FOREX Publication
Open Access | Rapid and quality publishing

International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 3 | Pages 807-815 | e-ISSN: 2347-470X

Secure Medical Image Transmission based on Confidence-Adaptive Chaos Encryption (CACE) over Healthcare IoT Networks

Zainab N. Abdulhameed[1*], Haraa Raheem Hatem[2], and Elaf H. Yahia[1]

[1]*Department of Electrical Engineering, University of Anbar, Iraq*
[2]*Department of Communication Engineering, University of Diyala, Iraq*

***Correspondence:** *zainab.abdulhameed@uoanbar.edu.iq*

ABSTRACT- Secure transmission of medical images over IoT networks requires strong encryption and maintenance of diagnostic value. To overcome this, this paper proposes an adaptive approach called Confidence-Adaptive Chaos Encryption (CACE) that is based on the SVM classifier confidence for choosing the strength of encryption for each image. Five rounds of the 4D chaotic Chen system are used for images classified as abnormal while only one round is used for those classified as normal with a high confidence. This is an adaptive method that performs a 19.65% decrease in the number of executed encryptions rounds relative to fixed five-round processing; end-to-end timing displayed no net latency benefit (the classifier overhead dominates), so the contribution is an adaptive cryptographic workload allocation instead of an acceleration. MRI scans for feature extraction by ResNet-50 are classified using an SVM classifier have an accuracy of 94.20% over 4000 MRI images with a five-fold cross-validation. As far as encryption is concerned, the system is able to obtain NPCR of 99.61% (fulfilling the requirement as 99.6093 %), UACI of 33.45 %, chi-square: 265.8, entropy of 7.9971 and key sensitivity is 99.62 % with the secret key consisting of four initial conditions (the fourth would be enough up to a nominal representation of 256 bits but not an effective representation of entropy figure). Reconstruction after Decryption is performed which gives infinity PSNR and 1.0 SSIM.All 800 test images were used to test the integrity of the diagnostic, and it was found that the SVM predictions remain intact through the encryption/decryption process and this has been validated by the equality of the SHA-256 cryptographic Hash of the test images before and after encryption and decryption. The results suggest that CACE can provide a secure medical image transmission system without any loss of medical image diagnostic information through the IoT.

Keywords: Medical Image Encryption, 4D Chaotic System, Confidence-Adaptive Encryption, Brain Tumor Classification, Deep Feature Extraction.

ARTICLE INFORMATION

Author(s): Zainab N. Abdulhameed, Haraa Raheem Hatem, and Elaf H. Yahia;

Received: 01/06/26; **Accepted**: 14/09/26; **Published**: 30/09/26;
E- ISSN: 2347-470X;
Paper Id: IJEER 0106B02;
Citation: 10.37391/ijeer.140314
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-14/ijeer-140314.html

Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

The healthcare industry has seen a rapid evolution of the Internet of Things (IoT) technology, which has brought about remote patient monitoring and online diagnostic services. Medical imaging (e.g., MRI) produces sensitive patient data that must be communicated over insecure communication channels. In [1], [2], [3], introducing challenges of preserving data confidentiality and maintaining diagnostic quality. Due to sensitivity to initial conditions and pseudo-random behaviour, chaos-based encryption has attracted considerable attention for image security [4]. Lai et al. [5] combined a 3D hyperchaotic map with DNA encoding for healthcare IoT, Subathra et al. [6] proposed a 5D hyperchaotic system with U-Net segmentation, Alexan et al. [7] introduced a 4D fractional-order Chen system with entropy of 7.997 and a key space of 2^744, and Zhang et al. [8]proposed an improved 4D Chen system achieving entropy of 7.9993.

At the same time, deep learning has revolutionized medical image classification. Remzan et al. [9] combined ResNet-50[10] and DenseNet-121 features achieving 97.71% accuracy. Karim et al. [11] fused ResNet-50 with SVM (Support Vector Machine) reaching 99.61%. Abdulhameed et al. [12] design a system to encrypt image using hybrid chaotic map, and Prayogo et al. [13] proposed a hybrid framework which achieving 98.75%.

Despite these achievements, most works treat classification and encryption separately. Singh et al. [14] proposed DeepENC for ROI (Region of Interest) selection before encryption. Rupa et al. [15] combined a chaotic logistic map with ResNet classification. Rezk et al. [16] integrated VGG16-DNN with chaotic encryption achieving 93.75–94.1%., Mohammed et al. [17] developed a cryptographic model based on AES (Advanced Encryption Standard) cryptosystem. None of them, however, establishes a feedback mechanism where classification outcome influences

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 3 | Pages 807-815 | e-ISSN: 2347-470X

encryption parameters. The idea of adaptive resource allocation based on intelligent classification has been found to work in other engineering areas, such as the adaptive artificial intelligence-based control in environmental live using [18] and the adaptive lightweight security for getting good efficiency in health monitoring [19].As per the above-mentioned adaptive principle, thus this work is proposed in medical image encryption technique. Maintains 19.65% fewer executed encryption rounds, and a 4D chaotic Chen system with lossless reconstruction whose secret key is the four initial conditions (up to a 256-bit nominal representation); has 94.20% image-level classification accuracy at 5 folds (88.67% on a conservative but deduplicated subset, n = 309); the full pipeline is not faster end-to-end compared to fixed encryption, but the classifier stage is lightweight; Preservation of diagnostic integrity 100% verified by equality of SHA-256 hash of 800 test images. Since patient identifiers are not available, we quantified potential subject overlap by comparing each screening with all other screenings using a duplicate/near-duplicate screening with deep-feature cosine similarity (>= 0.98) and perceptual-hash Hamming distance (<= 5). This flagged 61.4% of the test images, and the 88.67% accuracy above is calculated on the deduplicated subset (n = 309) of test images, but there is no guarantee of independence at the patient level.

The remainder of this paper is organized as follows. *Section 2* summarizes the previous studies on chaotic medical-image encryption and deep classification. *Section 3* presents the proposed CACE methodology, comprising of confidence-adaptive decision model, the 4D Chen chaotic system and the SHA-256 plaintext-dependent keystream perturbation. The experimental results are reported in *section 4*, covering both classification accuracy, encryption security, diagnostic integrity and robustness analysis. Finally, *section 5* discusses limitations and future directions.

2. RELATED WORK

Lai et al. [5] proposed the medical image encryption for healthcare IoT which achieving PSNR (Peak Signal-to-Noise Ratio) above 35 dB. Ravichandran et al. [20] implemented a chaotic encryption on Raspberry Pi for IoT e-health. Kaur et al. 21] proposed a lightweight encryption using 7D hyperchaotic map. Inam et al. integrated blockchain with chaotic fractal encryption that achieving entropy of 7.9998 and NPCR of 99.92%. Ahmed et al. proposed a 4D hyperchaotic S-box cryptosystem achieving entropy between 7.9991 and 7.9994. Deng et al. combined a 4D hyperchaotic system with Knight's Tour scrambling. There are, however, some limitations with each of the methods, Lai et al. [5] provides high key sensitivity but lacks content differentiation in encryption procedures. Inam et al. [22] has the highest entropy but they have added blockchain overhead that is not suitable for real time IoT transmission. The work by Ahmed et al.[23] is based on a static S-box that is not adaptable to image diagnostic value. Deng et al. [24] applies fixed scrambling which consumes computation in the diagnostically irrelevant background regions. None of these approaches creates a feedback loop between classification confidence and the strength of the encryption. For integrated approaches, Rosaline et al. [25] proposed DeepTeleNet for CT image compression and encryption. Alarood et al. [26] modified deep neural networks for ROI-based encryption. Table 1 reviews the research gap, which shows that no existing method establishes a feedback loop between the classification confidence and the encryption strength.

Table 1. Research gap: no existing method provides adaptive encryption with diagnostic feedback

Reference	Year	Encryption	Classification	Adaptive	Lossless	Contribution
Lai [5]	2024	3D Hyper	None	No	No	IoT encryption
Singh [14]	2024	2D hybrid	ROI select	No	N/A	DeepENC
Rupa [15]	2022	Logistic	ResNet	No	N/A	Multimedia
Rezk [16]	2025	Arnold	VGG16-DNN	No	N/A	Encrypted classif.
Proposed	2026	4D Chen	ResNet+SVM	Yes	Yes	CACE adaptive

3. PROPOSED METHODOLOGY

Fig. 1 presents the block diagram of the proposed CACE framework, which consists of four modules: classification, confidence-adaptive decision, chaotic encryption, and diagnostic integrity verification.

3.1. Deep Feature Extraction and Classification

As illustrated in Fig. 2, MRI images are resized to 224×224 pixels and then normalized using the ImageNet statistics. A pretrained ResNet-50 (with final FC layer removed) which retrieving 2048-dimensional features per image. Each cross-validation fold involved fitting the z-scores and PCA solely using data from the training folds, and then applying the parameters unchanged to the held-out data of the test folds. After z-score normalization and PCA reduction to 100 components, two classifiers are trained, first it is KNN (K-Nearest Neighbours) with k=5 and secondly SVM (RBF kernel C=10). Both apply 5-fold cross validation, where statistical significance is determined by the paired t-test, Cohen's d effect size and Cohen's kappa (reported for the final fold).

3.2. Confidence-Adaptive Chaos Encryption (CACE)

In addition to the encryption parameters, the SVM decision function is added in the CACE mechanism. These have calibrated class probabilities derived from the SVM for each of the images (Platt scaling [fit on the training folds only]) and the highest calibrated class probability (confidence) being compared to the tier thresholds (calibration quality ECE = 0.046, Brier = 0.046):

$$conf = 1/\left(1 + exp(-max|d_i|)\right) \quad (1)$$

The decision rules are:

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 3 | Pages 807-815 | e-ISSN: 2347-470X

(1) any abnormal class (glioma, meningioma, pituitary) → HIGH (5 rounds);
(2) normal class with conf ≥ 0.85 → LOW (1 round);
(3) normal class with conf < 0.60 → HIGH (safety margin);
(4) normal class with conf 0.60–0.85 → MEDIUM (3 rounds).

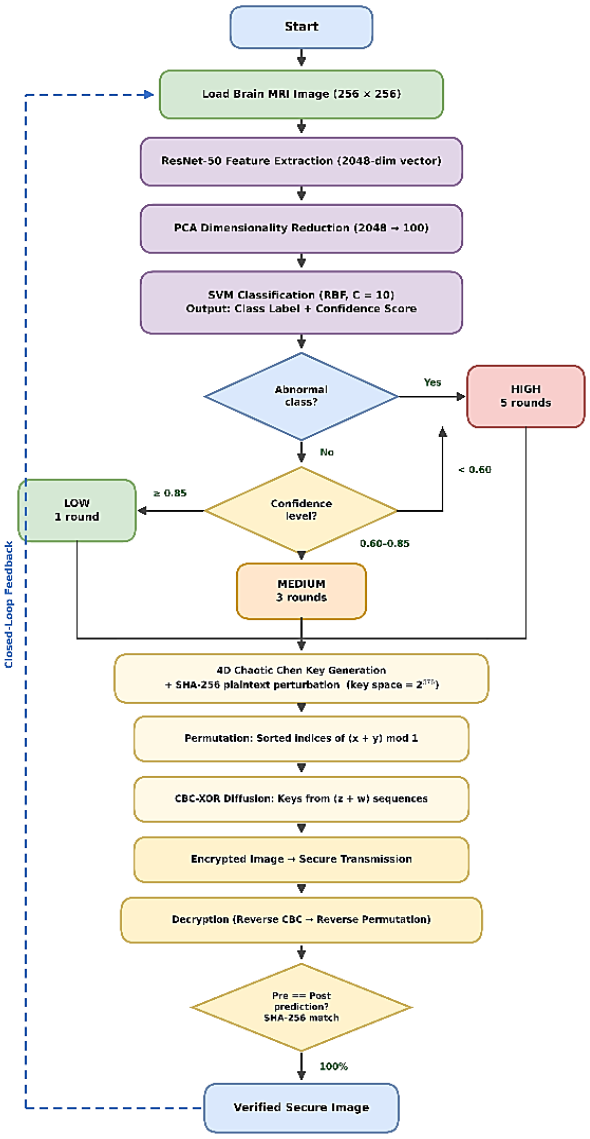

Figure 1. Diagram of Proposed CACE framework

3.3. 4D Chaotic Chen System

The encryption employs a 4D chaotic Chen system as in *eq. (2-5)*, with a=36, b=3, c=28, d=16, r=-0.4.;

$$dx/dt = a(y - x) + w \quad (2)$$

$$dy/dt = dx - xz + cy \quad (3)$$

$$dz/dt = xy - bz \quad (4)$$

$$dw/dt = yz + rw \quad (5)$$

Lyapunov exponent analysis, computed from the present implementation using a numerically stable RK4 estimator, yields L1=+0.6813, L2=-3.2162, L3=-3.3637, L4=-4.9086 (computed for the present implementation). confirming chaotic dynamics with one positive exponent as in Fig. 3. The system is integrated using the fourth order Runge-Kutta method (step 0.001, transient 500 iterations). Encryption consists of a cryptographically keyed Fisher–Yates permutation and a feedback-mode XOR diffusion whose domain-separated per-round keystreams are derived by SHA-256 in counter mode. The a, b, c, d, r are fixed public constants, and the secret key is the four initial conditions (up to nominal 256 bit – not an effective-entropy – value). For differential plaintext sensitivity, the cryptographic hash function of each plaintext image is calculated using the SHA-256 hash function before encryption image. The four initial conditions are perturbed by the digest as set forth in detail in the numbered protocol below.

3.3.1. Encryption protocol

The sender procedure is summarized below: (M×N = image size, $t_p = M \cdot N$).

(1) Compute the plaintext digest h = SHA-256(I) (32 bytes).

(2) Perturb the secret initial conditions: split h into four 8-byte words $q_0..q_3$; set $x_0' = x_0 + 10^{-3} \cdot (q_0/2^{64})$, and analogously for y_0 (q_1), z_0 (q_2) and w0 (q3).

(3) Generate the 4D Chen trajectory (RK4, step 0.001, 500-iteration transient) to obtain sequences X, Y, Z, W of length tp.

(4) Form the master seed S = SHA-256(X‖Y‖Z‖W ‖ K ‖ h), where K is the packed secret key. The secret key K is the four initial conditions (x_0, y_0, z_0, w_0) with 64-bit floating point, and the five most important Chen coefficients (a, b, c, d, r) are public fixed constants. No separate random initialization vector is used in the scheme, The per-image digest h = SHA-256(image) is included in the initial-condition derivation, making the keystream plaintext-dependent (but deterministic for identical plaintext/key pairs) and sent as metadata. The scheme is therefore deterministic per image; where indistinguishability across identical plaintexts is required, the digest can be replaced by a keyed value HMAC-SHA-256(K, image), as noted in the protocol enhancement.

(5) Derive the permutation π by a Fisher–Yates shuffle whose swap indices are read from the SHA-256 counter-mode stream CTR (S, "PERM", *tp*).

(6) Generate n (where n ∈ {1,3,5}) domain separated per round keystreams: k_r = CTR (S, "ROUND"‖r, tp) Here CTR (S, label, L) refers to a counter-based expansion of SHA-256 which is composed of S ‖ label ‖ encode(*j*) for *j* = 0, 1, … until a total length of *L* bytes is reached, then truncated to L bytes; the CTR gives domain-separated per-round keystreams.

(7) Permute the flattened plaintext: *P* = I_flat[π].

(8) Apply *n* feedback-diffusion rounds; within each round r: C[0] = P[0] ⊕ k_r[0], and C[i] = P[i] ⊕ C[i−1] ⊕ k_r[i] for i = 1..tp−1, using C as P for the next round.

The ciphertext is *C* reshaped to l enhancement.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 3 | Pages 807-815 | e-ISSN: 2347-470X

Decryption. This receiver possesses the secret key *K*, and *h*, and reproduces S, π and {k_r} identically, flips each round back to the beginning (feedback XOR), and then applies π^{-1} to recover *I*, with MSE = 0 in error-free delivery mode.

3.4. Decryption and Diagnostic Integrity

Decryption reverses the feedback-mode diffusion then the permutation. All operations are performed in the spatial domain and the reconstructions are mathematically loss-less under error free transmission which leads to (MSE=0, PSNR=infinity, SSIM (Structural Similarity Index Measure) =1.0). The diagnostic integrity is verified by the re-extracting ResNet-50 features from the decrypted image and comparing predictions against the pre-encryption predictions. Each original and decrypted image is subject to a SHA-256 cryptographic hash function, is used as an exact-reconstruction check; it is not an authentication mechanism.

4. EXPERIMENTAL RESULTS

4.1. Experimental Setup

The experiments used Python 3.14 with PyTorch 2.12 and scikit-learn 1.8 on an Intel CPU. The dataset contains 4000 brain MRI images (1000/class: glioma, meningioma, no tumor, pituitary) from the Brain Tumor MRI Dataset [27]. Images: 256×256 for encryption, 224×224 for ResNet-50. Random seed: 42. The dataset was split by image; not patient ID; as patient metadata is unavailable, and a common limitation in studies using this dataset discussed in [9], [11], [13].

4.2. Classification Performance

The SVM achieved 94.20% (±0.46%) with competitive accuracy to KNN at 87.93% (±0.90%) as in *table 2*.

Cohen's kappa was 0.9250 (SVM) and 0.8367 (KNN). *Table 3* indicates the per-class metrics, with meningioma having the lowest *F1 (mean 0.892 ± 0.006 across folds; 0.893 in the representative final fold shown in Figure 5).* Because patient identifiers were not available, a duplicate/near-duplicate screening was achieved using deep-feature cosine similarity (≥0.98) and perceptual-hash Hamming distance (≤5); the screening flagged 61.4% of the test images, and accuracy on the remaining deduplicated subset (n=309) was 88.67%.

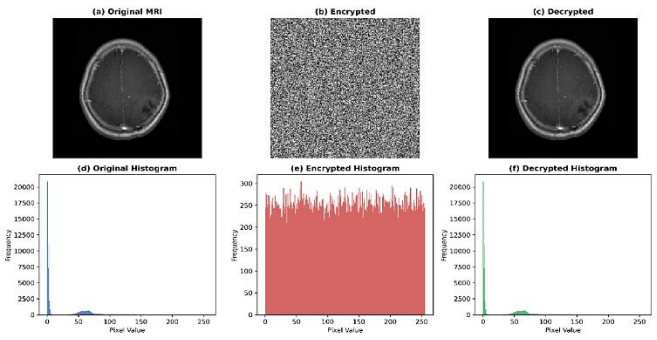

Figure 2. System pipeline: (a) original MRI, (b) encrypted image, (c) decrypted image, (d–f) histograms

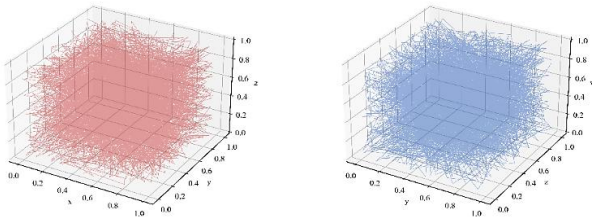

Figure 3. 4D chaotic Chen attractor: (a) x-y-z and (b) y-z-w projections

This provides an extra conservative robustness estimate, although patient-level independence cannot be ensured. The confusion matrices as shown in *fig. 5 (a)-(b)-(c)*, which introduces meningioma as the most confused class with F1=0.893. A fine-tuned ResNet-50 (layer4+FC, 5 epochs) achieves 96.38% but has an inference time of 173.4 ms/image versus approximately 0.17 ms/image for the PCA-SVM classifier stage; these are classifier-stage measurements only, distinct from the end-to-end pipeline latency in Section 4.3. The fine-tuned ResNet-50 reaches maximum accuracy (96.38% vs 94.20%, a 2.18-point difference), while the PCA-SVM classifier stage is lightweight and suitable for resource-limited IoT edge devices (*table 4*). The confusion matrix in *figure 5* shows the representative final fold for visualization.

Table 2. Five-fold cross-validation results

Fold	KNN Acc (%)	SVM Acc (%)	KNN F1	SVM F1
1	89.1	94.5	89.0	94.5
2	88.0	94.6	87.9	94.6
3	86.6	93.5	86.5	93.5
4	88.1	94.0	88.0	94.0
5	87.8	94.4	87.7	94.4
Mean±SD	87.93±0.90	94.20±0.46	87.82	94.21

Table 3. Per-class SVM metrics (mean ± SD across the five cross-validation folds)

Class	Precision	Recall	F1
Glioma	0.953 ± 0.018	0.921 ± 0.016	0.936 ± 0.012
Meningioma	0.882 ± 0.017	0.902 ± 0.012	0.892 ± 0.006
No tumor	0.976 ± 0.011	0.969 ± 0.017	0.972 ± 0.008
Pituitary	0.959 ± 0.010	0.975 ± 0.007	0.967 ± 0.004

Table 4. Comparison of computational complexity

Method	Accuracy (%)	F1 (%)	Inference Time
PCA-SVM (proposed)	94.20	94.21	~0.17 ms/img
Fine-tuned ResNet50	96.38	96.35	173.4 ms/img

4.3. CACE Adaptive Encryption Analysis

Approximately identical security is provided for all encryption levels *(Table 5 and Fig. 6)*. Across 800 test images: 599 received HIGH, 192 LOW, and 9 MEDIUM

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 3 | Pages 807-815 | e-ISSN: 2347-470X

under the calibrated policy, resulting an average of 4.02 rounds and a 19.65% round-count reduction relative to fixed five-round processing (no net end-to-end latency benefit), as seen in Fig. 7. A direct end-to-end measurement confirmed this: the complete calibrated pipeline exhibited a 29.0% latency increase relative to the fixed five-round baseline, because feature extraction and calibrated confidence estimation dominate the total time (the calibrated classifier alone required about 7.25 ms/image versus 0.74 ms/image for the plain SVM). The MEDIUM interval was initially unpopulated since the confidence score was uncalibrated; after Platt calibration (ECE=0.046) all three tiers are activated (LOW=192, MEDIUM=9 [1.1%], HIGH=599), with MEDIUM interpreted cautiously as a small fraction.

A threshold-sensitivity sweep over sixteen low/medium cut-off pairs (low in {0.40,0.50,0.55,0.60}, medium in {0.75,0.80,0.85,0.90}) confirmed that all three tiers remained populated throughout, with the MEDIUM tier ranging from 3 to 16 of the 800 test images and the LOW/HIGH assignments remaining dominant, indicating that the selected operating point (0.60,0.85) is not a knife-edge choice. Even with single-round LOW encryption yields an entropy of 7.9968 and NPCR of 99.62%.

The CACE mechanism decreases the number of rounds executed by 19.65% (without any end-to-end latency advantage). The main contribution is the allocation of workload, not the acceleration of computation.

The encryption uses SHA-256 computed over each image, producing a 32-byte digest, and is therefore negligible when compared to the sequence generation of the chaotic sequence.

The reliability diagram in *Fig. 4* confirms the calibrated confidence is well-calibrated (ECE = 0.046)

4.4. Encryption Security Analysis

Adjacent pixel correlation is decreased from above 0.96 to below 0.02 across all directions, as shown in *Fig.8.* The comprehensive encryption security metrics are summarized in *Table 6.*

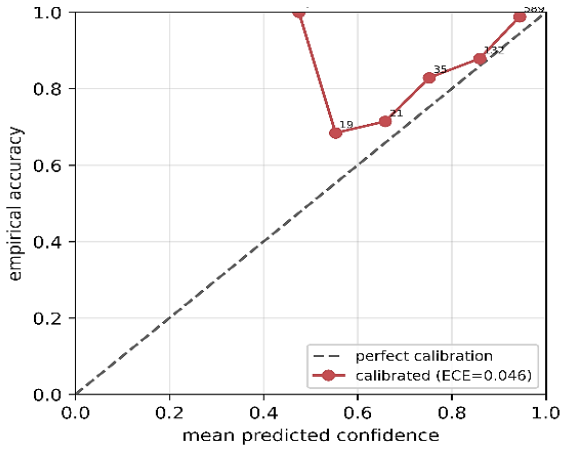

Figure 4. Reliability diagram of the Platt-calibrated SVM confidence (ECE = 0.046). Points near the diagonal indicate well-calibrated probabilities; bin counts are shown above each point

For UACI (Unified Average Changing Intensity) Analysis: The global UACI is 43.23% which is different from 33.46% because of the large area of black background in MRI scans (66.3% of the pixels, Otsu threshold=38).

The differential UACI computed using the standard 1-pixel change method (excluding the background) is 33.45% ± 0.06%, which is theoretically supposed to be 33.46%, as seen in *Fig. 9.*

The foreground UACI of 33.45% lies within the theoretical 95% CI [33.02%, 33.91%] derived from Wu et al. [28], which is expected because MRI brain tissue has a concentrated intensity distribution unlike uniformly distributed natural images.

Table 5. Encryption security metrics per-level

Level	Entropy	NPCR (%) *	Chi-Square	Time (ms)
LOW (1 round)	7.9968	99.62	293.1	369
MEDIUM (3)	7.9971	99.57	263.0	396
HIGH (5)	7.9971	99.61	265.8	555

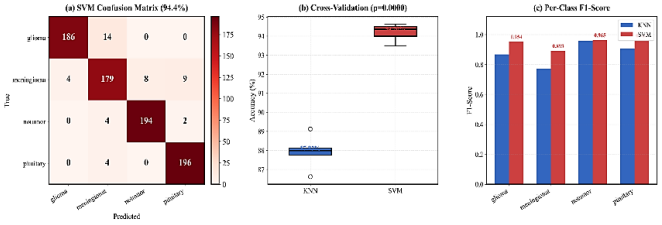

Figure 5. Classification: (a) SVM confusion matrix, (b) CV boxplot, (c) per-class F1

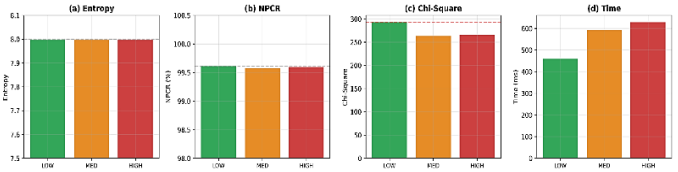

Figure 6. Per-level comparison: (a) entropy, (b) NPCR, (c) chi-square, (d) encryption time

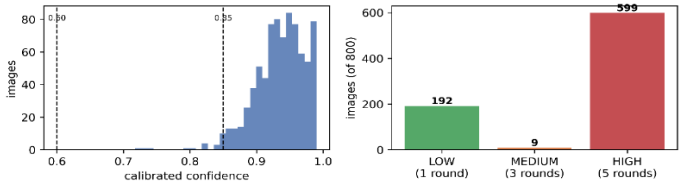

Figure 7. Distribution of CACE: (a) confidence histogram, (b) level assignment (599 HIGH, 192 LOW, 9 MEDIUM; calibrated)

4.5. Encryption Ablation

The ablation results in *table 7* and *fig. 10* prove that the permutation-only configuration makes significantly weaker encryption. The SHA-256 plaintext hash perturbation contributes to differential resistance, as No Feedback (99.59%) and No Perm (99.60%) maintain high pixel

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 3 | Pages 807-815 | e-ISSN: 2347-470X

dissimilarity due to hash-induced chaotic sequence divergence. Permutation disrupts spatial structure (entropy drops to 4.44), while the feedback mode ensures forward error propagation. The combined architecture presents defense-in-depth.

To separate the effect of the adaptive policy itself, we also compared fixed-round encryption (always 1, 3, and 5 rounds) and the calibrated adaptive assignment. All fixed configurations generate near-identical ciphertext statistics (entropy ~7.997, NPCR ~99.6%),

4.6. Threat Model and Security Analysis

The security analysis of the CACE framework, compared with standard cryptographic attacks, is summarized. The near perfect entropy of 7.9971 is a statistical randomness indicator, the chi-square of 265.8 is less than the critical value of 293.25, and these are not a formal measure of cryptographic security.

The secret key (four initial conditions, up to a 256-bit nominal representation) makes exhaustive search impractical. The SHA-256 hash perturbation mechanism: the plaintext-dependent perturbation produces different keystream material for different plaintexts in the tested configurations, derived experimentally through the CPA/KPA experiments below instead of plaintext-ciphertext pairs. Under the tested chosen-plaintext scenarios, initial conditions of hash-perturbed produced distinct chaotic trajectories for distinct plaintexts; this is empirical evidence, not a formal CPA-security proof. Standard differential analysis confirms NPCR = 99.61% (meeting the Wu et al. [28] critical value of 99.6093%) and UACI = 33.45% within the theoretical 95% confidence interval. The chosen-plaintext test showed no residual structure with all-black, all-white and a gradient image yielding approximately 7.997 in entropy and less than 0.022 in adjacent-pixel correlation; the known-plaintext test, where key material from one image was used on another, had an PSNR of 6.8 dB (noise-level)

The key sensitivity analysis result shows that the change in the number of pixels would be 99.62% assuming a small modification to the initial condition, which is consistent with the one presented in the Abstract and *table 6*. Per-image plaintext-dependent keystreams (or not an information-theoretic guarantee) are an empirical resistance to chosen plaintext attacks for LOW-mode encryption (1 round, applied to confidently classified normal images).

In the controlled known plaintext test, the recovered key material is used with a different image to reconstruct the PSNR of only 6.8 dB, which is equivalent to noise, showing that the key material recovered in this test scenario is not applicable to a different image. This is a reasonable compromise: the number of rounds is an experimental computational-allocation policy (not saying that normal images need less confidentiality); the single-round feedback diffusion with unique keystream was tested to be very secure under the considered chosen- and known-plaintext scenarios; we do not claim to have a formal proof of security.

Side-channel concern: If the abnormal images are processed more times, then an observer who knows the amount of per-image processing time or traffic characteristics can be used to deduce information that is correlated to the selected tier. The tier identifier does not actually broadcast in plaintext, but this is still considered a residual side-channel restriction, and constant-observable padding/batching (equalizing the amount of time and object size per image) is recommended as a deployment-level mitigation. We have established base line: for comparison we tested AES-256-GCM, a standard authenticated-encryption scheme, on these same images. AES-GCM achieves almost identical statistical randomness test results (entropy 7.9972, NPCR 99.61 and is substantially faster (about 0.6 ms per image versus 535 ms for our unoptimized multi-round scheme); it offers authenticated-encryption properties not given by the proposed statistical measures. Thus, adaptation and confidence driven cryptographic effort allocation is not a replacement for or a claimed improvement over AES-GCM, that is the contribution of CACE.

4.7. Diagnostic Integrity

All 800 original and decrypted test images are bytewise equal as confirmed by SHA-256 hash verification, and the encryption-decryption process causes no information loss. The SVM and KNN classifiers retain 100% of their predictions after the encrypt-decrypt cycle (SVM: 800/800; KNN: 800/800). To further validate the deterministic pipeline, inference was repeated 100 times using the same random seeds with the same images, to ensure that there were no non-deterministic outcomes.

4.8. Robustness

Under mild noise (σ=0.001), PSNR=29.8 dB and SSIM=0.978 as shown in *fig. 11*. When the noise is heavy (σ=0.05), the error is propagated by the feedback mode, which minimizes the to PSNR quality=9.4 dB.

Table 6. Encryption security metrics (HIGH level, 5 rounds)

Metric	Achieved	Ideal
Entropy	7.9971	8.0
NPCR (%)	99.61	>99.61
UACI global (%)	43.23	33.46
UACI brain ROI (%)	33.45 (differential)	33.46
Correlation H/V/D	0.0083/0.0048/0.0098	~0
Key Sensitivity	99.62%	>99%
Chi-Square	265.8	<293.25
Key Space	up to 256-bit nominal representation	—
PSNR	Infinity	Lossless

(**Secret-key representation: four initial conditions; nominal numerical representation only, not an estimate of effective key entropy. The Chen parameters a, b, c, d, r are fixed public constants)*

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 3 | Pages 807-815 | e-ISSN: 2347-470X

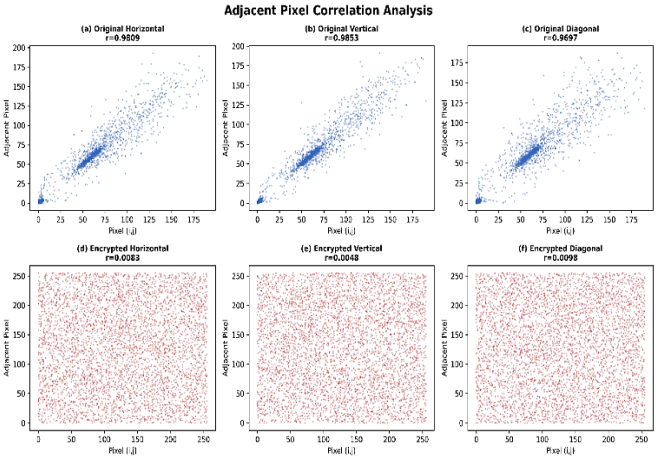

Figure 8. Correlation: original (r>0.96) vs encrypted (r<0.02)

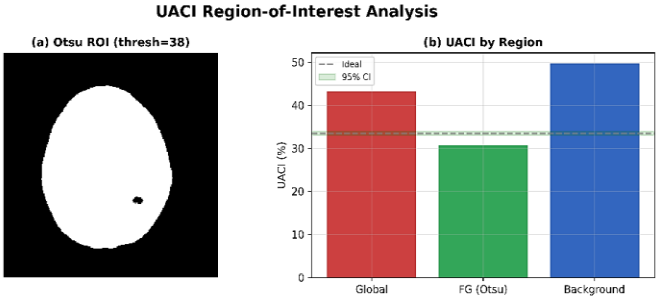

Figure 9. UACI ROI analysis: (a) Otsu mask, (b) UACI by region with 95% CI

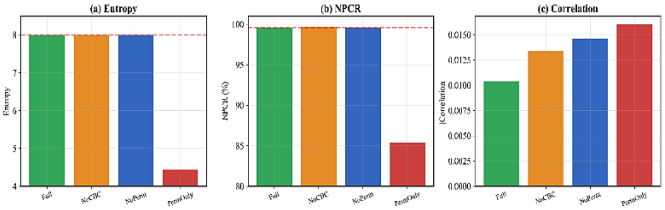

Figure 10. Encryption ablation: permutation-only shows dramatic degradation

Table 7. Encryption component ablation

Configuration	Entropy	NPCR (%) *	Corr |H|
Full (Perm+Feedback)	7.9968	99.62	0.010
No Feedback	7.9972	99.59	0.013
No Permutation	7.9972	99.60	0.015
Perm Only	4.4369	85.55	0.016

This sensitivity is a feature of feedback (CBC-like) mode, because if one byte is corrupted, all subsequent decrypted values will get corrupted too. IoMT Communication Channels: The suggested framework works at the application layer, and for the two possible deployment scenarios in IoMT (Internet of Medical Things) healthcare networks: 1- in the state of a hospital networks using Ethernet or reliable IEEE 802.11n/ac WLAN links, the guarantee of lossless encryption can be applied directly for which bit error rates are ignorable and lossless transport is certain by TCP retransmission. (2) Wireless IoT connectivity using popular protocols in healthcare such as IEEE 802.15.4 or ZigBee in short-range body area networks (BAN); IEEE 802.11ah or Wi-Fi HaLow in extended-range hospital coverage; and LTE-M/NB-IoT for cellular connected remote monitoring.

The wireless standards use physical-layer forward error correction (FEC) coding – such as turbo codes for LTE-M or LDPC codes for 5G NR and Wi-Fi 6 – that decrease bit errors caused by the channel before the data attains the application-layer decryption module.

The CACE framework does not depend on any particular channel model (AWGN, Rayleigh fading) as the encryption is independent of the physical-layer channel characteristics; physical-layer FEC decreases residual channel errors; lossless reconstruction conditions that residual transmission errors be corrected or detected before application-layer decryption, which reliable transport and link-layer or physical-layer error-control mechanisms can support [29-31] . If sufficient FEC protection is not provided in a channel, then counter-mode (CTR) encryption can be employed rather than feedback mode, avoiding error propagation as discussed in the channel bit errors limitations; *Table 8* presents the comparison of the channel bit errors recovered-PSNR performance.

Table 8. Reconstructed PSNR (dB) under channel bit errors

BER	Feedback	CTR
10^{-5}	47.42	54.96
10^{-4}	38.82	44.75
10^{-3}	28.59	34.62
10^{-2}	18.73	24.79

4.9. Comparison with Literature

Table 9 compares the proposed CACE framework with the recent methods of encryption and classification. In terms of encryption power, Inam et al. [22] gets highest entropy of 8.000 and NPCR of 99.92%, while the proposed system gets entropy of 7.9971 and NPCR of 99.61%, respectively, which satisfies Wu et al. criterion of 99.6093%. The comparison in *table 9* spans work with different datasets, image sizes and threat models and is therefore indicative instead of head-to-head. Rupa et al. [15] and Rezk et al. [16] have a classifier for classification but neither has adaptive encryption or diagnostic integrity verification. The proposed CACE uses adaptive encryption, lossless reconstruction and diagnostic-integrity verification and among the works compared, all have different datasets, image sizes and threat models.

5. CONCLUSIONS

This paper presents a secure adaptive medical image transmission system over an IoT network called CACE. The

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 14, Issue 3 | Pages 807-815 | e-ISSN: 2347-470X

framework integrates the deep feature extracted by ResNet-50 networks and PCA-SVM classification in closed loop with the chaotic Chen encryption. Key results are SVM accuracy of 94.20% (kappa = 0.9250), a fine-tuned baseline of 96.38% (the PCA-SVM one stage of the classifier is light weight, but the whole pipeline is not faster end-to-end than fixed encryption), entropy of 7.9971, NPCR of 99.61% (passing Wu et al. critical value), chi-square of 265.8, key space up to 256-bit nominal representation, and 100% diagnostic integrity checked equality of SHA-256 hash across 800 images. The CACE mechanism under the calibrated policy obtains a 19.65% reduction in the number of rounds encrypted during execution (with no end-to-end latency benefit), obtaining 599 images of category HIGH, 192 of category LOW and 9 of category MEDIUM (mean: 4.02 rounds).The main contribution is an adaptive computational/workload allocation based on the confidence of the classifiers; all the tiers, including LOW, use the same confusion–diffusion construction with LOW-mode entropy 7.9968 and NPCR 99.62%, just changing the number of diffusion rounds as the policy does.

Limitations: (1) 94.20% classification is below dedicated systems (96-99%) especially for edge deployment; justified as trade-off. (2) feedback-mode sensitivity to residual channel errors requires reliable error-controlled delivery or an error-resilient encryption mode. (3) Single data set with image-level splitting. (4) Global UACI deviation due to MRI backgrounds. (5) One positive Lyapunov exponent (chaotic, but not hyperchaotic). (6) With calibrated confidence, all three tiers were activated (LOW=192, MEDIUM=9, HIGH=599); the MEDIUM tier represents only 1.1% of samples and is therefore interpreted cautiously. (7) The chaotic sequence is made plaintext-dependent via SHA-256 hash perturbation; without this, differential NPCR would be insufficient. Future work includes: (a) Design and implementation of vision transformers for >97% accuracy; (b) ROI encryption for brain/background separation; (c) cross-modality evaluation; (d) integration with wireless testbed and development of FEC; (e) embedded deployment on Raspberry Pi/Jetson Nano; (f) CTR-mode encryption for noise resilience; (g) optimization of parameters for hyperchaotic regime.

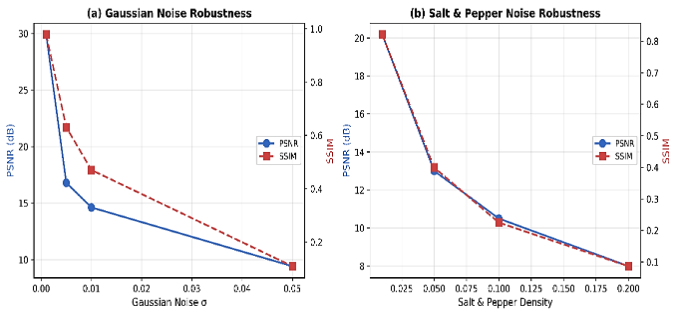

Figure 11. Robustness: (a) Gaussian noise, (b) salt-and-pepper noise

Table 9. Comparison with recent methods. Values are reported as published by each cited work on different datasets, image sizes, and threat models; the comparison is therefore indicative rather than strictly head-to-head

Method	Year	Entropy	NPCR%	UACI%	Chi-sq	Classif.	Adapt.
Lai [5]	2024	7.999	99.62	33.5	—	None	No
Alexan [7]	2023	7.997	99.62	33.0	—	None	No
Zhang [8]	2025	7.999	99.61	33.5	Pass	None	No
Inam [22]	2025	8.000	99.92	33.3	—	None	No
Ahmed [23]	2023	7.999	99.62	33.4	—	None	No
Deng [24]	2025	7.998	99.61	33.5	—	None	No
Rupa [15]	2022	7.99+	99.5+	—	—	ResNet	No
Rezk [16]	2025	—	—	—	—	94.1%	No
Proposed	2026	7.997	99.61	33.45	266	94.2%	Yes

Data and Code Availability: The Brain Tumor MRI Dataset is publicly available at https://www.kaggle.com/datasets/masoudnickparvar/brain-tumor-mri-dataset [27] .

The complete Python implementation is available at https://github.com/zainababdulhameed-create/CACE-framework. All experiments used random seed 42 for reproducibility.

Author Contributions: Zainab N.: conceived the methodology, implemented the framework, Software development. Haraa R. and Elaf Y. performed the validation, Formal analysis, Writing – review and editing.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

[1] World Health Organization, "Global Strategy on Digital Health 2020-2025," 2021, WHO. [Online]. Available: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf

[2] W. Q. Mohamed, M. Al–Sultani, and H. R. Hatem, "New 2-D interleaving grouping LBC applied on image transmission," International Journal of Electrical and Computer Engineering (IJECE), vol. 11, no. 5, p. 4241, Oct. 2021, doi: 10.11591/ijece.v11i5.pp4241-4249.

[3] Y. Allbadi, H. R. Hatem, I. H. Ali, and W. Q. Mohamed, "A Wearable Device-Based IoT for ECG and Heart Rate Measurements," Mathematical Modelling of Engineering Problems, vol. 12, no. 8, Aug. 2025, doi: 10.18280/mmep.120829.

[4] G. Alvarez and S. Li, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems," International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129–2151, 2006, doi: 10.1142/S0218127406016446.

[5] Q. Lai and H. Hua, "Secure medical image encryption scheme for Healthcare IoT using novel hyperchaotic map and DNA cubes," Expert Syst. Appl., vol. 264, p. 125854, Mar. 2025, doi: 10.1016/j.eswa.2024.125854.

[6] S. Subathra and V. Thanikaiselvan, "Enhanced Security for Medical Images Using a New 5D Hyper Chaotic Map and Deep Learning Based Segmentation," Sci. Rep., vol. 15, 2025, doi: 10.1038/s41598-025-04906-4.

[7] W. Alexan, M. Gabr, E. Mamdouh, R. Elias, and A. Aboshousha, "Color Image Cryptosystem Based on Sine Chaotic Map, 4D Chen Hyperchaotic Map of Fractional-Order and Hybrid DNA Coding," IEEE Access, vol. 11, pp. 54928–54956, 2023, doi: 10.1109/ACCESS.2023.3282160.

[8] X. Zhang and others, "A Secure Image Transmission Scheme Based on Improved 4D Hyperchaotic System and DNA Coding," Phys. Scr., vol. 100, 2025, doi: 10.1088/1402-4896/ada76c.

[9] N. Remzan and others, "Advancing Brain Tumor Classification Accuracy Through Deep Learning: Harnessing RadImageNet Pre-trained CNNs, Ensemble Learning, and Machine Learning Classifiers on MRI Brain Images," Multimed. Tools Appl., vol. 83, pp. 40289–40315, 2024, doi: 10.1007/s11042-024-18961-y.

[10] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," in 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), IEEE, Jun. 2016, pp. 770–778. doi: 10.1109/CVPR.2016.90.

[11] P. J. Karim and others, "Brain Tumor Classification Using Fine-Tuning Based Deep Transfer Learning and Support Vector Machine," International Journal of Computing and Digital Systems, vol. 13, pp. 809–823, 2023, doi: 10.12785/ijcds/130164.

[12] Z. N. Abdulhameed, H. R. Hatem, and W. Q. Mohamed, "Performance Evaluation of Hybrid Chaotic and Permutation Schemes for Image Transmission Based MC-CDMA," International Journal of Electrical and Electronics Research, vol. 13, no. 2, pp. 218–226, May 2025, doi: 10.37391/ijeer.130205.

[13] R. D. Prayogo and others, "Hybrid CNN-Based Transfer Learning Enhances Brain Tumor Classification on MRI Images," IEEE Access, vol. 13, 2025, doi: 10.1109/ACCESS.2025.3536783.

[14] K. Singh and others, "DeepENC: Deep Learning-Based ROI Selection for Encryption of Medical Images Through Key Generation With Multimodal Information Fusion," IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 2871–2880, 2024, doi: 10.1109/TCE.2023.3339498.

[15] Ch. Rupa and others, "Securing Multimedia Using a Deep Learning Based Chaotic Logistic Map," IEEE J. Biomed. Health Inform., vol. 27, no. 10, pp. 4614–4622, 2023, doi: 10.1109/JBHI.2022.3221484.

[16] N. G. Rezk and others, "Secure Hybrid Deep Learning for MRI-Based Brain Tumor Detection in Smart Medical IoT Systems," Diagnostics, vol. 15, no. 3, p. 275, 2025, doi: 10.3390/diagnostics15030275.

[17] H. J. Mohammed, A. H. Al-Adhami, Y. Yaseen, and L. Abed, "A developed cryptographic model based on AES cryptosystem," 2022, p. 020013. doi: 10.1063/5.0112123.

[18] A. S. Abdalkafor, Y. S. Yaseen, and A. A. Jihad, "Artificial Intelligence Techniques for Adaptive Controlled Air Conditions," in 2023 16th International Conference on Developments in eSystems Engineering (DeSE), IEEE, Dec. 2023, pp. 812–817. doi: 10.1109/DeSE60595.2023.10469179.

[19] I. Ahmad, F. Shahid, I. Ahmad, J. Islam, K. N. Haque, and E. Harjula, "Adaptive Lightweight Security for Performance Efficiency in Critical Healthcare Monitoring," Dec. 2024, doi: 10.1109/ISMICT61996.2024.10738175.

[20] D. Ravichandran and others, "An Efficient Medical Data Encryption Scheme Using Selective Shuffling and Inter-Intra Pixel Diffusion IoT-Enabled Secure E-Healthcare Framework," Sci. Rep., vol. 15, p. 4521, 2025, doi: 10.1038/s41598-025-85539-5.

[21] M. Kaur and others, "Lightweight Biomedical Image Encryption Approach," IEEE Access, vol. 11, pp. 57260–57270, 2023, doi: 10.1109/ACCESS.2023.3282826.

[22] S. Inam, S. Kanwal, M. Batool, S. Al-Otaibi, and M. M. Jamjoom, "A blockchain-integrated chaotic fractal encryption scheme for secure medical imaging in industrial IoT settings," Sci. Rep., vol. 15, no. 1, p. 7652, Mar. 2025, doi: 10.1038/s41598-025-89604-x.

[23] S. M. Ahmed and others, "A Hybrid Medical Image Cryptosystem Based on 4D-Hyperchaotic S-Boxes and Logistic Map," Multimed. Tools Appl., vol. 82, pp. 22375–22398, 2023, doi: 10.1007/s11042-022-13592-5.

[24] X. Deng and others, "An Image Encryption Algorithm Based on a Novel 4D Hyperchaotic System and Improved Knight's Tour Scrambling Algorithm," Phys. Scr., vol. 100, p. 35225, 2025, doi: 10.1088/1402-4896/adb44b.

[25] S. Rosaline and others, "Deep Learning-Based Compression and Encryption of CT Images for Secure Telemedicine Applications," Evolving Systems, vol. 16, p. 24, 2025, doi: 10.1007/s12530-024-09639-7

[26] A. Alarood and others, "Secure Medical Image Transmission Using Deep Neural Network in E-Health Applications," Healthc. Technol. Lett., vol. 10, pp. 45–56, 2023, doi: 10.1049/htl2.12043.

[27] M. Nickparvar, "Brain Tumor MRI Dataset," 2023. [Online]. Available: https://www.kaggle.com/datasets/masoudnickparvar/brain-tumor-mri-dataset

[28] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications, vol. 1, no. 2, pp. 31–38, 2011.

[29] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT Communications: A Survey," Sensors, vol. 20, no. 17, p. 4828, 2020, doi: 10.3390/s20174828.

[30] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," IEEE Internet Things J., vol. 8, no. 11, pp. 8707–8718, 2021, doi: 10.1109/JIOT.2020.3045653.

[31] Z. N. Abdulhameed, "Transmission of an encryption audio message using chaotic map in a noisy channel," Journal of Communications, vol. 14, no. 2, 2019, doi: 10.12720/jcm.14.2.142-147.

© 2026 by Zainab N. Abdulhameed, Haraa Raheem Hatem, and Elaf H. Yahia. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).