# Secure and Efficient Tele-Radiography Based on the Fusion of a Convolutional Autoencoder and Chaotic Latent Encryption

Rayane Cherifi[1,2], Mahdi Madani[1,*], El-Bay Bourennane[1], and Karima Amara[2]
[1]Université Bourgogne Europe, IMVIA UR 7535, 21000 Dijon, France
[2]LITAN Laboratory, Higher National School of Computer Science ESTIN, Béjaïa, Algeria
Emails: rayanecherifi83@gmail.com(R.C.); mahdi.madani@ube.fr(M.M.); el-bay.bourennane@ube.fr(E.B.B.); amara@estin.dz (K.A.)
Corresponding author *

*Abstract*—**This paper addresses the dual challenges of efficient compression and secure transmission for medical images, par -ticularly in band width-constrained telemedicine scenarios, like tele-radiography. We propose an end-to-end pipeline combining deep learning-based compression with chaos-based encryption. A Convolutional Autoencoder (CAE), optimized with a Structural Similarity Index Measure (SSIM) loss function and incorporat-ing residual connections and batch normalization, achieves an 8:1 (87.5%) compression ratio on Chest X-ray images while maintaining a high fidelity of 96% SSIM and 36 dB Peak Signal-to-Noise Ratio (PSNR). To secure the compact latent representation generated by the CAE, we introduce a lightweight, chaos-based encryption scheme operating directly on the latent space. This scheme utilizes a logistic map for confusion and secure permutations for diffusion. The experimental results confirm the effectiveness of the compression module in preserving high-frequency details and the encryption scheme' s resistance against statistical attacks, by achieving high entropy (7.92), strong randomness (0.99), without correlation (close to 0 in horizontal, vertical, and diagonal directions), and very sensitive to small changes in the key (1 single bit change conduct to a completely different keystream). Our work offers a promising solution for secure and efficient transmission of medical images over constrained networks.**

*Keywords*—**convolutional autoencoder, chaotic cryptosystem, image compression, protected latent space, SSIM, secure transmission**

## I. Introduction

Digital communication and transmission serve as the backbone of today's connected world, allowing users around the globe to exchange data ranging from text and emails to videos and images. Many domains, such as cloud services, Internet of Things (IoT) gadgets, and especially telemedicine, rely on secure and efficient data transmission over protected and unprotected communication channels, driving the digital realm to innovate solutions that respond to the increasing specific needs tailored towards each domain.

Healthcare facilities prioritize both patient privacy and transmission efficiency due to the critical nature of medical operations, which is particularly challenging as medical imaging modalities produce large volumes of medical data. Computed Tomography (CT), Magnetic Resonance Imaging (MRI), and X-rays require considerable storage and transmission bandwidth. Teleradiography, a medical subfield that enables remote consultations, X-ray images, and expertise sharing, faces major challenges in rural and remote settings, primarily due to bandwidth and internet connectivity limitations. These issues compromise effective and secure communications, particularly in urgent cases where transmission speeds affect patient health. To meet these requirements, telemedicine uses traditional compression methods such as Joint Photographic Experts Group (JPEG), which is based on the Discrete Cosine Transform (DCT). However, this solution introduces blocking artifacts at high compression rates, where block boundaries become evident [1]. Similarly, although JPEG 2000 is superior in many respects, it introduces blurring artifacts at high compression levels, affecting high-frequency details essential for accurate and clinically reliable diagnosis [1].

Moreover, communication security is a major factor in data transmission systems, checking to guarantee the confidentiality, integrity, and availability of patient records. To ensure these requirements, traditional cryptography such as symmetric (e.g., Data Encryption Standard (DES), Triple Data Encryption Standard (3DES)) and asymmetric (e.g., Rivest-Shamir-Adleman (RSA)) modalities have been applied to medical images. Although effective in text and binary data, these solutions face major challenges when applied to high-resolution images due to their unique characteristics: high correlation of pixels, high redundancy, and bulk data capacity, which make them unsuitable for real-time applications [2]. Furthermore, these methods do not adequately address the issue of bit errors that may occur during image transmission over noisy channels, further limiting their effectiveness in securing multimedia data [2].

The dual challenges of compressing and securing voluminous medical images require innovative solutions that can address both concerns simultaneously. Artificial intelligence, particularly Deep Learning (DL) technologies, has been proven to be transformative in numerous fields, offering promising solutions for medical image transmission. Firstly, DL technologies provided solutions in many domains, such as computer vision and image classification [3], natural language processing [4], autonomous navigation, and even anomaly

Manuscript received June 17, 2025; revised July 5, 2025; accepted August 13, 2025; published January 16, 2026.

doi: 10.18178/joig.14.1.49-57

detection in cybersecurity [5]. In the medical field, DL models, particularly Convolutional Neural Networks (CNN), excelled in disease detection such as pneumonia on chest radiographs [6], medical image segmentation to detect tumor regions [7], lossless medical image based on DL [8] and lossy compression [9].

Inspired by advances in the literature in the DL domain, particularly in compression and feature extraction tasks, in this work, we propose a fast and efficient medical image transmission solution utilizing a DL-based Convolutional Autoencoder (CAE) [10]. The CAE compresses the images into a compact, non-interpretable latent representation through nonlinear operations; an inherent protection mechanism that acts as the first defense layer, because it requires the right decoder and model parameters to restore the original image. Our neural compressor reduces the overhead on bandwidth-constrained channels, with an added benefit of lowering the cost of storage. Nonetheless, the autoencoder's outcome is not cryptographically secure. The learned latent space does not provide enough entropy and randomness to stop a determined hacker from restoring parts of the original image using differential and statistical attacks. To counter this issue, we proposed an additional security layer by encrypting the latent space with a lightweight, chaos-based cryptosystem with a logistic map. We explored the advantages of the properties of chaos theory, such as sensitivity to initial conditions and randomness while being deterministic, to confound and diffuse them into the data to be protected. The used logistic map control parameters are secret keys managed in the encryption scheme. In addition, our solution is optimized for the latent space mathematical properties, while traditional cryptographic methods are tailored to operate on raw pixel values.

The lossy neural encoding stage of our transmission pipeline uses a deep learning convolutional autoencoder, trained on the COVID-19 Chest X-ray radiography dataset in grayscale, with batch normalization, residual connections, and a Structural Similarity Index Measure (SSIM) based loss function. Our approach was able to achieve a high compression ratio, making the image 8 times smaller than the original size, while ensuring high reconstruction quality up to 96% SSIM score and 36 dB Peak Signal to Noise Ratio (PSNR) value. The encrypted latent space is evaluated using statistical (bit-level analysis, horizontal, vertical, and diagonal correlations, randomness score, and byte entropy), key sensitivity, and key space complexity analysis.

The major contribution of this work lies in the combination of innovative integration and optimization of these methods, particularly for the secure transmission of medical images. It includes the following three issues:

- Unlike traditional methods that encrypt raw images, we encrypt the compressed representation (latent space), achieving simultaneous compression and security with minimal computational overhead.
- Most of the literature has focused on the compression properties of autoencoders. However, our work focused on acknowledging the obfuscation properties of latent spaces and their security limitations. Then, addressed them with the integration of a chaos-based latent space symmetric encryption algorithm.
- In the encryption algorithm, we used adaptive key derivation, with a password-based key derivation function with unique cryptographically secure nonces to ensure that each encryption session used different round keys, preventing replay attacks and improving secrecy.

The rest of the paper is organized as follows. Section II reviews related work in medical image compression and encryption. Section III presents the end-to-end transmission designed pipeline. Section IV describes the proposed neural lossy compression module via the convolutional autoencoder, and Section V discusses the dataset and experimental setup. Section VI evaluates the compression performance. Section VII details the chaos-based latent space encryption method. Section VIII analyzes the security performance of the encrypted latent space. Finally, Section IX concludes the paper and outlines directions for future work.

## II. Related Work

The proposed solution is built upon existing literature in both DL-based image compression, and Chaos-based image encryption. To emphasize our contribution, we need to review the current landscape to capture the advancements and identify potential limitations. The following section is a review of works in efficient image compression using autoencoders and recent developments in chaos-based image encryption techniques.

### A. Deep Learning Approaches for Image Compression: Convolutional Recurrent Neural Network (Conv-RNNs), Variational autoencoders (VAEs), and Autoencoders (AEs)

Sushmit *et al.* [11] proposed an RNN-Conv network architecture for X-ray medical image compression. In their network, both the encoder and the decoder contain recurrent units. They performed the image compression experiments on the National Institute of Health (NIH) ChestX-ray8 dataset [12]. Their model exceeds a 0.96 SSIM score and a 36 dB in PSNR with an 8 fold compression ratio. In another study, Zhou *et al.* [13] proposed an end-to-end trainable image compression framework using a VAE that achieves a high compression ratio and good PSNR (32dB). Naveen *et al.* [14] proposed an AE-based image compression method that integrates dimensionality reduction with inherent encryption, using a composite loss for improved reconstruction and security. All the methods mentioned above exhibited high compression ratios and good reconstruction quality.

### B. Variable Rate Deep Image Compression with Modulated Autoencoder

Autoencoder Yang *et al.* [15] address variable-rate compression by introducing a modulated autoencoder (MAE), where a shared autoencoder is adapted to different Rate-Distortion (R-D) tradeoffs via a modulation network. The authors experimented on CLIC and Kodak datasets. On the other hand, Choi *et al.* [16] proposed a variable-rate image compression framework using a single conditional autoencoder, with rate control managed through a Lagrange multiplier and quantization bin size. Both approaches are superior to traditional methods especially at low bitrates.

### C. Color Image Encryption Through Chaos maps

Alexan *et al.* [17] offered a solution for RGB image encryption, by combining the KAA map with multiple chaotic maps like the 2D logistic sine, tent, and Bernoulli maps, while Qian *et al.* [18] used three-dimensional chaotic maps (Logistic and Cat maps) for pixel value diffusion and position confusion, also, Pak *et al.* [19] presented a color image encryption solution that employed a 1D Logistic and Sine map, derived from the output sequences of two existing chaotic maps. Additionally, Sharma [20] introduced a 2D Adjusted Logistic Map (2D-LALM) for image encryption, derived by coupling a 2D logistic map with two 1D logistic maps, which showed high statistical randomness for encryption. Madani *et al.* [21] proposed an image-based cryptosystem using three-dimensional chaotic maps combining a Discrete Skew Tent Map (STM) with a discrete Piecewise Linear Chaotic Map (PWLCM) to generate a dynamical key ensuring confusion, and a logistic map to generate keystream ensuring diffusion. All the solutions demonstrate robustness against visual, statistical, and differential attacks with large key spaces.

While the reviewed works demonstrate significant progress in their respective domains, our framework stands by its unique integration and targeted application. On the compression front, methods like Sushmit *et al.* [11] and Yang *et al.* [15] focus on DL-based compression techniques, laying the ground on rate-distortion optimization and variable-rate compression capabilities for general and medical image use cases. In contrast, our approach utilizes a CAE architecture for high-quality medical image reconstruction at a fixed, high compression ratio, with an SSIM-based loss function critical for preserving high-frequency details (lesions and bone structures), which are extremely relevant in clinical settings, particularly teleradiography under bandwidth constraints.

More fundamentally, regarding security, existing chaos-based encryption methods, such as those proposed by Alexan *et al.* [17] and Sharma [20], operate directly on the image pixel domain where they employ various chaos maps and techniques, like pixel shuffling or the KAA map for confusion and diffusion, on the raw image data. Our contribution lies in shifting the encryption process entirely to the compressed latent space, making it a hybrid strategy that offers several advantages:

- Efficiency: by only encrypting the dimensionally reduced latent space, reducing computation overhead.
- Syner gy: it leverages the inherent transformation performed by the autoencoder, applying a tailored chaos-based system optimized for the statistical properties of the latent space, rather than generic raw pixel data.
- Integrated security: security is embedded within the compression pipeline, not merely applied as a subsequent layer to the original or reconstructed image, offering a more holistic approach to secure transmission.

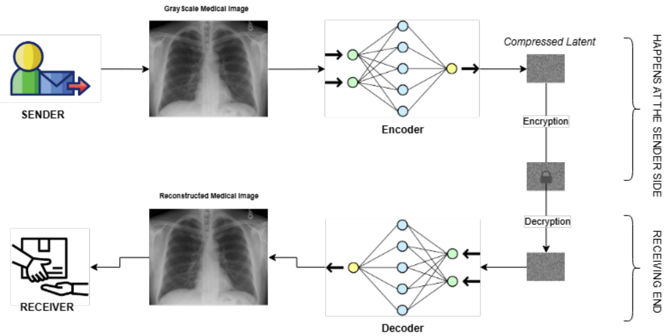

Fig. 1. End to End Transmission Pipeline.

Therefore, our work bridges the gap by presenting an end-to-end solution that combines neural compression optimized for medical fidelity with a lightweight, chaos-based cryptographic system operating directly and efficiently on the latent representation, addressing the specific dual challenges of secure and efficient medical image transmission in bandwidth-limited environments.

## III. End-to-End Transmission Pipeline

Our main system is built to allow secure and efficient medical image sharing over bandwidth constrained, potentially insecure communication channels. The sending process starts with the original $1 \times 128 \times 128$ grayscale X-ray image, and goes through two main phases :

- The compr ession : the input image is fed into the convolutional encoder module, which transforms the image to a compact latent space of $32 \times 8 \times 8$ (Channels, Height, Width), achieving a reduction of 8:1 in our case.
- The encryption phase : the latent tensor, resulting from the compression phase, is flattened and encrypted using the chaos-based cryptosystem. Only the encrypted vector will be transmitted over the communication channel.

At the receiver's location, like a central hospital, the reconstruction process starts by decrypting the received encrypted vector using the same cryptosystem and keys, allowing the recovery of the original latent space. After reshaping to the original tensor form, the decrypted latent space will be reconstructed back to the original medical image through the convolutional decoder while preserving fine details for accurate medical diagnosis. The architecture of the whole system is illustrated in Fig. 1.

## IV. Proposed Architecture: Neural Lossy Compression via CAE

The proposed compression module is based on a convolutional autoencoder, as detailed in Fig. 2. As we can see, the model is composed of two main modules: an encoder that downsamples the input image to a compact latent space through convolutional layers [14]. The bottleneck layer is a bridge between the two modules that further compresses the latent space, by selecting the most important features for learning, and a mirrored decoder that learns to restore the original image from the latent space through deconvolutional layers [14] while minimizing the reconstruction error. To stabilize training and allow deep feature extraction, we opted for residual connections, through residual skip connections inspired by the ResNet network [22].

### A. SSIM Loss Function

Our neural network was trained with an SSIM-based loss function defined by $Loss = 1 - SSIM$, working to minimize the loss to yield high SSIM values. We chose the SSIM parameter to evaluate images because it focuses on perceptual quality, focusing on factors such as luminance, contrast, and structural information. It is defined according to a general Formula 1 [23].

$$\mathrm{SSIM}(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \qquad (1)$$

On one hand, traditional loss functions such as Mean Squared Error (MSE) and Mean Absolute Error (MAE) fail to align with human visual perception and diagnostic requirements and focus on pixel perfect reconstruction. On the other hand, SSIM prioritizes structural coherence, essential in maintaining high-frequency details, highly relevant in maintaining pathological indicators for effective and accurate medical diagnosis.

Therefore, we optimized the SSIM calculations on the loss function to be efficient during training. Initially, we leverage GPU acceleration for faster SSIM computation, and applied reflective padding to minimize boundary artifacts, we also employed efficient convolutions for calculating local statistics.

## V. Experimental Setup and Dataset

### A. Training Dataset Description

To train and evaluate the proposed CAE, we opted for the publicly available COVID-19 radiography dataset. This specific dataset comprises 21,165 grayscale X-ray images spanning over four categories: normal, COVID-19, lung opacity, and viral pneumonia. The preprocessing included resizing images to 128×128 pixels format to ensure uniform input size for the model, and encoding the resized images as tensors with the shape (1, 128, 128). The dataset was randomly split into 70% for training, 15% for validation, and 15% for testing.

### B. Training the 8:1 Compression Model :

Pytorch framework based on Python was used to train our autoencoder, which provided powerful tools for building the architecture. To accelerate training, Nvidia's CUDA GPU technology was used with a Tesla K80 and 12GB of VRAM.

The autoencoder is composed of a convolutional encoder and a mirrored decoder. The input grayscale 1 × 128 × 128 (Channels, Height, Width) image is mapped into 256 channels of size 8 × 8 through four convolutional layers, with intermediate residual blocks and batch normalization for fast and stable training. The number of channels is reduced to 32 for a compressed latent space (32 × 8 × 8).

The goal of the mirrored decoder is to reconstruct the original image from the compact latent space by upsampling the feature maps through deconvolutional layers.

The model was trained over 45 epochs, with a learning rate of $10^{-3}$ and Adam optimizer. We also employed a learning rate scheduler that monitors the validation loss and reduces the learning rate by half if no improvement is noticed for three consecutive epochs, ensuring efficient training and preventing overfitting. The training and validation loss curves over the 45 epochs are presented in Fig. 3. The curves show that both the training and validation losses decrease steadily over the 45 epochs, which indicates effective learning and minimal overfitting.

## VI. Compression Performance Evaluation

Our experiments demonstrate the effectiveness of the proposed SSIM-based autoencoder for medical image compression at the target 8:1 (87.5%) compression ratio. It achieved superior reconstruction quality compared to an identical architecture trained with a standard MSE loss function.

Quantitative performance metrics for both models on the test set, comprised of 3176 images, are averaged and summarized in Table I. Notably, the SSIM-trained model achieved an average PSNR of 36.04 dB and an average SSIM score of 0.9599. This represents a significant improvement over the MSE-trained baseline (PSNR: 35.39 dB, SSIM: 0.9483), particularly the 1.2% higher SSIM score, indicating better preservation of high-frequency structural information critical for diagnostic purposes. The SSIM-based model exhibits sharper details and fewer blurring artifacts compared to the MSE-based model, particularly around complex anatomical structures often relevant in radiographic images. Three sample images are shown in Fig. 4.

Furthermore, we compared the performance of our neural compressor to the study of Sushmit *et al.* [11] to highlight the strong generalization and performance gains of our proposed solution. Both models are configured for 8:1 compression ratio, and a 128 × 128 input size. Both models are tested on a subset of (NIH) ChestX-ray8 dataset [12]. Our convolutional autoencoder achieved superior performance on both SSIM and PSNR metrics, with an increase of 0.56 dB in PSNR and 0.009 in SSIM compared to the reference method on the NIH dataset. These results, presented in Table II, showcase the strong performance and generalization capabilities of our medical autoencoder, performing better on both in-distribution and out-distribution of data, confirming the cross-dataset effectiveness, which is extremely valuable in real-world scenarios where deep learning models encounter data from various modalities and equipment. Three sample images are shown in Fig. 5. Both Figs. 4 and 5 compare SSIM-based reconstructions on the COVID-19 and NIH Chest X-ray datasets, respectively. As we can remark, these figures show original images, latent

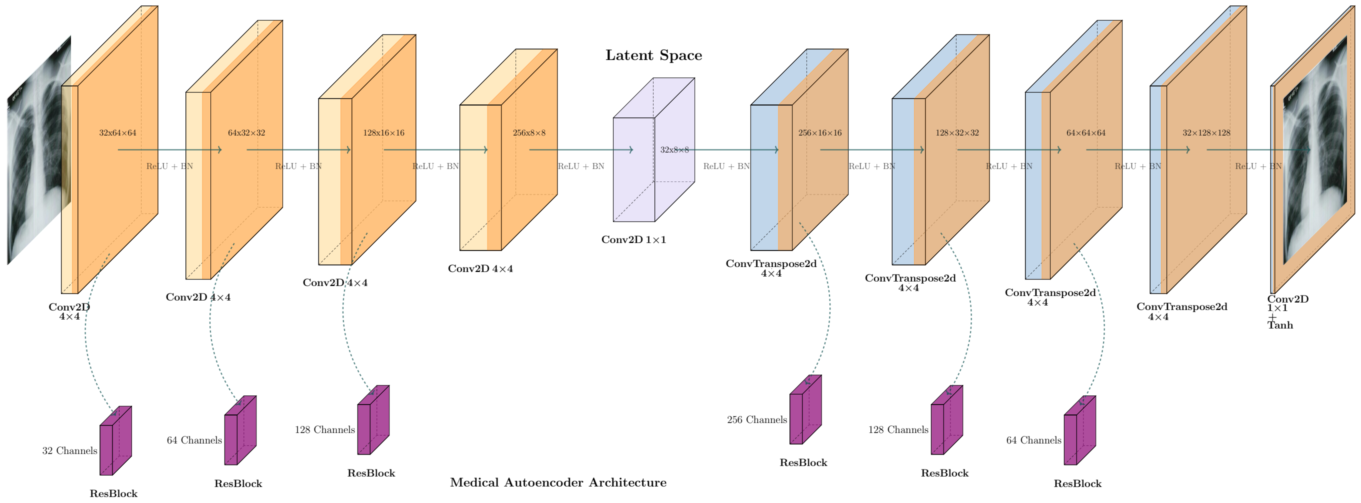

Fig. 2. CNN-based Lossy compression module.

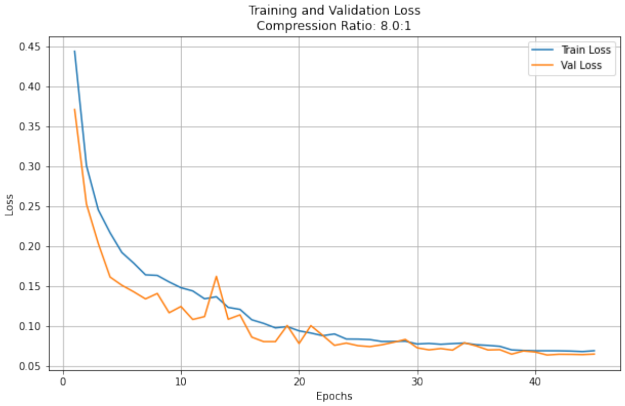

Fig. 3. Training and validation loss (1 - SSIM) curves over 45 epochs. The validation loss shows convergence without significant overfitting.

TABLE I
Quantitative Results at 8:1 Compression Ratio.

| Loss Function | MSE ↓ | PSNR (dB) ↑ | SSIM ↑ |
|---|---|---|---|
| MSE Loss | 0.000315 | 35.39 | 0.9483 |
| SSIM Loss (Ours) | 0.000277 | 36.04 | 0.9599 |

space encodings, and reconstructions, demonstrating consistent performance across two different datasets with minor variations in quality metrics scores.

Despite the good image reconstruction ratio of 96%, in a real application, a medical opinion is necessary to assess whether the quality of the received image is sufficient for diagnosis. However, the results obtained are still usable, and we can easily recognize the details, as shown in Figs. 4 and 5. This limit also remains relative and will always depend on the medical field of application.

TABLE II
Comparative Results at 8:1 Compression Ratio.

| Method | Test Dataset | PSNR (dB) ↑ | SSIM ↑ |
|---|---|---|---|
| Sushmit *et al.* [11] | NIH | 35.93 | 0.9579 |
| Proposed | NIH<br>COVID-19 | 36.50<br>36.04 | 0.9668<br>0.9599 |

## VII. Chaos-Based Latent Space Encryption Method

After compressing the input image into a latent space, we encrypted the result using a chaos-based cryptosystem based on a logistic chaotic map. The single-round algorithm applies a logistic map random sequence, defined by the iterative Eq. 2.

$$x_{n+1} = rx_n(1 - x_n) \tag{2}$$

where $x_0, x_n \in [0, 1]$ and $r \in [0, 4]$. The generated sequence is then bitwise XORed with the latent space to transform it, representing the confusion step. The result is followed by a cryptographically secure, yet deterministic permutation based on the Fisher-Yates algorithm [24], representing the diffusion step. This shuffle iterates through the data array and permutes each element with another chosen randomly from the remaining unvisited elements without repetition. At each step, the choice is made pseudo-randomly using Keyed-Hash Message Authentication Code (HMAC-SHA256). The cryptosystem is controlled using three secret keys: K1 representing the logistic map's initial seed, K2 representing the permutation key, and K3 representing the control parameter (r) of the chaotic map (see Eq. 2). Note that the three secret encryption keys are encoded in 64-bits format, and should be shared securely between the sender and the receiver before starting communication. The encryption process is presented in Fig. 6.

In a specific telemedicine application, the key exchange process can be implemented, for example, according to the following framework:

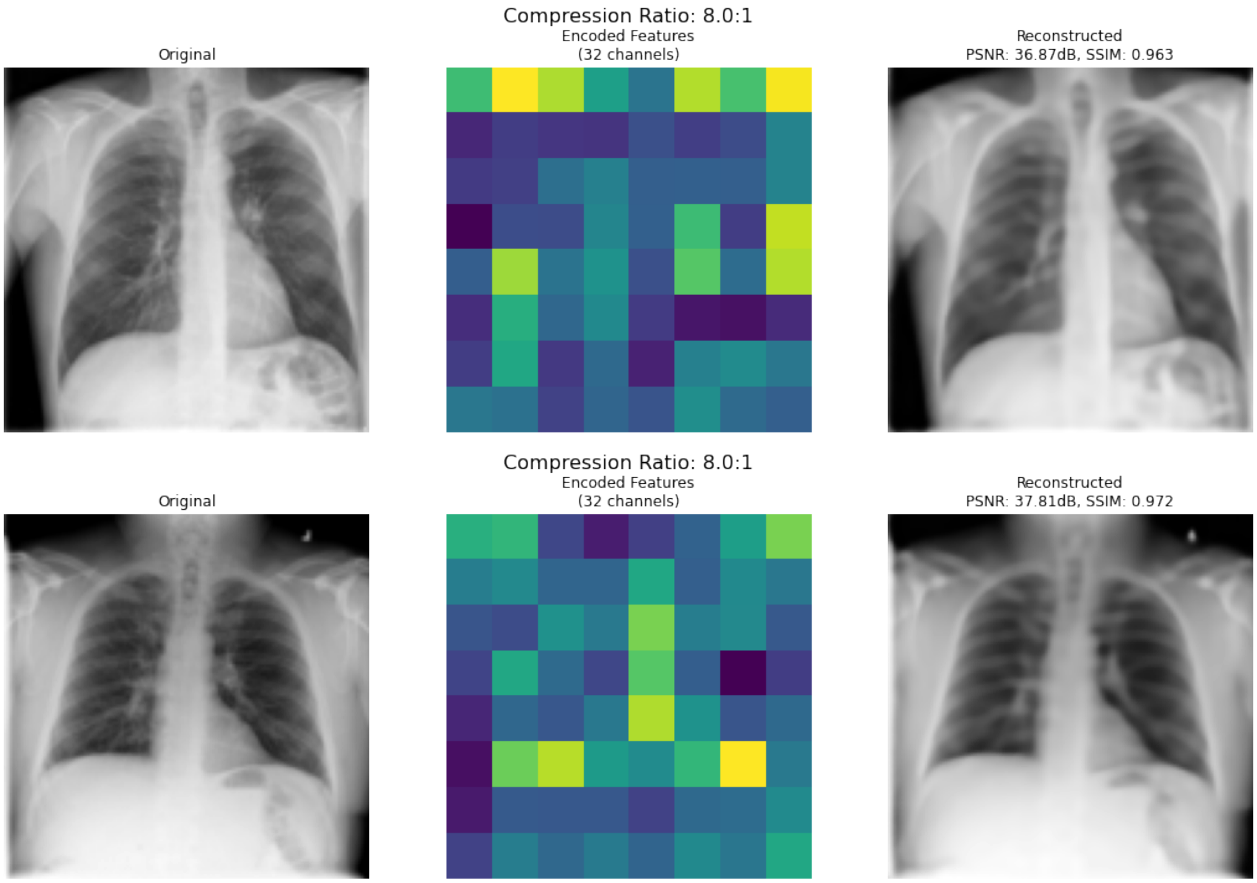

Fig. 4. Visual assessment of the SSIM model reconstruction on the COVID-19 chest X-ray dataset. Left: original X-ray images; Center: first channel of compressed latent space; Right: reconstructed images with PSNR and SSIM metrics.

- First, the medical entity generates the required keys during the patient's registration visit, for example, using a Public Key Infrastructure (PKI) approach, leveraging existing healthcare certification authorities. Next, an Elliptic Curve Diffie-Hellman (ECDH) key agreement can be used to establish the shared secrets between the telemedicine endpoints. Then, integrate it with existing key management systems for greater compatibility with the current healthcare IT infrastructure.
- The process is then monitored by an operational key management service to ensure the generation of session keys (a unique encryption key per telemedicine session) and automate key rotation (periodic key updates for the next session without user intervention).
- Finally, after sharing secret keys between the hospital entity and the patient, each party can start using the proposed encryption scheme for its needs (to encrypt the latent space on one side and to decrypt it and recover the original on the other side).

The output is the final encrypted vector $C_{final}$, which will be transmitted. To restore the original image, the receiver decrypts the received $C_{final}$ using the same cryptosystem and keys to recover the latent space vector. Then, it uses the mirrored CNN-based decoder to recover the plain image.

For the security evaluation, we opted for standard statistical analysis techniques, including correlation analysis (horizontal, vertical, diagonal), Shannon entropy calculation, Bit Randomness via Autocorrelation, key sensitivity, and key space tests. The results, summarized in Section VIII, attest to the scheme's effectiveness in decorrelating latent values, maximizing randomness, and exhibiting high sensitivity to key changes, indicating strong resistance against common cryptanalytic attacks.

To clarify the security context and the importance of our encryption scheme, we defined bellow two primary attacker models relevant to telemedicine networks.

- Eavesdropping Attacker: If a passive adversary monitors network traffic in transit, the chaos-encrypted latent space ensures that the intercepted ciphertext reveals no structure or content, even under statistical analysis, thanks to the randomness of the generated keystream and sensitivity of the chaotic map.
- Man-in-the-Middle Attacker: In the case of an active adversary capable of modifying or injecting packets into the transmitted data. Our encryption exhibits strong key

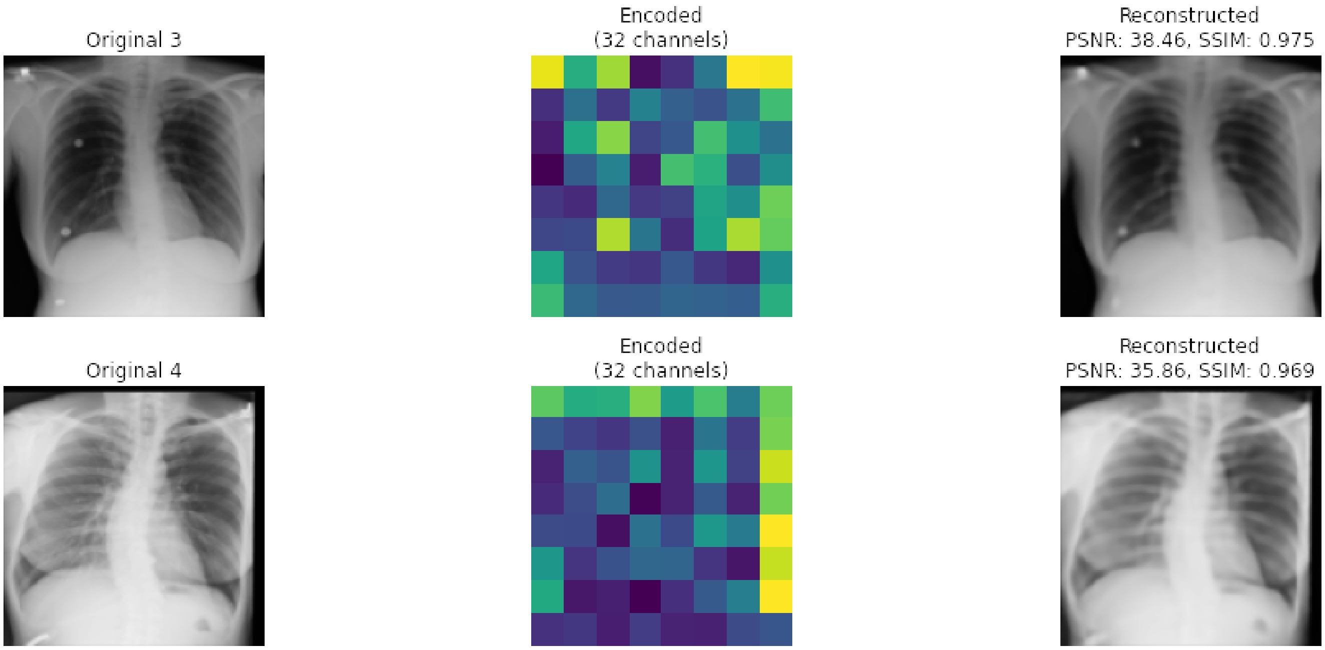

Fig. 5. Visual assessment of the SSIM model reconstruction on the (NIH) Chest X-ray8 dataset. Left: original X-ray images; Center: first channel of compressed latent space; Right: reconstructed images with PSNR and SSIM metrics.

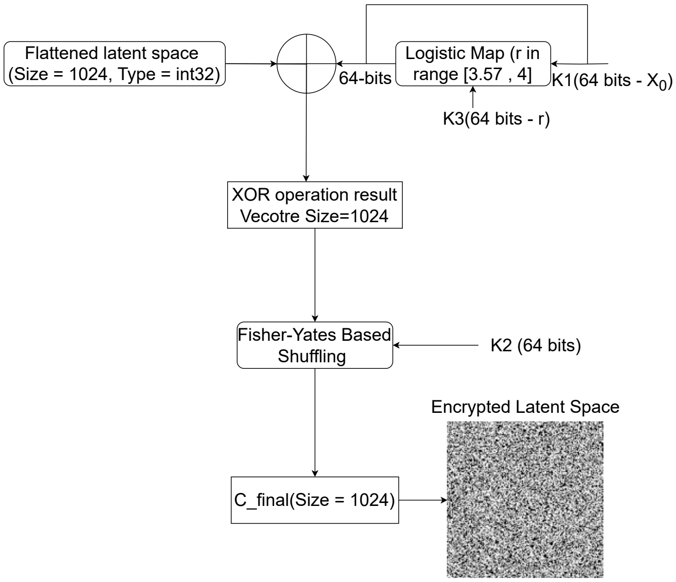

Fig. 6. Encryption diagram.

sensitivity to small changes in input or key, resulting in 48˘49% bit-level variation, effectively breaking predictable relationships and making unauthorized tampering easily detectable.

## VIII. Security Analysis of the Encrypted Latent Space

TABLE III
Comparative bit-level security metrics across images (1 round encryption).

| Metric | Original | Image 1 | Image 2 | Image 3 |
|---|---|---|---|---|
| Bit Change Rate (%) | – | 48.7 | 48.7 | 48.3 |
| Byte Entropy (bits) | 6.64 | 7.92 | 7.91 | 7.91 |
| Bit Randomness | 0.938 | 0.995 | 0.995 | 0.996 |
| Horizontal Correlation | 0.122 | 0.004 | -0.006 | -0.004 |
| Vertical Correlation | 0.028 | -0.005 | -0.009 | 0.002 |
| Diagonal Correlation | 0.029 | 0.004 | -0.007 | 0.003 |

To test the influence of the number of encryption rounds on the security level of our cryptosystem, we compared a single-round with a three-round encryption scheme scenario. But the results are similar. Therefore, we considered in this work only the one-round scenario to gain in terms of hardware resources. This will facilitate implementing the proposal in an embedded system real-life application.

### A. Bit-Level Latent Space Encryption Analysis

To validate the effectiveness of our encryption scheme, we tested 3 different latent spaces (images) using the same encryption process. The results, shown in Table III, confirm that all three achieve near-optimal bit change rates around 48–49%, which is close to the optimal value of 50%, indicating strong diffusion properties. Furthermore, the byte-level entropy significantly increases from 6.64 bits in the original latent spaces to over 7.9-bits, approaching the theoretical maximum of 8-bits while the bit randomness rises from a high baseline of 0.938 (highlighting the inherent obfuscation of the compact latent space) to a near-maximum of 0.995, suggesting a high degree of unpredictability. Additionally, the encryption process

TABLE IV
KEY SENSITIVITY ANALYSIS RESULTS.

| Rounds | Avg Change (%) | Test 1 | Test 2 | Test 3 |
|---|---|---|---|---|
| 1 | 48.55 | 48.54 | 48.97 | 48.13 |

effectively eliminates most spatial correlations present in the original latent space in the horizontal, vertical, and diagonal directions.

Consequently, by conducting this first preliminary security analysis evaluating the: Byte Entropy, Bit Randomness, and the Correlation (Horizontal, Vertical, and Diagonal), we proved the good resistance of the proposed algorithm to statistical attacks according to the results showed in Table III.

### B. Key Sensitivity Analysis

A key sensitivity test was conducted by measuring how changes in the secret key affect the encrypted output, which is an important property in cryptography where strong encryption algorithms should exhibit the avalanche effect, where a small change in the input causes a significant change in the output.

*1) Experimental Setup:* For each test, we generated a reference ciphertext using the original key by modifying exactly one bit of the encryption key. After generating a new ciphertext using the modified key, we calculated the change percentage of bits between the two ciphertexts. This experiment was repeated three times (3 tests). Theoretically, an ideal encryption scheme should produce approximately 50% bit change when a single bit of the key is modified.

*2) Results and Analysis:* As shown in Table IV, the results demonstrate excellent key sensitivity across all tested configurations. This proves that the proposed encryption exhibits strong avalanche characteristics, by producing an average of 48.55% bit change rate.

*3) Security robustness:* In addition to the best statistical resistance, the proposed cryptosystem is based on a chaotic map known for its best security properties, such as determinism (best randomness), non-linearity, extreme sensitivity to very small changes in the initial conditions and control parameters ($10^{-12}$). This layer has contributed considerably to improving the confusion and the key sensitivity of the whole algorithm. Furthermore, the results of the performed tests, the Bit Change Rate given in Table III, and the key sensitivity given in Table IV proved the satisfaction of the avalanche effect, proving the good resistance to linear cryptanalysis.

### C. Key Space Analysis

As we already mentioned, the proposed cryptosystem is based on three secret parameters (K1, K2, and K3). Each of them has a size of 64-bits. Therefore, our proposition reach a key space of $2^{64*3} = 2^{192}$. Consequently, this prove the resistance of our architecture to the brute-force-attacks because it surpasses the minimum key space complexity fixed actually in the literature to $2^{128}$.

Moreover, the key space of the proposed system reaches the best requirements compared with the state-of-the-art established encryption standards, as shown in Table V.

TABLE V
KEY SPACE COMPLEXITY COMPARISON.

| Encryption standard | Key size | Key space | Brute-force resistance |
|---|---|---|---|
| DES | 56-bits | $2^{56}$ | Weak |
| 3DES | 112-bits | $2^{112}$ | Low |
| 3DES | 168-bits | $2^{168}$ | Acceptable |
| AES-128 | 128-bits | $2^{128}$ | Acceptable |
| AES-192 | 192-bits | $2^{192}$ | High |
| AES-256 | 256-bits | $2^{256}$ | High |
| The proposed | 192-bits | $2^{192}$ | High |

As it is clearly presented in Table V, we can conclude that the proposed encryption algorithm key space and key complexity are similar to AES-192, which is known to be resistant to brute force attacks based on the current hardware advancements. However, the security of our cryptosystem is supported by the permutation applied function based on the Fisher-Yates Shuffling function using a 64-bits additional key. By considering this separate function, it reinforces the resistance against brute-force cryptanalysis.

### D. Discussion

In this work, we subjected our architecture to basic statistical tests, such as entropy, correlation, and bit randomness. The results showed the satisfaction of the expected theoretical requirements. Additionally, the used non-linear and extremely sensitive (a change of $2^{-12}$ in the initial conditions and control parameters) chaotic map improved the confusion and the key sensitivity properties of the proposed algorithm. Also, it satisfies the avalanche effect, proving good resistance to linear cryptanalysis. Furthermore, the key space complexity of the algorithm can reach $2^{192}$. This characteristic bolsters the resistance against brute force attacks.

Consequently, by considering all the performed security tests and the obtained results, we conclude that the proposed cryptosystem is robust against statistical, linear, and brute-force cryptanalysis.

## IX. CONCLUSION

This work proposes an adaptable end-to-end solution for tele-medicine applications, by allowing fast and efficient transmission with a modular deep learning-based convolutional autoencoder, optimized with SSIM loss. The proposed neural compressor exhibits 8 fold compression ratio while maintaining high-frequency details on the reconstructed images. We addressed the security weaknesses by embedding a lightweight chaos-based cryptosystem into the latent space. The system showcased excellent results on both fronts, with a 96% SSIM and 36 dB PSNR, preserving clinically sound high-frequency details, and showcased excellent generalization capabilities validated on the COVID-19 and NIH X-ray datasets. The cryptosystem demonstrated strong statistical resistance properties with 7.9 entropy, 0.995 randomness, and near-zero correlation scores. Our hybrid system offers a promising solution for real-time, secure medical diagnosis over bandwidth-limited networks.

Our future work will explore adaptive compression and experiment with different high-dimensional chaos maps for more cryptographic resistance. Additionally, it will explore more rigorous analysis, including resistance to known-plaintext attacks, chosen-plaintext attacks, and differential cryptanalysis. We will also improve the system to reach the clinical validation requirements by including in the system a multi-modality image testing (validation across different medical imaging types) and a clinical workflow (trying for assessment within real telemedicine environments) to facilitate the Radiologist evaluation study.

## Conflict of Interest

The authors declare no conflict of interest, and all of them have approved the final version.

## Author Contributions

R.C designed the model, carried out the experiment, and wrote the manuscript with support from M.M. and E.B.B. K.A. encouraged R.C. to finalize the work. E.B.B helped supervise the project. M.M conceived the presented idea and was in charge of the overall direction. All authors discussed the results and contributed to the final manuscript.

## Funding

This work was funded by the Bourgogne-Franche-Comté region as part of the ANER project number 2024PRE00022 entitled CIAPD.

## References

[1] D. A. Koff and H. Shulman, "An overview of digital compression of medical images: Can we use lossy image compression in radiology?" *Can Assoc Radiol J.*, vol. 57, no. 4, pp. 211–217, Oct. 2006.

[2] M. F. M. Mursi, H. E. H. Ahmed, F. E. Abd El-Samie, and A. H. Abd El-Aziem, "Image encryption based on development of Hénon chaotic maps using fractional Fourier transform," Int. J. Strateg. *Inf. Technol. Appl.*, vol. 5, no. 3, pp. 62–77, July 2014. https://doi.org/10.4018/ijsita.2014070105

[3] M. M. Krishna, M. Neelima, M. Harshali, and M. V. G. Rao, "Image classification using deep learning," *Int. J. Eng. Technol.*, vol. 7, no. 2.7, pp. 614–617, 2018. https://doi.org/10.14419/ijet.v7i2.7.10892

[4] A. Torfi, R. A. Shirvani, Y. Keneshloo, N. Tavaf, and E. A. Fox, "Natural language processing advancements by deep learning: A survey," arXiv preprint, arXiv:2003.01200, 2020. https://doi.org/10.48550/arxiv.2003.01200

[5] G. Pang, C. Shen, L. Cao, and A. V. D. Hengel, "Deep learning for anomaly detection: A review," *ACM Comput. Surv.*, vol. 54, no. 2, pp. 1–38, Mar. 2022. https://doi.org/10.1145/3439950

[6] P. Szepesi and L. Szilágyi, "Detection of pneumonia using convolutional neural networks and deep learning," *Biocybern. Biomed. Eng.*, vol. 42, no. 3, pp. 1012–1022, 2022. https://doi.org/10.1016/j.bbe.2022.08.001

[7] S. Anantharajan, S. Gunasekaran, T. Subramanian, and R. Venkatesh, "MRI brain tumor detection using deep learning and machine learning approaches," *Meas. Sensors*, vol. 31, 101026, 2024. https://doi.org/10.1016/j.measen.2024.101026

[8] M. A. U. R. Khan, M. A. Khan, and F. Ahmed, "Lossless medical image compression based on anatomical information and deep neural networks," *Biomed. Signal Process. Control*, vol. 74, 103499, 2022. https://doi.org/10.1016/j.bspc.2022.103499

[9] X. Liu, L. Zhang, and Z. Guo et al., "Medical image compression based on variational autoencoder," *Math. Probl. Eng.*, vol. 2022, 7088137, 2022. https://doi.org/10.1155/2022/7088137

[10] M. Madani and E. Bourennane, "Visually image encryption and compression using a CNN-based autoencoder," *Int. J. Comput. Netw. Commun.*, vol. 17, no. 2, pp. 113–123, Mar. 2025. https://doi.org/10.5121/ijcnc.2025.17207

[11] A. S. Sushmit, S. U. Zaman, A. I. Humayun, T. Hasan, and M. I. H. Bhuiyan, "X-ray image compression using convolutional recurrent neural networks," in *Proc. 2019 IEEE EMBS Int. Conf. Biomed. Health Inform.*, 2019, pp. 1–4.

[12] X. Wang, Y. Peng, L. Lu, Z. Lu, M. Bagheri, and R. M. Summers, "ChestX-Ray8: Hospital-scale chest X-ray database and benchmarks on weakly-supervised classification and localization of common thorax diseases," in *Proc. 2017 IEEE Conf. Comput. Vis. Pattern Recognit.*, 2017, pp. 3462–3471.

[13] L. Zhou, C. Cai, Y. Gao, S. Su, and J. Wu, "Variational autoencoder for low bit-rate image compression," in *Proc. CVPR Workshops*, 2018.

[14] A. K. Naveen, S. Thunga, A. Murki, M. Kalale, and S. Anil, "Autoencoded image compression for secure and fast transmission," in *Proc. 2024 IEEE Int. Conf. Comput. Vis. Mach. Intell.*, 2024, pp. 1–6.

[15] F. Yang, L. Herranz, J. v. d. Weijer, J. A. I. Guitián, A. M. López, and M. G. Mozerov, "Variable rate deep image compression with modulated autoencoder," *IEEE Signal Process. Lett.*, vol. 27, pp. 331–335, 2020.

[16] Y. Choi, M. El-Khamy, and J. Lee, "Variable rate deep image compression with a conditional autoencoder," in *Proc. 2019 IEEE/CVF Int. Conf. Comput. Vis.*, 2019, pp. 3146–3154.

[17] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color image encryption through chaos and KAA map," *IEEE Access*, vol. 11, pp. 11541–11554, 2023.

[18] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," *IEEE Access*, vol. 9, pp. 61334–61345, 2021.

[19] C. Pak, K. An, P. Jang, J. Kim, and S. Kim, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 9, pp. 12027–12042, May 2019. https://doi.org/10.1007/s11042-018-6739-1

[20] M. Sharma, "Image encryption based on a new 2D logistic adjusted logistic map," *Multimedia Tools Appl.*, vol. 79, no. 1–2, pp. 355–374, Jan. 2020. https://doi.org/10.1007/s11042-019-08079-x

[21] M. Madani, S. El Assad, F. Dridi, and R. Lozi, "Enhanced design and hardware implementation of a chaos-based block cipher for image protection," *J. Differ. Equations Appl.*, vol. 29, no. 9–12, pp. 1408–1428, 2022. https://doi.org/10.1080/10236198.2022.2069496

[22] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, 2016, pp. 770–778. https://doi.org/10.48550/arXiv.1512.03385

[23] D. Brunet, E. R. Vrscay, and Z. Wang, "On the mathematical properties of the structural similarity index," *IEEE Trans. Image Process.*, vol. 21, no. 4, pp. 1488–1499, Apr. 2012.

[24] A. O. Ade-ibijola, "A simulated enhancement of Fisher-Yates algorithm for shuffling in virtual card games using domain-specific data structures," *Int. J. Comput. Appl.*, vol. 54, no. 11, pp. 24–28, Sep. 2012. https://doi.org/10.5120/8612-2469