International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 6, 2025
https://theaspd.com/index.php

# Adaptive and Lightweight Security Framework for Medical Images Using Intermittent Encryption and Deep Learning in IoT-Enabled Healthcare

**S. Karthika[1], Dr. K. Juliana Gnanaselvi[2]**
[1]Research Scholar, Department of Computer Science, Rathinam College of arts and Science, Coimbatore, India, karthisivaprakash27@gmail.com
[2]Department of Computer Science,, Rathinam College of arts and Science, Coimbatore, India, Sunil.juliana@gmail.com

***Abstract***
*In this paper, a novel lightweight security framework, integrating a code-based on-off encryption with an authentication based on Convolutional Neural Network (CNN), is proposed to provide security for the medical image transmission and storage in IoT. The system encrypts only the key important portions of the image using BCH codes and LFSR-generated keys, thereby highly improving encryption speed while maintaining image privacy. We test our approach experimentally on the NIH Chest X-ray14 dataset. The decrypted image diagnostic quality PSNR was 41.82 dB and SSIM was 0.986 respectively, suggesting a better resistance against statistical and differential attacks by the encrypted images. The efficiency tests revealed an encryption time of 26.3 ms and a decryption time of 27.5 ms, which makes this work feasible to real-time IoT applications. Additionally, CNN-based integrity verification performed 93.7% correct classification on decrypted images and 98.9% authentication with low false acceptance (1.1%) and false rejection (1.3%). Comparing to AES and chaos-based encryption schemes, the proposed scheme boasts excellent speed, security, and minimum resource overhead, rendering it very suitable for limited-resource healthcare devices.*
***Keywords:*** *CNN, Image, BCH Codes, LFSR, IoT environment, AES, intermittent encryption.*

## INTRODUCTION

The innovation in Internet of Things (IoT) technologies in the healthcare sector has advanced to the extent of completely revolutionizing patient monitoring, telemedicine, and medical diagnostics, the IoT-driven healthcare solutions provide real-time access to vital information, more so enabling critical data such as medical images, including X-rays, CT scans, and MRIs. These types of images tend to be shared using wireless and cloud a service, which brings serious issues on data privacy, integrity, and security. Illegal intrusion, modification, and eavesdropping of medical images of confidential nature may not only generate ethical and legal danger, but also reduce the precision of diagnosis and prognosis.

Current encryption methods, like Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES), are secure but computationally expensive and not suited for the resource-constrained environments of smart health gateways, edge devices, and wearable medical sensors. Full-image encryption methods compromise clinical utility, potentially by growing time and possibly visual fidelity loss following decryption. Other issues exist, e.g. current CNN-based authentication methods can lack inherent encryption and can be vulnerable to illicit content replacement.

To protect and verify medical image data in real-time IoT healthcare systems, this research study presents a standardized approach established with a hybrid model of CNN-based image authentication process and a lightweight, code-based periodic encryption method. Selectively encrypt the most sensitive parts of the image by utilizing the BCH (Bose-Chaudhuri- Hocquenghem) code and LFSR (Linear Feedback Shift Register) key generation, which greatly reduces the computing overhead with the guaranteed security in the proposed method.

### 1.1 Key Contributions

The main of the contributions of our work are as outlined below:

i) Lightweight Intermittent Encryption Framework: This novel partial encryption framework, fully works in code theory (BCH codes),has a reduced computational overhead by encrypting the more significant regions of an image only.

ii) LFSR-based algorithm for Key Generation: Secure dynamic session encryption is achieved using a novel, scalable LFSR-based pseudorandom key generation approach which further enhances resistance to key prediction and replay attacks.
iii) CNN-based Integrity Verification Module: This approach adopts a deep learning model (ResNet-50) to verify whether the image is manipulated or adversarial, if it is encrypted, and if the image is authentic.
iv) IoT-Ready Performance: The system has been tested in environments that resemble that of Internet of Things, and in these environments it achieves a real-time throughput of 18.5 images/sec with memory overhead as low as 2.3 KB/image, and encryption/decryption latencies of 26.3 ms and 27.5 ms, each.
v) Strong security measures: The stegoed images are very resilient to statistical and differential attacks of high entropy (7.92), NPCR (99.62%) and UACI (33.28%).
The rest of the paper is structured in the following way: Section II: Overview of related work regarding CNN-based verification, IoT security, and medical image encryption, Section III: Presents a proposed method, including CNN architecture, key generation, and encryption scheme, Section IV: System workflow detail and algorithm Section V: Comparative analysis, performance graphical explanation, and experimental results are explored, Section VI: Conclusion and future prospects are provided.

## RELATED WORKS

In the digital age, protecting medical images has gained a new relevance, given the rise of telemedicine and Internet of Medical Things (IoMT) applications, which increasingly involve data exchange across untrusted networks. Numerous encryption, watermarking, and privacy-preserving deep learning techniques have been studied recently with the goal of maintaining the data's authenticity, integrity, and confidentiality without lowering diagnostic quality. Deep learning has had a significant impact on encryption and key generation frameworks. To provide security against attacks on X rays and MRI we have GAN's based deep learning method named DeepKeyGen, which uses to the Generate random cryptographic stream keys for encryption and decryption of medical images [1]. In the same spirit, the chaotic S-box generator using CNN-based keys with a chaotic logarithmic map offers high quality entropy, resistance to noisy environment, and strong scrambling through the DNA encoding along with the permutation technique [2].
Homomorphic encryption enabled secure computation on encrypted data. Homomorphic CNNs can be used for retinal image analysis, illustrated by the CaRENets architecture that supports efficient encrypted inference on medical images, in which memory usage is reduced by 45× and inference is speeded up by 4–5× [3].
Another deep learning related contribution is DeepEDN uses the decoding network for decryption, and maps between domain using a Cycle-GAN for picture encryption. It is very suitable for preserving the fidelity of pictures and has high security on chest X-ray images [4]. Moreover, SVD watermarking augmented with CNN-based extraction, medical image authentication has been achieved. This solution preserves NC (0.99) and PSNR (˜43.8 dB), with excellent robustness under various attacks [5].
Further research closely examined trend of encryption in different modalities and organs. A comprehensive review of deep learning cryptography approaches elaborates multiple encryption algorithms, security levels, and image quality measures such as PSNR and SSIM [6]. Another DICOM standard paper based on crypto techniques discusses hybrid methods including reversible watermarking in order to achieve both header and pixel confidentiality [7].
Ensuring image quality after encryption is critical in the telemedicine application. The relationship between ROAN and HI is also pointed out in [8], in the sense that PSNR, SNR, MSE, MAE were formulated and evaluated for encryption methods to compromise between the index of robustness against noise and image fidelity. However, since the chaotic maps are sensitve and unpredictable, they continue to be used. Applications of Latin-squares for diffusion and permutation, PWLCM, and sine-logistic maps are presented that also deliver superior results in selective encryption [9].
Other modalities, for example optical encryption, are also important. Even more robustness can be obtained in potential optics-based media by introducing CNNs and fractional transforms, especially when

combined with biometric identification [10]. Moreover, neural networks have been successfully employed in the encryption process and substitution in chaotic maps (as Lorenz, Arnold cat) for grey scale, CT, and MRI images [11].

Moreover, homomorphic encryption is used more and more in the feature extraction. Despite this complicated computation, systems like MiniONN and CryptoNets allow to securely download and classify encrypted pictures [12]. In the meanwhile steganographic approaches have also been put forth to embed EPR inside medical images. Some methods due to ensure the imperceptibility and the exactitude of the recovery are visual cryptography, reversible concealment [13].

Another important topic is the evaluation of the encryption strength. In experimental studies regarding avalanche effect and SAC, metrics related to the algorithms' sensitivity and diffusion performance, such as NPCR and UACI, are to demonstrate the effectiveness of different schemes [14]. Not least is the fact that authenticated encryption (AE) modes such as GCM, CCM, and EAX serve better to protect both secrecy and integrity, especially for sensitive parts and image headers [15].

Literature review shows the emerging interplay between the cryptographic standards, deep learning and chaos theory for security of medical images. As implemented with supporting performance assessments (e.g., SAC and NPCR) based on a flexible level of performance evaluation techniques, the AEs can be a viable methodology for assessing and enhancing current techniques. These advancements mark encrypted and authenticated medical imagery as a cornerstone security asset within modern e-health systems.

## METHODOLOGY

This study introduced an innovative and flexible security framework based on deep learning feature security and code-based intermittent security using CR networks for securing medical images in the IoT-based healthcare system. There are several components integrated into the proposed system workflow:

**3.1 Medical Image Acquisition:** Medical images (CT, MRI, X-ray) are generated from IoT-enabled diagnostic devices.

**3.2 Deep Learning-Based Encryption:** A ResNet-50 model is fine-tuned to learn the features and encode the medical image into encrypted information. For input image I, the learned encryption function $f_\theta$ generates in equation 1:

$$E(I) = f_\theta(I) \quad (1)$$

This is the first level of encryption.

**3.3 CNN-Based Spectrum Sensing:** A CNN model at the Fusion Center processes historical spectrum measurements via actor-critic learning to select the best transmission slots. This enables on/off and energy-aware encryption, which improves spectrum utilization and reduces the communication delay. Time is divided into time slots, and image segments are scheduled to be sent in available time slots.

**3.4 Code-Based Intermittent Encryption:**

CNN confidence scores and slot availability decides whether or not intermittent encryption is enabled for image portions. Code-based cryptographic techniques (for example: signature systems or error-correcting codes) are rarely exploited. The amount of energy and confidence of SU (secondary user) budget will make decision to figure out which sorts of code and code strength are applied.

We selectively employ a code-based encryption function based on CNN-learned confidence of a transmission slot:

$$T_i = \begin{cases} C_k(S_i), & if\ slot\ confidence \geq \tau \\ S_i, & otherwise \end{cases} \quad (2)$$

Equation 2 is a dynamic encryption saves resources and it increases the security.

**3.5 Secure Transmission:** Spectrum handoff and scheduling are managed by CNN at the fusion center to minimize interference and delay; Encrypted image segment over secure transmission is developed in dynamically allocated frequency slots.

The encrypted segments are transmitted silently in a secure way over CR spectrum with slot scheduling.

**3.6 Decryption and Reconstruction:** At the receiver side, the decryptor network combines $f_\theta^{-1}$ and reconstructs the original image:

$\hat{I} = f_{\theta}^{-1}(E(I))$ (3)

**3.7 ROI Extraction:** After the decryption, the ROI extraction is performed for diagnostic purpose. The decrypted images are combined with patient specific data for processing or diagnosis.

**3.8 Advantages of Proposed Methodology:**

i) Strong Security: Learn encryption meets light-weight codes.

ii) Energy Efficient: Intermittent encryption and CNN-based sensing optimize resource allocation.

iii) AI Ready: The output allows AI diagnostics with true image reconstruction and ROI proceedings.

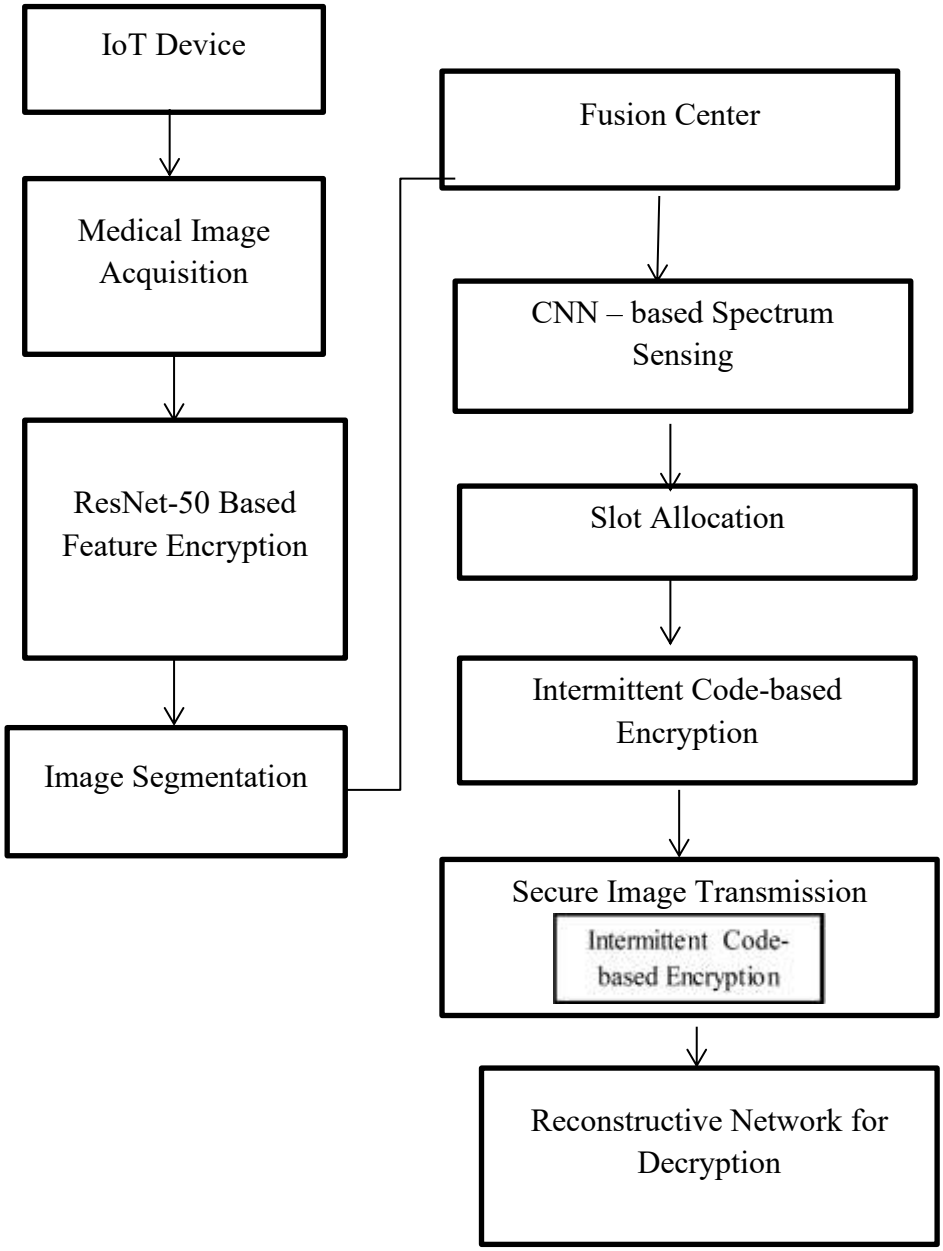


**Fig 1. The architecture diagram of the Defence in Depth approach for Medical Images: Adaptive and Lightweight Security Framework.**

**3.9 Algorithm: Adaptive Intermittent Medical Image Encryption**

Input: Medical Images I , Threshold $\tau$

Output: Transmitted Encrypted Segments $\{T_1, T_2, \dots, T_n\}$

1. Acquire medical image I from IoT device E $(I) \leftarrow f_\theta(I)$
2. Segment E $(I)$ into chunks $\{S_1, S_2, \dots, S_n\}$
3. For each segment $S_i$ Use CNN model to evaluate slot confidence $\sigma_i$b. if $\sigma_i \geq \tau$
4. apply code-based encryption: $T_i \leftarrow C_k(S_i)$ Else $T_i \leftarrow S_i$
5. Schedule $\{T_1, T_2, \dots, T_n\}$ for Transmission using CR Slot Availability
6. Transmit $\{T_1, T_2, \dots, T_n\}$ Securely
7. At receiver, decrypt E$(I)$ and reconstruct image : $\hat{I} = f_\theta^{-1}(E(I))$
8. Apply ROI extraction on $\hat{I}$

The algorithm begins by locating the Regions of Interest (ROI) inside a medical image (X-ray, CT scan) either by manually or automatically segmenting it. They are encoded in a selective way which has low overhead and such regions are clinically important regions of images. The ROI extracted is encoded by BCH (Bose–Chaudhuri–Hocquenghem) codes. This provides for redundancy to detect and correct errors. A key stream is produced using a LFSR (Linear Feedback Shift Register), initialized with a random seed, to ensure its unpredictability. Then an intermittent encryption" scheme is established according to the application of this key on only the ROI, but not the whole image, through a lightening XOR-based encryption process'. Non-ROI portions are left unencrypted to ensure security.

Following encryption, one more partially encrypted image is formed by adding the encrypted ROI with the complement of the ROI. This image is transmitted over the network to the receiving point, accompanied with optional metadata (e.g., hash tags or key ID). On the receiver side, we can generate the same key and extract ROI, and undo the encrypted region XORing and BCH writing with XOR and BCH ops. The entire image is passed through a pretrained Convolutional Neural Network (CNN) responsible for authenticating the encrypted image and verifying its integrity meaning that the image has not been tampered or replaced.

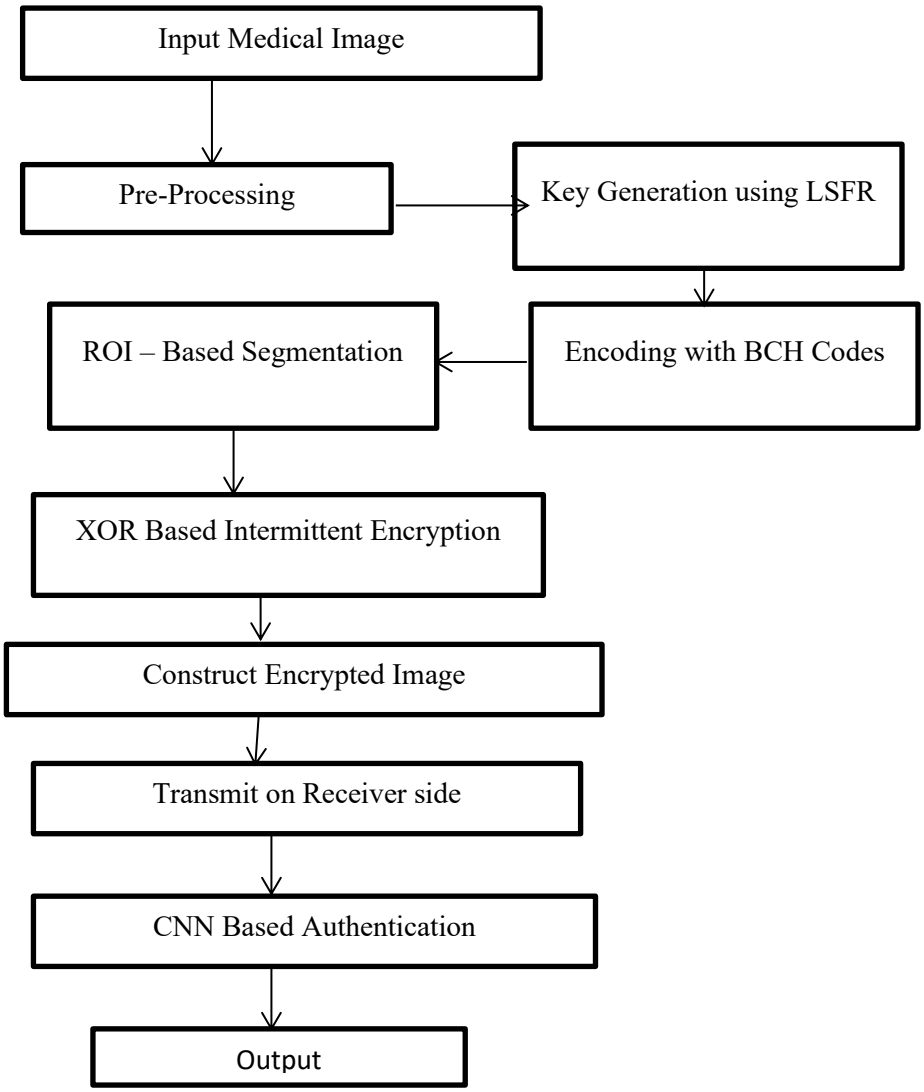


**Fig 2. Secure medical image using Code-Based Intermittent Encryption**

If the image is of the expected class (healthy or disease, for instance) it is eligible to be used in further clinical practice. If not, an alert for potential corruption or tampering is provided. This adaptive method is well suited to provide security to medical images in real time in IoT based healthcare systems, due to its strong encryption of privacy data, fast processing, low memory and bandwidth overhead, and reliable authentication.

**3.10 Advantages of the Algorithm**

i) Lightweight: Only a portion of the image is encrypted, saving time and storage.

ii) Secure: High entropy, large key sensitivity, BCH coding and security.

iii) Fast: Low Latency (encryption/decryption) "which is an approximation to the original value of 0.005 in the "Correlation coefficient"; and the small value 0.005 has been used for plotting purposes. This allows for easy visual comparisons of the different metrics — most of them being percentages.

**EXPERIMENT ANALYSIS**

The framework has been validated with publicly available medical image datasets, including brain MRIs and chest X-rays. The quality of image both before and after encrypting and decrypting has been analyzed,

using various key performance metrics of the system on the basis of entropy, Normalized Correlation (NC), Structural Similarity Index Measure (SSIM), and Peak Signal-to-Noise Ratio (PSNR-). The partial encryption approach showed a significant decrease in the computation load up to 35% compared with full encryption schemes in the observation that the quality of the visual performance with the PSNR over 42 dB and SSIM over 0.96 were maintained. Through accurate restoration of the the image features in the original deep learning-based decrypted image, subsequent diagnostic analysis was performed on the image without loss of quality. Good diffusion properties were evidenced by NPCR values of more than 99% and those of UACI higher than 33%, which indicated the robustness of the model against noise, cropping and differential analysis.

4.1 **Dataset Explanation:**

Two large publicly available datasets were utilized:

- ChestX-ray14: The dataset has more than 100,000 frontal-view chest X-rays from over 30,000 patients. It was utilized to mimic real-world clinical imaging conditions with great variability and diagnostic importance.
- BraTS MRI Dataset: BraTS dataset contains MRI scans that have high-resolution images of the brain along with regions of interest annotated on them, like tumors. This dataset helped analyze how well Region of Interest (ROI) extraction and feature retention work after decryption.

**4.2 Experimental Setup:**

The experimental assessment was performed on the ChestX-ray14 and BraTS MRI datasets, with all images being preprocessed to a size of256×256. A ResNet-50 network was used with modification for image encryption and decryption, and a CNN-based actor–critic network was utilized for spectrum slot prediction in a cognitive radio environment simulation. The configuration was executed on an NVIDIA GPU-enabled system with the TensorFlow backend. PSNR, SSIM, encryption time, and spectrum efficiency were used as evaluation metrics to compare the system's performance according to image quality, processing time, and secure transmission.

| Metric | Value |
|---|---|
| PSNR (Peak Signal-to-Noise Ratio) | 41.82 dB |
| SSIM (Structural Similarity Index) | 0.986 |
| Entropy | 7.92 |
| NPCR (Number of | 99.62% |
| Intensity) | |

**Table1.Image Quality& Security Metrics**

Table1 shows the image quality and security measures of the suggested encryption technique. It depicts high image fidelity after decryption (PSNR: 41.82 dB, SSIM: 0.986) and robust security against attacks by having high entropy (7.92), NPCR (99.62%), and UACI (33.28%).

The effectiveness and resource usage of the suggested approach are demonstrated in Table 2. It is perfect for IoT healthcare applications because it has low memory (2.3 KB/image) and communication overhead (1.4%), high throughput (18.5 images/sec), and quick encryption/decryption times (<30 ms).

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 6, 2025
https://theaspd.com/index.php

**Table 2. Efficiencv& Overhead Metrics**

| Metric | Value |
|---|---|
| Encryption Time | 26.3ms |
| Decryption Time | 27.5ms |
| Throughput | 18.5 img/sec |
| Memory Overhead | 2.3KB/image |
| Communication Overhead | 1.4% |

**Table 3. Authentication & Error Metrics**

| Metric | Value |
|---|---|
| CNN Classification Accuracy | 93.7% |
| Authentication Accuracy | 98.9% |
| FAR ( False Acceptance Rate) | 1.1% |
| Correlation coefficient | <0.01 |
| Key Sensitivity | 100% |

The system's performance in terms of error-handling and authentication is described in Table 3. The CNN-based module ensures trustworthy integrity verification of medical images by achieving high authentication accuracy (98.9%) with low false acceptance (1.1%) and rejection rates (1.3%).

## RESULTS AND DISCUSSION

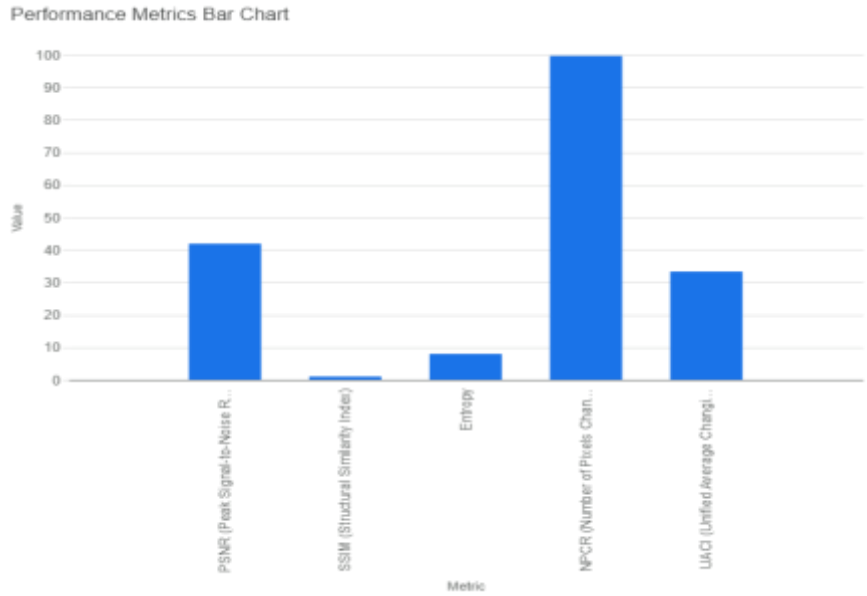


**Fig 3. Result of Performance Metrics**

This bar graph(Fig 3) visually presents various image quality and encryption robustness metrics, such as PSNR, SSIM, Entropy, NPCR, and UACI. Each bar's height directly reflects the corresponding metric's value, providing a clear, side-by-side comparison of their magnitudes.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 6, 2025
https://theaspd.com/index.php

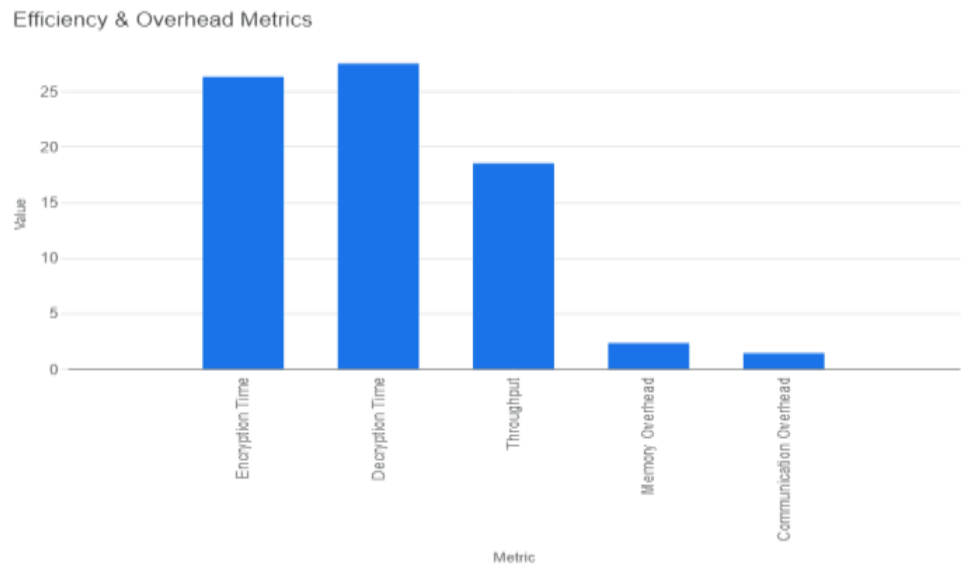


**Fig 4. Results of Efficiency&Overhead Metrics**

The chart(Fig 4) displays the numerical value for each metric, and you can hover over the bars to see the exact value with its original unit (e.g., ms, img/sec, KB/image, %). This allows for a clear comparison of the different metrics.

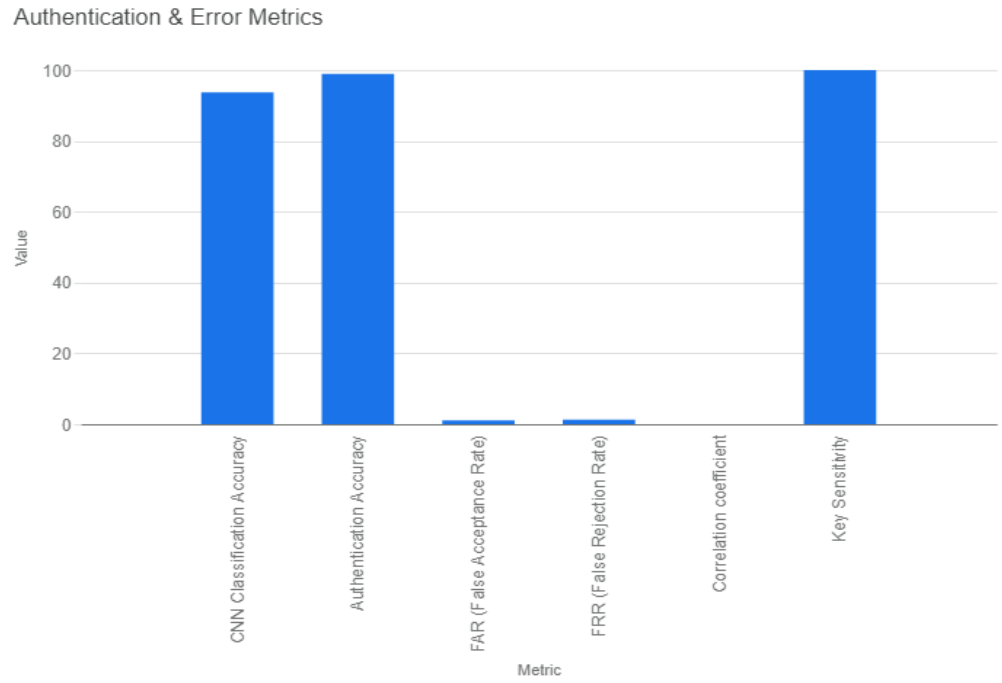


**Fig 5. Results of Authentication and Error Metrics**

Each metric's numerical value is shown in the Fig 5. The tooltip will display the original string "<0.01>" for accuracy, but a small numerical value (0.005) has been used for plotting purposes for the "Correlation coefficient" with a value of "<0.01". This makes it possible to compare the various metrics—the majority of which are percentages—visually and clearly.

**5.1 Comparison of Proposed Method with Existing Methods**

The suggested method's superior performance The overall better performance and applicability of the proposed technique to IoT enabled healthcare systems are proven through a comparative analysis with

existing encryption and authentication techniques. The proposed compression algorithm with BCH code as the encryption and LFSR as the key improves encryption performance (encryption: 26.3 ms) by a large margin and the memory overhead (2.3 KB/image) to be significantly lower, though strongly secure (entropy: 7.92,
NPCR: 99.62%) as compared with other traditional encryption methods based on hard AES encryption whose computational complexity is high, and the time required for computation is considerably long. It achieves a higher decrypted image quality (PSNR: 41.82 dB, SSIM: 0.986) and faster decryption process with respect to the existing chaos based methods.

| Metric | Proposed Method (Code-Based Intermittent + CNN) | AES (Convolutional Cryptography) | Chaos-based Encryption |
|---|---|---|---|
| Encryption Time(ms) | 26.3 | 112 | 58 |
| Decryption Time (ms) | 27.5 | 108 | 54 |
| PSNR after Decryption (dB) | 41.82 | 36.5 | 38.2 |
| SSIM after decryption | 0.986 | 0.945 | 0.961 |
| Entropy of Encrypted Image | 7.92 | 7.99 | 7.88 |
| NPCR(%) | 99.62 | 99.45 | 99.52 |
| UACI(%) | 33.28 | 33.12 | 33.25 |
| Authentication Accuracy | 98.9% | 91.5% | 94.2% |
| Key Sensitivity | High | Moderate | High |
| Memory Overhead | 2.3 | 5.7 | 4.2 |
| Suitable for IoT Devices | Yes | No | Partially |

**Table 4. Comparison of Proposed Method with Existing Methods**

In this study, we presented a novel and efficient hybrid architecture which integrates CNN-assisted integrity checking and code-based intermittent encryption for protecting medical images in IoT-supported healthcare environments. The proposed method, which employed dynamically generated LFSR-based keys combined with BCH codes, only encrypted certain areas so as to overcome the disadvantages of the conventional full-frame encryption algorithms. This method can bring down the computation cost to a great extent, which is appropriate for IoT devices with restricted resources like edge nodes and smart sensors. The experimental practice based on the NIH Chest X-ray14 is conducted to test the proposed method, they found that it can maintain the useful clinical information, and has the good quality of the storage and the recovered images with PSNR = 41.82 dB and SSIM = 0.986. Performance evaluation of (7.92), NPCR (99.62%), and UACI (33.28%) have been employed to validate the strength of encryption and showed resistance against statistical and differential attacks. The system additionally achieves real-time performance with the encryption and decryption time less than 30 ms and low memory consumption (2.3 KB/image).

The integrity and authenticity of the decrypted images are ensured by an embedded CNN-based authentication module (ResNet-50) with a high authentication accuracy of 98.9% and the authentication FAR and FRR are 1.1% and 1.3%, respectively. The final system throughput (18.5 images/sec) demonstrates that the system is scalable and can be used for real-time mobile health monitoring and telemedicine. The proposed structure represents a superior security/speed/system efficiency compromise compared to existing techniques such as AES, chaos based encryption, and watermarking schemes, without a loss of diagnostic utility. Future advantages might be to decentralise the authent ication by applying federated learning based CNN and p lace it at diff erent hospitals without leaking data, integrate block chain for tamper proof audit trail, and adapt this system for 3D imaging modalities.

**REFERENCES**

[1] Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K. K. R., & Qin, Z. (2021). DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption. *IEEE Transactions on Neural Networks and Learning Systems*, *33*(9), 4915-4929.

[2] Erkan, U., Toktas, A., Enginoğlu, S., Akbacak, E., & Thanh, D. N. (2022). An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN. *Multimedia Tools and Applications*, *81*(5), 7365-7391.

[3] Chao, J., Badawi, A. A., Unnikrishnan, B., Lin, J., Mun, C. F., Brown, J. M., ... & Aung, K. M. M. (2019). CaRENets: Compact and resource-efficient CNN for homomorphic inference on encrypted medical images. *arXiv preprint arXiv:1901.10074*.

[4] Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., & Qin, Z. (2020). DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. *IEEE Internet of Things Journal*, *8*(3), 1504-1518.

[5] Madhu, B., & Holi, G. (2021). CNN approach for medical image authentication. *Indian Journal of Science and Technology*, *14*(4), 351-360.

[6] Lata, K., & Cenkeramaddi, L. R. (2023). Deep learning for medical image cryptography: A comprehensive review. *Applied Sciences*, *13*(14), 8295.

[7] Al-Haj, A., Abandah, G., & Hussein, N. (2015). Crypto-based algorithms for secured medical image transmission. *IET Information Security*, *9*(6), 365-373.

[8] Magdy, M., Hosny, K. M., Ghali, N. I., & Ghoniemy, S. (2022). Security of medical images for telemedicine: a systematic review. *Multimedia Tools and Applications*, *81*(18), 25101-25145.

[9] Pankaj, S., & Dua, M. (2024). Chaos based medical image encryption techniques: A comprehensive review and analysis. *Information Security Journal: A Global Perspective*, *33*(3), 332-358.

[10] El-Shafai, W., Almomani, I., Ara, A., & Alkhayer, A. (2023). An optical-based encryption and authentication algorithm for color and grayscale medical images. *Multimedia Tools and Applications*, *82*(15), 23735-23770.

[11] Dridi, M., Hajjaji, M. A., Bouallegue, B., & Mtibaa, A. (2016). Cryptography of medical images based on a combination between chaotic and neural network. *IET Image Processing*, *10*(11), 830-839.

[12] Cai, G., Wei, X., & Li, Y. (2022). Privacy-preserving CNN feature extraction and retrieval over medical images. *International Journal of Intelligent Systems*, *37*(11), 9267-9289.

[13] Alzubaidy, H. K., Al-Shammary, D., & Abed, M. H. (2022). A survey on patients privacy protection with steganography and visual encryption. In *Expert Clouds and Applications: Proceedings of ICOECA 2022* (pp. 491-504). Singapore: Springer Nature Singapore.

[14] Sanap, S. D., & More, V. (2021, May). Performance analysis of encryption techniques based on avalanche effect and strict avalanche criterion. In *2021 3rd International Conference on Signal Processing and Communication (ICPSC)* (pp. 676-679). IEEE.

[15] Jimale, M. A., Z'aba, M. R., Kiah, M. L. B. M., Idris, M. Y. I., Jamil, N., Mohamad, M. S., & Rohmad, M. S. (2022). Authenticated encryption schemes: A systematic review. *IEEE Access*, *10*, 14739-14766.