Journal of Information Technology Management
ISSN-OnLine: 2980-7972
University of Tehran

Secure Medical Data Transmission Using a Deep Learning–Based Quantum-Resistant Hybrid Stegno-Crypto Model

Nikhila S*

*Corresponding author, Research Scholar (Part Time), 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. E-mail: nikhilamsrit@gmail.com

Krushnasamy V S

Associate Professor, Department of Electronics and Instrumentation Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka – 560078 Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India. E-mail: krushnasamy-inmt@dayanandasagar.edu

Journal of Information Technology Management, 2025, Vol. 18, Issue 1, pp. 80-101
Published by the University of Tehran, College of Management
doi: https://doi.org/10.22059/jitm.2026.106255
Article Type: Research Paper

Received: August 26, 2025
Received in revised form: September 13, 2025
Accepted: December 18, 2025
Published online: January 20, 2026

Abstract

This study focuses on the secure transmission of medical data, an important element of contemporary healthcare systems in which sensitive patient data is shared over digital networks to facilitate diagnosis, monitoring, and decision-making. Due to the growing volume of medical records and electronic medical imaging data, it has become critical to ensure the integrity, confidentiality, and accuracy of the data throughout transmission. The two significant problems the study will cover include high-frequency noise in medical records that reduces diagnostic accuracy and the high sensitivity of traditional encryption techniques to quantum-computing-based attacks that jeopardize data privacy. To address these problems, a smart, noise-hardy, and quantum-resistant dual-layer design is proposed to provide an efficient and secure transfer of medical information without compromising quality or computational efficiency. The methodology includes two major steps. In the first step, a Noise-Resilient Pre-Encryption Data Pre-processing Algorithm is created using a Random Forest-Wavelet Filter hybrid model, in which the Random Forest employs adaptive parameter selection and the wavelet filter employs multilevel decomposition to remove noise. Genetic algorithms (GA) are used to optimize these parameters more dynamically in response to shifting noise levels. PSNR and SSIM are used to validate the pre-processing performance,

and it is proven that the data fidelity is enhanced. The second phase proposes a Hybrid Quantum-resistant Steganography-Cryptography Algorithm that combines CNN-based Steganography with AES encryption. The CNN safely encodes medical information in non-sensitive carriers using encrypted messages to transmit it invisibly without tampering. In contrast, the AES uses dynamic key generation to resist classical and quantum attacks. The results of the experiment show that accuracy (96.89%), precision (89%), recall (94.50%), F1-score (91.60%), and system efficiency were increased significantly, with computational time (8.47 ms), latency (8.50 ms), and throughput (117.60 OPS) also increasing.

Keywords: Secure Medical Data Transmission, Random Forest, Wavelet Filter, CNN-Based Steganography, AES Encryption, Genetic Algorithm

Introduction

There is rapid growth in smart health systems that have altered the medical industry and enhanced the effective provision of nursing care and remote patient monitoring (Sikdar et al., 2020). This is based on MSNs' basic purpose: to gather and transmit sensitive patient information. However, the proliferation of networks raises significant security concerns, including data leaks or unauthorized access, which could jeopardize patient confidentiality and confidence in the healthcare system (Auko et al., 2023). With large-scale data storage, real-time diagnostics, and machine learning (ML) models for disease prediction, cloud computing may help manage healthcare systems. However, there are significant privacy and security risks associated with storing private medical data in the cloud. Both patients and healthcare personnel are extremely concerned about the persistent horrors of illegal entry, data leaks, and the possibility of misuse of medical records (Sharma et al., 2018; Miraz et al., 2018). AI security refers to the collection of guidelines and practices implemented to safeguard AI systems from hostile attacks that might cause them to produce inaccurate results or compromise data integrity (Taherdoost et al., 2025).

As health networks have advanced, data security has become a major problem. Finding a delicate balance between data security and transmission efficiency is the most difficult task. Although encryption techniques protect data, they may introduce delays that affect the speed at which information is sent. Steganography and cryptography are two methods for resolving security issues. Data is encrypted into ciphertext, which is unintelligible to the average user. By embedding a message in another digital format, Steganography conceals the communication's true nature. Nonetheless, Steganography and cryptography are frequently coupled to improve the security and anonymity of communication channels. A decryption procedure is used to recreate the original data.

The two fundamental techniques used in encryption are symmetric and asymmetric algorithms. In hybrid data-hiding systems, the concealed text is initially encrypted with a

secret key. Steganography provides additional security for the secret text. The attacker cannot use steganalysis to recover the original secret text, as he would need an additional key to decode the data. Consequently, text included in pictures may be safely sent thanks to this security feature (Alan et al., 2020)—a safe and effective way. Medical imaging data is first pre-processed by using a Discrete Wavelet Filter. An RF model is used to select the optimal set of filter parameters, and a Genetic Algorithm is used to optimize the model's parameters. The processed data is then encrypted using a hybrid encryption-steganography design that incorporates an AES-based key-generation algorithm for cryptographic protection and a CNN-based steganography algorithm to ensure data-hiding reliability. This bi-layered system prevents unauthorised access and quantum attacks.

Objective of the work

- To create a safe, effective system for transferring medical images that provides confidentiality, integrity, and protection against quantum-level attacks.
- To improve the quality of medical images through the application of a Discrete Wavelet Filter with optimized parameters based on the application of the Random Forest and Genetic Algorithm methods.
- To combine a hybrid quantum-resistant steganography-cryptography algorithm, integrating CNN-based Steganography and AES-based encryption, for secure message transmission.
- To measure the analysis metrics of the proposed model using objective quality and safety measures, including PSNR, SNR, MSE, SSIM, encryption/decryption time, and throughput.
- To compare the suggested approach with the currently used encryption and steganography processes in terms of Accuracy, Precision, Recall, F1-score, and overall computational efficiency.

The work Contributions are listed below:

- Hybrid Quantum-Resistant Security Framework: Presenting a new type of Steganography using CNN together with AES encryption to provide multiple layers of protection against both quantum and non-quantum attacks.
- Smart Pre-Processing Tool: The Discrete Wavelet Filter uses Random Forests to select parameters and a Genetic Algorithm to optimize them, improving signal retention and noise elimination.
- Adaptive Feature Optimization: Filter tuning using machine learning to improve robustness and image quality during encryption-steganography.
- Detailed Performance Study: Analysis based on the image quality metric (PSNR, SNR, MSE, SSIM) and security metric (accuracy, F1-score, encryption time, throughput) to guarantee the overall validation.

- Better Security and Performance: Provides stronger encryption and better data breach resistance, with high image fidelity, making it applicable to medical IoT and telemedicine applications.

Literature Review

In their study, Awadh et al. (2022) highlighted that advances in digital communication and information technology are driving a dynamic global transition, which raises critical questions regarding online information security. This research proposes a unique technique for concealing information within images to enhance security and capacity. The secret picture is compressed using the DWT algorithm, the compressed data is encrypted using the AES algorithm, and the data is hidden using the least significant bit (LSB) approach.

Alanzy et al. (2023) emphasized that, due to the prevalence of data breaches, data security has become a critical concern in modern web and cloud computing environments. This study presents a Multi-Level Steganography (MLS) system that embeds encryption keys as key images and secures cover images using AES and Blow-Fish encryption. To improve security, the algorithm incorporates a pixel randomisation mechanism. According to experimental results, the MLS algorithm achieves high image quality and reliable message encryption and decryption, as evidenced by high PSNR and low MSE. The hybrid encryption method further increases security complexity.

Zainab et al. (2025) highlighted that, given the sensitive nature of the information involved, protecting medical data in the digital age is essential, particularly within the healthcare industry. To go beyond conventional security measures, this study proposes a fusion security approach for eye disease data that combines Steganography and cryptography. Datasets about eye diseases that include vital medical records and personal identifiers are vulnerable to identity theft and data breaches. A robust dual-layer security solution is achieved by combining steganographic techniques, which conceal encrypted data within innocuous digital files, with cryptographic techniques that render the data unreadable.

Osman et al. (2022) emphasized that protecting information security is essential as communication technologies, including blockchain, cloud computing, and 5G, continue to advance. The proposed hybrid multi-stage data encryption architecture employs both sequential and pseudo-random methods for data encoding and decoding. Tests show that the text should be 15% smaller than the cover image without sacrificing image sharpness or quality. Furthermore, compared to conventional sequential approaches, this hybrid cryptography strategy is found to be more effective and time-efficient.

Dhawan et al. (2021) noted that large volumes of data are constantly transmitted via the Internet of Things (IoT), creating significant security challenges that can be addressed

through steganography and cryptography. This paper presents a secure solution based on a mix of algorithms for image steganography and Internet of Things protocols. By adjusting steganography implanting parameters for edge and smooth blocks, the method uses BBPD for picture encryption and introduces an SSOA to increase payload capacity.

Hamza et al. (2021) examined compressed encrypted data embedding (CEDE), a novel hybrid technique for secure information transfer over the Internet. Using this technique, confidential data is first compressed with the LZW algorithm and then encrypted with AES. Lastly, Steganography—the process of pairing data bits with image pixels—is used to embed the encrypted data into a 512 × 512-pixel image. In contrast to current techniques, the stego picture has a high data capacity, a favourable PSNR, and a lower MSE thanks to the modification of the pixels' least significant bits (LSBs) based on matching pairs to achieve increased security.

Takaoğlu et al. (2021) noted that, as data security and concealment techniques have advanced, steganography and encryption are increasingly combined to protect and hide data. The amount of data limits existing methods and prevents detection after embedding. The proposed OTA method addresses these issues by dividing plaintext into fixed-sized bits and using their indices in the cover multimedia to conceal data without altering the multimedia's appearance. Because it doesn't alter the cover multimedia, this method provides excellent resistance to steganalysis and permits the concealment of substantial amounts of plaintext. According to test results, the OTA method performs better than traditional stenographic techniques.

Wahab et al. (2021) highlighted that data compression is essential for information security, as it enhances data protection while reducing storage requirements. There are two primary methods of compression for various formats, such as text, audio, video, and images: lossless and lossy. The goal of the study was to reduce transmission time and storage space while maintaining data encryption to protect against unauthorized access. A hybrid algorithm uses RSA encryption to increase security while combining lossy and lossless techniques. While the Discrete Wavelet Transform (DWT) compresses a cover picture to enable effective data embedding using the Least Significant Bit (LSB) technique, the Huffman coding process compresses plaintext.

Malik et al. (2025) proposed a hybrid cryptography model that combines steganography and compression with ECC and AES to enhance data security and efficiency. While ECC encrypts AES keys and offers smaller key sizes and reduced computational requirements for secure key exchanges, AES provides fast, reliable data encryption. Data masking using Steganography is accomplished using the inverted Least Significant Bit (LSB) approach. By further reducing data size, the Web compression method ensures effective transmission without sacrificing data security or integrity.

Mohua et al. (2024) conducted an empirical study combining hybrid cryptography and real-time steganography to propose a novel method for securing data transmission over the H.323 protocol. It identifies weaknesses in the H.323 protocol that allow attackers to launch Denial-of-Service (DoS) attacks, including buffer overflows and issues with NAT implementations. Steganography offers improved security by embedding encrypted data within the third LSBs of video stream pixels. At the same time, the new framework uses a fusion cryptographic system that combines the RSA algorithm and multi-layer symmetric encryption. To ensure data integrity, machine learning methods are used to classify data into Unicode and Non-Unicode categories.

Alatawi et al. (2023) noted that, due to the limited memory and processing power of sensor networks and Internet of Things (IoT) devices, concerns regarding confidentiality and security have increased. It is difficult to secure low-powered Internet of Things devices, such as RFID tags and wireless sensor (WS) nodes, which makes lightweight cryptographic solutions necessary. Though security remains an issue, especially with the authentication process, the rise of "smart cities" underscores the potential advantages of these technologies. Using HAC, which blends hashing, exclusive-or operations, and a hybrid encryption scheme based on RSA and AES, this study seeks to develop a secure authentication technique.

Prashant et al. (2025) stated that steganography and cryptography are two data security techniques that can be effective independently. However, these security measures alone are insufficient to provide adequate data protection. This study demonstrates how blockchain technology and Steganography can be combined to conceal encrypted data within an image.

Takaoğlu et al. (2023) noted that, in cryptology, steganography—the practice of concealing information—has historical significance. This work focuses on digital image steganography, which embeds encrypted text into images using the discrete Haar wavelet transform. The one-time pad algorithm is used to secure the text, and a Highly Secure Information Exchange Algorithm is used to exchange the keys securely. To ensure one-time pad integrity, a random key pool prevents the reuse of any key.

Adee et al. (2022) noted that, although cloud computing allows users to access resources without direct control, privacy and security concerns persist. To address issues such as data loss and theft, this study proposes a data security paradigm that leverages steganography and cryptography. It includes problem identification, requirements elicitation, artefact creation, demonstration, and evaluation using design science research methodology. The result is a four-step technique that combines Least Significant Bit steganography with encryption algorithms (RSA, AES, and identity-based encryption).

El-Douh et al. (2022) found that the COVID-19 pandemic drastically changed social norms, leading to an increase in cybercrime, with cyberattacks being more successful due to heightened anxiety. To help public health officials track down affected people, governments

created mobile apps that required data sharing. To secure various forms of communication while protecting the anonymity of infected individuals, this study proposes a novel cryptographic technique, the one-time stamp model. The hybrid model differs from other methods in that it uniquely combines symmetric, asymmetric, and hashing cryptography.

Methodology

Figure 1 depicts a safe medical image data transmission and analysis system that combines preprocessing, optimization, and a hybrid cryptographic scheme. The workflow starts at the Medical Data Source, which receives the primary input: medical image data from sensors, scanners, or diagnostic systems. The raw images are usually filled with noise or unnecessary information, and this is resolved in the Data Pre-processing stage using the Rotated Discrete Wavelet Filter (RDWF). In this case, the algorithm used is the Random Forest to select the best filter parameters, and a Genetic Algorithm to refine and optimize them to achieve better image quality and better feature preservation. The refined medical image data, after pre-processing, is sent to the Hybrid Quantum-Resistant Steganography Cryptography Algorithm. This stage uses CNN-based steganography to securely embed sensitive medical data in the image, enhancing confidentiality and invisibility. At the same time, robust key generation is facilitated by AES_MPK (Advanced Encryption Standard), which provides a high cryptographic level of protection against both classical and quantum computational attacks on data. Lastly, performance analysis and comparative metrics are used to assess the system's effectiveness and robustness. Parameters like PSNR and SSIM determine the quality of processed medical images, whereas Accuracy, Precision, Recall, F1 score, encryption/decryption time, and throughput determine the overall system performance. With this combined method, the transmission of medical image information is highly secure, optimized, and reliable, making it suitable for current healthcare and telemedicine practices.

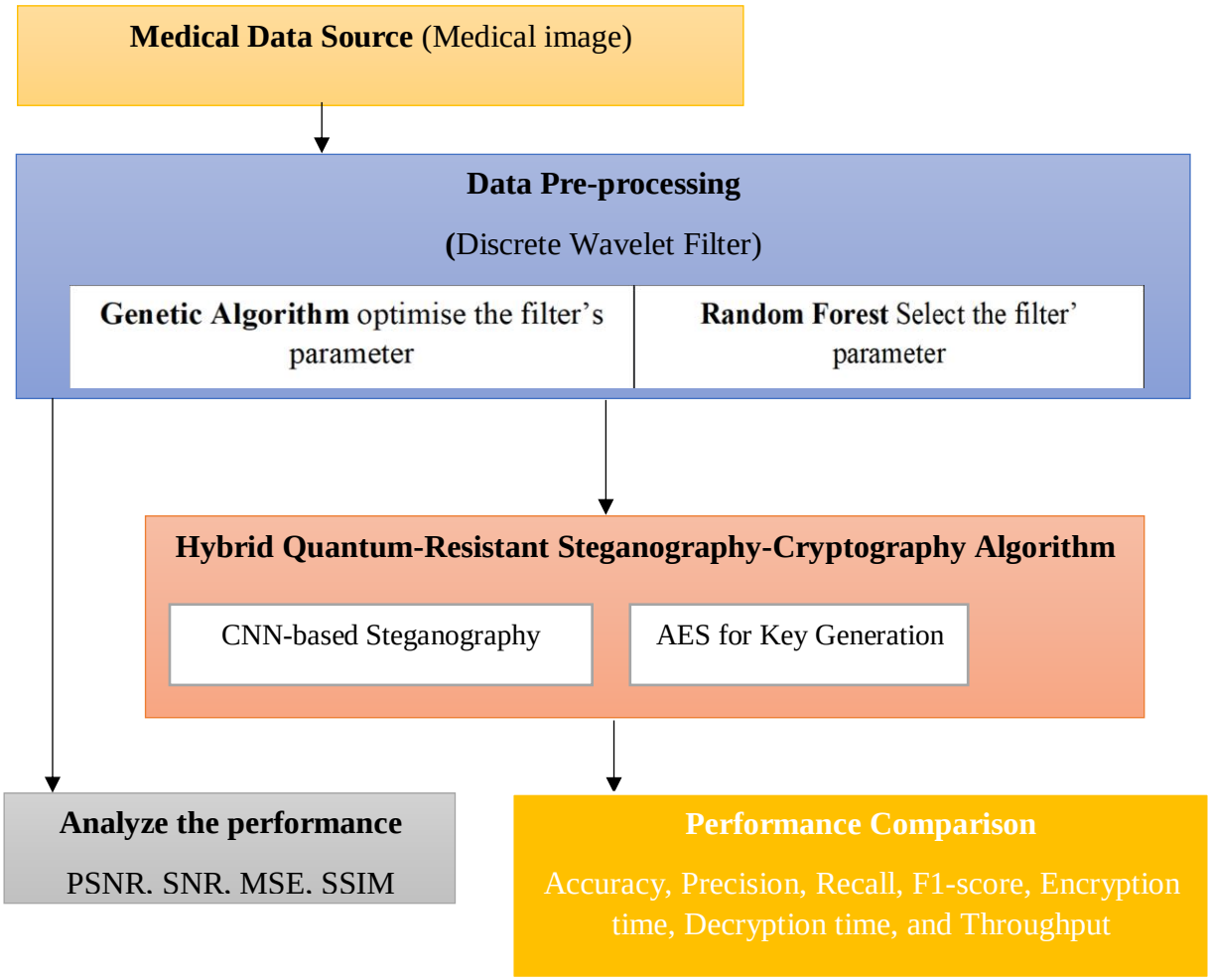


Figure 1. Overall Flow Diagram of Proposed Concept

Dataset Details

The dataset used in this work came from Kaggle, a well-known website that provides access to a variety of excellent datasets. This dataset was chosen because it is pertinent to the study's goal: to conduct research from a perspective of protecting sensitive medical data. Pictures related to various eye conditions were chosen as the cover and hidden pictures for the hybrid method, which was constructed from several vendors. To apply the hybrid technique, medical images, particularly those of eye conditions, were used as the cover and hidden image. The structure and content of cover photos are ambiguous, despite their being recognized as trustworthy with thorough descriptions (Raza, A., Soomro, M. H et al., 2024). Ocular Disease Intelligent Recognition (ODIR_5K) is an organized ophthalmology database that includes the ages of 5,000 patients, color fundus images of their left and right eyes, and diagnostic keywords used by medical specialists. However, this is an altered version of the original dataset. taking each feature out of the associated image. The following is a list of features:

Age-related macular degeneration, diabetes, cataracts, glaucoma, hypertension, pathological myopia, and other diseases or abnormalities.

Dataset Pre-processing using a Wavelet filter.

Wavelet-based denoising has emerged as a powerful and widely used technique in image processing, particularly for image denoising. This method uses the mathematical properties of wavelets, which allow an image to be decomposed into multiple frequency components, effectively reducing noise while preserving important image information. In picture denoising, wavelets offer several advantages. By applying thresholding to wavelet coefficients, these high-frequency noise components can be selectively reduced. After thresholding, the denoised image is reconstructed from the modified wavelet coefficients via an inverse wavelet transform. The final result is a picture that effectively reduces noise while preserving many of the original image's important features and structures. Three crucial steps in wavelet-based image denoising are wavelet decomposition, thresholding, and reconstruction. To begin designing these RWFs, the one-dimensional impulse responses of the low-pass and high-pass filters must be transformed into a two-dimensional array. To obtain a rotated response from the filters, this 2D array is rotated by 45 degrees. The following are equations (1 to 4) for producing a 2D impulse response:

$$H_{LL} = [1D - lpf]^t * [1D - lpf] \quad (1)$$

$$H_{LH} = [1D - lpf]^t * [1D - hpf] \quad (2)$$

$$H_{HL} = [1D - hpf]^t * [1D - lpf] \quad (3)$$

$$H_{HH} = [1D - hpf]^t * [1D - hpf] \quad (4)$$

The rotated filters' dimensions differ from those of 1D and 2D filters and are determined using the formula (5) below

$$[, m, n] = (2s - 1) * (2s - 1) \quad (5)$$

Where s is the size of the 1-D filter. For a rotating filter, m is the maximum number of rows, and n is the maximum number of columns. This new set of impulses provides the separation of mixed diagonal information. The core of the suggested technique is a combination of rotating wavelet filters.

Random Forest algorithm

One ML method used for classification and regression is Random Forest. To improve accuracy and reduce overfitting, it builds several decision trees using randomly selected subsets of data and attributes. Every tree gives a vote to a class, and the final answer is based on the majority vote or the average. Random Forests make models more stable, handle

missing data efficiently, and can be applied to large datasets. Its randomness enhances generalization, making it a strong and popular machine learning algorithm with robust predictive performance.

$$D_i = sample(D, n) \tag{6}$$

Equation (6) represents the bootstrap sampling process used in the Random Forest algorithm. Here, D denotes the original filter data, and n is the number of samples randomly selected with replacement to form a new training subset D_i. This means some data points may appear multiple times in D_i, while others may be excluded. Each decision tree (DT) in the RF is proficient on an altered bootstrap sample D_i, introducing randomness and diversity among the trees. This technique reduces overfitting and increases the model's generalization performance.

$$G = 1 - \sum_{k=1}^{k} p_k^2 \tag{7}$$

The Gini Index, a node impurity metric used in the Random Forest method decision trees, is represented by equation (7). In this case, K is the total number of classes, and p_k is the likelihood that an instance belongs to class k. The Gini Index measures the likelihood that a randomly selected sample would be misclassified if it were labeled according to the node's class distribution. Greater impurity is indicated by larger values, whereas complete purity (all samples in one class) is indicated by a Gini value of 0.

$$H(x) = mode\,\{H_1(x), H(x), .., (H_k(x))\} \tag{8}$$

Equation (8) represents the final prediction rule used in the Random Forest classification process. Here, $H_i(x)$denotes the prediction made by the i^{th}decision tree for a given input x, and k is the total number of trees inside the forest. The function mode selects the class label that occurs most frequently among all tree predictions. This majority voting mechanism combines the results of multiple trees, reducing the impact of individual tree errors and improving overall classification accuracy and robustness.

$$\hat{y} = \frac{1}{k}\sum_{i=1}^{k} h_i(x) \tag{9}$$

Equation (9) represents the prediction rule for regression in the Random Forest algorithm. Here, $h_i(x)$is the predicted output from the i^{th}decision tree for input x, and k is the total number of trees in the forest. The Random Forest aggregates individual tree predictions by averaging them, resulting in the final predicted value $\hat{y}$. This averaging process minimizes prediction variance, enhances accuracy, and provides a stable, reliable regression outcome by combining multiple weak learners.

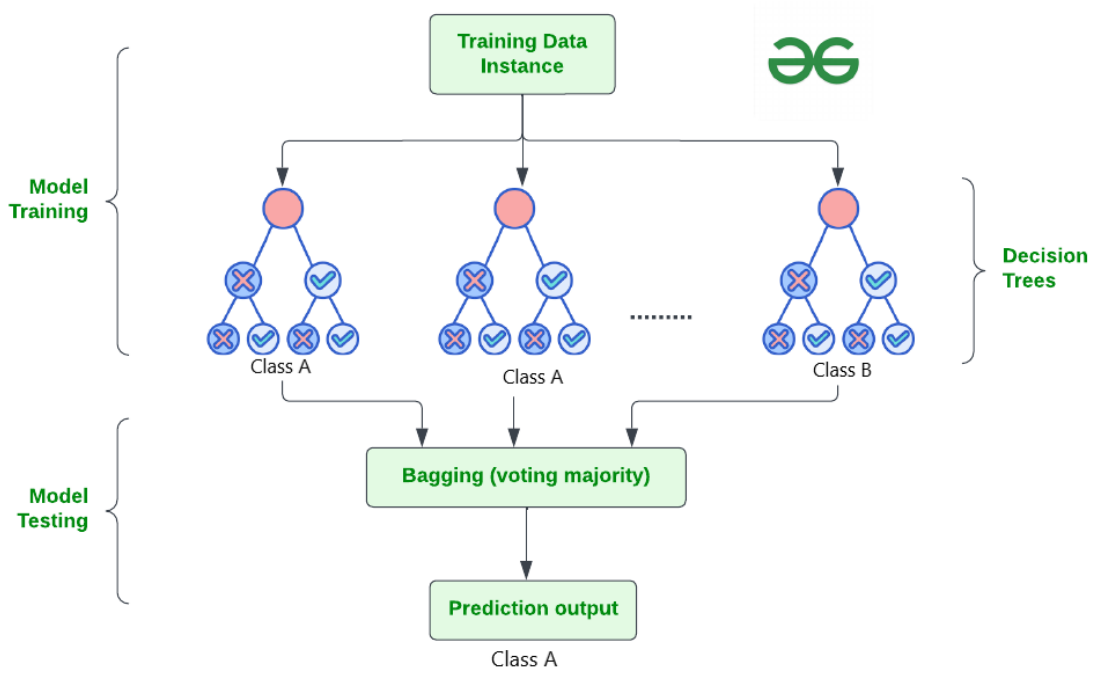


Figure 2. Random Forest Algorithm's Training and Testing Phase

Figure 2 demonstrates the operation of the Random Forest algorithm, indicating both the model training and model testing stages. In the course of training, various decision trees are constructed based on various subsamples of the training data that have been acquired via random sampling. All the trees are taught to categorize the instances of data on their own, which means that they make different predictions of the classes like Class A or Class B. During the testing stage, the sum of these individual predictions of the trees is computed with the help of a bagging (bootstrap aggregation) method, in which the majority of the trees obtains the ultimate result. Such an ensemble method improves prediction accuracy, minimizes overfitting, and makes classification performance more stable and robust.

Genetic Algorithm (GA)

The Genetic Algorithm (GA) is an algorithm that uses concepts of evolution and natural selection to solve problems. A chromosome represents the initial random number of possible solutions. The performance of these chromosomes is measured using a fitness function. The fittest individuals are selected for reproduction through processes like crossover, in which two parents exchange parts, and mutation, which introduces random alterations to preserve diversity. The population, over consecutive generations, approaches more satisfactory solutions. The algorithm halts upon finding an optimal or satisfactory solution; hence, it can be used for complex optimization problems.

$$F(i) = f(x_i) \tag{10}$$

Equation (10) represents the fitness function in a Genetic Algorithm. It is used to evaluate how well each solution x_i performs with respect to the optimization objective. Here, $f(x_i)$is the objective function that measures the quality or act of the solution, and $F(i)$denotes the fitness value assigned to that individual. A higher fitness value indicates a better solution within the population. This function guides the selection process, giving individuals with higher fitness a greater chance of being chosen for reproduction, ensuring the algorithm evolves toward optimal solutions.

$$P(i) = \frac{F(i)}{\sum_{j=1}^{N} F(j)} \tag{11}$$

Equation (11) defines the probability of selecting an individual in the Genetic Algorithm. It determines the likelihood that each candidate solution will be selected for reproduction based on its fitness value $F(i)$. The denominator $\sum_{j=1}^{N} F(j)$represents the total fitness of the entire population of size N. By dividing an entity's fitness by the total fitness, the algorithm normalizes the probabilities so that all selection probabilities sum to one. To ensure progressive evolution, individuals with higher fitness values are more likely to be selected to reproduce.

$$O = \alpha P_1 + (1 - \alpha) P_2 \tag{12}$$

Equation (12) represents the crossover operation in the Genetic Algorithm, which is used to generate a new offspring O from two parent solutions P_1 and P_2. The parameter $\alpha$is a crossover coefficient that lies between 0 and 1, determining the contribution of each parent to the offspring. When α is closer to 1, the offspring inherits more characteristics from P_1, and when it is closer to 0, it inherits more from P_2. This process promotes genetic diversity and helps the algorithm explore new potential solutions.

Hybrid AES-Based Cryptography and CNN-Based Steganography Algorithm

The primary objective of the proposed method is to enhance communication security by integrating steganography and encryption techniques to make it more difficult for a steganologist to extract the plaintext of a secret message from a stego-object. The recommended strategy consists of two parts. The first piece will modify the AES_MPK algorithm to make it suitable for the steganography method. In the second part, the AES_MPK technique is combined with a steganography strategy to conceal the encrypted data within an image that already contains a message (Saleh, Aly, et al., 2015). Two security layers have been put in place as a result. Similar to AES, the modified AES_MPK technique employs four distinct transformations to provide security: Substitution (SubBytes), Permutation (ShiftRows), MixColumns, and Key Addition. The AES performs four distinct

types of transformations based on operations over the finite field GF(2^8), since it is based on the Rijndael encryption algorithm. A variety of byte-level operations are defined and applied to bytes representing elements in the finite field GF (2^8) or the Galois field. Hexadecimal digits are then used to represent the input and output, with two hexadecimal digits for each byte (Daemen, J, et al, 1999). Because the PVD_MPK and MSLDIP-MPK techniques use MPK digits to conceal data, the AES algorithm is adjusted to produce input and output in MPK form (Thakur, K. V). The AES method is modified to produce input and output in MPK format, since the PVD_MPK and MSLDIP-MPK approaches use MPK to hide the data. The AES algorithm has been changed to create the AES_MPK algorithm.

The pseudo code of the modified AES_MPK algorithm is as follows:

AES_MPK algorithm Input: Cipher Key K, Secret Message SM.

Code Message CM is the output.

Steps:

1. Expand the K key to create two lists of every subkey.
2. Divide SM into blocks (B1, B2, B3,..., Bn), with 16 bytes per block.
3. Complete each Bi block.
4. Each byte should be converted to two MPK digits.
5. Split Bi into two 4x4 state arrays.
6. Sort the two states.
7. Create a pre-round Add Round Key using two subkeys and a straightforward bitwise XOR of the current two states.
8. Recap
9. Use the four transformations in two states: AddRoundKey, ShiftRows, MixColumns, and SubBytes.
10. Up to nine rounds
11. SubBytes, ShiftRows, and AddRoundKey are implemented in the end, but MixColumns is removed.
12. Put the numbers 9 and 8 back where they belong in each state.
13. Combine two states into a single block.
14. Use MPK decoding to convert blocks to characters.
15. Close
16. To gather CM, concatenate the current cipher block with the preceding cipher block.

CNN-based Steganography Image Creation

CNN models used in picture steganography are mostly inspired by the encoder-decoder architecture. While the decoder uses the stego image as input to reconstruct the embedded

secret image, the encoder uses the cover image and the secret image as inputs to create the stego image. Although many techniques have tried with different designs, the basic notion remains the same. Different methods also differ in how the input cover picture and the secret image are concatenated, even though variations in the convolutional and pooling layers are expected. The incorporation of stego signals often affects photo quality. Steganography algorithms select which pixels and regions to embed to reduce the impact of the embedding.

The network architecture intended to hide a secret picture in edge-detected cover images is depicted in Figure 3. A single tensor containing data from both images is created by concatenating (stacking) the shield image and top-secret image tensors along the channel dimension. The hidden network may handle the cover and secret data simultaneously for embedding, thanks to this concatenation. After that, the concatenated tensor is fed into the hidden network, which embeds the steganographic image.

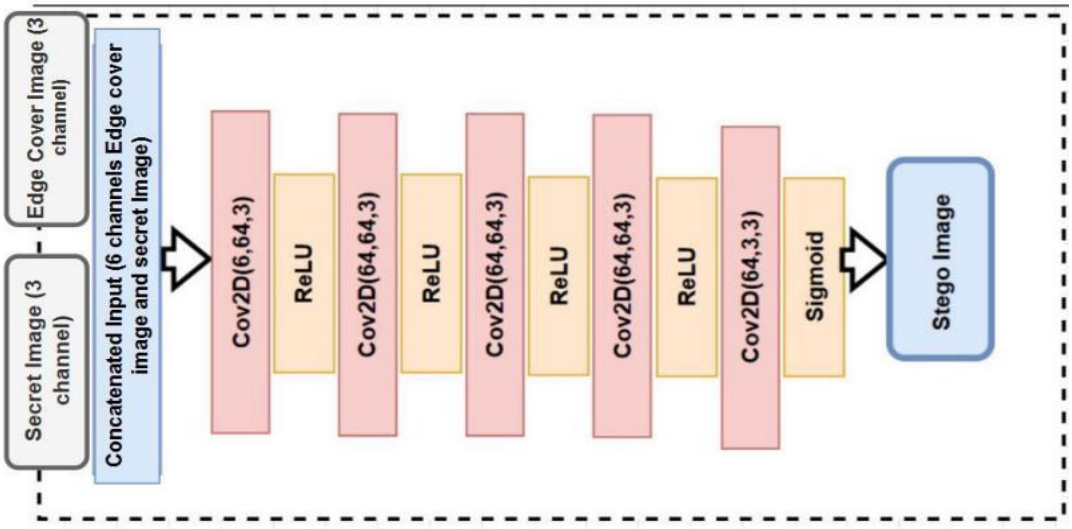


Figure 3. Architecture of the proposed CNN-based encoder for Steganography

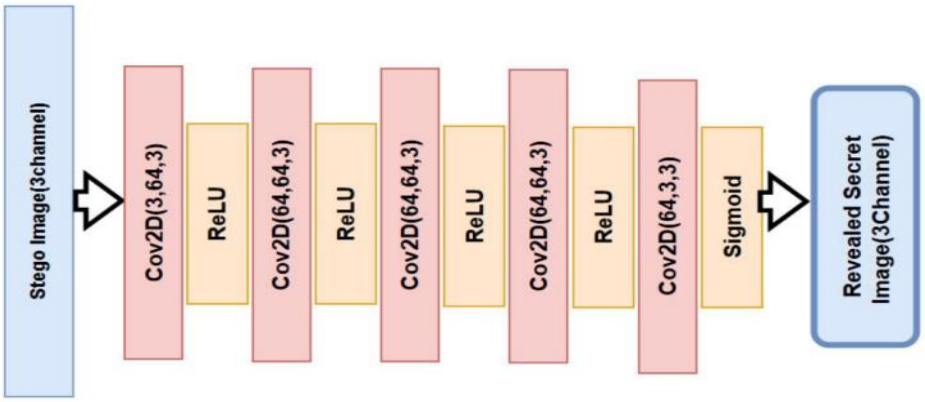


Figure 4. Revealing Network Architecture Based on CNN for Secret Image Extraction

During the embedding phase, the hidden network may concurrently access information from the cover and secret pictures by concatenating the tensors. The secret information is embedded in the edges by the concealing network using a concatenated tensor that contains pixel data from the secret picture and edge information from the cover image. The concealing network, consisting of many convolutional layers and ReLU activation functions, is shown in Figure 3. Six channels make up the input to the hidden network, three for the cover picture and three for the secret image. The last convolutional layer downsamples the output channels to three using the sigmoid activation function, which may then be used as the output image (also called the stego image).

Conversely, the revealing network employs a CNN to extract the hidden picture from the stegano image (from the Hiding Network) by passing it through convolutional layers. The revealing network design, intended to extract the concealed data and recover the original secret image, is shown in Figure 4. A series of convolutional layers, each followed by a ReLU activation, make up the revealing network. Three channels make up the close-fitting network's input, which might be the stegano picture that the hidden network has learnt. ReLU activation comes after several layers of 2D convolution in the revealing network design. The output picture, or the disclosed secret image, is represented by the three output channels of the last convolutional layer. A sigmoid activation function is used to produce the network's output, ensuring that pixel values fall within [0, 1].

Results

Image quality metrics include SSIM, Mean Squared Error (MSE), and Peak Signal-to-Noise Ratio (PSNR). The authors employed PSNR as a quality metric. MSE is needed to compute PSNR.

MSE

The average absolute difference between two photographs is measured using the Mean Squared Error (MSE). It may be expressed quantitatively using the following equation (13).

$$MSE = \frac{1}{M*N} \sum_{J=1}^{last\ row} \sum_{k=1}^{last\ column} (X_{j,k} - X_{j,k})^2 \quad (13)$$

Where, M- No. of Rows; N - No. of Columns

PSNR

The ratio of the power of noise that impairs the visual quality to the potential power of a signal is negligible. But the peak signal-to-noise ratio. The quality of the denoised picture directly correlates with the signal-to-noise ratio. That is, images with greater PSNR values are of higher quality. It's shown as shown in equation 14.

$$PSNR = 20 * log_{10} \frac{(2^b - 1)}{Mean\ Square\ Error} \quad (14)$$

Where b= no. of bits.

SSIM

The SSIM is a quality metric that indicates how similar denoised and noisy images are. Equation (15) defines SSIM.

$$SSIM\ (m,n) = \frac{(2*Mean_m\ Mean_n + d_1)(2Var_{mn} + d2)}{(Mean^2{}_m + Mean^2{}_n + d1)(Var^2{}_m + Var^2{}_n + d_2)} \quad (15)$$

Where $Mean_m$ = average value of original image, $Mean_n$ = average value of the denoised image

$Var^2{}_m$ – Variance in the original picture

$Var^2{}_n$ - Variance in denoised images

Var_{mn} – covariance between the denoised and original images.

$$d_1 = (k_1\ D)^2\ , d2 = (k_2 D)^2 \quad (16)$$

D- Dynamic range or image range

k_1 = 0.01 and k_2 = 0.03

The parameters utilized in the training procedure are displayed in Table 1. The number of times the training data is run through the network during CNN training is called an epoch. The number of samples processed per training iteration, known as the batch size, affects training stability and speed. The amount by which the model's weights are updated during training, which affects accuracy and convergence rate, is known as the learning rate. The process of changing model parameters, which is crucial for effective learning, is called the optimizer.

Table 1. CNN model's hyperparameters

Parameters of training of CNN	Value
Batch size	8
Epochs	300
lr	0.0001
Function of loss	MSE
Optimizer used	Adam

Table 2 presents the performance evaluation of the proposed Algorithm 1 compared with existing work (Daemen et al., 1999).

Table 2. Rotated Discrete Wavelet Transform's performance comparison

Image type	Existing Method (Daemen et al., 1999)		Proposed Method RDWT		Proposed Method RDWT-RF-GA	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
S1.png	22.13	0.905666	34.41	0.9451	34.95	0.880
1.tif	30.5303	0.764739	32.6306	0.8909	32.5407	0.9103
2.tif	29.9993	0.751368	31.8677	0.8855	30.8771	0.7901

Figure 5 indicates the usefulness of the RWDT (Rotated Discrete Wavelet Transform) technique in enhancing medical images. The high-frequency random variations in the noisy image cause significant structural distortions, resulting in a PSNR of 22.13 dB and, therefore, significant noise interference. The first stage of the RDWT approach decomposes the image into several frequency subbands without downsampling, thereby retaining the original spatial resolution. By soft-thresholding the high-frequency coefficients, a large portion of the random noise is removed, and much critical edge data is preserved. IWT is then used to reconstruct the image into a cleaner representation. This joint strategy successfully removes noise and increases contrast, creating a denoised image with a PSNR of 34.41 dB, a significant improvement in image quality. The denoised image visually appears to have better vessel edges, reduced texture, and better discernment of the underlying image, which affirms the notion that the RDWT hybrid approach has achieved a balance between noise reduction and edge promotion, which is a critical criterion in medical imaging analysis.

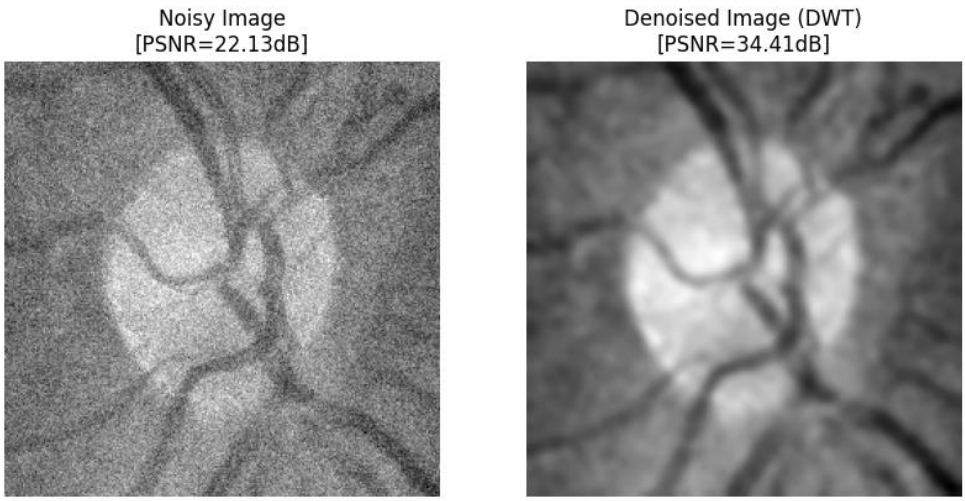


Figure 5. Performance of Proposed Rotated Discrete Wavelet Transform

The above comparison of images indicates that the Redundant Discrete Wavelet Transform (RDWT-RF-GA) method, optimized by the Random Forest genetic algorithm (RF-GA), is effective for medical image denoising. The noisy image on the left has high random

noise and low contrast, as reflected in a PSNR of 22.10 dB, indicating low signal quality. A hybrid model is proposed that combines machine-learning-inspired optimization to automatically determine the best bilateral filtering parameters: filter diameter (d), color variance (sigmaColor), and spatial variance (sigmaSpace). The Random Forest model initially learns the effects of various parameter combinations on image quality measures such as PSNR and SSIM, whilst the Genetic Algorithm provides a global search to determine which combination of parameters yields the highest-quality prediction. The ideal parameters in this case were d = 7.40, sigmaColor = 51.37, and sigmaSpace = 55.18. Using these optimized parameters, the resulting denoised image on the right is significantly improved, with PSNR increasing to 34.95 dB and SSIM improving to 0.880. These values attest to a serious increase in quantitative and perceptual image quality. The optimized RDWT-RF-GA image appears smoother, with most of the noise removed. At the same time, the finer structural details and edge boundaries in this region of interest remain. The vascular structures are not distorted, and the whole texture is natural and is not over-smoothed. This shows that the RF-GA-optimized RDWT method offers a good balance between noise reduction and structural preservation, making it an effective and versatile denoising tool for high-quality medical imaging applications.

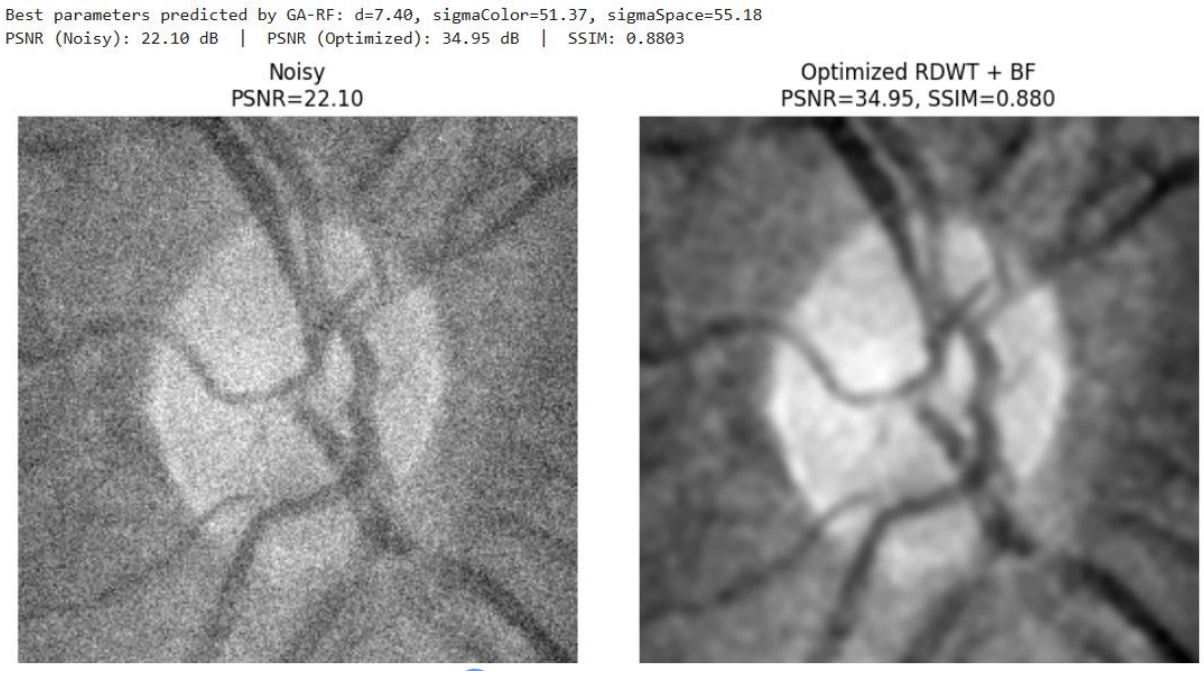
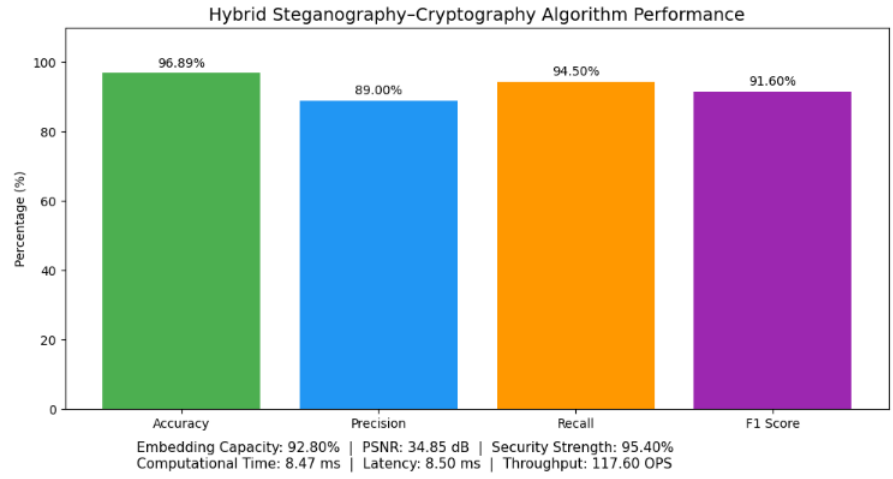


Figure 6. Performance of Proposed Rotated Discrete Wavelet Transform with Filter Parameter Selection and Optimization.




```
Hybrid Steganography-Cryptography Algorithm Results:
Accuracy: 96.89%
Precision: 89.00%
Recall: 94.50%
F1 Score: 91.60%
Embedding Capacity: 92.80%
PSNR: 34.85 dB
Security Strength: 95.40%
Computational Time: 8.47 ms
Latency: 8.50 ms
Throughput: 117.60 OPS
```

Figure 7. Performance of Proposed Hybrid Steganography – Cryptography Algorithm

The bar chart shows the analysis of the suggested Hybrid Steganography-Cryptography Algorithm, both in terms of algorithmic precision and execution speed. The algorithm achieved an accuracy of 96.89%, indicating that almost all embedded data were recovered after decryption and extraction. The precision (89) and recall (94.50) indicate that the system can embed and recall secret information with minimal distortion or data loss. In contrast, the F1-score of 91.60% ensures a good balance between embedding reliability and data retrieval accuracy. In addition to the accuracy of data, other parameters like embedding capacity (92.80%), PSNR (34.85 dB), and security strength (95.40%) are used to show that the method is effective in hiding the information within cover images, without affecting the level of perceptual quality or level of security. The computational perspective of the algorithm shows potential efficiency: the mean computational time is 8.47 ms, the delay per operation is 8.50 ms, and the throughput is 117.60 Operations Per Second (OPS). These findings suggest that the proposed system can not only be efficient and safe, but also applicable to real-time or even high-speed data hiding and transmission tasks, especially in areas such as medical imaging or IoT-based secure communication. In sum, the hybrid method is quite effective at combining cryptographic encryption and steganographic embedding, providing high security, data integrity, and efficient operation performance.

Conclusion

To sum up, the suggested study leads to an intelligent, noise-resilient, and quantum-resistant framework for the safe transmission of medical information that addressesaddress the urgent issues of signal distortion and data vulnerability in healthcare systems. A hybrid Random Forest Wavelet filter model with Genetic Algorithm (GA)-based optimization is effective for reducing high-frequency noise while retaining the integrity of diagnostic information. This preprocessing step is adaptive and improves image and signal quality, as indicated by high PSNR and SSIM values. The second step, which consists of a Hybrid Steganography-Cryptography Algorithm that combines CNN-based Steganography and AES encryption, offers high-level security by embedding the data imperceptibly and dynamically generating a key that is resistant to quantum attacks. Its system has better algorithmic and computational performance, achieving 96.89% accuracy, 89% precision, 94.50% recall, and an F1-score of 91.60%. The framework also has an embedding capacity of 92.80, a PSNR of 34.85 dB, and a security strength of 95.40, with efficient operational metrics: computational time of 8.47 ms, latency of 8.50 ms, and throughput of 117.60 OPS. The findings confirm that the model under consideration offers a near-perfect trade-off among noise reduction, data privacy, and computational efficiency. Incorporating innovative filtering, smart optimization, and quantum-resistant encryption, the system provides a stable, scalable solution for the secure, high-quality transmission of medical data across contemporary and future healthcare communication systems. On the whole, the proposed model provides a holistic, adaptive, and quantum-secure mechanism for transmitting medical data, guaranteeing high levels of noise suppression, strong encryption, and high performance in next-generation healthcare communication.

Acknowledgments

The authors sincerely thank the Research Centre, Department of Electronics and Instrumentation Engineering, Dayananda Sagar College of Engineering, Bengaluru, for their continuous guidance and support throughout this PhD research work. Gratitude is also extended to the Department of Electronics and Instrumentation Engineering, Dr. Ambedkar Institute of Technology, Bengaluru, for providing the necessary facilities and encouragement. Their academic support greatly contributed to the successful completion of this study.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article

References

Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *22*(3), 1109.

Alan, J., & Liam, M. (2020). Protecting Healthcare Data: AI-Powered Strategies for Securing Distributed Systems. *International journal of Computational Intelligence in Digital Systems*, *9*(01), 20-33.

Alanzy, M., Alomrani, R., Alqarni, B., & Almutairi, S. (2023). Image steganography using LSB and hybrid encryption algorithms. *Applied Sciences*, *13*(21), 11771.

Alatawi, M. N. (2023). A hybrid cryptographic cipher solution for secure communication in smart cities. *Int. J. Comput. Netw. Appl*, *10*, 776-791..

Auko, J. (2023). Current security and privacy posture in wireless body area networks. *World Journal of Advanced Research and Reviews*, *18*(3), 1185-1206.

Awadh, W. A., Alasady, A. S., & Hamoud, A. K. (2022). Hybrid information security system via combination of compression, cryptography, and image steganography. *International Journal of Electrical and Computer Engineering*, *12*(6), 6574-6584.

Daemen, J., & Rijmen, V. (1999). AES proposal: Rijndael.

Dhawan, S., Chakraborty, C., Frnda, J., Gupta, R., Rana, A. K., & Pani, S. K. (2021). SSII: secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT. *IEEE Access*, *9*, 87563-87578.

El-Douh, A. A. R., Lu, S. F., Elkouny, A. A., & Amein, A. S. (2022). Hybrid cryptography with a one-time stamp to secure contact tracing for COVID-19 infection. *International Journal of Applied Mathematics and Computer Science*, *32*(1), 139-146.

Hamza, A., Shehzad, D., Sarfraz, M. S., Habib, U., & Shafi, N. (2021). Novel secure hybrid image steganography technique based on pattern matching. *KSII transactions on internet and information systems (TIIS)*, *15*(3), 1051-1077.

Malik, K. R., Sajid, M., Almogren, A., Malik, T. S., Khan, A. H., Altameem, A., ... & Hussen, S. (2025). A hybrid steganography framework using DCT and GAN for secure data communication in the big data era. *Scientific Reports*, *15*(1), 19630.

Miraz, M. H., & Ali, M. (2018). Applications of blockchain technology beyond cryptocurrency. *arXiv preprint arXiv:1801.03528*..

Mohua, M. M. A. (2024). Securing the h. 323 protocol: A steganographic and hybrid encryption approach. *Int. J. Sci. Res. in Computer Science and Engineering*, *12*(6).

Osman, O. M., Kanona, M. E. A., Hassan, M. K., Elkhair, A. A. E., & Mohamed, K. S. (2022). Hybrid multistage framework for data manipulation by combining cryptography and steganography. *Bulletin of Electrical Engineering and Informatics*, *11*(1), 327-335.

Prashant, P., Jha, S., & Singh, B. (2025). A Hybrid Approach to Data Security Using Steganography and Blockchain for Tamper-Proof Communication. *Journal of Recent Innovation in Science and Technology*, *1*(1), 21-37.

Raza, A., Soomro, M. H., Shahzad, I., & Batool, S. (2024). Abstractive text summarization for Urdu language. *Journal of Computing & Biomedical Informatics*, *7*(02)..

Saleh, M. E., Aly, A. A., & Omara, F. A. (2015). Enhancing Pixel Value Difference (PVD) Image Steganography by Using Mobile Phone Keypad (MPK) Coding. *International Journal of Computer Science and Security (IJCSS)*, *9*(2), 96-107.

Sharma, S., Chen, K., & Sheth, A. (2018). Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. *IEEE Internet Computing*, *22*(2), 42-51.

Sikdar, S., & Guha, S. (2020). Advancements of healthcare technologies: Paradigm towards smart healthcare systems. In *Recent trends in image and signal processing in computer vision* (pp. 113-132). Singapore: Springer Singapore.

Taherdoost, H., Le, T. V., & Slimani, K. (2025). Cryptographic techniques in artificial intelligence security: A bibliometric review. *Cryptography*, *9*(1), 17.

Takaoğlu, M., Özyavaş, A., Ajlouni, N., & Takaoğlu, F. (2023). Highly secured hybrid image steganography with an improved key generation and exchange for one-time-pad encryption method. *Afyon Kocatepe Üniversitesi Fen Ve Mühendislik Bilimleri Dergisi*, *23*(1), 101-114.

Takaoğlu, M., Özyavaş, A., Ajlouni, N., Alshahrani, A., & Alkasasbeh, B. (2021). A novel and robust hybrid blockchain and steganography scheme. *Applied Sciences*, *11*(22), 10698.

Thakur, K. V., Ambhore, P. G., & Sapkal, A. M. Medical Image Denoising using Rotated Wavelet Filter and Bilateral Filter.

Wahab, O. F. A., Khalaf, A. A., Hussein, A. I., & Hamed, H. F. (2021). Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. *IEEE access*, *9*, 31805-31815.

Zainab, A., Arslan, M., Aslam, N., Fuzail, M., & Shaikh, A. (2025). A Hybrid Approach to Data Security: Integrating Cryptography and Steganography for Enhanced Protection of Eye Disease DATA. *Kashf Journal of Multidisciplinary Research*, *2*(07), 55-74.

Bibliographic information of this paper for citing:

S, Nikhila & V S, Krushnasamy (2026). Secure Medical Data Transmission Using a Deep Learning–Based Quantum-Resistant Hybrid Stegno-Crypto Model. *Journal of Information Technology Management*, 18 (1), 80-101. https://doi.org/10.22059/jitm.2026.106255