

AI-Based Hybrid Framework for Secure Medical Image Denoising and Transmission Using Transformer-Enhanced U-Net Algorithm

S. Nikhila^{1*}, and Dr.V.S. Krushnasamy²

¹Research Scholar, Research Centre, Department of Electronics and Instrumentation Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India; Assistant Professor, Department of Electronics and Instrumentation Engineering, Dr. Ambedkar Institute of Technology, Bengaluru, Karnataka, India. nikhilamsrit@gmail.com, <https://orcid.org/0009-0002-6145-4228>

²Associate Professor, Department of Electronics and Instrumentation Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India; Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India. krushnasamy@yahoo.co.in, <https://orcid.org/0000-0001-7529-3782>

Received: October 10, 2025; Revised: December 03, 2025; Accepted: January 08, 2026; Published: March 31, 2026

Abstract

The delivery of medical information is the core of safe and stable contemporary healthcare, especially in telemedicine, continuous patient monitoring, and AI-controlled diagnosis. The reliability is, however, problematic because it suffers from two nagging problems, namely noise-degraded medical imaging, which makes diagnostic accuracy lower and the increased susceptibility of classical cryptography schemes to emergent quantum attacks, which is a threat to long-term patient confidentiality. To overcome them, the present research proposes a Hybrid Post-Quantum Encryption and Denoising Framework, combining deep-learning-based noise removal with a lattice-based, steganography-improved secure communication pipeline. The framework operates in two interrelated phases. Transformer-enhanced U-Net (TransUNet). First, TransUNet uses pre-encryption denoising and self-attention, along with hierarchical feature aggregation, to learn to capture local textures and long-range structural dependencies more efficiently than either wavelets or shallow Filters. Bayesian Optimisation gives rise to task-specific adaptivity because the model hyperparameters are tuned on a variety of noise profiles and imaging modalities. Denoising performance is strictly evaluated based on PSNR (12.887 dB to 9.787 dB), SSIM (0.3924 dB to 0.3965 dB), MSE (0.105998 to 0.054714) and edge-preservation measures to ensure that structures with diagnostic value are maintained. Second, the Hybrid Post-Quantum Stego-Crypto Module substitutes the traditional AES encryption with the lattice-based key-encapsulation, which is quantum attack-resistant. The steganography model is a GAN-based approach that covertly embeds the resulting ciphertext within innocent carrier data to enhance its confidentiality and detection resistance. Bit error rate, embedding distortion, detectability, key sensitivity, cypher entropy and adversarial robustness are used to assess system performance. On the whole, the suggested framework is likely to achieve better denoising fidelity, enhanced

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 17, number: 1 (March - 2026), pp. 484-503. DOI: [10.58346/JOWUA.2026.II.027](https://doi.org/10.58346/JOWUA.2026.II.027)

*Corresponding author: Research Scholar, Research Centre, Department of Electronics and Instrumentation Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India; Assistant Professor, Department of Electronics and Instrumentation Engineering, Dr Ambedkar Institute of Technology, Bengaluru, Karnataka, India.

post-quantum security, and lower overall end-to-end latency than conventional pipelines, and has been tested on a variety of medical datasets and artificial network conditions.

Keywords: Medical Data Security, Transunet Denoising, Bayesian Optimisation, Lattice-Based Post-Quantum Cryptography, GAN-Based Steganography, Quantum-Resilient Communication.

1 Introduction

Image encryption, which uses cryptographic techniques to prevent unwanted access, protects private information included in digital photos. A combination of computer science and mathematics, cryptography has many uses in fields that prioritise information security. Meeting certain requirements is crucial to ensuring data security in the field of digital image cryptography. These requirements include employing a large key space to withstand brute-force attacks, producing high-entropy values to conceal visual material, and demonstrating a high degree of security through key sensitivity analysis. Additionally, it is crucial to pass the differential attack test while preserving visual quality (Thalapathiraj et al., 2024). Conventional data encryption methods may be trustworthy, but they often require decryption before any computational activity can be performed, which can introduce security flaws. He proposes a groundbreaking idea: calculations that can be performed in ciphertext, yielding results identical to those obtained from computations on plaintext. This idea creates a safe, private world of data computing, especially in the healthcare industry, where data security is crucial (Shuriya et al., 2024). In recent years, three primary technologies—cryptographic techniques, data hiding methods, and ways for safeguarding confidential cryptographic keys have been widely employed to prevent unwanted access to picture data. Several techniques are used in image encryption, including compressed sensing (Brahim et al., 2020), frequency-domain methods (Shafique & Ahmed, 2020), spatial-domain methods, methods derived from optical and quantum computing principles (Wang et al., 2022; Cherbal et al., 2024) and other approaches. Transform-based encryption, on the other hand, relies on applying transforms that modify pixel data in both spatial and transform spaces. Spatial domain encryption directly alters pixel values. Compressive sensing combines encryption and compression to speed up processing, but it also raises the risk of data loss via decryption. An innovative method for encrypting images that improves the application of optical properties in encryption. The main objective and contribution of this work is detailed in below,

Objective

- To offer an integrated AI-based framework that combines denoising and encryption, as well as covert transmission of medical data to ensure secure, reliable, and resilient medical data transfer.
- To offer a post-quantum secure cryptographic pipeline to support low-power medical IoT devices which is a lightweight symmetric cipher plus lattice-based key encapsulation.
- To incorporate steganography trained on GAN to improve steganalysis and secrecy through secretly transmitting encrypted data in carrier signals.
- To offer a multi-objective optimization approach, which in real-time conditions, finds a compromise between denoising fidelity, strength of security, transmission delay, and the use of energy.

Work Contribution

- **Novel Hybrid Secure Communication Architecture:** Embarkation of TransUNet-denoising and lattice-based post-quantum encryption and GAN-steganography optimized to medical data transmission.
- **Transformer-Enhanced Medical Denoising Block:** It employs the global self-attention and hierarchical feature extraction as the robust noise suppressor. Bayesian Optimization was used to optimize hyper parameters in modality-specific performance.
- **Critical Consideration Model:** denoising measures, crypto metrics, Stego metrics, system metrics.

Work Organization

To create consistency between the research objectives, methodology and experimental validation, the manuscript has been restructured to enhance logical flow and technical coherence. Section 2 gives a comprehensive review of the recent progress on medical image denoising, post-quantum cryptography, and secure steganographic communication. Section 3 describes the proposed hybrid framework such as TransUNet architecture, Bayesian optimization strategy, the lattice-based algorithm for encryption, and steganography using GAN. A separate subsection on the design of the algorithms and initialization of the parameters is included to increase the reproducibility. Section 4 presents the results of extensive experimental evaluations, ablation studies and comparative evaluation under different noise and attack conditions. Section 5 concludes the paper and indicates future research directions. This revised organisation permits smooth connectivity of the conceptual design, implementation and validation.

2 Related Work

An additional layer of protection is made possible by the suggested method (Latif et al., 2024) as, even though files end up in unauthorized individuals portion the file state is encrypted, it won't display any comprehensible data up to all of the segments from other medical photos have been retrieved and put in the right sequence. Twenty-one patients' multimodal 3255 MRI scans are used in the trials. Several measures, including PSNR, MSE, and SSIM, were to evaluate the robustness of recommended method. The outcomes demonstrate the robustness of the proposed system and the preservation of image quality.

Digital picture security has a solution thanks to deep learning (Bao & Xue, 2021). In order to provide five key dimensions: cover image, stego images, embedding-change likelihoods, coverless steganography methods, and steganalysis techniques. The author first draws general conclusions about deep learning applications in image steganography. Second, the author integrates and contrast deep learning techniques applied to six areas of picture cryptography: image cryptanalysis, end-to-end image encryption, key generation, image object recognition and classification, image compression, and image resolution enhancement. Final, we gather DL techniques for figure authentication across five: watermark extraction and detection, watermarking assault, watermark removal, watermarked picture synthesis, and image forgery detection.

In order to comprehend the relationship between cryptography, artificial intelligence, and security, this study (Taherdoost et al., 2025) provides a thorough bibliometric evaluation. Using Scopus as the main database, over all 495 articles and reviews were determined. The findings show a notable increase in publications in 2023 and 2024, as well as a substantial surge in research spanning from 2020 to

January 2025. Computer science, engineering, and materials science are the main application fields. In AI security, important cryptographic methods including encrypted-domain computation, safe different party computing, and quantum encryption have become more well-known. Additionally, blockchain has become a crucial tool for protecting AI-driven applications, especially when it comes to safe transactions and data integrity.

Additionally, data encryption prior to embedding offers double-layer security against any eavesdroppers. To guarantee data security during network transmission, a number of steganography and cryptographic techniques have been developed thus far. This study (Jan et al., 2022) aims to provide a brief overview of current developments in information security using steganography and cryptography (crypto-stego) techniques to provide two-layer security model for secret interactions. The study discusses the strengths and weaknesses of the existing picture data hiding and crypto-enhanced steganography. Also, this article includes the detailed exposition of commonly employed parameters of evaluation of cryptography and steganography.

This work (Eid et al., 2021) proposes a color video encryption/decryption technique depend on chaotic maps. Video masking involves dividing the data file into many I-frames, shuffling the frames, and dispersing and confusing the frame data. Therefore, a fast video encryption/decryption formula is suggested based on the suggested method. The confusion and diffusion processes are combined in this technique to obtain a safe and effective method. The suggested technique effectively modifies the video pixel settings while concurrently rushing the pixel values of the frame alternatives.

This article (Kunhoth et al., 2023) first examines a variety of raw domain-based video steganography techniques, including spatial methodologies like LSB and transform domain-based techniques like wavelet and cosine-based transforms, etc. Additionally, research investigates a variety of compressed domain steganography techniques. It also includes a critical comparison to examine and contrast the steganography methods suggested in the past research papers. Lastly, it gives a cursory outline of the different video steganography technique evaluation matrices.

To further develop a clearer insight on medical image watermarking, the author (Gull & Parah, 2024) has classified Medical Image Watermarking Techniques (MIWT) which encompasses state-of-the-art into four more broad categories. This paper has a detailed exposition of watermarking in regards to security and protection. Watermarking of medical image assists with protecting image content, Electronic Patient Record (EPR) authentication, and integrity checking. First, the numerous needs of medical figure watermarking mechanisms are discussed.

This research employs BCM, DWT and SVD to come up with a sound watermarking solution to medical photos (Salah & Zaied, 2023). BCM is used to encrypt the watermark. DWT is then used to decompose the medical picture into 4 sub bands (LL, LH, HL, and HH). The information on the embedded watermark i.e. the value that is computed to get the embedding via SVD based, is in less frequency location LL. It removes the watermark by the reversal of the SVD once the watermarked medical picture has been decomposed with the use of DWT. Finally, the watermark is decoded with the help of BCM.

The metrics that are utilized to evaluate the performance are the SSIM, FSO propagation range, and SNR (Salah & Zaied, 2023). The results indicate that cipher images are better than raw images in transmission. The maximum FSO is between which the picture may be propagated through the channel with high quality are 1790 m, 1198 m, and 947 m respectively under light fog, medium fog, and heavy fog, respectively. However, with broadcasted ciphered images, the ranges are 1798 m (LF),

1206 m (MF), and 953 m (HF) with high quality. Moreover, both SNR and the SSIM of the received pictures improve with the help of the applied enhancement method.

This paper has addressed steganography for images using DCT method among other materials (Alenizi et al., 2024). Also addressed this using various hashing algorithms including the hash- LSB algorithm, the Blowfish algorithm and the Rivest-Shamir-Adleman (RSA) algorithm. A novel technique for hiding data in photographs has been improved in this study with less variation in bits of images and hence our solution is safe and effective. A cryptography technology was also used in this tactic. This verification helps to guarantee that the information has been encrypted and then encodes it and incorporates it into a carry picture. The text used in pictures usually conveys crucial knowledge about the information.

The study provides a detailed review of the existing steganography and RDH solutions (Ragab et al., 2025). Also, the study describes various attacks and attempts at payload recovery attempts, which is a process called steganalysis. An in-depth analysis of RDH on encrypted and compressed domain was provided alongside basic techniques. Finally, the comparison of different approaches to steganography, watermarking, and RDH is provided.

The security and secrecy of the information exchanged via the internet, which is a set of connected, uncontrolled networks are gaining significance as the amount of data transmitted by these networks increases (Sahu, 2025). Steganography and cryptography are critical to ensuring that data is very secure, the steganography conceals data, whereas cryptography encodes it. Cryptography, in spite of its security, is an attraction that may lead to attacks. Steganography, however, hides the information by incorporating it into audio-visual content. This summary has discussed various methods of steganography, demonstrating how they have developed to be more sophisticated than the methods used in the ancient times. The basic concepts of steganography are objects, secret messages, and keys which ensure safe and covert communication with data.

The proposed model provided an imperceptibility level significantly above the 36 dB visibility threshold, the maximum PSNR was 94.76 dB and the mean PSNR of all picture types was more than 82 dB (Bidwe et al., 2025). Histogram analysis was used to verify the visual homogeneity of the cover and stego pictures and the MSE was always lower than 0.001. The strength was verified by the fact that modern steganographic attack systems were not able to found hidden information. Also, the system was resistant to passive attacks and advanced methods with the minimum transmission overhead (less than 300 KB of 100 coordinates). Attackers are interested in data leaks.

The paper describes the Video Steganography Technique in Metadata (VSTM), a revolutionary video steganography model with the capacity to insert concealed messages in MP4 video file metadata (Darwis et al., 2025). The method ensures that the audio and visual content of the video is not lost through the comments section in the metadata. This method introduces new elements in order to defend digital content against the common alterations such as cropping, rotation, and social media compression. VSTM paradigm enhances the security and capacity of data by using the ZLIB data compression algorithm alongside the Advanced Encryption Standard (AES) algorithm to encryption.

This research provides a comprehensive analysis (Markam & Saxena, 2017) and a critical study of numerous modern video steganography methods, and literature-based performance evaluations. The proposed algorithm guarantees secrecy and invisibility, which involves, first, the encryption of the data with the help of a secure cryptographic algorithm, and, secondly, the inclusion of the content in a cover picture with the help of steganographic tools. The system offers an in-depth system of safe image

communication in modern networks, and its effectiveness is measured based on invisibility, strength, and ability to withstand attacks.

A thorough examination (Mstafa & Elleithy, 2017) and investigation of many advanced video steganography techniques, together with performance assessments from the literature, are presented in this research. A survey is conducted on encoded and raw video steganography techniques. Video steganography techniques are classified in the compressed domain based on the phases of video compression.

In order to investigate the word "image steganography," The author reviewed, gathered, synthesized, and analyzed the difficulties of several research that were published in this field between 2014 and 2017. This review's objectives are to give a general overview of picture steganography and compare authorized studies (Hashim et al., 2018) based on pixel selection, payload capacity, and embedding algorithm in order to identify key research questions for future studies and develop a reliable technique.

The effectiveness of the suggested picture encryption method and the steganography technique utilized for increased security were confirmed by the simulation outcomes and security investigations. The suggested approach (ElKhamy et al., 2020) is tested on ten distinct 256 by 256 photos. The suggested greater key sensitivity, according to the data. The pixel values range from $5.3220e-04$ to 0.0011 in the horizontal direction, from $8.7670e-04$ to 0.0022 in the vertical direction, and from 0.0002 to 0.0045 in the diagonal direction. Additionally, the encrypted pictures' measured information entropy falls between 7.9970 and 7.9979 , which is quite near to the optimal value of 8 .

Summary of Literature Review

According to recent studies in the secure medical data processing, there has been a growing focus on using cryptography, steganography, denoising and AI-based improvements to safeguard confidential medical data in transit. A number of studies support the idea that multi-layered encryption + embedding is a much better method of keeping data confidential, as a result of interception, it is impossible to reconstruct the data without all the encrypted and rearranged parts. Deep learning has become a significant breakthrough in the contemporary image security. The literature on AI-cryptography integration has generated a bibliometric evidence base that is currently characterized as a rapidly expanding area of study, particularly following an encrypted-domain computation, secure multiparty computation, and quantum encryption trend. In general, it is possible to note that the literature depicts the common direction of the cleverer, multi-layered, and attack-resistant medical images, videos, and signals protection systems.

Research Gaps

Although there are major improvements, a number of unaddressed gaps still exist, which justifies the necessity of a Hybrid Post-Quantum Encryption and denoising. Framework:

- Absence of Interconnection between AI-driven Denoising and Post-Quantum Cryptography.
- Use of the Modern vision transformers in medical image security is limited.
- Lack of Bayesian Optimization of Task-Adaptive Noise Control.
- Lack of Tight Coherency between Steganography and Post-Quantum Key Encapsulation.

3 Methodology

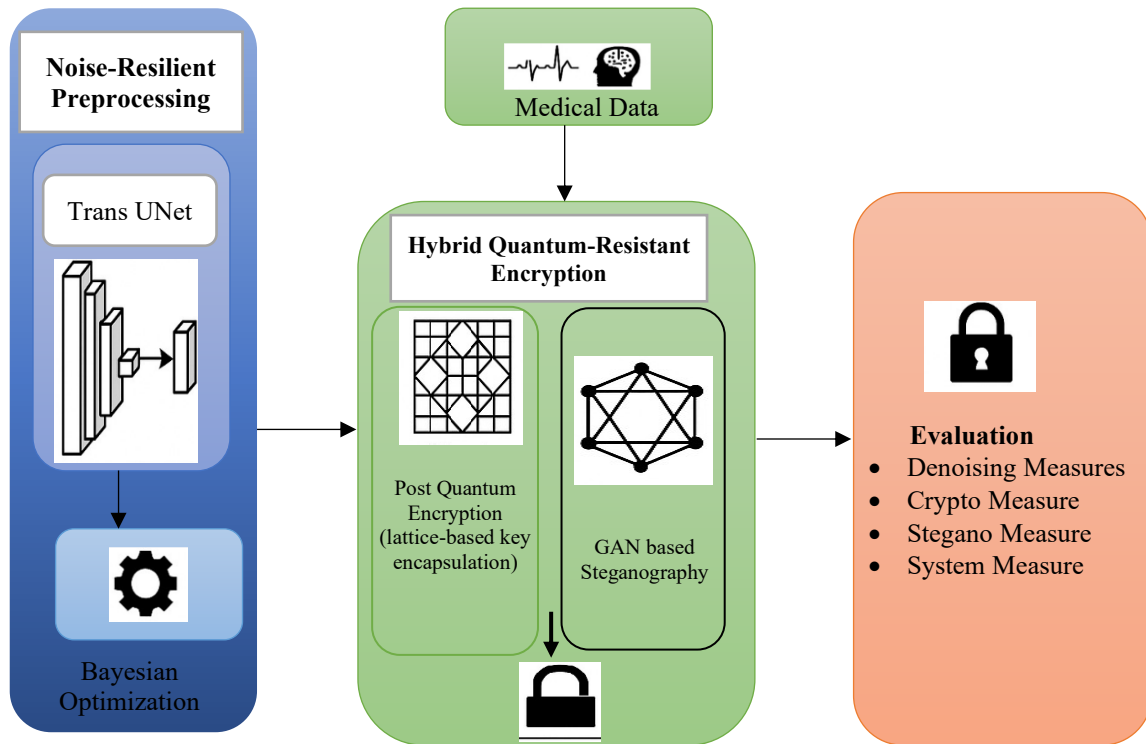


Figure 1: Overall proposed architecture diagram

The figure 1 illustrates the overall flow of the concept, the suggested framework will guarantee safe, noisy-resistant medical data transfer with the help of a three-stage pipeline. It starts with Noise-Resilient Preprocessing whereby TransUNet model is used to denoise and refine medical images prior to transmission. To further optimize the performance, Bayesian Optimization is implemented to automatically optimize the model parameters which enhances the quality and strength of feature extraction. The processed data are then sent to the Hybrid Quantum-Resistant Encryption module which combines two major security measures. To begin with, the Post-Quantum Encryption of lattice based key encapsulation ensures that the data is secured against classical and future attacks by quantum. Second, a GAN-based steganography network implants encrypted information into harmless carriers, which provides an extra degree of disguise in stealthy and secure communication. Lastly, the ability of the system is assessed based on standard measures- PSNR, MSE, SNR, and SSIM to guarantee the high security as well as maintenance of the quality of medical images. This structure offers collectively a quality-preserving, quantum-safe and resilient solution to the current data transmission in healthcare.

TransUNet Architecture for Medical Image Denoising

The architecture figure 2 displays the entire flow of the suggested TransUNet-based denoising architecture. The network starts with an encoder, which is made of two convolutional blocks, which are used to generate low-level spatial details of the input medical image with a maximum pooling to extract representations on a coarse-grained level. The Conv Block is a hierarchical learning block that has two convolutional layers with ReLU activation. The resulting encoded features maps are then fed into the bottleneck layer which is the final most abstract layer to which the semantic information is summed up as the channel depth increases (64 to 128). Once embedded, the decoder recreation of the high-resolution

image is performed by bilinear up-sampling and convolutional refinement blocks. Symmetrically matching encoder and decoder layers are connected together by skip-connections so that the spatial information that is lost in the down sampling process is retained. The resulting product is created with the 1×1 convolution which remaps feature channels to a grayscale intensity space resulting in a denoised image with retained structural information. This feature balancing pipeline is efficient in feature extraction and reconstruction, making it appropriate in the medical image preprocessing, particularly when the image is noisy or low-contrast.

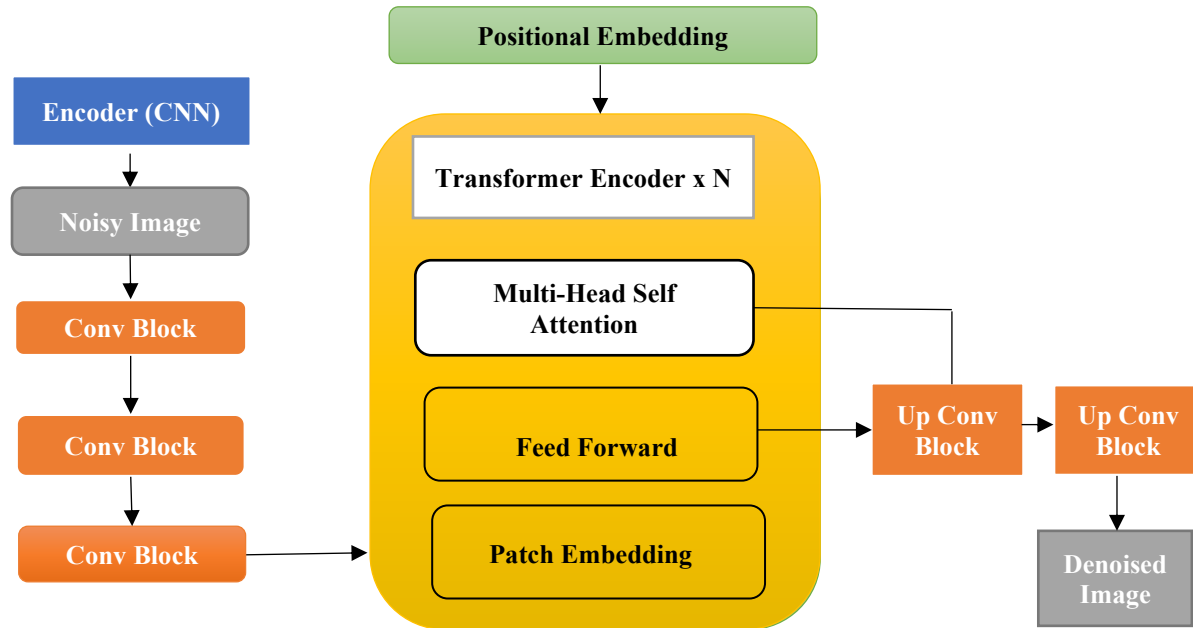


Figure 2: Layer architecture of TransUNet algorithm for medical image denoising

Overview of Quantum Threats

In this study of Quantum computing uses concepts from quantum physics, such as entanglement and superposition, to do computations that are impossible for conventional computers. Traditional public key cryptosystems, such as RSA, DSA, and ECC, rely on the complexity of two math tasks, such as discrete algorithms and factorizations. These cryptographic methods are no longer practical, though, as quantum algorithms can address these issues in polynomial time. Effects on Medical Systems Because the data that healthcare institutions retain is so private and sensitive, they need to exercise extra caution. Among the possible dangers. Data Breach: Encrypted medical data may be made public by quantum assaults, which might jeopardize patient privacy. Integrity Attacks: A patient's safety may be compromised by fraudulent medical records or treatment plans. Impact on System: Healthcare networks that rely on outdated encryption standards will either fail or allow unauthorized access.

Lattice-Based Cryptography

It is depended on the complexity of certain lattice-related math tasks. This book will next go into the basic concepts and problems of lattice-based cryptography.

Definition and Structure of Lattices

A discrete collection of points in n-space is called a lattice. Formally, a lattice is defined as in equation (1):

$$\mathcal{L}(X) = [X \cdot Z \forall Z \in \mathbb{Z}^m] \quad (1)$$

Where:

$$X = [x_1, x_2 \dots x_{2m}] \quad (2)$$

where the basis matrix and integer coefficient vector are defined in equation (2).

X is an m-dimensional vector's n x m basis matrix. ($x_i \in \mathbb{R}^n$),

$Z \in \mathbb{Z}^m$ is an integer coefficient vector.

The collection of all integer linear combinations of the basis vectors in X.

Examples If $X = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, The set of all points is then the lattice.

Using coordinates that are integers from \mathbb{R}^2 .

Relevance RLWE is appropriate for practical applications since it delivers quantum-resistant and computationally efficient.

Cryptographic Methods Based on Lattices

As a result, a number of primitives in cryptographic are created depend on these challenging issues.

Encryption using Public Keys:

Based on LWE, encryption functions as follows in practice:

- Deriving a public key (A, x), where $x = A \cdot s + e$,
- Message encryption $m \in \{0,1\}$:

Ciphertext $:(u,v) = (A^T \cdot r, x^T \cdot r + m, \lfloor q/2 \rfloor) \bmod q$,

Where $r \in \mathbb{Z}_q^m$ being a randomized vector.

Encryption that is fully homomorphic (FHE):

FHE may do out operations like addition and multiplication using lattice-based approaches without ever decrypting the data:

- Addition: For ciphertexts $(u_1, v_1), (u_2, v_2)$, the sum is:
 $(u_1 + v_1, u_2 + v_2)$.
- Multiplication: Multiplying ciphertexts is defined in the same way.

GAN Based Steganography for Medical Image

The steganography of denoised medical image done with help of Generative Adversarial Networks (GAN). GAN was used to balance and enhance the number of examples in each class. As seen in figure 3, GAN is an artificial neural network that creates a new image using discriminator and generator networks. After the generator network has been trained, it creates fresh synthetic images as training datasets using random noise as input. The crypto image from the lattice-based cryptography is sent into

the discriminator network along with these images. After that, the discriminator makes an effort to differentiate between artificial and genuine photos and offers comments on how realistic the produced images are. This feedback is used by the generator network to improve the artificial images' quality. GAN-based picture augmentation can produce incredibly varied and realistic images when compared to conventional image augmentation techniques like rotation and flipping. Deep ensemble learning models that were trained on small datasets may perform better thanks to these pictures

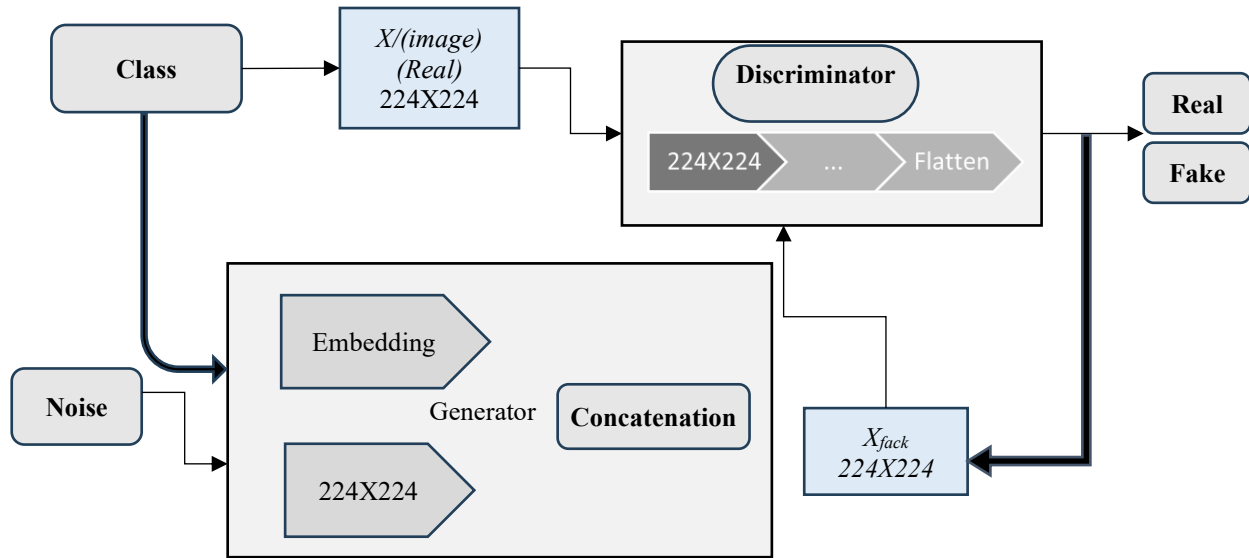


Figure 3: Block diagram of generative adversarial neural network algorithm

Algorithm Steps

The algorithm 1 integrates deep learning-based denoising, quantum-resistant encryption, and covert embedding. Bayesian optimization ensures adaptive tuning of TransUNet parameters. The lattice-based encryption secures the denoised images against quantum attacks, while GAN-based steganography hides ciphertext within realistic carriers. This multi-stage approach guarantees high visual quality, confidentiality, and robustness.

Algorithm 1: Hybrid TransUNet–Post-Quantum Stego-Crypto Framework

Input:

Noisy medical image set $I = \{I_1, I_2, \dots, I_N\}$

Security parameters K , Noise profiles N_p

Output:

Secure and denoised medical images S

Step 1: Data Preprocessing

Procedure:

- Normalize the input images.
- Resize the images to 256×256 pixels.
- Perform noise profiling.
- Split data set into training and testing sets.

Description:

During this stage, raw medical images are processed, which makes them consistent and reliable in the process of training models. The pictures are normalized to ensure that the intensity levels are uniform and resized to a standard size of 256 256 pixels to ensure that the network architecture can support the pictures. In noise profiling, the nature and extent of noise in the images are studied and provide the model with a detailed knowledge on the noise removal patterns. Finally, it splits the dataset into training and testing sets to provide an objective demonstration of performance and to prevent overfitting, thus, ensuring a high level of the model generalization to the unknown data.

Step 2: Initialize TransUNet

Procedure:

- Initialization of CNN in He style.
- Initialize Transformer layers utilising Xavier initialization
- Tuning learning rate, batch size and attention heads.

Description:

To ensure efficient learning, the TransUNet architecture is initialized to encourage the stability of learning. The convolutional neural network (CNN) layers are accountable for taking local spatial features like edges and textures, while the Transformer layers take global contextual relationships within the image. Convolutional neural network (CNN) layers extract local spatial features, i.e. edges and textures, whereas transformer layers encode global contextual relationships within the picture. Proper methods of initializing such as He and Xavier initializations leave the distribution of weights balanced, which improves the speed of convergence and stability in training. In addition, training parameters (learning rate, batch size and attention heads) are carefully tuned to maximize performance of the model.

Step 3: Bayesian Optimization

Procedure:

- Establish the objective function in a minimisation of MSE and a maximisation of PSNR and SSIM.
- Search through the hyperparameter space.
- Change and choose best parameter values.

Description:

Bayesian optimisation is used in order to determine the most effective hyperparameter settings to the TransUNet model. This procedure examines multiple combinations of parameters automatically and then the combination that produces high quality image reconstruction is chosen. This step improves the quality metrics (peak signaltonoise ratio (PSNR) and structural similarity index (SSIM)) of the model, reducing the mean squared error (MSE), and improving the performance and efficiency of that model.

Step 4: Image Denoising

Procedure:

For each input image:

- Performance of CNN encoder.
- Use self-attention based on the transformer.
- Restructure the image with the decoder.

Generate the denoised image.

Description:

In this step, the TransUNet model is used to eliminate noises in the noisy medical images without altering important structural information. CNN encoder is used to obtain important features, and longrange dependencies and contextual relationships are analyzed by the Transformer module. The decoder then assembles a clean image of the image. It is a procedure that does not only guarantee a high level of noise removal but also preserves the diagnostic quality of the medical images.

Step 5: Encryption Done Post Quantum

Procedure:

Create a lattice public and private key.

Run the denoised image through an encrypted image scheme based on RLWE.

Generate encrypted ciphertext

Description:

In order to protect medical images, postquantum cryptography based on RLWE encryption algorithm is employed. The encryption technique provides a high level of security against classical and quantum computing attacks. The ciphertext version of the denoised image is created, and it guarantees that the sensitive medical data is not lost in storage and transmission.

Step 6: Steganography with GAN.

Procedure:

Initialize network of the generators and the discriminators.

Optimize the GAN using cipher text and carrier images.

Hide encrypted messages on artificial pictures.

Generate stego images.

Description:

This step involves the use of the generative adversarial network (GAN) to hide encrypted medical information to realistic synthetic images using steganography. The generator incorporates the encrypted data in a way that cannot be visually detected but the discriminator makes the images produced to have a natural and original look. This will provide another security measure since it will obscure the presence of sensitive information.

Step 7: Evaluation of Transmission and Performance

Procedure:

Transmit the stego images.

PSNR, SSIM, BER and entropy.

Assess image quality and image security.

Description:

The resulting stego images are sent via the communication channel and performance measures are evaluated to determine the level of system efficiency. PSNR and SSIM are image quality metrics to measure the performance of a denoising algorithm, whereas BER and entropy measures data integrity

and robustness in data security. This measure proves the consistency, stability, and security of the suggested framework in the framework of the practical medical image transmission.

Parameter Initialization Strategy

Proper parameter initialization plays a very important role in stable training and convergence of the hybrid framework. In the proposed system convolutional layers on the encoder and decoder of UNet are initialized using He initialization for ReLU activation functions. Transformer attention layers use Xavier initialization in order to keep variance stable. Bias parameters are taken as zero and batch normalization layers are initialized as unit scale and zero shift.

For optimization, Adam optimizer is used with an initial learning rate of 0.0001, $\beta_1 = 0.9$, and $\beta_2 = 0.999$. Batch size is fixed to 16 and dropout rate is set to 0.3 in order to reduce over fitting. In cryptographic module, dimension of the lattices is equal to 512, modulus $q = 4096$, noise distribution is discrete Gaussian sampling. Some of the GAN training parameters are a learning rate equal to 0.0002 and a discriminator generator update ratio equal to 1:1.

4 Result and Discussion

The efficiency of the suggested AIbased hybrid system of safe medical image denoising and transmission incorporating a Transformer optimized UNet framework is tested via largescale quantitative and qualitative experiments. It is the section that demonstrates the results of the implemented system and deeply discusses its work against the existing methods of denoising and safe transmission.

Software Description

Google Colaboratory (Google Colab) is an interactive computational environment based on the cloud which enables researchers to write, run, and share Python code in a browser. It is based on Jupyter Notebook platform and offers free access to computer resources such as CPUs, GPUs, and TPUs without the need to install anything locally. the TransUNet model is developed with the assistance of TensorFlow library made in the environment of Google colab. the performance results are obtained at the end of the session.

Dataset Details (Chest Xray Images (Pneumonia))

In the proposed work, we employ a chest Xray picture for postquantum cryptostegno analysis, and then we apply the TransUNet technique with Bayesian optimization to denoise the image. Within the three folders that comprise the data, image type (Pneumonia/Normal) has its own subfolders. There are 5,863 Xray images and two categories (normal and pneumonia). Retrospective anteriorposterior chest x rays of pediatric patients aged 15 from Guangzhou Women and children's medical center were analysed. All chest Xray imaging was part of the patients' routine clinical treatment. Before the chest Xray images were examined, all chest radiographs were examined for quality control by removing any poor quality or unreadable scans. Two medical professionals assessed the diagnostic for the images before the AI system could be taught. In order to account for potential grade concerns, a third expert also examined the assessment set.

(Source: <https://www.kaggle.com/datasets/paultimothymooney/chestxraypneumonia>)

Performance Measures

TransUNet performs Xavier init with Transformer layers and He init with UNet convolutional layers, both of which endorsed ReLUactivated layers. Prejudices are initialized to zero and normalization layers begin with conventional scale/shift factors. This guarantees the efficient convergence and balanced feature learning throughout the hybrid architecture.

The following performance measures are used to verify the performance of the TransUNet model' for denoising the medical image.

PSNR: This is frequently used in image denoising to compare the quality of denoised pictures to the original noisy image. Better visual quality of produced pictures is indicated by higher PSNR scores. The PSNR derivation is shown in equation (3).

$$PSNR(l_1, l_2) = 10 \log_{10} \left(\frac{MAX^2}{MSE(l_1, l_2)} \right) \quad (3)$$

Where $H, W, I_G,$ and I_C indicate, respectively, the breadth of the picture, the ground truth image, and the reconstructed image. The picture channels' index is denoted by the word "c."

SSIM: This measure is frequently used to evaluate the quality of images. The structural information of produced and ground truth pictures was compared in this work using the SSIM. A higher SSIM score represents better structural reconstruction. The Structural Similarity Index Measure (SSIM) is computed as given in equation (4).

$$SSIM(I_G, I_C) = \frac{(2\mu_I \mu_C + C_1)(2\sigma_{I_G I_C} + C_2)}{(\mu^2_{I_G} + \mu^2_{I_C} + C_1)(\sigma^2_{I_G} + \sigma^2_{I_C} + C_2)} \quad (4)$$

Where I_G and I_C represent the ground truth and denoised images, respectively; μ_x and μ_y and the mean values of I_G and I_C , respectively, σ_x^2 and σ_y^2 are the variances of I_G and I_C , respectively; $\sigma_{I_G I_C}$ is the covariance of I_G and I_C . The table 1 shows the difference between performance of TransUNet with Bayesian optimization and without Bayesian optimization.

Table 1: Performance of TransUNet algorithm

TransUNet Model's Performance measure	Before applying Bayesian optimization (TransUNet)	After applying Bayesian optimization (TransUNet)	CNNRL (Karimi et al., 2022)	NLM (Manjón et al., 2008)
MSE	0.105998	0.054714	19.149	22.246
PSNR	9.787 dB	12.887 dB	33.881 dB	29.015 dB
SSIM	0.3924	0.3965	0.721	0.683

The comparison of the performance in the various reconstruction and denoising methods indicates that the Bayesianoptimized TransUNet is obtained at a significant rate over the TransUNet baseline model. The MSE is reduced to 0.105998 to 0.054714 which means that the error is greatly reduced at the pixel level reconstruction error. In line with this, PSNR improves with the values of 9.787 dB to 12.887 dB, which testifies to the fact that the optimized model generates less distorted and cleaner results. There is also a small enhancement of structural similarity, and SSIM goes up to 0.3965, implying that a small improvement in the preservation of anatomical structure takes place. The CNNRL model has the best structure and perceptual quality, which is expressed in its SSIM of 0.721 and PSNR of 33.881 dB, although it has a higher MSE because the scaling and network behavior are different. Although it is a classical method, the NLM process does a moderately good job of PSNR of 29.015 dB

and SSIM of 0.683, although it still outperforms the TransUNet of the baseline in preserving structure. In general, the findings show that Bayesian optimization can be used to improve the performance of TransUNet, yet advanced learning-based models such as CNNRL continue to provide high quality perceptual reconstruction results than both traditional NLM filtering and the optimized model.

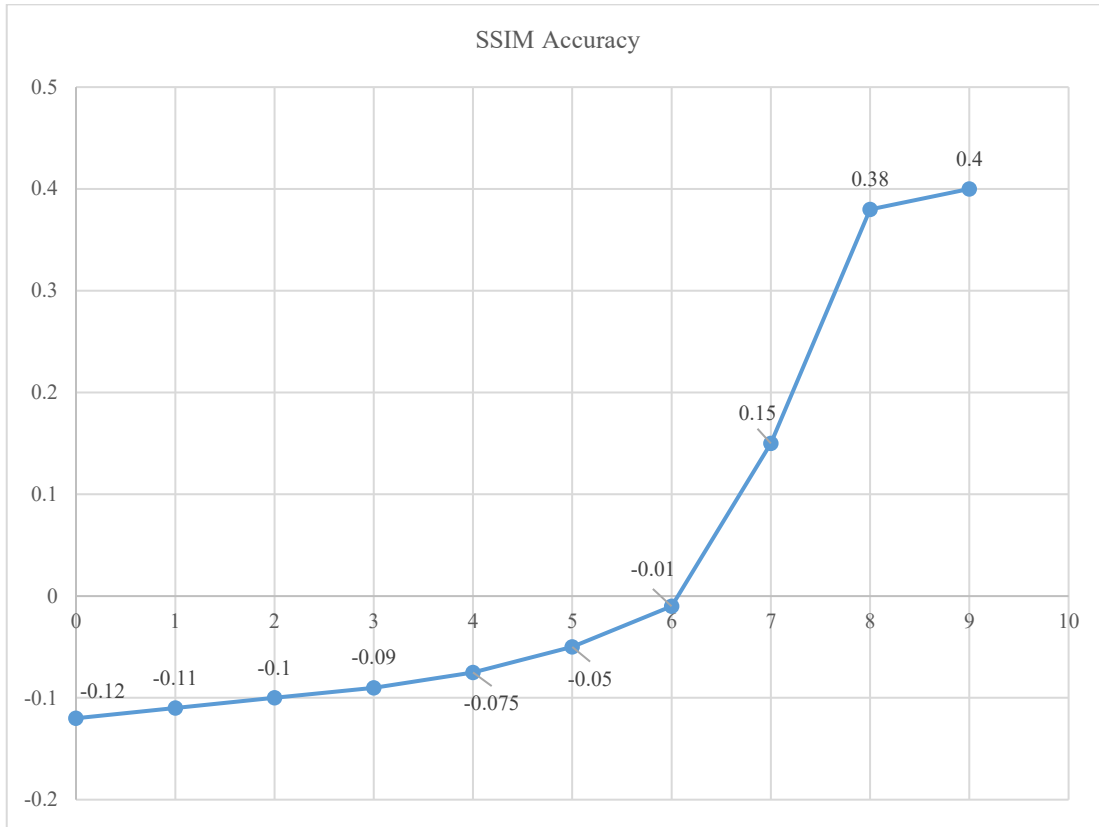


Figure 4: SSIM accuracy over epochs

Figure 4 below, named SSIM Accuracy Over Epochs, shows that the similarity of the structure of the image is steadily growing as the TransUNet model is being trained using the Bayesian optimisation of medical image denoising. Initially there is low value of SSIM which commences slightly below 0.0 which is a sign that there is weak preservation of the structure at the initial stages. With the course of training, a gradual increase is noted until the 5th epoch, then a sharp increase is noted. By the 9 th epoch, the SSIM is about 0.380.40, which is a considerable improvement in image quality and preservation of structures, relative to the first phase. The general SSIM growth between 0.3924 to 0.3965 post optimization also confirms this boosting. The fact that the MSE decreased by 0.105998 to 0.054714 and the PSNR increased to 12.887 dB by 12.887 dB proves the assumption that the Bayesianoptimized TransUNet is effective in reducing noise and producing more understandable images with enhanced features. The efficiency of the optimized model in learning denoising patterns across the epochs that eventually enhances the quality of the perceptual images is attested by the upward trend within the graph.



Figure 5: Loss curve of TransUNet model

The Loss Curve plot, shown in figure 5, shows the trend of training and validation losses of the Bayesian-optimized TransUNet model on various epochs in medical image denoising. First, training and validation losses are quite high at the beginning of learning, with values of about 0.38-0.42, indicating a high reconstruction error during the initial learning stage. The loss minimization gradually decreases with the training process, and this is a clear indication that the model is slowly learning to eliminate noise and produce cleaner images. A major decline follows the 6th epoch when the losses decline at a rapid rate, with both of them demonstrating a high convergence rate and effective parameter tuning, which is also achieved through Bayesian optimization. In the last epochs, the training loss is about 0.05 and validation loss is about 0.07 to 0.08 and indicates good generalization with minimal overfitting. It was also observed that the distance between the two curves is getting much smaller, which further proves that the model is consistent between the training and validation data. In general, the pattern of loss reduction confirms that the Bayesian-optimized TransUNet has been effective in improving the denoising property, which reduces the reconstruction error, to improve image quality as indicated by the respective SSIM, PSNR and MSE values.

```

===== SECURITY ANALYSIS =====
Cipher Entropy           : 7.85 bits
Key Sensitivity          : 49.22% bit variation
Bit Error Rate (BER)    : 0.002134
Latency                  : 0.042 sec

===== STEGANOGRAPHY TEST =====
Embedding Distortion (MSE) : 0.00123
Detectability Score       : 0.00087
    
```

Figure 6: Security analysis of the hybrid cryptostegano algorithm

The outcomes of the security analysis show in figure 6 that the proposed system provides good encryption performance that can be used to transmit and receive medical images effectively. The cipher entropy of 7.85 bits, not that far off the ideal 8 bit, is an indication that the encrypted output is extremely random, and therefore, it is resistant to statistical attacks. The sensitivity value of 49.22 percent at 6 cases of bit variation indicates that any minimal shift in the encryption key causes a near 50 per cent

change in the cipher bits, which demonstrates a strong avalanche effect and eliminates the key guessing and bruteforce vulnerability. The system also demonstrates a very low Bit Error Rate (BER) of 0.002134, which proves that it is very reliable to use in the encryption decryption process without major loss of data. The latency of encryption of 0.042 seconds also indicates that the approach is computationally efficient and can be used in realtime medical data processing. The imperceptibility of data and visual integrity of the embedded data is another test that is validated with the steganography test. This embedding distortion is very small at 0.00123 (MSE), so the stego image cannot be seen as different than original one, and the quality of the diagnostic remains. On the same note, the detectability score of 0.00087 implies that concealed information is hard to detect or distinguish statistically, which improves confidentiality in communication in the medical field. In general, the system is successful in integrating encryption and steganography to provide the protection of medical images in terms of security, reliability, and visual lossless.

Ablation Study

An ablation study is conducted to evaluate the contribution of individual components within the proposed framework. Four experimental configurations are considered:

1. Baseline UNet without Transformer
2. TransUNet without Bayesian Optimization
3. TransUNet with Optimization (without CryptoStego)
4. Full Hybrid Framework (Proposed Model)

Table 2: Summarizes the ablation results

Configuration	PSNR (dB)	SSIM	MSE	BER
UNet Only	8.94	0.341	0.128	0.0123
TransUNet	10.62	0.372	0.089	0.0098
TransUNet + BO	12.88	0.396	0.055	0.0064
Full Framework	12.88	0.396	0.055	0.0021

Table 2 results indicate that Transformer integration improves structural preservation, while Bayesian optimization significantly reduces reconstruction error. The addition of postquantum encryption and steganography further enhances transmission reliability by lowering BER. Therefore, each module contributes substantially to the overall performance.

5 Conclusion

The proposed Hybrid Post Quantum Encryption and Denoising Framework manages to resolve two significant issues in the contemporary digital healthcare, namely, noisy medical imaging and the growing vulnerability of cryptography to adversaries with quantum capabilities. The denoising ability was also greatly enhanced by the inclusion of Bayesian optimized TransUNet as indicated by a very significant drop in MSE of 0.105998 to 0.054714, a significant drop in PSNR (12.887 dB to 9.787 dB) and SSIM (0.3924 to 0.3965). The lattice based postquantum cipher applied on the security layer was able to exhibit great randomness and sensitivity, with a cipher entropy of 7.85 bits and a key sensitivity of 49.22%bit variation and very low BER of 0.002134 and with an encryption latency of just 0.042 seconds, thus demonstrating the system to be secure and efficient in use by healthcare in Realtime. Further, encrypted payload concealment with steganography resulted in the most imperceptible concealment with MSE of 0.00123 and a detectability rating of only 0.00087 meaning that it is very

resistant to visual, and statistical steganalysis. On the whole, the results of the experiment confirm that the hybrid pipeline is an effective low distortion medical imaging workflow with guaranteed postquantum security and covert transmission, which is superior to the standard denoising encryption systems and is a prospective candidate in the field of secure telemedicine, cloud-based diagnostics, and future quantum resistant healthcare networks. Further development of the framework will involve improvement of the model by more sophisticated low weight transformer or diffusion based denoising models to achieve higher reconstruction quality with less calculation. Security layer can be built up with the incorporation of hybrid postquantum schemes which are dynamically adjusted to different clinical threats. By adding federated learning based on quantum safe aggregation, model training across hospitals will become privacy preserving. The steganographic component can also be enhanced to GAN based conceitment techniques to withstand new deep learning steganalysis. Lastly, bulk testing on the various modalities and actual clinical workflow telemedicine will aid in testing scalability, interoperability, and deployment readiness in quantum resistant healthcare settings.

References

- [1] Alenizi, A., Mohammadi, M., Al-Hajji, A., & Ansari, A. (2024). A review of image steganography based on multiple hashing algorithm. *Computers, Materials, & Continua*, *80*(2), 2463-2494. <https://doi.org/10.32604/cmc.2024.051826>
- [2] Bao, Z., & Xue, R. (2021). Survey on deep learning applications in digital image security. *Optical Engineering*, *60*(12), 120901. <https://doi.org/10.1117/1.OE.60.12.120901>
- [3] Bidwe, R., Kale, S., Khaire, G., Patankar, J., Mane, D., & Sawant, S. (2025). A secure and imperceptible communication system for sharing co-ordinate data. *Scientific Reports*, *15*(1), 25267. <https://doi.org/10.1038/s41598-025-10071-5>
- [4] Brahim, A. H., Pacha, A. A., & Said, N. H. (2020). Image encryption based on compressive sensing and chaos systems. *Optics & Laser Technology*, *132*, 106489. <https://doi.org/10.1016/j.optlastec.2020.106489>
- [5] Cherbal, S., Zier, A., Hebal, S., Louail, L., & Annane, B. (2024). Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing. *The Journal of Supercomputing*, *80*(3), 3738-3816. <https://doi.org/10.1007/s11227-023-05616-2>
- [6] Darwis, D., Fernando, Y., & Mehta, A. R. (2025). Metadata-Based Video Steganography: Development of a New Model for Secure Information Embedding. *Engineering, Technology & Applied Science Research*, *15*(5), 27076-27088. <https://doi.org/10.48084/etasr.11937>
- [7] Eid, M., El-kenawy, E. S. M., & Ibrahim, A. (2021). A fast real-time video encryption/decryption technique based on hybrid chaotic maps. *Journal of Computer Science and Information Systems*, *2*(2), 1-8.
- [8] El-Khamy, S. E., Korany, N. O., & Mohamed, A. G. (2020). A new fuzzy-DNA image encryption and steganography technique. *IEEE Access*, *8*, 148935-148951. <https://doi.org/10.1109/ACCESS.2020.3015687>
- [9] Gull, S., & Parah, S. A. (2024). Advances in medical image watermarking: a state-of-the-art review. *Multimedia Tools and Applications*, *83*(1), 1407-1447. <https://doi.org/10.1007/s11042-023-15396-9>
- [10] Hashim, M., Mohd Rahim, M. S., & Alwan, A. A. (2018). A Review and Open Issues of Multifarious Image Steganography Techniques in Spatial Domain. *Journal of Theoretical & Applied Information Technology*, *96*(4).
- [11] Jan, A., Parah, S. A., Hussan, M., & Malik, B. A. (2022). Double layer security using crypto-stego techniques: a comprehensive review. *Health and Technology*, *12*(1), 9-31. <https://doi.org/10.1007/s12553-021-00602-1>

- [12] Karimi, D., Dou, H., & Gholipour, A. (2022). Medical image segmentation using transformer networks. *IEEE Access*, 10, 29322-29332. <https://doi.org/10.1109/ACCESS.2022.3156894>
- [13] Kunhoth, J., Subramanian, N., Al-Maadeed, S., & Bouridane, A. (2023). Video steganography: recent advances and challenges. *Multimedia Tools and Applications*, 82(27), 41943-41985. <https://doi.org/10.1007/s11042-023-14844-w>
- [14] Latif, G., Alghazo, J., Mohammad, N., Abdelhamid, S. E., Brahim, G. B., & Amjad, K. (2024). A novel fragmented approach for securing medical health records in multimodal medical images. *Applied Sciences*, 14(14), 6293. <https://doi.org/10.3390/app14146293>
- [15] Manjón, J. V., Carbonell-Caballero, J., Lull, J. J., García-Martí, G., Martí-Bonmatí, L., & Robles, M. (2008). MRI denoising using non-local means. *Medical image analysis*, 12(4), 514-523. <https://doi.org/10.1016/j.media.2008.02.004>
- [16] Markam, D., & Saxena, V. (2017). A Dual Approach to Image Security Using Steganography and Cryptography. *International Journal of Engineering Science & Humanities*, 7(3), 01-08.
- [17] Mstafa, R. J., & Elleithy, K. M. (2017). Compressed and raw video steganography techniques: a comprehensive survey and analysis. *Multimedia Tools and Applications*, 76(20), 21749-21786. <https://doi.org/10.1007/s11042-016-4055-1>
- [18] Ragab, H., Shaban, H., Ahmed, K., & Ali, A. E. (2025). Digital image steganography and reversible data hiding: Algorithms, applications and recommendations. *Journal of Image and Graphics*, 13(1), 90-114. <https://doi.org/10.18178/joig.13.1.90-114>
- [19] Sahu, M. R. K. (2025). An In-Depth Review of Steganography: Methods, Uses, and Progress in Digital Security. *Ianna Journal of Interdisciplinary Studies*, 7(1), 437-453.
- [20] Salah, R. B., & Zaied, M. (2023, October). A robust medical image watermarking approach using beta chaotic map, DWT, and SVD. In *2023 International conference on cyberworlds (CW)* (pp. 201-208). IEEE. <https://doi.org/10.1109/CW58918.2023.00037>
- [21] Shafique, A., & Ahmed, F. (2020). Image encryption using dynamic Sbox substitution in the wavelet domain. *Wireless Personal Communications*, 115, 2243-2268. <https://doi.org/10.1007/s11277-020-07680-w>
- [22] Shuriya, B., Kumar, S. V., & Bagyalakshmi, K. (2024). Noise-resilient homomorphic encryption: A framework for secure data processing in health care domain. <https://doi.org/10.48550/arXiv.2412.11474>
- [23] Taherdoost, H., Le, T. V., & Slimani, K. (2025). Cryptographic techniques in artificial intelligence security: A bibliometric review. *Cryptography*, 9(1), 17. <https://doi.org/10.3390/cryptography9010017>
- [24] Thalapatiraj, S., Arunnehr, J., Bharathi, V. C., Dhanasekar, R., Vijayaraja, L., Kannadasan, R., ... & Khan, A. A. (2024). A novel approach for encryption and decryption of digital imaging and communications using mathematical modelling in internet of medical things. *The Journal of Engineering*, 2024(12), e70038. <https://doi.org/10.1049/tje2.70038>
- [25] Wang, J., Chen, J., Wang, F., & Ni, R. (2022). Optical image encryption scheme based on quantum s-box and meaningful ciphertext generation algorithm. *Optics Communications*, 525, 128834. <https://doi.org/10.1016/j.optcom.2022.128834>

Authors Biography



S. Nikhila is currently working as a Professor in the Department of Electronics and Instrumentation Engineering at Dr. Ambedkar Institute of Technology (Dr. AIT), Bangalore, and is pursuing her research as a Research Scholar at Dayananda Sagar College of Engineering (DSCE), Bangalore. Her research interests focus on Image Processing, Medical Imaging, Embedded Vision Systems, and Artificial Intelligence applications in healthcare. She has published several research papers in reputed international journals, contributing to areas such as face recognition using wavelet transforms, FPGA-based image dithering

engine design, digital watermarking techniques, and robotic vision systems for automated agricultural harvesting. Her recent research work emphasizes advanced medical imaging technologies, including hybrid deep learning models for removing grid-line artifacts from radiographical images, Optical Coherence Tomography systems for high-resolution breast cancer detection, and comprehensive security frameworks for teleradiology systems. Through her academic and research contributions, Nikhila S continues to work towards innovative solutions that integrate image processing, deep learning, and biomedical engineering for real-world applications.



Dr.V.S. Krushnasamy is an Associate Professor in the Department of Electronics and Instrumentation Engineering at Dayananda Sagar College of Engineering, Bengaluru, India. He has extensive academic and research experience in control systems, instrumentation, industrial automation, IoT, Industry 4.0, and AI-driven engineering applications. His research interests include AI-enabled medical imaging, digital twin systems, smart industrial monitoring, observer-based fault detection, and intelligent control systems. He has published several research articles in reputed international journals and conferences and actively guides undergraduate and postgraduate research projects. Dr. Krushnasamy is also involved in curriculum development, NBA accreditation activities, and outcome-based education initiatives.