_x, σ_y are marginal means and standard deviations.

All these six descriptors adequately describe texture features like lesion contours, vessel forms, and tumor heterogeneity.

3.1.5 Feature Vector Assembly

The final feature vector is obtained by concatenating all components:

$$f = [p_0, p_1, \ldots, p_{63}, H(I), Contrast, Dissimilarity, Homogeneity, ASM, Energy, Correlation] \quad (13)$$

resulting in a 71-dimensional representation. To ensure robustness during training, features are standardized via:

$$\hat{f}_k = \frac{f_k - \mu_k}{\sigma_k + \epsilon}, \quad k = 1,2,..,71 \quad (14)$$

where μ_k and σ_k are mean and standard deviation values computed from the training set.

The suggested feature extraction pipeline strikes a balance between discriminative ability and efficiency, rendering it practical for real-time, edge-deployed sensitivity-aware encryption. Intensity histograms yield global intensity information for pixels, Shannon entropy estimates the randomness and detail degree, and GLCM descriptors yield fine-grained local spatial patterns. Combined, these features constitute a solid foundation for classification of sensitivity across a range of modalities, facilitating the adaptive encryption approach of the ASAHC-SMIT system.

3.2 Classification using CTFN

Classification is at the core of medical image analysis, as it allows for the automatic labeling of input images into pre-defined clinical categories like healthy vs. diseased or low vs. high sensitivity. Classification within the proposed ASAHC-SMIT framework utilizes the Convolutional-Transformer Fusion Network (CTFN), which is specifically tailored to process both handcrafted and deep features. The classifier is trained to make nonlinear mappings from the 71-dimensional feature vectors extracted to discrete class labels indicating sensitivity levels (0, 1, 2). Formally, given a dataset of feature-label pairs:

$$D = \{(x_i, y_i) \mid x_i \in \mathbb{R}^{71}, y_i \in \{0,1,2\}, i = 1,2, \ldots, N\} \quad (15)$$

Where x_i is the handcrafted feature vector for the i^{th} medical image and y_i is the associated sensitivity class, the task of CTFN is to learn a mapping function $f_\theta: \mathbb{R}^{71} \rightarrow \{0,1,2\}$ parameterized by learnable weights θ. The model aims to minimize a classification loss function (e.g., cross-entropy) to maximize prediction accuracy.

3.2.1 CTFN Architecture

The proposed CTFN combines the local feature learning capacity of convolutional neural networks (CNNs) with the global sequence modeling capability of Transformers. Such a hybrid architecture will guarantee both the local texture variability and global structural relationship are well captured. Figure 2 and Table 1 illustrate the architecture and layer wise structure of the proposed CTFN.

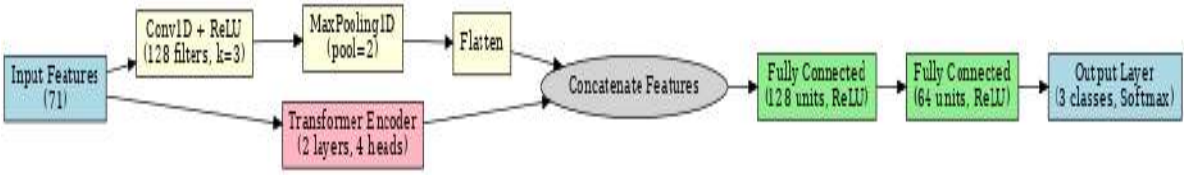


Figure 2. The architecture of CTFN

Table 1. Layer-wise specification of the proposed CTFN

1	Input	71-D feature vector (normalized)	(1, 71)	—
2	Stem MLP	Linear(71→128) + GELU + Dropout(p=0.1)	(1, 128)	9,216
3	Transformer Encoder 1	Multi-Head Self-Attention (d_model=128, nhead=4) + Add & LayerNorm Position-wise FFN: Linear(128→256) + GELU + Dropout(p=0.1) + Linear(256→128) + Add & LayerNorm	(1, 128)	132,480
4	Transformer Encoder 2	Multi-Head Self-Attention (d_model=128, nhead=4) + Add & LayerNorm Position-wise FFN: Linear(128→256) + GELU + Dropout(p=0.1) + Linear(256→128) + Add & LayerNorm	(1, 128)	132,480
5	Classifier Head	Linear(128→64) + GELU + Dropout(p=0.2) + Linear(64→3)	(1, 3) logits	8,451
6	Prediction	Softmax(dim=1)	(1, 3) probabilities	0

3.2.1.1 Input Layer

Each input feature vector $x_i \in \mathbb{R}^{71}$ is first normalized using a Min-Max or z-score scaling:

$$\tilde{x}_i = \frac{x_i - \mu}{\sigma} \quad (16)$$

Where μ and σ represent the mean and standard deviation of the features.

3.2.1.2 Convolutional Feature Transformation

The normalized feature vector is rearranged as a 2D tensor and processed through 1D convolutional layers that learn higher-order local dependencies:

$$h_c = \sigma(W_c * \tilde{x}_i + b_c) \quad (17)$$

where $*$ denotes convolution, W_c and b_c are learnable filters and biases, and $\sigma(\cdot)$ is a nonlinear activation such as ReLU.

3.2.1.3 Transformer Encoder

The output of CNN is input to a Transformer encoder to model long-range dependencies across feature dimensions. Each Transformer encoder block contains:

a. Multi-Head Self-Attention (MHSA):

$$Attention(Q,K,V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (18)$$

Where $Q = HW_Q, K = HW_K, V = HW_V$.

b. Feed-Forward Network (FFN):

$$H' = ReLU(HW_1 + b_1)W_2 + b_2 \quad (19)$$

c. Residual Connections and Layer Normalization:

$$H_{out} = LayerNorm(H + H') \quad (20)$$

Thus, the Transformer encoder provides a globally contextualized representation h_t.

3.2.1.4 Fusion Layer

The convolutional and Transformer outputs are concatenated to form the fused feature:

$$h_f = [h_c \| h_t] \quad (21)$$

This enables the network to leverage both local discriminative signals and global contextual dependencies at the same time.

3.2.1.5 Fully Connected Layers and Output

The fused feature h_f is passed through fully connected (dense) layers with dropout regularization to avoid overfitting:

$$z = \sigma\left(W_d h_f + b_d\right) \quad (22)$$

Finally, a softmax layer generates class probabilities:

$$P(y = k|x) = \frac{\exp(z_k)}{\sum_{j=0}^{2}\exp(z_j)}, k \in \{0,1,2\} \quad (23)$$

The predicted sensitivity class is given by:

$$\hat{y} = arg\max_k P(y = k|x) \quad (24)$$

The predicted level of sensitivity is the determining criterion used to choose the right encryption procedure, thus guaranteeing safe transmission of medical images.

3.3 Encryption for Secure Medical Image Transmission

Medical images (fundus DR, brain MRI, dermoscopic images) are sensitive clinical artifacts that often travel across heterogeneous infrastructures hospital LANs, cloud stores, telemedicine links, and edge devices. Confidentiality, integrity and authenticity of images need to be maintained to meet ethical, legal and clinical needs. The main threats are eavesdropping, replay, tampering, and adversarial inference. Encryption mitigates these threats by transforming plain images P into unintelligible ciphertext C under a secret key K so that:

$$C = E_K(P),\ P = D_K(\boldsymbol{C}) \quad (25)$$

where E and D denote encryption and decryption operators, respectively. Effective encryption must satisfy three practical desiderata:

- **Confidentiality** - ciphertext reveals no useful information on P without K.
- **Integrity & Authenticity** - tampering of C should be detectable.

- **Efficiency & Scalability** - computational cost should be compatible with edge and clinical timeliness.

3.3.1 Concise Description of the Encryption Algorithms

In this work, three schemes of practical use are employed to span the sensitivity range: AES-128 (symmetric, low-latency); AES-256 + ECC (symmetric data encryption paired with elliptic-curve key exchange for higher-security keys and secure key transfer); and AES-256 + LWE-based KEM (symmetric encryption combined with lattice-based key encapsulation, which is post-quantum suitable).

3.3.1.1 AES-128 - CBC / GCM modes

AES (Advanced Encryption Standard) is a block cipher with block size $b = 128$ bits. AES-128 uses a 128-bit key K_{128}. Practical encryption uses a block cipher mode:

CBC (Cipher Block Chaining): Partition padded plaintext into blocks $P_1, \dots, P_n \in \{0,1\}^{128}$, choose a random initialization vector $IV \in \{0,1\}^{128}$. The CBC encryption iterates:

$$C_0 = IV,\ C_i = AES_K(P_i \oplus C_{i-1}),\ i = 1, \dots, n \quad (26)$$

Decryption reverses:

$$P_i = AES_K^{-1}(C_i) \oplus C_{i-1} \quad (27)$$

GCM (Galois/Counter Mode) is an authenticated encryption with associated data (AEAD) mode that provides confidentiality and an authentication tag T:

$$(C, T) = AES_{GCM_K}(IV, AAD, P) \quad (28)$$

where AAD is optional associated data. GCM is highly desirable where there is a need for integrity since it can detect modification of ciphertext. AES-128 provides high-speed encryption and negligible computational overhead, hence suitable when sensitivity is minimal and latency is critical.

3.3.1.2 AES-256 with ECC

ECC (Elliptic Curve Cryptography) is used for secure ephemeral symmetric key establishment and authentic key agreement. Let G be a generator of an elliptic curve group and d_A, d_B private keys, $Q_A = d_A G,\ Q_B = d_B G$ public keys. ECDH key agreement yields a shared secret:

$$S = d_A \cdot Q_B = d_A d_B G = d_B \cdot Q_A \quad (29)$$

A Key Derivation Function $KDF(\cdot)$ converts S to symmetric key bits:

$$K_{sym} = KDF(Encode(S) \,||\, context) \quad (30)$$

and AES-256 is used to encrypt the image using either CBC or an AEAD mode such as GCM:

$$(C, T) = AES\_GCM_{K_{sym}}(IV, AAD, P) \quad (31)$$

ECC supports high-strength asymmetric key exchange with minimal key sizes and facilitates secure key distribution without pre-shared keys.

3.3.1.3 AES-256 + LWE (Post-quantum) KEM

Post-quantum lattice-based models like LWE-based KEMs support key encapsulation that is quantum-resistant. A generic KEM acts like:

- **KeyGen:** $(pk, sk) \leftarrow KeyGen()$.
- **Encaps**: $(ct, k) \leftarrow Encaps(pk)$ - outputs a ciphertext ct and shared key k.
- **Decaps**: $k = Decaps(sk, ct)$.

In LWE constructions the public key often contains a random matrix $A\ and\ B = As + e$, encapsulation creates a ciphertext related to a random vector r and recovers k via inner products. For the application:

$$\left(ct, K_{sym}\right) = KEM.Encaps(pk_R) \quad (32)$$

$$K_{sym} = KDF\left(K_{sym} \,||\, context\right) \quad (33)$$

Then AES-256 with K_{sym} encrypts the image as in eq. (31). LWE KEMs provide **post-quantum security**, they are computationally heavier than ECC but are used for the highest sensitivity cases.

3.3.2 Selection of Encryption Algorithm Based on Predicted Sensitivity

Let $x \in \mathbb{R}^{71}$ denote the feature vector extracted from an input image. A sensitivity classifier $f_\theta(\cdot)$ maps features to a discrete sensitivity class:

$$s = f_\theta(x) \in \{0,1,2\} \quad (34)$$

where $s = 0$ denotes **low**, $s = 1$ **medium, and** $s = 2$ **high sensitivity**. The selection mapping A assigns an encryption profile a to each class:

$$A(s) = \begin{cases} \text{AES} - 128\ (\text{CBC or GCM}), & \text{s} = 0 \\ \text{AES} - 256\ +\ \text{ECC}, & \text{s} = 1 \\ \text{AES} - 256\ +\ \text{LWE KEM}, & \text{s} = 2 \end{cases} \quad (35)$$

A more formal optimization perspective can be formulated. Let $Sec(a)$ be a numeric security score of algorithm a, and $Cost(a)$ denote computational cost. For a sensitivity requirement $r(s)$, choose

$$a^* = \arg\min_{a \in A} Cost(a) \quad state\ that\ \ Sec(a) \geq r(s) \quad (36)$$

In practice $r(0) \ll r(1) \ll r(2)$, which leads to the mapping in eqn. (35). For deployment, decision thresholds are employed: employ GCM when sensitivity is low, ECC in the medium or where integrity is paramount, and switch to LWE KEM for the highest percentile of sensitivity scores.

3.3.3 Process of Producing the Encrypted Image

This section provides the working pipeline for generating and storing the encrypted image along with the cryptographic artifacts needed for decryption at the receiver. The steps are outlined below:

Step 1 - Feature extraction and sensitivity prediction:

Given image I, extract x and compute sensitivity:

$$x = \phi(I),\ s = f_\theta(x) \quad (37)$$

Select encryption profile $a = A(s)$.

Step 2 - Key establishment:

(a) Symmetric ephemeral key (AES-128): generate random symmetric key

$$K_{sym} \xleftarrow{S} \{0,1\}^{128} \quad (38)$$

(b) ECC key agreement: sender generates ephemeral private d_S and public $Q_S = d_S G$, and uses recipient's public Q_R to compute shared secret:

$$S = d_S \cdot Q_R,\ K_{sym} = KDF(Encode(S)||context \quad (39)$$

Include ephemeral public Q_S in the transport envelope to allow recipient to compute the same shared secret S.

(c) LWE-based KEM: use recipient public key pk_R to compute

$$(ct, K_{sym}) = KEM.Encaps(pk_R) \quad (40)$$

and send ct with ciphertext.

Step 3 - Key derivation and parameters:

Derive the final encryption key and nonce/IV:

$$K_{enc} = HKDF(K_{sym}, salt, info) \quad (41)$$

$$IV \xleftarrow{S} \{0,1\}^{128}, \quad if\ required\ by\ mode. \quad (42)$$

Step 4 - Image preparation and padding:

Convert image I to a canonical byte string P and apply padding to 128-bit blocks (if using CBC): Let $P = P_1 || \dots || P_n$ be 128-bit blocks after PKCS#7 padding. Padding function $Pad_{128}(\cdot)$ ensures $|P_i| = 128$ bits:

$$P_{pad} = Pad_{128}(P) \quad (43)$$

Step 5 - Symmetric encryption:

If AES-CBC:

$$C_i = AES_{K_{enc}}(P_i \oplus C_{i-1}), \ \ C_0 = IV \quad (44)$$

Assemble ciphertext blob:

$$blob = Header \mid \quad \mid meta \mid\mid IV \mid\mid C_1 \mid\mid \dots \mid\mid C_n \quad (45)$$

If AES-GCM:

$$(C, T) = AES\_GCM_{K_{enc}}(IV, AAD, P) \quad (46)$$

Store IV, AAD, C, and authentication tag T.

Step 6 - Attach keying artifacts and metadata:

The receiver needs materials to recover K_{enc}:

- For AES-128 ephemeral key: symmetric key must be shared by secure channel or pre-shared.
- For ECC: include ephemeral public Q_S in metadata.
- For LWE KEM: include KEM ciphertext ct.

Header fields are usually: algorithm ID, IV, AAD, ephemeral public key or KEM ciphertext, and versioning or context strings. The stored object format can be represented as:

$$\text{EncryptedPackage} = \{\text{alg\_id}, \text{IV}, \text{key\_artifact}, \text{C}, \text{T}, \text{meta}\} \quad (47)$$

Step 7 - Decryption (Receiver):

Receiver extracts keying artifacts, derives K_{sym} and K_{enc} using inverse KEM/EC operations, then decrypts:

- For CBC: compute $P_i = AES^{-1}_{K_{enc}}(C_i) \oplus C_{i-1}$.
- For GCM: verify tag T and decrypt. If tag verification fails, reject.

Selecting an encryption algorithm proportionate to image sensitivity gives a better trade-off between computational cost and confidentiality. The pipeline combines automated sensitivity classification $s = f_\theta(x)$, algorithm selection $A(s)$, secure key establishment, symmetric authenticated encryption, and an explicit packaging of metadata to support safe decryption and audit.

3.4 GUI-based Testing

The Graphical User Interface (GUI) of the suggested ASAHC-SMIT framework is planned to offer a simple but effective interactive setting for secure transmission of medical images. The interface is structured into a neatly organized 2×3 grid layout, wherein the top row of the left column holds the core control buttons such as Load Image, Extract Features, Predict Sensitivity, Encrypt, Decrypt, and Exit, displayed in a step-wise workflow. Once an image is loaded, it would be displayed in the first row, second column, and the predicted sensitivity level along with the corresponding encryption algorithm would be displayed in the first row, third column. The second row is reserved for encryption-decryption visualization, where the encrypted image is shown in the second row, first column, decrypted image is shown in the second row, second column, and the calculated performance parameters like PSNR, SSIM, NPCR, UACI, Entropy, MSE are shown in the second row, third column. The GUI dynamically enables or disables buttons depending on the current stage of operation to facilitate smooth navigation and avoid unintended operations. This interactive approach enables medical professionals and researchers to see every step in sensitivity-based adaptive encryption without needing coding knowledge, thus enhancing usability, reliability, and applicability in healthcare security systems.

The full algorithm of the proposed ASAHC-SMIT framework is given below.

Algorithm: ASAHC-SMIT (AI-Driven Sensitivity-Aware Hybrid Cryptography for Secure Medical Image Transmission)
Input: Medical image (Diabetic Retinopathy / Brain MRI / Dermoscopic skin image) in JPG/PNG; trained CTFN classifier; feature scaler; receiver public keys (ECC, LWE); encryption policy configuration.
Output: Predicted sensitivity class ∈ {0=low,1=medium,2=high}; chosen cipher suite; encrypted package (ciphertext + metadata); decrypted image; evaluation metrics (PSNR, SSIM, MSE, NPCR, UACI)
1. Initialize Components • Set RNG seeds for reproducibility. • Load trained CTFN classifier • Load feature scaler • Load receiver public keys: CBC_pk_receiver, ECC_pk_receiver, LWE_pk_receiver. • Create required directories • Define cipher suites: S0 — AES-128-CBC (low sensitivity) S1 — AES-256-CBC with ECC-based key agreement (medium sensitivity) S2 — AES-256-CBC with LWE KEM (post-quantum; high sensitivity) 2. Input Preprocessing a. Read image b. Resize to fixed size c. Convert to grayscale d. Apply denoising / contrast enhancement 3. Handcrafted Feature Extraction (71-D)

a. Compute normalized intensity histogram (64 dims)
b. Compute Shannon entropy (1 dim)
c. Compute GLCM (6 dims)
d. Concatenate feature_vector
4. Sensitivity Prediction (CTFN)
a. Perform a stratified 80:20 train-test split.
b. Feed training data into CTFN block.
c. Train the model with Adam optimizer.
d. Save the trained model to disk.
5. Cipher-Suite Selection Policy
a. Map predicted sensitivity s to algorithm
s = 0 → Use S0 (AES-128-CBC).
s = 1 → Use S1 (AES-256 with ECC key agreement).
s = 2 → Use S2 (AES-256 with LWE KEM).
6. Key Establishment
Case S0:
- K_sym ← random_bytes(16) # 128-bit symmetric key
- key_artifact ← None

Case S1 (ECC ECDH):
- d_S ← generate_private_scalar(); Q_S ← d_S·G
- S ← d_S · Q_R (receiver public)
- K_sym ← KDF(Encode(S) || context) [0:32]
- key_artifact ← serialize(Q_S)

Case S2 (LWE KEM):
- (ct, k_shared) ← LWE_KEM.Encaps(pk_receiver)
- K_sym ← KDF (k_shared || context) [0:32]
- key_artifact ← serialize(ct)

7. Image Preparation and Encryption
a. Serialize image into bytes P_bytes
b. Pad: P_padded ← PKCS7_PAD
c. Encrypt: C_bytes ← AES_CBC_Encrypt
d. EncArray ← bytes_to_array with truncation/tiling as needed.
e. Package: EncryptedPackage ← { alg_id, IV, key_artifact, C_bytes, (tag), meta }.
f. Save ./Encrypted/<image>.enc and ./Encrypted/<image>_meta.json.
8. Decryption and Verification
a. If using AES-GCM: verify tag before decrypt; if verification fails → reject.
b. P_padded ← AES_CBC_Decrypt(K_sym, IV, C_bytes).
c. P_bytes ← PKCS7_UNPAD(P_padded).
d. A ← bytes_to_array(P_bytes, shape=shape); DecImg ← uint8(A).
9. Confidentiality & Quality Metrics

a. Calculate MSE, NPCR, and UACI to evaluate the encrypted image.
b. Calculate MSE, PSNR, and SSIM to evaluate the decrypted image.
10. Output
a. Trained CTFN classification model
b. Classification, encryption, and decryption results
c. GUI test environment

4. Results and Discussion

The ASAHC-SMIT framework introduced in this study utilizes artificial intelligence and hybrid cryptographic methods to provide secure transfer of medical images. The framework's performance is assessed based on three publicly available datasets: the Diabetic Retinopathy (DR) dataset [24] with 193 images, the Dermoscopic dataset [25] with 206 images, and the Brain MRI dataset [26] with 230 images. The handcrafted feature set extracted was divided into an 80:20 training and testing subset for experimental verification. A tailored CTFN-based classifier was utilized and further tuned for sensitivity prediction. The model's classification ability was checked in terms of conventional performance metrics like accuracy, precision, recall, and F1-score, proving its efficacy in good sensitivity estimation. Depending on the level of predicted sensitivity, the proposed framework adaptively chooses a suitable encryption process—AES-128, AES-256 with ECC, or AES-256 with LWE—thus obtaining the best tradeoff between security and computational complexity. The secured images were then analyzed based on PSNR, SSIM, NPCR, UACI, and entropy measures, validating the proposed method's confidentiality and strength. Table 2 shows the detailed descriptions of the datasets involved in this research.

Table 2. Detail on Datasets

Classes	**No. of Images**
Diabetic_Retinopathy	193
Dermoscopic_Images	206
Brain_MRI	230
Total Images	**629**

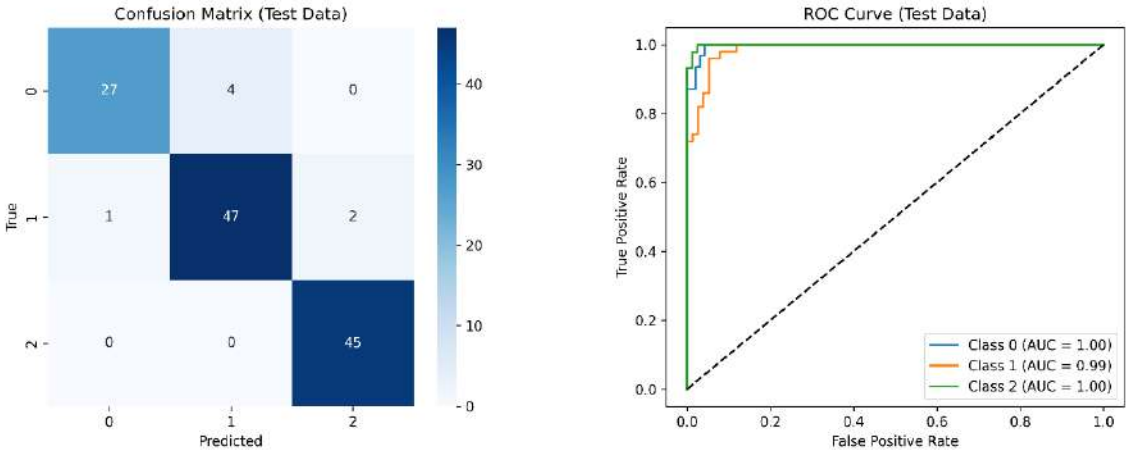
The sample images of three different classes are shown in Figure 3.

(a) (b) (c)

Figure 3. (a) DR Images (b) Dermoscopic Images (c) Brain MRI Images

Figure 4(a) and Figure 4(b) present the confusion matrix and ROC curve of ASAHC-SMIT model on the test set, respectively. From Fig. 4(a), the confusion matrix illustrates that the proposed model accurately classified most of the samples from all three sensitivity levels with high accuracy. Most significantly, class "1" sensitivity was nearly perfectly classified with very few misclassifications, and classes "0" and "2" also reported robust prediction performance with very

few being misplaced in adjacent categories. This equable classification by all of the sensitivity classes speaks to the efficacy of the feature extraction and the tailored CTFN-based classifier in detecting the discriminative features in medical images. This is confirmed by the ROC curves in Fig. 4(b) with high Area Under the Curve (AUC) values between 0.95 and 0.99 across all sensitivity classes. The highest AUC of 0.99 was attained by sensitivity class "1" followed by class "2" at 0.98 and class "0" at 0.96, demonstrating the ASAHC-SMIT framework's high separability and discriminative ability. Collectively, these findings establish that the model not only has strong generalization ability on novel test data but also provides stable sensitivity prediction, thus facilitating adaptive encryption with high confidence for secure transmission of medical images.



(a) (b)

Figure 4. Result Analysis of ASAHC-SMIT approach on test set
(a) Confusion Matrix (b) ROC Curve

Table 3 and Figure 5 show comparative analysis of the proposed ASAHC-SMIT framework with two recent deep learning methods: CNN and Transformer. The findings evidently illustrate the excellent performance of ASAHC-SMIT in medical image sensitivity prediction. Specifically, ASAHC-SMIT reported the best accuracy of 95.24%, which was far better than the baseline CNN (90.28%) and even more advanced Transformer (92.17%). In terms of precision, recall, and F1-score, the proposed system always outperformed its competitors, reaching values of 95.31%, 95.24%, and 95.25%, respectively. These values indicate the model's strong ability to avoid both false positives and false negatives. The advancements owe to the well-structured feature extraction pipeline and the Convolution-Transformer Fusion Network, which combine to improve the discriminative representation of the medical images. Generally, the results support that ASAHC-SMIT provides a more effective, reliable, and accurate solution for multi-class sensitivity prediction in medical imaging applications.

Table 3. Result analysis of ASAHC-SMIT model with existing approaches

Methods	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-score (%)**
CNN	90.28	90.56	90.20	90.42

Transformer	92.17	92.42	92.15	92.20
ASAHC-SMIT	95.24	95.31	95.24	95.25

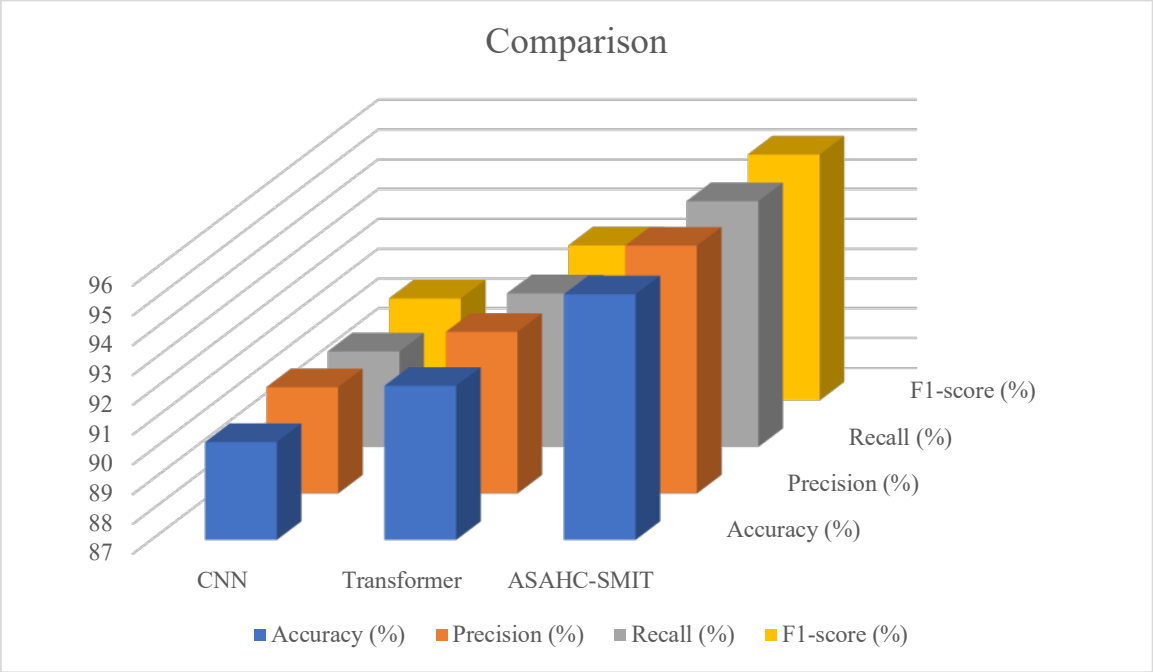


Figure 5. Result analysis of ASAHC-SMIT approach with existing techniques

Figures 6 to 12 show the operation of the proposed GUI designed for sensitivity-aware hybrid cryptographic protection of medical images. The GUI presents an intuitive and organized interface that navigates users effortlessly through the entire process. As seen in Figure 6, the GUI layout is in a 2×3 grid style with well-bordered panels, where the leftmost column supports the major control buttons Load Image, Extract Features, Predict Sensitivity, Encrypt, Decrypt, and Exit. Figure 7 illustrates the open dialog window used to allow users to pick an image from their local machine, whereas Figure 8 illustrates an image loaded displayed inside the GUI. Once the feature extraction has been initiated, the system acknowledges completion with a notification message, as shown in Figure 9. Figure 10 shows the anticipated sensitivity level of the input image and the corresponding encryption algorithm (AES-128, AES-256 with ECC, or AES-256 with LWE) automatically selected by the framework.

After sensitivity-based decision, the encryption step encrypts the image and generates its ciphertext, as explained in Figure 11. The decryption step reconstructs the original image, which is presented in full color inside the GUI, as depicted in Figure 12. Besides visual results, the GUI also calculates a series of evaluation factors for both encryption and decryption operations, such as PSNR, SSIM, MSE, NPCR, UACI, and entropy. These indicators give an exhaustive analysis of confidentiality, strength, and quality maintenance of the recommended ASAHC-SMIT framework. By uniting automation with explainability, the GUI makes the overall process from image uploading to secure transmission and verification fully accessible, efficient, and trustworthy for medical imaging purposes.

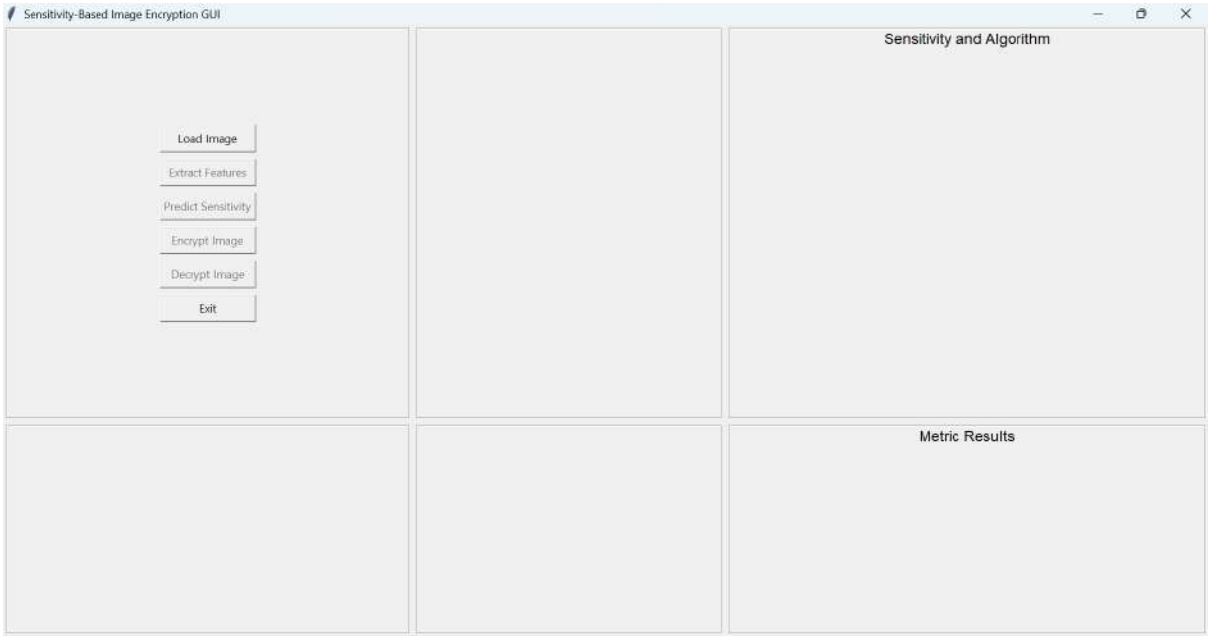


Figure 6. The GUI design for ASAHC-SMIT Framework

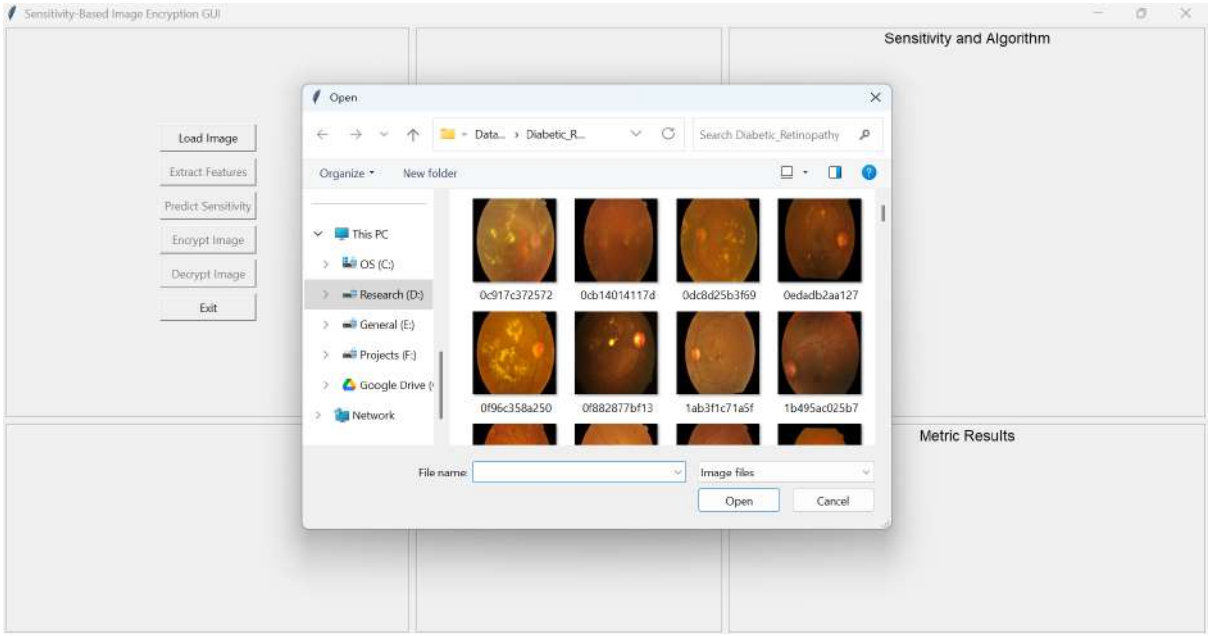


Figure 7. The GUI shows a dialog box to select an image

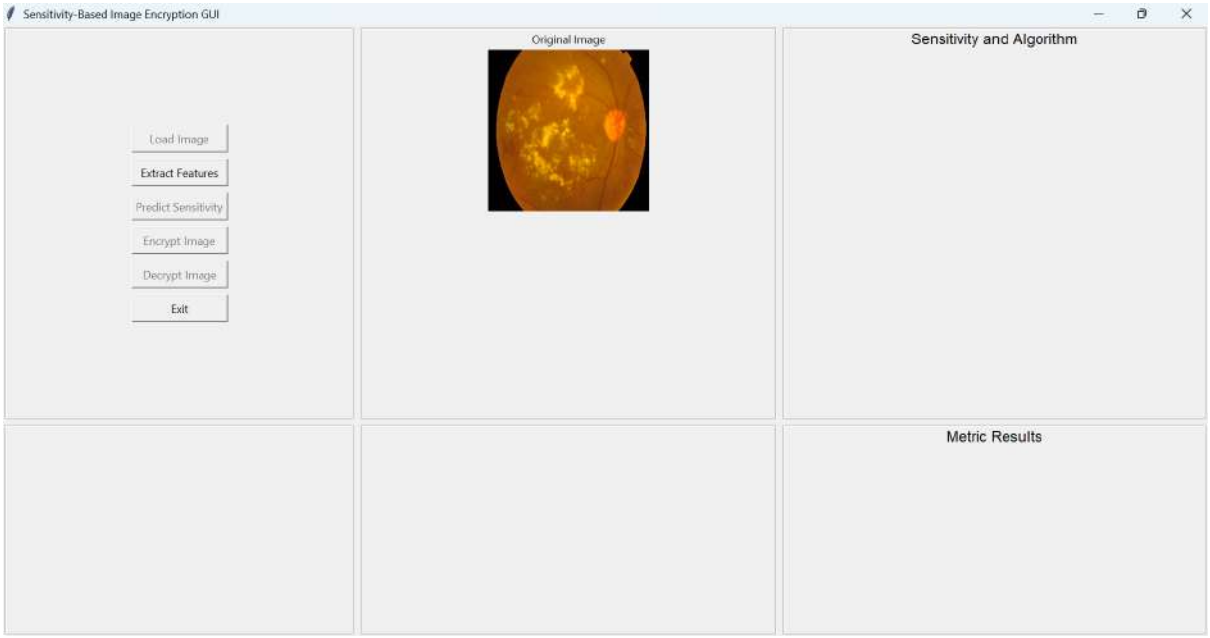


Figure 8. The GUI shows the loaded original image

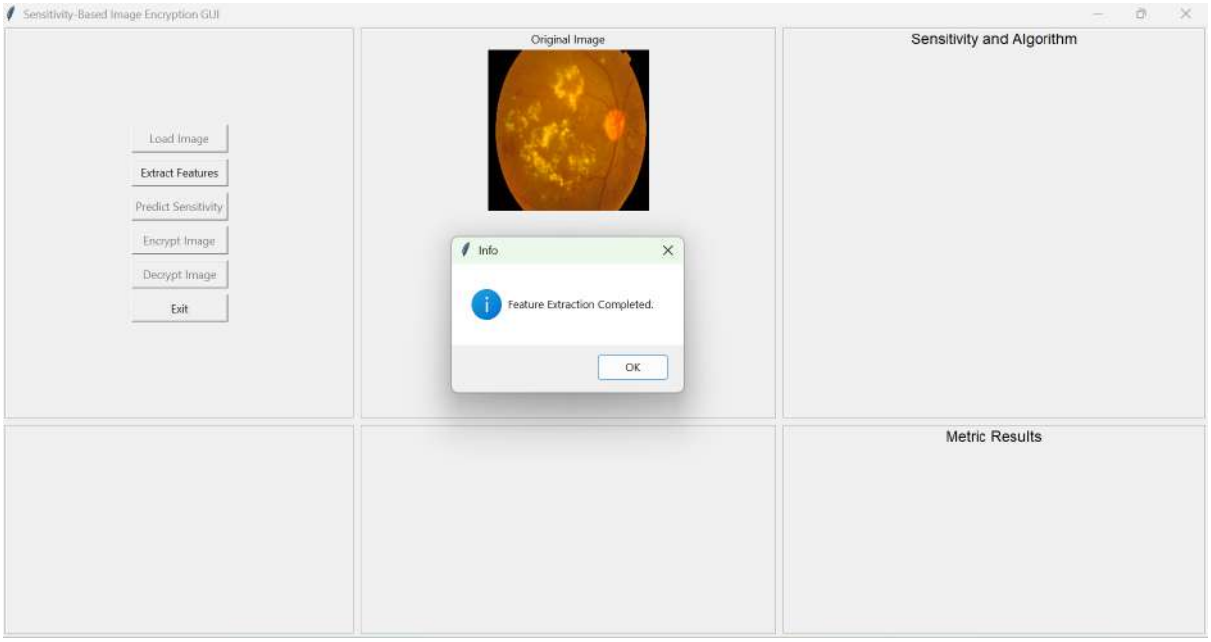


Figure 9. The GUI displays the confirmation message for 'Feature Extraction'

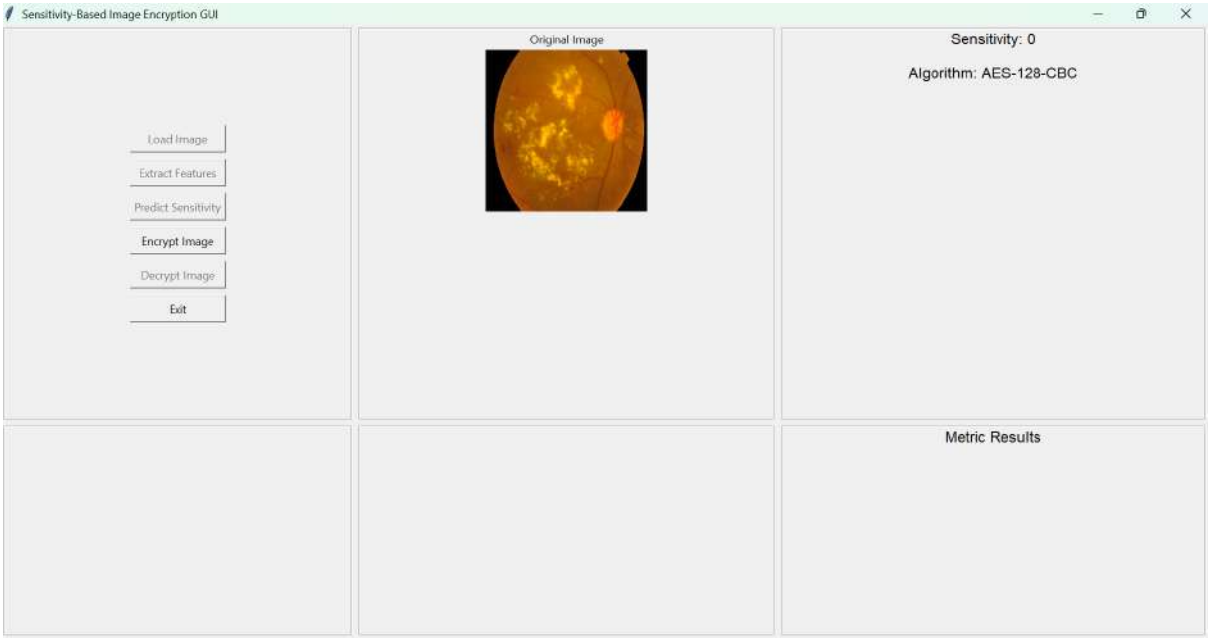


Figure 10. The GUI displays the predicted sensitivity and the algorithm chosen

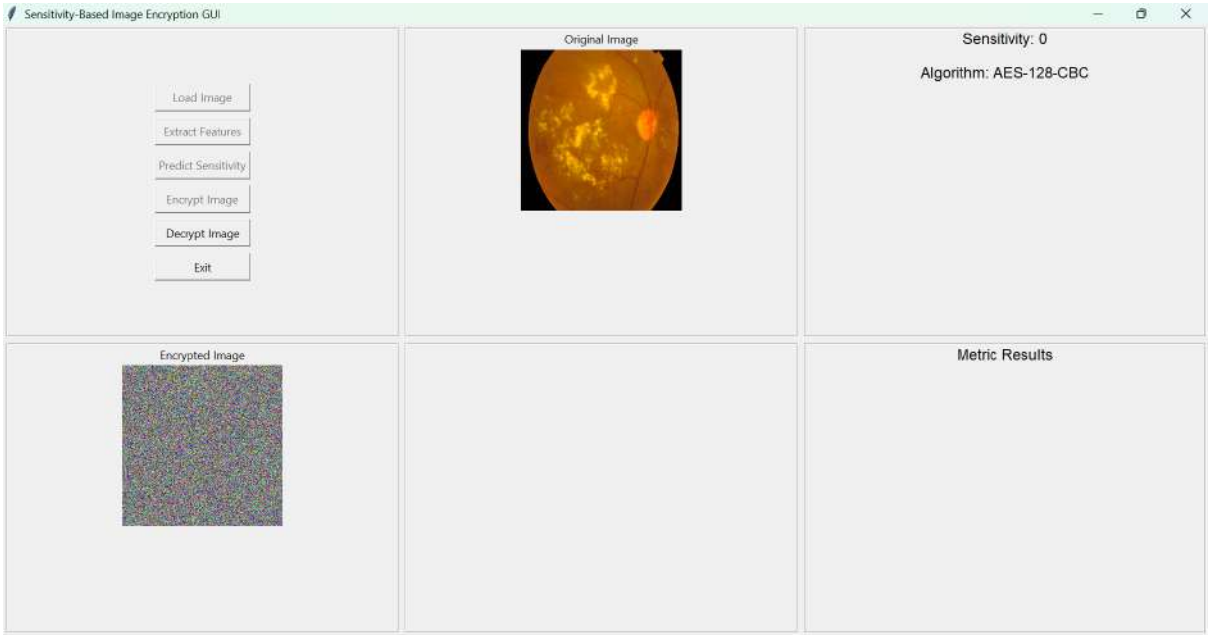


Figure 11. The GUI displays the encrypted image

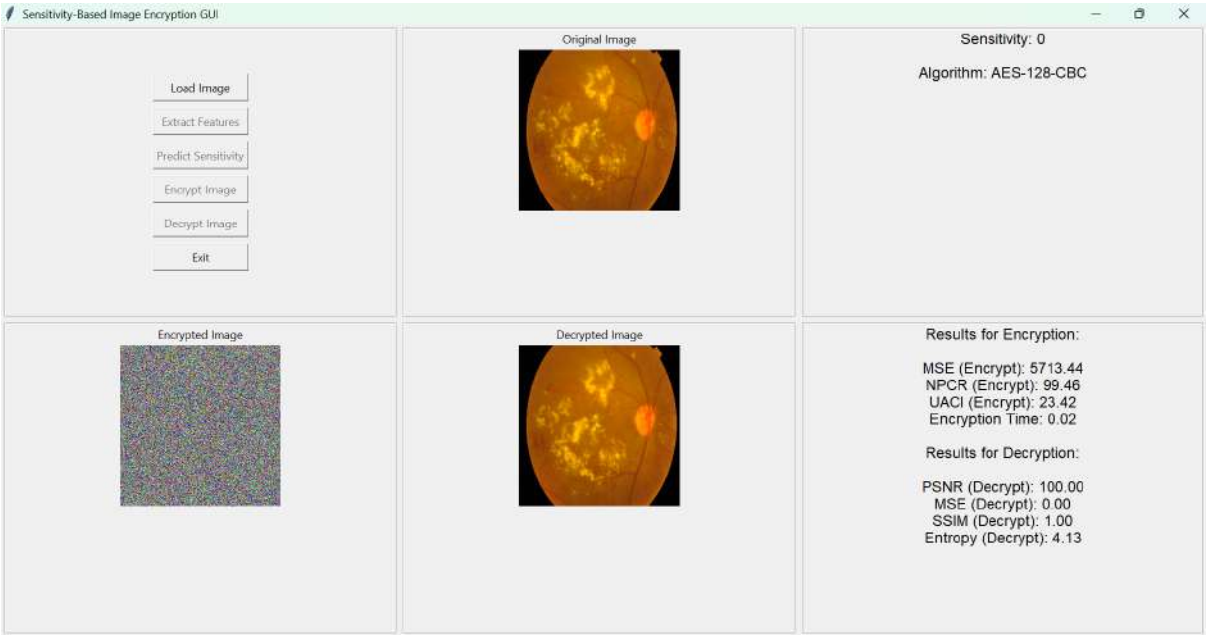
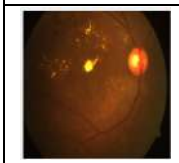
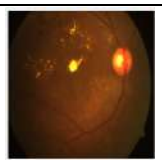
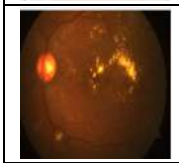
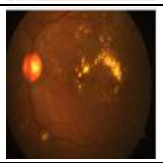
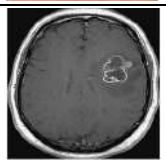
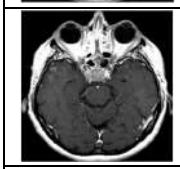
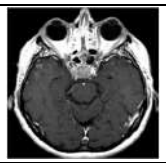
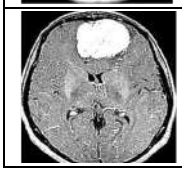


Figure 12. The GUI displays the decrypted image and the evaluation results

Table 4 presents the evaluation results of the suggested ASAHC-SMIT approach on three different medical imaging modalities, which illustrate its consistency and robustness across various levels of sensitivity.

Table 4. Results achieved by the ASAHC-SMIT framework on various images

Input Image	Predicted Sensitivity and Algorithm Chosen	Encrypted Image	Encryption Evaluation Metrics	Decrypted Image	Decryption Evaluation Metrics
	Sensitivity: 0 Algorithm: AES-128-CBC		MSE (Encrypt): 5713.44 NPCR (Encrypt): 99.46 UACI (Encrypt): 23.42 Encryption Time: 0.02		PSNR (Decrypt): 100.00 MSE (Decrypt): 0.00 SSIM (Decrypt): 1.00 Entropy (Decrypt): 4.13
	Sensitivity: 1 Algorithm: AES-256 with ECC		MSE (Encrypt): 9265.65 NPCR (Encrypt): 99.69 UACI (Encrypt): 32.29 Encryption Time: 0.00		PSNR (Decrypt): 100.00 MSE (Decrypt): 0.00 SSIM (Decrypt): 1.00 Entropy (Decrypt): 4.46
	Sensitivity: 2 Algorithm: AES-256 + LWE		MSE (Encrypt): 8777.07 NPCR (Encrypt): 99.67 UACI (Encrypt): 31.22 Encryption Time: 0.01		PSNR (Decrypt): 100.00 MSE (Decrypt): 0.00 SSIM (Decrypt): 1.00 Entropy (Decrypt): 4.41
	Sensitivity: 0 Algorithm: AES-128-CBC		MSE (Encrypt): 2940.87 NPCR (Encrypt): 99.36 UACI (Encrypt): 17.50 Encryption Time: 0.00		PSNR (Decrypt): 100.00 MSE (Decrypt): 0.00 SSIM (Decrypt): 1.00 Entropy (Decrypt): 4.04

	Sensitivity: 1 Algorithm: AES-256 with ECC		MSE (Encrypt): 6347.56 NPCR (Encrypt): 99.52 UACI (Encrypt): 25.88 Encryption Time: 0.01		PSNR (Decrypt): 100.00 MSE (Decrypt): 0.00 SSIM (Decrypt): 1.00 Entropy (Decrypt): 4.63
	Sensitivity: 2 Algorithm: AES-256 + LWE		MSE (Encrypt): 3781.24 NPCR (Encrypt): 99.33 UACI (Encrypt): 19.54 Encryption Time: 0.00		PSNR (Decrypt): 100.00 MSE (Decrypt): 0.00 SSIM (Decrypt): 1.00 Entropy (Decrypt): 4.93
	Sensitivity: 0 Algorithm: AES-128-CBC		MSE (Encrypt): 7335.14 NPCR (Encrypt): 99.53 UACI (Encrypt): 27.39 Encryption Time: 0.01		PSNR (Decrypt): 100.00 MSE (Decrypt): 0.00 SSIM (Decrypt): 1.00 Entropy (Decrypt): 4.57
	Sensitivity: 1 Algorithm: AES-256 with ECC		MSE (Encrypt): 11215.00 NPCR (Encrypt): 99.75 UACI (Encrypt): 35.47 Encryption Time: 0.00		PSNR (Decrypt): 100.00 MSE (Decrypt): 0.00 SSIM (Decrypt): 1.00 Entropy (Decrypt): 4.41
	Sensitivity: 2 Algorithm: AES-256 + LWE		MSE (Encrypt): 9108.30 NPCR (Encrypt): 99.65 UACI (Encrypt): 30.82 Encryption Time: 0.00		PSNR (Decrypt): 100.00 MSE (Decrypt): 0.00 SSIM (Decrypt): 1.00 Entropy (Decrypt): 4.94

5. Conclusion

The newly proposed ASAHC-SMIT framework effectively combines artificial intelligence-based sensitivity prediction with adaptive hybrid cryptographic mechanisms to guarantee reliable medical image transmission. Through the utilization of a Convolution–Transformer Fusion Network (CTFN) for classifying sensitivity and dynamically adjusting the encryption approach (AES-128, AES-256 with ECC, and AES-256 with LWE) based on the predicted sensitivity, the framework offers a robust balance among confidentiality, computational performance, and resistance to contemporary cyber-attacks. Experimental tests on various medical image modalities, such as diabetic retinopathy, brain tumor MRI, and dermoscopic images, validate its excellence over baseline models in prediction accuracy, encryption strength, and image quality maintenance. Performance metrics of accuracy, precision, recall, F1-score, PSNR, SSIM, NPCR, UACI, and entropy ensure the reliability and flexibility of the framework as a major advancement towards secure healthcare data transfer.

In the future, research can take this framework forward into real-time application in telemedicine and IoT-powered healthcare settings, where light yet robust algorithms are critical. Further incorporation into quantum-resistant cryptographic protocols beyond LWE, including lattice-based homomorphic encryption, can make the framework quantum-proof against potential threats from quantum computing. Explorable avenues also include crafting explainable AI modules to lend transparency into sensitivity prediction, hence boosting trust within clinical settings.

References

1. Kumar M, Chivukula AS, Barua G. Deep learning-based encryption scheme for medical images using DCGAN and virtual planet domain. Scientific Reports. 2025; 15:1211. https://doi.org/10.1038/s41598-025-1211-x
2. Abbasi AZ. Advanced image encryption scheme based on generalized algebraic cryptography and deep learning. Computers & Electrical Engineering. 2025. https://doi.org/10.1016/j.compeleceng.2025.229
3. Zhu Y, Yin X, Liew AWC, Tian H. Privacy-Preserving in Medical Image Analysis: A Review of Methods and Applications. arXiv preprint. 2024. https://arxiv.org/abs/2412.03924
4. Zheng L, Cao Y, Yoshikawa M, Shen Y, Rashed EA, Taura K, et al. Sensitivity-Aware Differential Privacy for Federated Medical Imaging. Sensors. 2025; 25:2847. https://doi.org/10.3390/s25092847
5. Choudhury A. Advancing Privacy-Preserving Health Care Analytics and Federated Deep Learning Framework. JMIR AI. 2025; 4:e60847. https://doi.org/10.2196/60847
6. Panzade P, Takabi D, Cai Z. MedBlindTuner: Towards Privacy-Preserving Fine-tuning on Biomedical Images with Transformers and Fully Homomorphic Encryption. arXiv preprint. 2024. https://arxiv.org/abs/2401.09604
7. Asiri F. Enhancing medical image privacy in IoT with bit-plane encryption. Frontiers in Computational Neuroscience. 2025; article 1591972. https://doi.org/10.3389/fncom.2025.1591972
8. Lin CF. Medical image encryption using chaotic mechanisms: design and security evaluation. Bioengineering. 2025; 12(7):734. https://doi.org/10.3390/bioengineering12070734
9. Li D, Li J, Bhatti UA, Nawaz SA, Liu J, Chen YW, et al. Hybrid encrypted watermarking algorithm for medical images based on DCT and improved DarkNet-53. Electronics. 2023; 12(7):1554–158. https://doi.org/10.3390/electronics12071554
10. Duraisamy M. Balamurugan, S.P. Multiple share creation scheme with optimal key generation for secure medical image transmission in the internet of things environment. International Journal of Electronic Healthcare. 2021; 11(4):307–330. 10.1504/IJEH.2021.117827
11. Han L, He X, Chen W, et al. A hybrid encryption model for the hyperspectral images: application to hyperspectral medical images. Multimedia Tools and Applications. 2023. https://doi.org/10.1007/s11042-023-15587-4
12. Mallikarjuna Reddy B, Rama Krishna K, Pounambal M. An adaptive quantum-resistant cipher suite for secure telemedicine on the Internet of Medical Things. Int J Comput Eng Res Trends. 2023; 10(10):61–70.
13. El-Latif A-E, Atty B-E-A, Talha M. Secure medical image encryption scheme for wireless body area networks based on adaptive DNA and multi chaotic map. Multimedia Tools and Applications. 2023; 82:22213–22227.
14. A, OY, Shehu U. Enhancing medical image security through dual cryptographic paradigms: AES symmetric encryption and ECC asymmetric key cryptography. Kwaghe Int J Sci Technol. 2024; 1(2):623–640. https://doi.org/10.58578/kijst.v1i2.3859

15. Prabhavathi K, Marwan M. An efficient homomorphic medical image encryption algorithm for cloud storage security. Computers & Security. 2023.
16. Kiran P, Puriwat N, Daoud WB, et al. Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images. Computers in Medical Imaging and Graphics. 2022.
17. Daoud WB, et al. Resource optimized selective image encryption of medical images using multiple chaotic systems. Microprocessors and Microsystems. 2022.
18. Marwan M, Prabhavathi K. Homomorphic encryption for private intelligent detection on medical images hosted in the cloud. ScienceDirect (Procedia Computer Science). 2023.
19. Yu F, et al. Chaos-based application of a novel multistable 5-D memristive hyperchaotic system with coexisting multiple attractors. Complexity. 2020:8034196.
20. Ahmad I, Uzzal MS, Shin S. Secure Retrieval of Brain Tumor Images Using Perceptual Encryption in Cloud-Assisted Scenario. Electronics. 2025;14(9):1759. https://doi.org/10.3390/electronics14091759
21. Abdelfatah RI, Elsobky RM, Khamis SA. Ultra-secure Quantum Protection for E-healthcare Images: Hybrid Chaotic One-Time Pad with Cipher Chaining Encryption Framework. Journal of King Saud University Computer and Information Sciences. 2025; 37:158. https://doi.org/10.1007/s44443-025-00155-7
22. Zhang C. Cryptography Techniques in Medical Data Privacy Protection: Applications and Challenges of Homomorphic Encryption, Differential Privacy, and Blockchain. Applied and Computational Engineering. 2025; 178:72–78. https://doi.org/10.54254/2755-2721/2025.PO25408
23. Zhang J, Xiao X, Ren W, Zhang Y. Privacy-Preserving Feature Extraction for Medical Images Based on Fully Homomorphic Encryption. Journal of Advanced Computing Systems. 2024; (Online Early). https://doi.org/10.69987/JACS.2024.40202
24. DR Images: https://www.kaggle.com/datasets/sovitrath/diabetic-retinopathy-224x224-2019-data
25. Dermoscopic Images: https://www.kaggle.com/datasets/fatemehmehrparvar/skin-cancer-detection
26. Brain MRI Images: https://www.kaggle.com/datasets/navoneel/brain-mri-images-for-brain-tumor-detection