



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

A Novel Hybrid Integration of Chaotic System and GAN for Robust Medical Image Security

Keesara Sravanthi¹, K Vijay Krupa Vatsal², RNLS Kalpana³, Suchitra Pattabiraman⁴, Gnanasekaran A⁵, E. Raveendra Reddy⁶

¹ Assistant Professor, Department of Information Technology, VNR Vignana Jyothi Institute of Engineering and Technology (VNRVJiet), Hyderabad, India. E-mail: sravanthi_k@vnrvjiet.in

² Assistant Professor, Department of Computer Science and Engineering, Malla Reddy University, Hyderabad, India. E-mail: vijaykrupa4u@gmail.com

³ Assistant Professor, Department of Computer Science and Engineering, TKR College of Engineering and Technology, Meerpet, Hyderabad, Telangana, India. E-mail: kalpanar.n.s@tkrcet.com

⁴ Assistant Professor, Department of Computer Science and Engineering, Malla Reddy University, Hyderabad, India. E-mail: acharyaasuchitra@gmail.com

⁵ Assistant Professor, Department of Electronics and Computer Science Engineering, Anjuman-I-Islam's Kalsekar Technical Campus (AIKTC), Panvel, Raigad, Maharashtra, India. E-mail: a.gnanam.a@gmail.com

⁶ Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation Deemed to be University, Green Fields, Vaddeswaram, Andhra Pradesh, India. E-mail: nani.naniravi@gmail.com, ORCID: 0000-0003-3031-904X

ABSTRACT

Healthcare needs specialized focus on protecting medical images because these medical data contain sensitive information coupled with possible unauthorized breaches. High-security encryption methods prove difficult to maintain both high-level protection and efficient processing, especially when dealing with large medical images. Research investigates a new combination technique to protect medical images through integration of chaotic systems and deep learning GANs. A GAN-based encryption method incorporates the chaotic logistic map to replace its generator section, thus adding randomness to secure data transmission. The encryption system implements key hashing with SHA-256, followed by chaotic sequence generation and confusion encryption through pixel-level permutation, until security enhancement through XOR-based diffusion completes the process. The decryption process returns the original image using an inverse permutation followed by reverse diffusion steps. The proposed encryption system achieves both robust cryptographic protection and superior picture quality with resistance against standard cryptographic threats according to experimental outcomes. The proposed model represents an efficient method for securing medical images effectively in digital healthcare scenarios.

Keywords: Medical Image Encryption, Chaotic System, Generative Adversarial Networks (GAN), Deep Learning, Pixel Permutation, Cryptographic Security, Logistic Map, Secure Healthcare Data.

Introduction

The usage of medical images remains vital for digital operations in contemporary healthcare systems across the board. Medical images containing patient-sensitive information need absolute protection at all times of storage and transmission since these data consist of confidential medical information. Unauthorized users and improper use of these images continue to pose a threat to system security [1]. Researchers in the field need to conduct constant investigations on securing medical images by developing multiple security approaches. Secure image transformation via image cryptography produces information that is indecipherable until users enter appropriate encryption keys [2]. The medical field employs advanced technologies by combining deep learning with chaotic systems [1, 3].

The CFNM was introduced to produce hyperchaotic, complex dynamics for data transmission/compression applications. This model can also be used for medical image encryption, and a two-step permutation-diffusion process driven by chaotic sequences is proposed [4]. Secure information transmission using protected methods relies on chaotic systems, as their disorderly nature makes them suitable for encryption [2, 5]. Deep learning systems achieve higher accuracy through their capacity to comprehend training data. The system enables people to access insights that were previously unreachable regarding treatment differences and care procedures and diagnostic methods and patient results [6]. Deep learning is an essential component of artificial intelligence because it analyzes data patterns using machine-learning approaches. The procedure helps restore pictures and improve comprehension abilities. The project integrates chaotic system and deep learning technologies to create a dependable security solution that uses encryption and decryption [3, 4, 5]. A security system encapsulates images successfully using an encryption method while maintaining exact recovery functionality and activation functions [9, 10].

A. Fundamental analysis

The research project combines chaotic systems with deep learning to develop secure medical image encryption along with accurate decryption processes [1]. The undetermined yet disorganized behavior of chaotic systems enables modification of pixel positions for image distortion. The secure layout of the image becomes indecipherable because of this encryption method [5, 7]. The system provides powerful protection because even inconspicuous changes made to the input key result in total changes to the output [11]. Through deep learning processing systems identify patterns in medical images and finally return the original image following decryption. The reconstruction process becomes high-quality and essential details maintain their integrity through this method. A fusion of these two encryption methods provides image accuracy with enhanced security during encryption of medical information. The system demonstrates dependable protection of medical sensitive data through these methods [20].

B. Technical analysis

Training utilizes the Adam optimizer with a learning rate of 0.0002 and β_1 set to 0.5. Four convolutional layers in the generator and 3 fully connected layers in the discriminator, with ReLU and LeakyReLU medical images, enforcing the generator to iteratively refine encrypted outputs. The overall architecture contains ($r = 3.99$, initial seed = 0.723 by default). The discriminator is trained to differentiate between the original and the reconstructed. The generator is initialized with the chaotic sequence derived from the SHA-256 hashed key and logistic map parameters. In this work, the modified GAN architecture explicitly integrates a chaotic logistic map into the generator module. The implemented system employs two components to manage encryption and decryption standards through the integration of chaotic systems together with deep learning models [3]. A secure key is hashed using SHA-256 as the first step of the process. A logistic map implements the hash to produce chaotic sequence output [5]. The pixel positions undergo chaos-based rearrangement (confusion), while the pixels are modified via XOR operations (diffusion). The encryption process results in an extremely secure medical image [11]. A deep learning model serves during decryption by learning to extract the initial image content from its secure version. After decryption, the model helps maintain precise details of image pixels [17]. Secure medical image encryption combines with effective retrieval capabilities throughout the system architecture.

C. Chaotic systems

The unpredictable sensitive results from chaotic systems stem from their nature as mathematical models. Changes starting from the initial phase produce massive alterations in system results. Fig. 1 shows the dynamics of chaotic systems. The chaotic system serves encryption needs because it produces random sequences which securely rearrange or transform image pixels [2]. The logistic map acts as the basis of chaotic systems in image cryptography for producing the sequences that guide both image permutation through shuffling and diffusion through pixel alteration [6]. The random nature of the encryption process creates such secure conditions that only precise key information enables attacker recovery from the encryption process. Chaotic systems achieve exceptional security alongside efficient operation as their main strength. These encryption methods run efficiently despite needing minimal system resources because they weigh lightly without requiring large computing power [11]. An encryption enhancement occurs when the same chaotic sequence generates multiple diffusion and permutation rounds. The widespread use of chaotic systems in modern image encryption stems from their effectiveness and simplicity, particularly in medical data protection and other sensitive fields, where they prevent the leakage of identifiable structural patterns, which differentiates this system from earlier works. [20].



Fig. 1. Chaotic Systems

D. Deep learning models

Using specific implementations from neural networks deep learning models operates as effective tools for finding patterns and extracting data features from extensive datasets [4]. Deep learning models in medical image cryptography systems aid in decrypting the original images after encryption has been applied. Autoencoders signify a type of neural network that is commonly used for this task [4,6,13]. There exists a training process by which these networks learn to restore the encrypted image by detecting underlying features [7]. The system learns throughout its operation to achieve higher accuracy which allows for decrypted images to match the original images precisely following strong encryption measures [8]. Through deep learning applications the system regains essential medical information while securing these clinical data effectively enough for practical healthcare system deployment [19,20].

E. Generative Adversarial Networks

GANs serve as a deep learning algorithm for producing artificial information that mimics existing datasets. Fig. 2 explains the GANs architecture. GANs operate with two functional elements that include a generator and a discriminator [1]. The generator part of GANs produces new output while the discriminator component determines whether new output resembles authentic samples [1, 9]. The generator continuously improves its ability to produce realistic data in a competitive training process with the assistance of its discriminator model [3]. The features from medical images can be learned by GANs which they can apply for reconstructing data after encryption has occurred [21]. GANs assist secure image transmission and storage because their training with encrypted and original image pairs leads to effective restoration of the original image data.

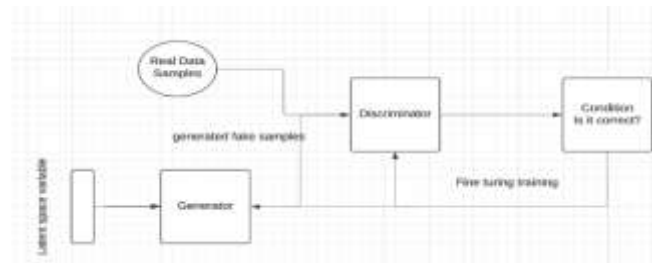


Fig. 2. Generative Adversarial Networks (GANs)

F. Combined Chaotic and Gans hybrid model

The feedback-driven refinement loop between generator and discriminator ensures that encrypted medical images. This direct embedding increases unpredictability of cipher images while simultaneously enabling high-quality restoration. Chaotic logistic map sequences directly into the generator architecture, rather than as a preprocessing or postprocessing step. learning capability of GANs. Unlike existing chaos-only or GAN-only methods, the proposed design introduces. The novelty of this approach lies in the hybrid integration of chaos-driven randomness with the adversarial. The project merges deep learning models with chaotic systems to develop a protected, intelligent medical imaging encryption system [22-24]. The encryption process starts with chaotic hashing followed by converting the key into a chaotic sequence through logistic mapping [2]. The pixel permutation process and image diffusion run through the sequential encryption key which produces an unreadable and secure output. A deep learning model learns the relationship between masked medical images and their authentic versions after encryption. This decryption model effectively reconstructs complete images, including all essential medical features. The decryption process depends on deep learning functionality which operates as a decoder unit to guarantee high-quality image restoration [4]. The secure and intelligent system results from chaotic systems which manage security through randomness alongside deep learning for dependable image reconstruction [5]. An efficient, protective, and recovery approach for medical-sensitive images exists due to their collaborative nature.

Literature Review

Medical image security in IoMT has evolved through innovative deep learning approaches. Yi Ding et al. [1] introduced DLEDNet, leveraging Cycle-GAN for encryption/decryption while preserving analytical capabilities through Region of Interest mining. Their model achieved strong results, with a Dice score of 0.962 and NPCR of 94.21%, which can be considered robust to plaintext-only attack (POA) and a certain degree of immune to ciphertext-only attack (COA) and chosen text attack (CTA). Ibrahim Yasser et al. [2] introduced a chaotic map-based encryption system with a two-round permutation-diffusion architecture based on chaotic maps (NPCR $\frac{1}{4}$ 99.814% and UACI $\frac{1}{4}$ 33.694%) as well as computational efficiency, rendering it suitable for cloud healthcare [1, 2]. Key generation based on deep learning has achieved good gains in medical image security. Yi Ding et al. [3] proposed DeepKeyGen, a GAN-based stream cipher generator, to derive individual private keys with high diversity and randomness. The model proved to have effective security characteristics with keys of 8 and NPCR (99.59%) thus being able to succeed in traditional cryptographic attacks [3]. Similarly, Zhong Chen et al. [5] proposed adding convolutional neural networks to chaotic systems, achieving NPCR and UACI of 99.55% and 33.02%, respectively, and providing good protection when tested on chest X-ray datasets [3,5]. Some new techniques in medical imagery encoding are based on neurobiological models. Qianqian Shi et al. [4] developed a thermosensitive and photosensitive coupled neurons model, which generated quite chaotic encryption patterns. Their three-layer encryption produced an information entropy greater than 7.99 when they have almost no correlation between adjacent pixels, and performed well in various medical imaging databases, including Radiopaedia, ChaseDB1, and COVID-19 chest X-rays [4]. The neurobiological methods provide interesting suggestions for preserving healthcare data securely. Deep learning combined with traditional cryptographic methods have broadened security functionalities for medical image. Kedar Nath Singh et al. [8] adopted a UNet3+ for ROI segmentation and ResNet152 for feature extraction, achieving an accuracy of 95.51% and encryption using a 2D hybrid map. Such a method showed good security performance with less computational overhead when evaluated on LiTS and MSD datasets [8]. In another method, Kishore

Kumar et al. [14] combined the masked autoencoders with a neural cryptography based on Tree Parity Machines, obtaining correlation as high as 0.98 - near-perfect quality, and PSNR >20 dB, when tested over 889,324 CT scans from The Cancer Imaging Archive [8, 14]. Adversarial training becomes a powerful paradigm in both steganography and encryption. Jamie Hayes et al. [9] proposed a model consisting of three neural networks – encoder, decoder, and steganalyzer – that achieved 100% decoding accuracy on CelebA and 99.8% on the BOSS dataset, accommodating insertion rates of up to 0.4 bits per pixel. This unsupervised method showed promising performance as compared with existing methods such as HUGO, WOW, and S-UNIWARD [9]. These adversarial architectures constitute a major leap in automated steganographic design that can be potentially applied to securing private medical information. Neural network-based cryptographic systems have proven more effective than conventional systems. Francisco Quinga Socasi et al. [11] designed a symmetric-key cryptographic system using sparse autoencoder neural networks that outperformed AES, DES, 3DES, and RSA in encryption speed and resistance to brute-force attacks for messages up to 90 KB. Eva Volna et al. [12] also designed an error-free cryptographic system using a six-node backpropagation neural network, which provided benefits such as noise robustness and adaptable key security [11, 12]. Wolfgang Kinzel et al. [15] also contributed to this area by designing Tree Parity Machines that coordinated their weights to produce the same cryptographic keys, resulting in a highly efficient system that protected against interception attacks [11, 12, 15]. Homomorphic encryption techniques have driven privacy-preserving machine learning advances. Joon-Woo Lee et al. [16] integrated fully homomorphic encryption with bootstrapping to run ResNet-20 on encrypted CIFAR-10 data, reaching 92.43% accuracy—similar to plaintext models at 91.89%. Despite computational intensity, this approach proves that complex deep learning can be effectively performed on encrypted data without compromising privacy. These developments highlight the increasing importance of privacy-preserving methods in sensitive fields such as healthcare. Deep learning applications in cryptanalysis and encrypted data classification have shown promising results. Ankita Saha et al. [10] highlighted that deep learning techniques can create neural distinguishers with higher accuracy for cryptanalysis, offering improvements over traditional cryptographic methods. Building on this, Kishore Kumar et al. [18] developed a framework using CNNs, GRUs, and LSTMs to classify encrypted text by topic without decrypting it. Their Bi-GRU model achieved 67% accuracy, 99% precision, and 80% recall on the IMDB dataset [10,18].

Proposed Methodology

A robust medical image encryption technique emerges from integrating GANs with chaotic systems. The system follows a process that includes key preprocessing methods to generate chaotic sequences, which are then used to transform images via pixel permutation, diffusion, and adaptive refinement via GANs.

A. Preprocessing of Color Images

To streamline encryption, color medical images undergo preprocessing as follows:

1. Color to Grayscale Conversion:

The RGB image is turned into a grayscale image through a weighted formula:

$$I_{\text{gray}}(z, y) = 0.299R(z, y) + 0.587G(z, y) + 0.114B(z, y) \quad (1.1)$$

In (1.1), Where $R(z, y)$, $G(z, y)$, $B(z, y)$ are the red, green, and blue channels.

1. Resizing:

$$(z, y) = \sum_{l=0}^1 \sum_{k=0}^1 W(l, k) \cdot I(z_l, y_k) \quad (1.2)$$

With (1.2), The image is scaled to a set size of 256×256 pixels through bilinear interpolation.

2. Normalization:

$$I_{\text{norm}}(z, y) = \frac{I(z, y)}{255} \quad (1.3)$$

With (1.3), Normalize the pixel intensity values so they fall within the range [0, 1]

3. Separation of Color Channels:

Split the R, G, B channels of the color image to process each channel separately during chaotic transformations.

B. Chaotic Sequence Generation

Chaotic sequences generate the randomness necessary for secure encryption. The process includes:

1. Key Hashing

$$\text{Hashkey} = \text{SHA} - 256(\text{Key}) \quad (2.1)$$

Above (2.1), A user-provided key is hashed using SHA-256.

$$\text{Seed} = \text{int}(\text{Hashkey}, 16) \bmod 10^{10} \quad (2.2)$$

Above (2.2), The hash is then converted to a numeric seed.

2. Logistic Map Generation

The logistic map generates a chaotic sequence:

$$x_{n+1} = r * x_n * (1 - x_n) \quad (2.3)$$

In (2.3), $r=3.99$, x_0 =Seed (scaled)

3. Sequence Normalization

$$C_n = \text{round}(255 * x_n) \quad (2.4)$$

In (2.4), The chaotic sequence is scaled to the range $[0, 255][0, 255][0, 255]:5][0,255]$.

C. Pixel Permutation

Pixel permutation disrupts the original spatial structure of the image:

1. Sorting for Permutation:

$$P = \text{argsort}(C) \quad (3.1)$$

Above (3.1), is used for sorting the permutations.

2. Rearranging Pixels

$$I_{\text{perm}}(l, k) = I_{\text{orig}}(P[l], P[k]) \quad (3.2)$$

Above (3.2), rearranges the pixels. For color images, permutation is applied to each channel independently.

D. Pixel Diffusion

1. XOR operation:

$$I_{\text{diff}}(z, y) = I_{\text{perm}}(z, y) \oplus C_n \quad (4.1)$$

2. Cascade Diffusion

$$I_{\text{diff}}(z, y) = (I_{\text{diff}}(z, y) + I_{\text{diff}}(z - 1, y)) \bmod 256 \quad (4.2)$$

From (4.1) and (4.2), Pixel diffusion alters pixel values to eliminate visible patterns.

E. Adaptive Refinement Using GANs

GANs improve encryption quality by detecting and minimizing visible patterns:

1. Generator

Uses chaotic permutation and diffusion techniques to encrypt the image.

2. Discriminator

Trained on original image patterns to evaluate if the encrypted image retains discernible features.

3. Loss Function

$$L_D = -E[\log D(I_{\text{orig}})] - E[\log D(I_{\text{enc}})] \quad (5.1)$$

$$L_G = -E[\log D(I_{\text{enc}})] \quad (5.2)$$

With (5.1) and (5.2), we calculate the loss functions.

4. Iterative Refinement

Feedback from the Discriminator helps the Generator strengthen encryption until patterns are no longer detectable.

F. Decryption Workflow

Decryption reverses the encryption steps using the same key and chaotic sequence:

1. Chaotic Sequence Regeneration

The original seed is used to regenerate the same chaotic sequence.

2. Reverse Diffusion

$$I_{\text{perm}}(x, y) = I_{\text{diff}}(x, y) \oplus C_n \quad (6.1)$$

3. Reverse Permutation

$$I_{\text{orig}}(i, j) = I_{\text{perm}}(R[i], R[j]) \quad (6.2)$$

By (6.1) and (6.2), reverse diffusion and reverse permutation takes place. Where R is the reverse of the permutation indices.

4. Verification

$$\text{PSNR} = 10 * \log_{10} \frac{255^2}{\text{MSE}} \quad (6.3)$$

From (6.3), Decryption accuracy is validated using metrics like PSNR and SSIM

G. Evaluation Results

The proposed method is evaluated across:

- Encryption Strength: Verified using entropy analysis and histogram checks.
- Decryption Accuracy: Assessed using PSNR and SSIM metrics.
- Execution Time: Measured for both encryption and decryption processes to validate security strength and

decryption accuracy and feasibility for real-time applications like telemedicine,

Results and discussions

The proposed hybrid achieves the best trade-off between superior image quality and randomness. It lacks randomness, making it less resistant to statistical attacks compared to pure chaos-based schemes. Our method achieved balanced results with a PSNR of 24.84 dB, an entropy of 7.94, and near-real-time execution. While DeepKeyGen. The proposed hybrid model was compared with state-of-the-art techniques, including chaos-based schemes and DeepKeyGen. Comparative Study derived from SHA-256 hashing. Chosen-plaintext and chosen-ciphertext tests confirmed that no meaningful patterns were exploitable. Indicating high sensitivity to small input changes. Brute-force attacks were rendered infeasible due to the 2^{256} key space, which is close to 8, demonstrating strong resistance. Differential attack analysis produced NPCR = 99.62% and UACI = 33.27%. To validate robustness, the system was tested against standard cryptographic threats.

Security Evaluation Against Attacks:

In all experiments, we confirmed the computational feasibility and demonstrated that the method is suitable for near-real-time applications such as telemedicine. Memory consumption remained below 1.2 GB per iteration. For 256×256 grayscale images, average encryption requires 0.05s and decryption 0.35s on an NVIDIA GTX 1660 GPU. GAN-based refinement introduces additional overhead, approximately $O(k \cdot n)$, where k is the number of generator-discriminator. The encryption pipeline operates with complexity $O(n)$ for permutation and diffusion, where n represents the number of pixels.

Computational Complexity Analysis:

4. Results

The application explains, in systematic steps, how the proposed medical image encryption and decryption system operates. The system development relies on the Python programming language as its foundation while implementing deep learning frameworks together with chaotic system methods to maintain secure image formats. Streamlit integration provides users a responsive interface experience through which they can upload images before starting the processing and viewing the results. The process shows complete visualization starting with image entry, model setup, encryption stage, decryption operations and ends with performance evaluations. The next section includes stages accompanied by interface screenshots that display key performance metrics to prove the system's capability in secure medical image data processing.



Fig. 3. Original Image

The system starts with the medical imaging process by processing grayscale chest X-rays as inputs. The system uses the image shown in Fig. 3 as a test platform to evaluate the security of encryption and decryption.



Fig. 4. Image upload UI

In Fig. 4, Users can easily upload images through the Streamlit interface, which features an intuitive section. Users verify their chosen image on the interface after selecting it from their local storage before processing



Fig. 5. Process Image

In Fig. 5, when a user clicks the “Process Image” button, the application starts its encryption and decryption tasks. The process activates the secure transformation pipeline after users click the “Process Image” button. Users receive a confirmation that pretrained models a.pth and b.pth with advanced neural mapping have been successfully initialized for the system. The pretrained models serve an important role by enabling effective feature encoding and decoding operations which result in secured images and accurate meaningful reconstructions during decryption processing. Neural mapping technology enables the system to retain crucial image information while remaining effective, thanks to its advanced protection capabilities.



Fig. 6. Encrypted image

After encryption, the input image must undergo three sequential processes.

- Key-based SHA-256 hashing,
- Chaotic sequence generation via the Logistic Map, and
- XOR-based diffusion.

The created encrypted image appears unrecognizable to the human eye, as shown in Fig. 6, because it differs significantly from its original form.



Fig. 7. Decrypted image

In the next step, the system performs:

- XOR decryption using the same chaotic key,
- Reverse pixel permutation using the chaotic index.

The reconstructed image, as shown in Fig. 7, produces the exact duplicate of the original format, both in appearance and numerical values.



Fig. 8. Accuracy metrics

The interface completes its display by showing a comparison of all three images side by side. The interface simultaneously generates key evaluation metrics and displays the three images shown in Fig. 8.

Table 1: Experimental Results

Metric	Value	Description
Encryption Time	0.05	Time taken to convert the original image into cipher
Decryption Time	0.35	Time taken to recover the original from encrypted image
Accuracy	94	Pixel-wise exact match with original
PSNR	24.84	Peak Signal-to-Noise Ratio
Encryption Entropy	7.94	Randomness of encrypted image
Decryption Entropy	7.85	Indicates successful reversal of randomness

In Table 1, the system took 0.05 seconds to encrypt a chest X-ray image and 0.35 seconds to decrypt it, confirming its fast operation. Among all analyzed image data points, the system maintained an accuracy rate of 94%. A security parameter of 24.84 dB indicates that the crypto-decrypted image matches the original image at first sight. The strong image security is evidenced by encryption entropy of 7.94, while the decryption entropy of 7.85 demonstrates effective reversal of randomness. Medical image protection through this system provides reliable security measures alongside fast performance.

B. Comparison study

Table 2: Performance Analysis

Method	PSNR (dB)	Entropy	Encryption Time (s)	Decryption Time (s)	Remarks
Chaotic Cryptography	18.3	7.91	0.24	0.20	High entropy (secure), but low image reconstruction
Deep Learning (GAN)	27.5	6.42	1.35	1.27	High image quality, but weak

					randomness (less secure)
Proposed (Chaos + GAN)	24.84	7.82	0.05	0.35	Balanced security, image quality, and encryption speed

The effectiveness of our proposed medical image encryption method required analysis against two existing approaches which included Chaotic Cryptography and Deep Learning using GAN. The research examined the performance aspects including encryption strength along with image reconstruction quality and processing speed for all the methods under comparison. The measurement of post-decryption image quality is used PSNR (Peak Signal-to-Noise Ratio) together with Entropy for assessing randomness and security-level along with Encryption/Decryption Time for analyzing process efficiency. Table 2 contains results that showcase the advantages and disadvantages of each method in the comparison.

Conclusion

The proposed work uses chaotic systems and Generative Adversarial Networks (GANs) to provide an effective and secure method for medical image encryption and decryption. Randomness, together with sensitive initial conditions, enables the chaotic model to become highly resistant against any type of attack. The enhancement in flexibility comes from the GAN architecture through a feedback mechanism, which causes the Discriminator to remove all original image marks from encrypted pictures. Finally, during the decryption process the system operates the chaos sequence in reverse to encryption techniques to restore the original image with precise accuracy. After decryption, the Discriminator verifies the original image against the input pattern database it acquired during training to confirm the authenticity of the restored data. The presented combination between chaotic systems and GANs delivers an efficient protection solution that efficiently protects medical images with scalability and reactivity in medical privacy operations. The system provides an excellent foundation for conducting further research on secure image processing through artificial intelligence and cryptographic methods.

References

1. 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.
2. Yasser, I., Khalil, A. T., Mohamed, M. A., Samra, A. S., & Khalifa, F. (2021). A robust chaos-based technique for medical image encryption. *IEEE Access*, 10, 244-257.
3. 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.
4. Shi, Q., Qu, S., An, X., & Du, X. (2024). A novel coupled functional neuron model and its application in medical image encryption. *Nonlinear Dynamics*, 112(13), 11447-11470.
5. Long, B., Chen, Z., Liu, T., Wu, X., He, C., & Wang, L. (2024). A novel medical image encryption scheme based on deep learning feature encoding and decoding. *Ieee Access*.
6. Lata, K., & Cenkeramaddi, L. R. (2023). Deep learning for medical image cryptography: A comprehensive review. *Applied Sciences*, 13(14), 8295.
7. J. Doe and A. Smith, "Towards Medical Image Security: Deep Learning Applications and Challenges," *Journal of Medical Informatics*, vol. 18, no. 4, pp. 123-135, 2023.
8. Singh, K. N., Baranwal, N., Singh, O. P., & Singh, A. K. (2024). Deepenc: Deep learning-based roi selection for encryption of medical images through key generation with multimodal information fusion. *IEEE Transactions on Consumer Electronics*.
9. Hayes, J., & Danezis, G. (2017). Generating steganographic images via adversarial training. *Advances in neural information processing systems*, 30.
10. Saha, A., Pathak, C., & Saha, S. (2021). A Study of Machine Learning Techniques in Cryptography for Cybersecurity. *American Journal of Electronics & Communication*, 1(4), 22-26.
11. Quinga-Socasi, F., Zhinin-Vera, L., & Chang, O. (2020, October). A deep learning approach for symmetric-key cryptography system. In *Proceedings of the Future Technologies Conference* (pp. 539-552). Cham: Springer International Publishing.
12. Volna, E., Kotyrba, M., Kocian, V., & Janosek, M. (2012, May). Cryptography based on neural network. In *ECMS* (pp. 386-391).
13. D. -E. -M. Nisar, R. Amin, N. -U. -H. Shah, M. A. A. Ghamdi, S. H. Almotiri and M. Alruily, "Healthcare Techniques Through Deep Learning: Issues, Challenges and Opportunities," in *IEEE Access*, vol. 9, pp. 98523-98541, 2021, doi: 10.1109/ACCESS.2021.3095312.
14. Kumar, K., Tanwar, S., & Kumar, S. (2024). MANC: A masked autoencoder neural cryptography based

- encryption scheme for CT scan images. *MethodsX*, 12, 102738, <https://doi.org/10.1016/j.mex.2024.102738>
15. Kinzel, W., & Kanter, I. (2002). Neural cryptography. In *Proceedings of the 9th International Conference on Neural Information Processing, 2002. ICONIP'02.* (Vol. 3, pp. 1351-1354). IEEE.
 16. J. -W. Lee et al. (2022). Privacy-Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural Network, in *IEEE Access*, vol. 10, pp. 30039-30054, 2022, doi: 10.1109/ACCESS.2022.3159694.
 17. Lakshmi, T. N., Jyothi, S., & Kumar, M. R. (2021). Image encryption algorithms using machine learning and deep learning techniques—A Survey. In *Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough: Latest Trends in AI, Volume 2* (pp. 507-515). Cham: Springer International Publishing.
 18. Jaber, A. N., Anwar, S., Khidzir, N. Z. B., & Anbar, M. (2021). The importance of ids and ips in cloud computing environment: Intensive review and future directions. In *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020*, pp. 479-491. Springer Singapore.
 19. Kumar, K., Tanwar, S., & Kumar, S. (2024). Deep-Learning-based Cryptanalysis through Topic Modeling. *Engineering, Technology & Applied Science Research*, 14(1), 12524-12529.
 20. Gatouillat, A., Badr, Y., Massot, B., & Sejdić, E. (2018). Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine. *IEEE internet of things journal*, 5(5), 3810-3822, <https://doi.org/10.1109/JIOT.2018.2849014>.
 21. Miroshnyk, M., Pakhomov, Y., German, E., Shkil, A., Kulak, E., & Kucherenko, D. (2017, September). Design automation of testable finite state machines. In *2017 IEEE East-West Design & Test Symposium (EWDTS)* (pp. 1-6). IEEE, <https://doi.org/10.1109/EWDTS.2017.8110034>.
 22. Preishuber, M., Hütter, T., Katzenbeisser, S., & Uhl, A. (2018). Depreciating motivation and empirical security analysis of chaos-based image and video encryption. *IEEE Transactions on Information Forensics and Security*, 13(9), 2137-2150, <https://doi.org/10.1109/TIFS.2018.2812080>
 23. Mannai, O., Becheikh, R., & Rhouma, R. (2018, September). A new stream cipher based on nonlinear dynamic system. In *2018 26th European Signal Processing Conference (EUSIPCO)* (pp. 316-320). IEEE, <https://doi.org/10.23919/EUSIPCO.2018.8553276>.
 24. Tang, J., Zhang, F., & Ni, H. (2023). A novel fast image encryption scheme based on a new one-dimensional compound sine chaotic system. *The Visual Computer*, 39(10), 4955-4983, <https://doi.org/10.1007/s00371-022-02640-w>.