

## Research Article

# Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things

Hussah N. AlEisa 

*Department of Computer Sciences, College of Computer and Information Sciences,  
Princess Nourah Bint Abdulrahman University, Riyadh 11671, Saudi Arabia*

Correspondence should be addressed to Hussah N. AlEisa; [haleisa@pnu.edu.sa](mailto:haleisa@pnu.edu.sa)

Received 22 March 2022; Revised 5 April 2022; Accepted 13 April 2022; Published 6 May 2022

Academic Editor: Mohamed Elhoseny

Copyright © 2022 Hussah N. AlEisa. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Recently, with the availability of fast and reliable Internet, the distance between a patient and a doctor is becoming unimportant. Physicians will be able to request the medical images of their patients regardless of the geographical area. However, a lot of challenges face such successful implementation. To facilitate remote diagnosis, patient electronic medical record (EMR), including medical images, that originates in one system needs to be exchanged either within the same organization or across different organizations. Steganography is the practice of concealing a secret message inside a cover medium. In this paper, steganography will be used to embed the patient's personal information securely and imperceptibly in their medical images to enhance confidentiality in case of a distant diagnosis. The security of the medical data is improved to maintain confidentiality and integrity using IoT. The least significant bit of the approximate coefficient of integer wavelet transform is proposed. The distortion between the cover image and stego-image is obtained by measuring the mean square error and PSNR, and normalized cross-correlation is utilized to estimate the degree of closeness between the cover image and stego-image.

## 1. Introduction

Communication through digitized media has been increasingly evident with the development of the Internet. All individual and commercial communication takes place on the Internet, where computerized media is the primary means. When sensitive data from businesses and organizations is shared, the security of the information is a major problem. They are required to keep their data safe from interfering eyes. However, everyone in today's world has access to the Internet, so there is a great danger in transmitting data digitally. The conservation of data during transmission is addressed in this way [1].

In today's world, the confidentiality of secret data is paramount, and advances in the security of computers have positioned steganography as a superior technique for acquiring secured data. Steganography is the method of concealing secret data in a message, audio file, picture, or video by embedding it in another image, audio file, video, or

message [2–4]. It is used to keep sensitive information safe from hackers. Nowadays, the volume of data shared via the Internet is expanding. As a result, data security is considered a severe concern when data is communicated through the Internet [5, 6].

In steganography methods, each pixel of the cover picture is hidden with an equivalent number of secret bits. The embedding alteration in the cover image is equal. Individual pixels in a digital picture, on the other hand, have complicated statistical connections. As a result, the picture quality is automatically lowered while modifications with equal number of bits are made in the cover image pixel [7]. Different adaptive embedding techniques have been included within the steganography method to address these concerns. Each pixel of the cover picture is embedded with a changing number of bits using this adaptive embedding approach. As a result, the majority of researchers concentrated on adaptive strategies to increase the safety of the steganography approach [8–12]. Additionally, the value of

edge pixels is unaffected by modifications made during the embedding process. As a result, edge pixels can hold more hidden bits than smooth pixels. In most applications, metaheuristic algorithms are employed to tackle optimization problems [13–16].

To safeguard data, IoT transmitted data in the cloud through the Internet is employed. High data security is provided via complicated encryption and decryption technology. Only encryption and decryption are used, but data concealment offers a greater benefit [17, 18].

For security difficulties in the data communication between two devices in an IoT network as shown in Figure 1, several security criteria such as authentication, integrity, and secrecy were applied. Attacks are classified as low-, medium-, high-, and extremely high-level attacks based on their behavior and threat level.

The two types of image steganographic methods are spatial domain and frequency domain [19]. Spatial domain approaches deal with the direct change of picture pixels, and while they have a higher payload and imperceptibility, they are vulnerable to statistical assaults [20]. Frequency domain approaches, on the other hand, use changed coefficients resulting from different transformations such as DWT, DFT, and DCT for data embedding. These approaches are more resistant to image processing assaults, but they are computationally demanding and have a small payload, making them unsuitable for real-time applications [21, 22].

There are two ways to classify steganography techniques. Steganography methods are classified into image steganography, video steganography, text steganography, audio steganography, and network steganography, depending on the kind of cover image [23]. Steganography techniques are divided into two categories based on the embedding domains: spatial domain techniques, such as least significant bit and pixel value differencing approaches; transform domain techniques, such as discrete cosine transform (DCT), discrete wavelet transform (DWT), and integer wavelet transform (IWT); spread spectrum systems; masking distortion systems; and filtering methods [24].

## 2. Related Work

For securing information in an IoT architecture, three-color picture steganography algorithms are proposed. The first and third techniques employ red, green, and blue components for information transmission, whereas the second technique utilizes green and blue components. The dynamic positioning techniques were developed by utilizing the shared secret key to hide data in the deeper layer of the image channels [25].

The performance analysis of the secret image steganography technique for the security of images and data is discussed. For image steganography, modified LSB replacement and data mapping algorithms have been developed. Initially, the secret picture was preprocessed utilizing the data mapping method which was used to embed the secret picture in the cover image. In general, the majority of LSB approaches did not rely on pixel correlation or picture content. As a result, it might be detected through RS analysis.

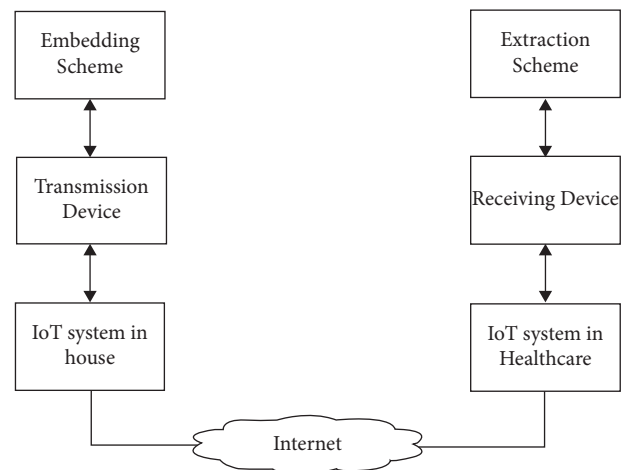


FIGURE 1: Data hiding and extraction for broadcasting between IoT devices.

Consequently, some preventive measures are required to enhance the security of LSB-based steganography approaches. An edge detection procedure has been implemented in the LSB-based steganography approach to address this problem. Furthermore, before incorporating the secret images into the cover image, they should be encrypted to increase security. Due to the lack of encryption methods preceding the embedding process, the security level of several current approaches has been decreased [26].

The data secured in the fog cloud IoT system is presented. The user in one region of the system uploads substantial data using the suggested quantum steganography convention and then transmits the protected data to the fog cloud. The intended receiver receives the data from the mist cloud and extracts the anticipated material using the specified extraction method [27].

A method for encrypting any form of an image, particularly medical images, has been developed. They intended to secure the integrity of electronic medical data while also sustaining its availability and authentication to ensure that only authorized personnel had access to it. In the first stage, the AES encryption technology was used. With seven values retrieved from the ear image as feature vectors, the ear print is also included. By delivering medical pictures over the Internet, the suggested approach increased the security of these images and protected them from unauthorized access [28].

The decision tree approach is used to present a novel method for shifting the medical data of the patient by securing the data into the medical cover image. The encryption is performed in the form of several chunks which are disseminated uniformly. Secret numbers are allocated to the cover image in the mapping method based on the breadth-first search to insert the data. Before embeddings, the data was encrypted using the RSA technique [29].

A safe approach that can meet the security and protection requirements while also overcoming the SPECS flaws is offered. In addition, this demonstrates the plan's success through execution assessments in terms of confirmation postponement and transmission overhead [30].

Developments and security adjustments attempting to solve the vulnerabilities of the security approach are presented to overcome the instinctive safety flaws of the 2-factor substantiation method. The proposed security enhancements may be used with the 2-factor authentication approach to achieve a more secure and robust two-factor client verification through WSNs [31]. For embedding reasons, the interblock approach is utilized. Images in the JPEG format are referred to as host or stego-images. This approach is only used to conceal patient information in medical JPEG photos. The difference in the coefficients is calculated using discrete cosine transform (DCT) [32].

In today’s healthcare systems, Internet of Things (IoT) devices play a critical role. To incorporate patient data in any cover media, 2D DWT is applied. For the cover photos, grayscale and color photographs are utilized. Text data is encrypted using standard methods before being embedded in the cover medium. Various numerical methods are used to validate the imperceptibility of the cover image [33, 34].

On the segmented image, the region of the object and the reversible watermarking technique are employed. If image modes such as X-rays, magnetic resonance imaging (MRI), or computed tomography (CT) images have been tampered with or forged, the presented methodologies perform effectively to identify the tampering using the hash code. As medical systems are more prone to fabrication or manipulation, reversible watermarking methods are particularly useful [35, 36].

Steganography is a method for embedding data in many images, as compared to classical steganography, which uses just one image at a time for embedding. In the event of an exceptional state in the communication media during data transmission, secret data bits can be recovered from many shares. Compressed JPEG images are extensively useful for communication channels. An intermediate image is constructed before transmitting it to the channel, which is near enough to the stego-image [37].

A novel method for securing secret data in a fingerprint image created from a hidden message is proposed. Unlike traditional steganography techniques, there is no requirement for a cover signal for the embedding process. The secret message is transferred to the polynomial, encoded at diverse points of polarities, and utilized as a portion of the hologram to generate the fingerprint image [38–40].

### 3. Methodology

This section discusses the proposed methodology for maintaining data confidentiality during the IoT distribution process. Because information is passed across numerous hops in the Internet of Things, data security is critical. Due to the ease with which data may be accessed, the mixture of various gadgets and the interconnections established through a multitude of data give space for privacy breaches in IoT. As a result, in such a case, data may be secured by a reliable encoding technique. Accordingly, this study proposes a dependable data transmission model for a safe IoT connection, as shown in Figure 2, which is a depiction of a setup in healthcare that uses an IoT dispersed structure.

**3.1. Steganography.** A steganography approach based on encryption is proposed for conveying secret data. Normally, a digital image consists of disparate picture parts known as pixels. As a cover picture, a grayscale image and a color image are utilized in this work. As a result, a picture is represented by a large array of bytes. Image encryption, embedding phase, quality improvement, and extraction phase are the four key aspects of the system proposed. This programme is commonly used in photos, although the method’s characteristics are generally stated in some figures, including hash marking. Steganography protects against unauthorized users and illegal copyrights.

Steganography is a progression in which secret data is hidden so that its presence cannot be recognized. This is why steganography is sometimes referred to as “covered writing.” The goal of steganography is not only to secure the encryption but also to hide it so that no one can detect or determine the presence of the hidden secret data. This system or technique aims to hide the presence of any secret data. The person who is not permitted to push for knowledge access should not even know if any secret information is available.

The basic components of steganography are the message, the carrier and the stego-key. The message is that the secret text, image, video, or audio has to be safeguarded using the steganography process. The carrier is the path or medium through which the key and, hence, the covered message are sent. The stego-key is the password by which confidential data is protected and exposed as shown in Figure 3.

**3.2. Image Encryption.** In the encryption process, the hidden image is processed with binary by plane decomposition which is utilized to decompose the image into binary bit planes. The image is represented with binary planes in this method for a decimal number which is given as

$$\begin{aligned}
 B &= \sum_{i=0}^{n-1} b_i 2^i, \\
 B &= b_0 2^0 + b_1 2^1 + \dots + b_{n-1} 2^{n-1}, \\
 B &= b_0 + 2b_1 \dots + 2^{n-1} b_{n-1}.
 \end{aligned}
 \tag{1}$$

The grayscale image has the pixel value in the range of 0 to 255, which is decomposed into binary bit values. With the support of secret key binary, keystreams are generated. These binary keystreams enter the two stages of the encryption model. The piecewise linear chaotic map is utilized to produce the keystreams, which are represented as

$$x_{i+1} = \begin{cases} \frac{x_i}{\delta}, & 0 \leq x_i \leq \delta, \\ \frac{x_i - \delta}{0.5 - \delta}, & \delta \leq x_i \leq 0.5, \\ F(1 - x_i, \delta), & 0.5 \leq x_i \leq 1. \end{cases}
 \tag{2}$$

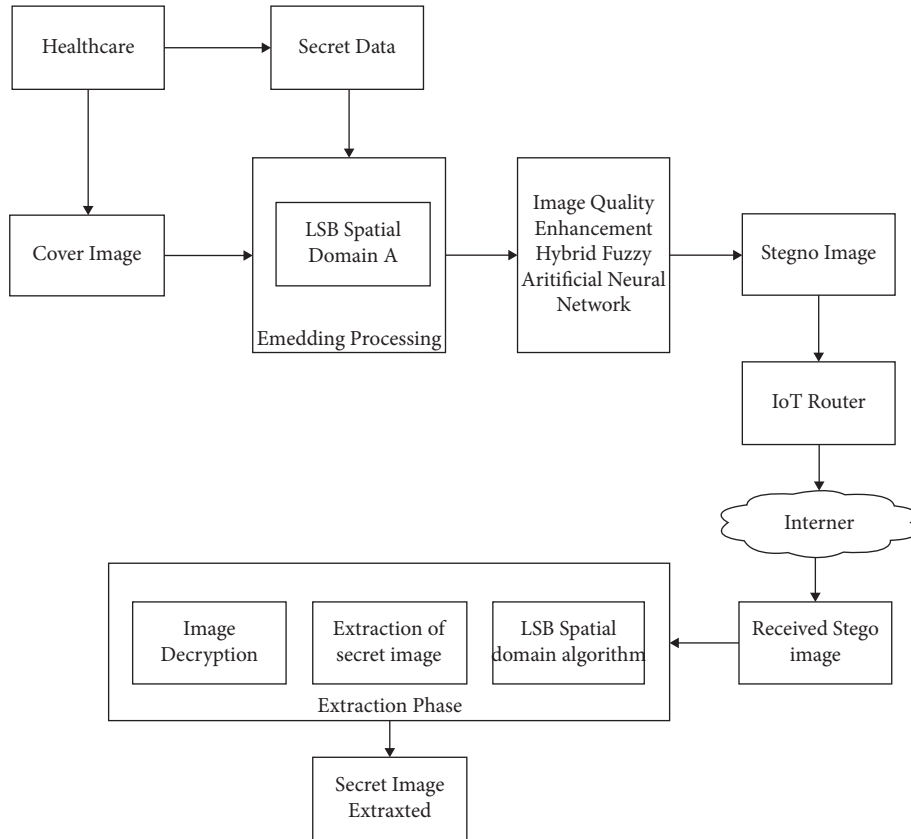


FIGURE 2: Block diagram of the proposed methodology.

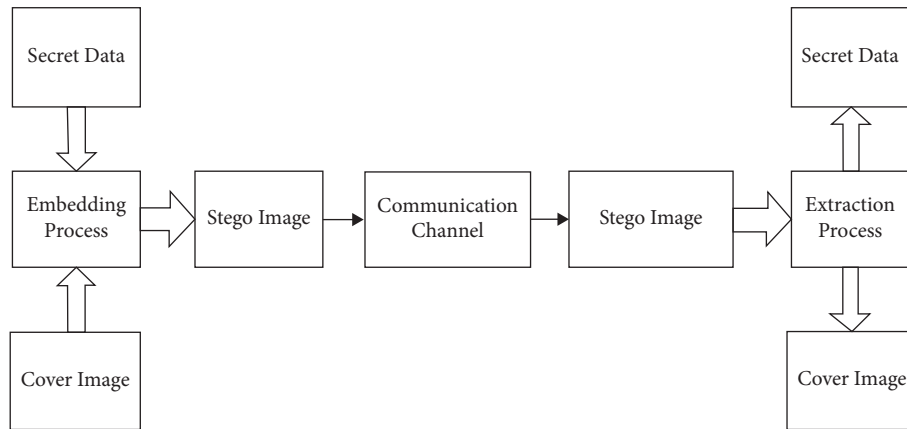


FIGURE 3: Steganography scheme.

The control parameter is represented as  $\delta$ , and  $x_i$  provides the initial condition of piecewise linear chaotic mapping. The set of the hidden image  $\delta$  is encrypted with the initial value  $x_0$ .

The keystream  $X = \{x_1, x_2, \dots, x_n\}$  is converted into the integer sequence  $X_1(i)$ .

$$X_1 = \text{mod}(\text{floor}(X \times 10^{14}), 256). \quad (3)$$

The bit-plane decomposition utilizes the keystream into bit planes to obtain the binary sequence  $k_1$  and  $k_2$  in which the bits are arranged from a higher bit plane to a lower bit plane.

**3.2.1. Diffusion Stage.** The diffusion stage is performed by the following steps.

- (1) Elements  $M$  are added as

$$S_1 = \sum_{i=0}^{n-1} M_1(i). \quad (4)$$

- (2) Cyclic operation is performed in  $M_1$  to obtain the matrix  $M_{11}$ , and  $M_1$  element is shifted right by  $S_1$  bits.

- (3) First element  $M_1$  is encrypted, and the key of the first element  $M_1$  is given as

$$P_1(i) = M_{11}(i) \oplus M_{11}(i-1) \oplus M_2(i) \oplus k_1(i). \quad (5)$$

- (4) Element P is given as

$$S_2 = \sum_{i=1}^{n-1} P_1(i). \quad (6)$$

- (5) Cyclic operation is performed in  $M_2$  to obtain the matrix  $M_{22}$ , and  $M_2$  element is shifted right by  $S_2$  bits.

- (6) First element  $M_{22}$  is encrypted, and the key of the first element  $M_2$  is given as

$$P_2(i) = M_{22}(i) \oplus M_{22}(i-1) \oplus P_1(i) \oplus k_1(i). \quad (7)$$

3.2.2. *Confusion Stage.* The steps performed in confusion matrix are given as follows.

- (1) The elements  $P_1$  and  $P_2$  are added as given below:

$$S_3 = \sum_{i=0}^{nm} P_1(i) + P_2(i). \quad (8)$$

- (2) The keystreams  $k_1$  and  $k_2$  are generated using the secret key  $k(x, \delta)$ . The initial value  $a_0$  is generated using the following:

$$a_0 = \text{mod}\left(\frac{a_0 + S_3}{nm, 1}\right). \quad (9)$$

- (3) The chaotic sequence is generated as

$$\begin{aligned} A_1 &= \{a_1, a_2, \dots, a_{nm}\}, \\ A_2 &= \{a_{nm+1}, a_{nm+2}, \dots, a_{nm}\}. \end{aligned} \quad (10)$$

- (4) The integer sequence  $X_1$  and  $X_2$  is given as

$$\begin{aligned} X_1 &= \text{mod}(\text{floor}(A_1 \times 10^{14}), 4nm) + 1, \\ X_2 &= \text{mod}(\text{floor}(A_2 \times 10^{14}), 4nm) + 1. \end{aligned} \quad (11)$$

- (5) The row vector  $R_1$  is obtained by encrypting the swapping elements  $P_1$  and  $P_2$ :

$$\begin{aligned} \text{temp} &= P_1(i), \\ P_1(i) &= P_2(X_1(i)), \\ P_2(X_1(i)) &= \text{temp}. \end{aligned} \quad (12)$$

- (6) The row vector  $R_2$  is obtained by encrypting the swapping elements  $P_1$  and  $P_2$ :

$$\begin{aligned} \text{temp} &= P_2(i), \\ P_2(i) &= P_1(X_2(i)), \\ P_1(X_2(i)) &= \text{temp}. \end{aligned} \quad (13)$$

- (7)  $R_1$  and  $R_2$  are the row vectors which are transformed into  $n \times m$  images to obtain the secret image.

3.3. *Embedding Process.* The embedding approach involves some cover image and secret image preparation, as well as secret key extraction and data hiding. The cover picture was chosen based on certain conclusions drawn from earlier steganography studies. This should be done carefully so that the superiority of the stego-image created after hiding is preserved. Certain pixels or blocks are chosen from the cover image using a random key. Before embedding, the secret picture is compressed and encrypted. Compression reduces the quantity of data to be hidden, while encryption improves security. Even if the primary concern of steganography is exploited, data should not be exposed. The secret image is compressed using a sophisticated wavelet-based compression algorithm. Simple bit operations like AND and OR are used to encrypt data. After that, the secret picture is transformed into a bitstream, referred to as the secret data. The LSB approach is utilized to disguise the secret data in the chosen pixels. It is sufficient to swap the final two bits if the quantity of data is less. Otherwise, the secret data is swapped for the least significant 3 bits of the chosen pixels to generate the stego-image as shown in Figure 4.

3.4. *LSB Domain Algorithm.* The algorithm for hiding a hidden text in an image is the LSB. The LSB embedding technique uses the secret text bitstream to be hidden to substitute the LSBs of the pixels in the cover picture. Because deviations in the LSBs of pixels do not produce variation in the image, the stego-image is virtually identical to the cover image.

The pixel value  $I(a, b)$  of LSB is similar to message bit which is embedded in  $I(a, b)$ , and it remains unchanged. The stego-image is obtained as follows:

$$I_s(a, b) = \begin{cases} I(a, b) - 1, & m = 0, \text{LSB}(I(a, b)) = 1, \\ I(a, b), & \text{LSB}(I(a, b)) = m, \\ I(a, b) + 1, & m = 0, \text{LSB}(I(a, b)) = 1, \end{cases} \quad (14)$$

where  $m$  is the next bit for embedding each pixel by changing a bit.

The pixels of an image must be adjusted to incorporate a hidden message. It is hard to differentiate between the cover image and the stego-image. This approach often generates significant distortion in the cover image when the number of hidden bits for each pixel reaches three. There are many steganographic to be utilized to mitigate the distortion induced by LSB replacement. Adaptive approaches alter the number of concealed bits in each pixel, resulting in a higher image quality compared to systems that rely only on LSB replacement. However, this comes at the expense of lowering the embedding capacity.

3.5. *IWT Technique.* An integer data set is transformed into another integer data set using the IWT. When the data is hidden in the coefficients of the wavelet filters used in the

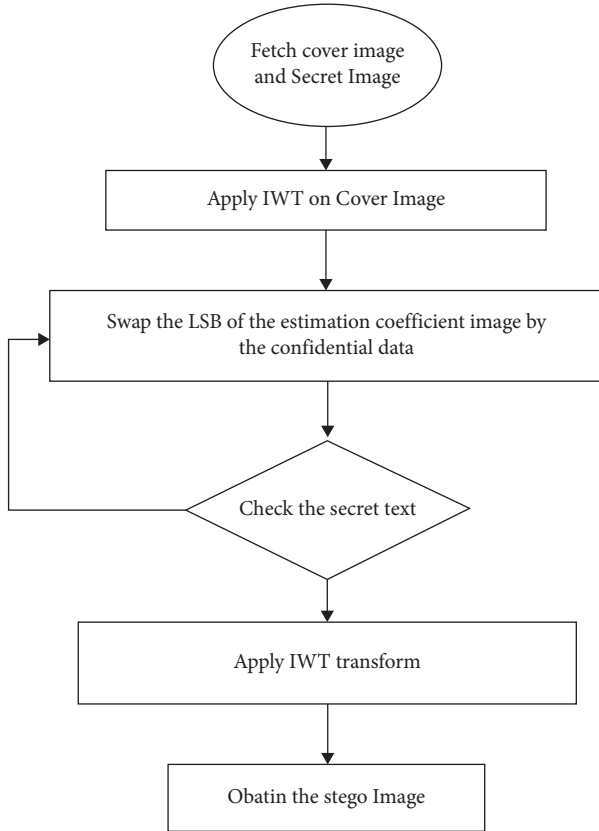


FIGURE 4: Flowchart of the LSB-IWT embedding process.

DWT, any method that is most effective for the floating-point values of the pixels that should be integers may result in the loss of the hidden data, failing the data hiding system. To avoid difficulties with wavelet filters' floating-point accuracy when the input data is an integer, such as in digital images, the output data will no longer be an integer, preventing perfect recreation of the original image and preventing information loss through forward and inverse transforms. The lifting technique is one of the approaches for performing the IWT. IWT can transform integer wavelet coefficients from pixel values and recreate the image from integer wavelet coefficients due to its numerical advantages.

The image pixel is decomposed into four subband wavelets of DWT: LL, LH, HL, and HH. The coefficient of the image is approximated using the LL subband, vertical details of the image are given using the LH subband, horizontal details of the image are examined in HL, and diagonal details of the image are given using the HH subband. The coefficient of IWT is computed as

$$\begin{aligned}
 LL_{a,b} &= \left[ \frac{(I_{2a,2b} + I_{2a,2b})}{2} \right], \\
 LH_{a,b} &= I_{2a,2b+1} - I_{2a,2b}, \\
 HL_{a,b} &= I_{2a+1,2b} - I_{2a,2b}, \\
 HH_{a,b} &= I_{2a+1,2b+1} - I_{2a,2b}.
 \end{aligned} \quad (15)$$

The coefficient of inverse IWT is given as

$$\begin{aligned}
 I_{2a,2b} &= LL_{a,b} - \left[ \frac{HL_{a,b}}{2} \right], \\
 I_{2a,2b+1} &= LL_{a,b} - \left[ \frac{HL_{a,b+1}}{2} \right], \\
 I_{2a+1,2b} &= I_{2a,2b+1} + LH_{a,b} - HL_{a,b}, \\
 I_{2a+1,2b+1} &= I_{2a+1,2b} + HH_{a,b} + LH_{a,b}.
 \end{aligned} \quad (16)$$

The steps of the algorithm for the embedding process in IWT-LSB are as follows:

- (1) The cover image is read.
- (2) The secret image is read.
- (3) IWT is applied for the cover image.
- (4) Change the LSB of the coefficient image by the secret image.
- (5) Until the secret data is completely hidden in the cover image, step 4 will be continued.
- (6) Inverse IWT is applied.
- (7) Stego-image is obtained.

**3.6. Image Quality Enhancement.** The obtained stego-image from the embedding process is of insufficient quality. As a result, a processing procedure on the unique intelligent system is required. This phase is necessary for reducing the chances of numerical identification and other types of image modification attempts.

**3.7. Hybrid Fuzzy Neural Network.** An HFNN with a backpropagation learning method is employed to improve the image quality in this study. In general, neural networks resemble HFNNs that are inhomogeneous. The neural network refers to a framework that can simulate how the human brain learns. The stego-image transformed to binary bit values in order to identify free bits and bits that encompass secret bits. A buffer is built to keep the free bits that are not used by the embedding process. The stego-and cover images are also used to extract statistical and perceptual attributes. The statistical and visual aspects are represented by the chi-square probability and the Euclidian norm. The HFNN is provided with the free bits buffer as well as the two characteristics of the stego-image. The cover attributes are then compared to the HFNN outputs. By integrating the changed free bits with the secret bits, a new stego-image is created if the outputs match the characteristics of the cover image. The HFNN weights are modified using a back-propagation learning process.

- (1) The stego-image is generated by hiding the secret image, which is implemented using embedding approach algorithms.
- (2) Features are extracted from the stego-image using the feature extraction technique.

- (3) A buffer is generated which is not utilized in the steganographic algorithm. The secret is not hidden in the buffer bit, and it is called free bits.
- (4) The statistical and visual measure of the stego-image is measured using a fuzzy neural network with backpropagation. The statistical and visual measure of the stego-image is measured using a fuzzy neural network with backpropagation. Therefore, for an updated stego-image, the free bit buffer, statistical and visual measures are contained in the output layer.
- (5) The output of the fuzzy network is compared with the cover image. The stego-image is formed if the output and cover image get matched and the output with the free bit is used by assembling the other bit in which the secret image is hidden. Otherwise, step 4 is repeated.

The input layer, rule layer, fuzzification layer, inference layer, and defuzzification layer are the five layers that compose HFNN as shown in Figure 5. The input neurons of the HFNN were trained using five layers of backpropagation, using inputs from the free bits buffer, and numerical and graphic characteristics. Following that, all hidden neurons in the fuzzification layer get the inputs. The membership function is used to perform fuzzy process on input characteristics at this layer. For the excellent approximation of input space, the Gaussian membership function is utilized. By altering the parameter values, this bell-shaped function produces several membership functions for the input characteristics. The strength of fuzzy rules is determined in the rule layer using the logical AND operator. On fuzzy inference, the inference layer executes OR operations. The HFNN output will emerge from the defuzzification layer. The weight parameter is used to link the nodes of all layers in HFNN.

The dimensionality reduction is a feature extraction in which set of features is transformed form stego image. The statistical features are obtained from chi-square probability and visual features from the Euclidean norm. Let  $x$  and  $y$  be the input, then linguistic input variable  $A_1, A_1$  and  $B_1, B_1$ . The linguist state is given as

$$A_j(u) = \exp\left[-\frac{1}{2}\left(\frac{a - u_{j1}}{v_{j1}}\right)^2\right],$$

$$B_j(u) = \exp\left[-\frac{1}{2}\left(\frac{a - u_{j2}}{v_{j2}}\right)^2\right].$$
(17)

$\{u_{j1}, u_{j1}, u_{j1}, u_{j1}\}$  are the parameter set. The logical operator is used to strength the output of the network layer:

$$F_1 = A_1(x_0) \wedge B_1(y_0),$$

$$F_2 = A_2(x_0) \wedge B_2(y_0).$$
(18)

The defuzzification is obtained as the normalization:

$$F_{d1} = \frac{F_1}{F_1 + F_2},$$

$$F_{d2} = \frac{F_2}{F_1 + F_2}.$$
(19)

The error function is given by

$$E = \frac{1}{2}(y - 0)^2.$$
(20)

The desired output is represented as  $y$ .

**3.8. Extraction Process.** The extraction process is used to extract the hidden image from the embedded process in adjustable order. The cover image used in the first step is not used to extract the secret image. The data is provided by the LSB, and the procedure was enhanced using the secret key.

#### 3.8.1. Algorithm for Extraction Process in IWT-LSB

- (1) Stego-image is read.
- (2) Median filter is applied.
- (3) IWT is applied for stego-image.
- (4) The secret data is extracted for the approximate image coefficient of stego-image.
- (5) Until the secret data is extracted, step 4 will be continued.
- (6) Inverse IWT is applied.
- (7) Image gets extracted.
- (8) Extract the secret data.

#### 3.9. Special Cases

**3.9.1. IWT-LSB Algorithm for Grayscale Image.** The proposed hybrid IWT-LSB technique for grayscale images involves an embedding phase and an extraction phase as shown in Figure 6. In the embedding phase, the grayscale cover image is transformed using IWT, then the secret text is embedded in the LSBs of the cover image's coefficients, and finally the inverse IWT is used to construct the stego-image. Without knowing anything about the original image, the hidden text might be extracted throughout the extraction process. The hidden secret text is retrieved from the LSBs of the filtered stego-image's coefficients, and the inverse IWT is useful for creating the extracted image.

The  $512 \times 512$  bitmap grayscale images are utilized as cover images for the hybrid IWT-LSB algorithms on grayscale images. The size of the estimated coefficient images after performing the IWT is  $256 \times 256$ , which implies that a secret text with up to 8 and 192 digits may be secured. To improve the system's robustness and secure the message from external impacts such as noise, compression, and filtering, the secret data is placed in the LSBs of the estimated coefficient images of the cover images.

**3.9.2. IWT-LSB Algorithm for Color Image.** The color image is split into R, G, and B components in the proposed methodology, and the three components are employed to hide data as shown in Figure 7. In the embedding phase, the RBG component is used to decompose the color of cover image in which the IWT transform is used with the signature of the user and the secret data is embedded with actual

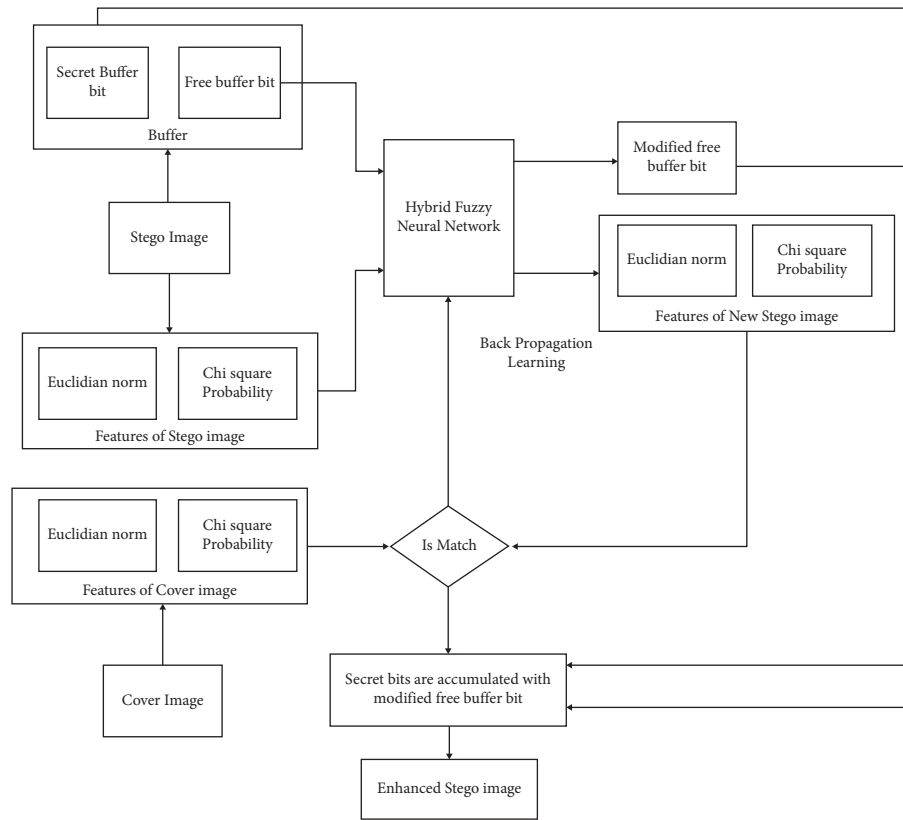


FIGURE 5: Quality enhancement of stego-image using HFNN.

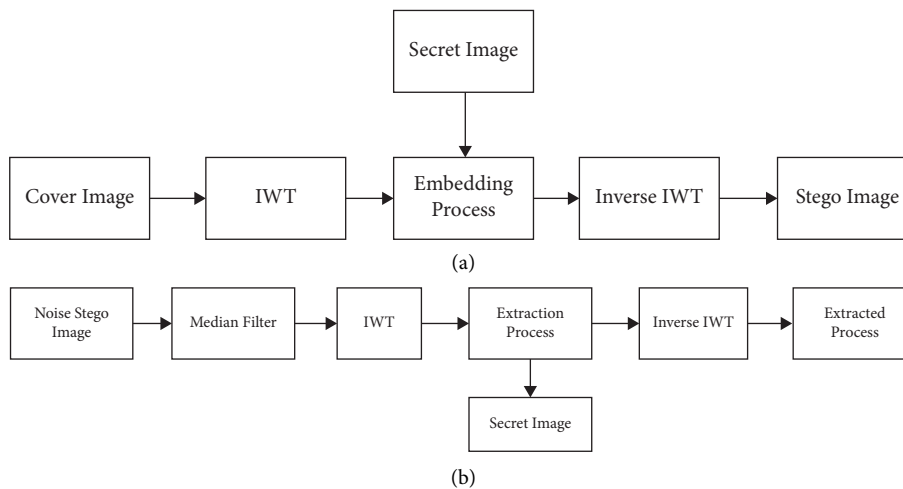


FIGURE 6: Proposed embedding and extraction process for grayscale image steganography.

length in LSB and coefficient image is approximated for the red component of cover image. The image's approximated green and blue components coefficient are used to secure the secret data. Then, the inverse IWT is applied to each component once the embedding process is complete, and then these components are recombined to generate a stego-image.

The hidden data may be extracted during the extraction process without knowing anything about the original image. The R, G, and B components are decomposed from the noisy stego-image in which median filter is utilized for filtering

and then transformed using IWT. The LSB of the approximated image coefficient is used for extracting the actual length of the secret image by utilizing the G and B components, and the inverse IWT is utilized to extract the original image.

#### 4. Result and Discussion

The result of the IWT-LSB algorithm for the steganography image such as grayscale image and color image is analyzed.



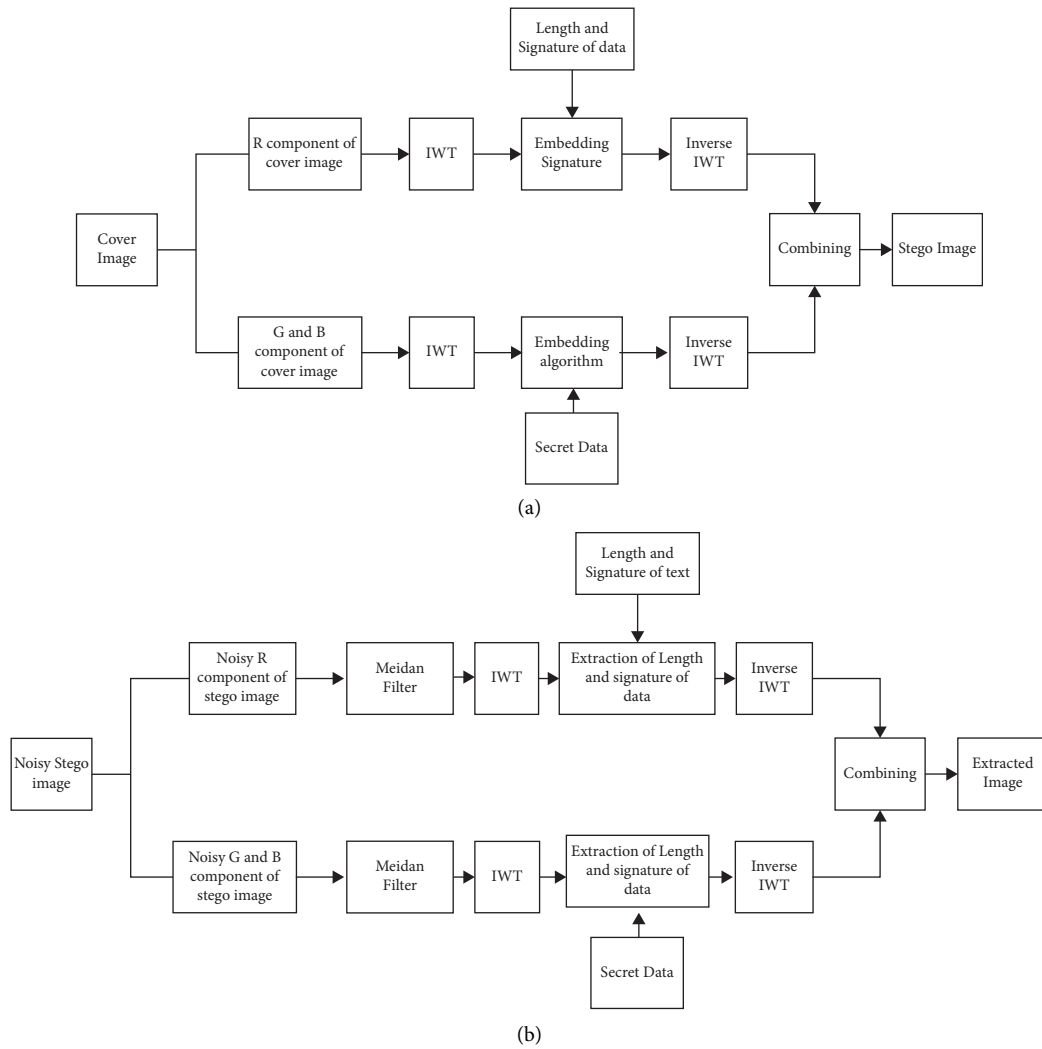


FIGURE 7: Proposed embedding and extraction process for color image steganography.

Parameters such as MSE, NCC, and PSNR are used for the performance evaluation. The error among the cover image and stego-image is examined using MES and PSNR and compared with the existing techniques.

The cover image is represented as  $I_C$ , and stego-image is represented as  $I_S$ . The mean square error is calculated using the following equation:

$$MSE = \frac{1}{nm} \sum_{a=0}^{m-1} \sum_{b=0}^{n-1} [I_S(a, b) - I_C(a, b)]^2. \quad (21)$$

The peak to signal noise ratio is given as

$$PSNR = 10 \log \left( \frac{I_{max}^2}{MSE} \right). \quad (22)$$

The number of rows and columns is represented as  $n$  and  $m$ , and  $I_{max}$  is the maximum hold of the original image.

The similarity and dynamic extent of the cover image and secret image are quantified using the mean square error. The mean square error in the total number of pixels in color and grayscale image is given in Figure 8.

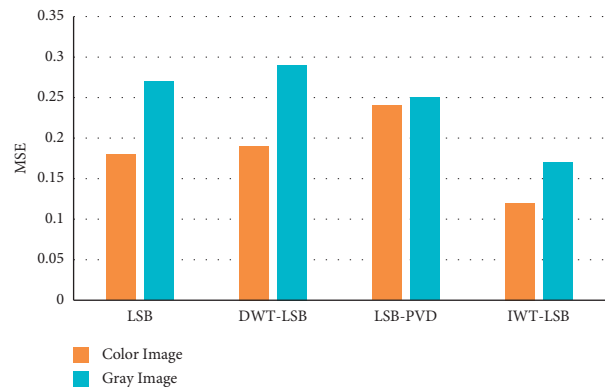


FIGURE 8: Comparison of mean square in color and grayscale image using proposed and existing technique.

The PSNR of the suggested algorithm compared with the existing technique is given in Figure 9. The PSNR regulates the difference in the dynamic range of invisibility in cover image and secret image in which the value is greater than

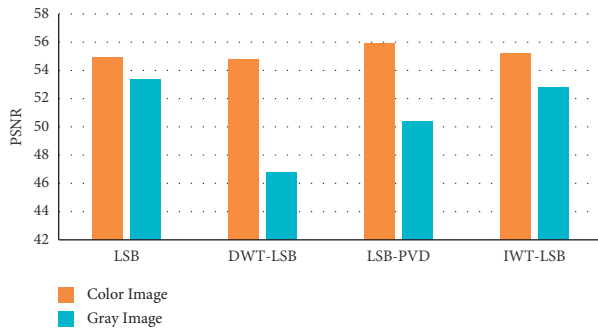


FIGURE 9: Comparison of PSNR in color and grayscale image using proposed and existing technique.

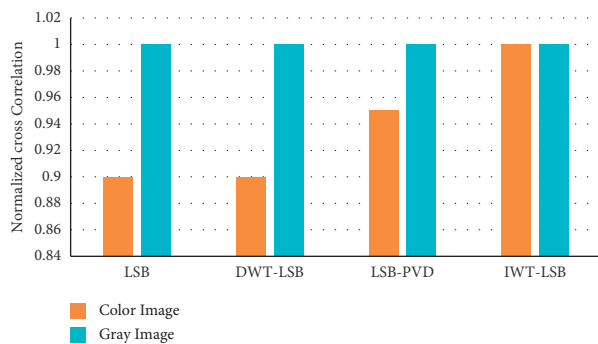


FIGURE 10: Comparison of NCC in color and grayscale image using proposed and existing technique.

53 dB in grayscale and color image compared to the existing techniques.

The degree of closeness between the cover image and stego-image is obtained using NCC which is shown in Figure 10. The degree of closeness is obtained after embedding the data in the secret image.

## 5. Conclusion

This paper used image steganography to securely and imperceptibly embed the patient's personal information in their medical images to enhance confidentiality in case of distant diagnosis. The least significant bit of the approximate coefficient of integer wavelet transform is proposed. This technique is analyzed for grayscale image and color image. IWT is utilized to hide the secret image in LSB in the grayscale image, while IWT with R, B, and G component is used for hiding the secret image in color image. The distortion between the cover image and stego-image is obtained by measuring the mean square error and PSNR, and the degree of closeness between the cover image and stego-image is estimated by utilizing the normalized cross-correlation. The result shows that the IWT-LSB technique can hide secret data with large length with better MSE, PSNR, and NCC.

## Data Availability

The data used to support the findings of this study are included within the article.

## Conflicts of Interest

The author declares that she has no conflicts of interest to report regarding the present study.

## Acknowledgments

The author would like to thank the Deanship of Scientific Research at Princess Nourah Bint Abdulrahman University.

## References

- [1] A. A. J. Altaay, S. B. Sahib, and M. Zamani, "An introduction to image steganography techniques," in *Proceedings of the International Conference on Advanced Computer Science Applications and Technologies*, pp. 122–126, ACSAT, Kuala Lumpur, Malaysia, November 2012.
- [2] K. A. Al-Afandy, O. S. Faragallah, A. Elmhawly, E.-S. M. El-Rabaie, and G. M. El-Banby, "High security data hiding using image cropping and LSB least significant bit steganography," in *Proceedings of the 4th IEEE International Colloquium on Information Science and Technology (CiSt)*, pp. 400–404, IEEE, Tangier, Morocco, October 2016.
- [3] A. Elhadad, S. Hamad, A. Khalifa, and A. Ghareeb, "High capacity information hiding for privacy protection in digital video files," *Neural Computing & Applications*, vol. 28, no. 1, pp. 91–95, 2017.
- [4] S. Hamad, A. Khalifa, and A. Elhadad, "A blind high-capacity wavelet-based steganography technique for hiding images into other images," *Advances in Electrical and Computer Engineering*, vol. 14, no. 2, pp. 35–42, 2014.
- [5] M. Hashim and M. Rahim, "Image steganography based on odd/even pixels distribution scheme and two parameters random function," *Journal of Theoretical and Applied Information Technology*, vol. 95, no. 22, 2017.
- [6] B. M. Krishna, C. Santhosh, S. Suman, and S. K. Shireen, "Systems, and computers, "evolvable hardware-based data security system using image steganography through dynamic partial reconfiguration," *Journal of Circuits, Systems, and Computers*, vol. 31, no. 1, Article ID 2250014, 2022.
- [7] C. Qin, W. Zhang, F. Cao, X. Zhang, and C.-C. Chang, "Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection," *Signal Processing*, vol. 153, pp. 109–122, 2018.
- [8] Q. Li, X. Liao, G. Chen, and L. Ding, "A novel game-theoretic model for content-adaptive image steganography," in *Proceedings of the IEEE 37th International Conference on Distributed Computing Systems Workshops*, pp. 232–237, ICDCSW, Atlanta, GA, USA, June 2017.
- [9] D. B. Khadse and G. Swain, "Data hiding using quotient value differencing and remainder value substitution avoiding incorrect extraction problem," *Sensing and Imaging*, vol. 22, no. 1, pp. 1–21, 2021.
- [10] R. Sonar and G. Swain, "A hybrid steganography technique based on RR, AQVD, and QVC," *Information Security Journal: A Global Perspective*, pp. 1–20, 2022.
- [11] R. Sonar and G. Swain, "Steganography based on quotient value differencing and pixel value correlation," *CAA Transactions on Intelligence Technology*, vol. 6, no. 4, pp. 504–519, 2021.
- [12] G. Swain and A. Pradhan, "Image steganography using remainder replacement, adaptive QVD and QVC," *Wireless Personal Communications*, vol. 123, no. 1, pp. 273–293, 2022.

- [13] S. I. Nipanikar, V. Hima Deepthi, and N. Kulkarni, "A sparse representation based image steganography using particle swarm optimization and wavelet transform," *Alexandria Engineering Journal*, vol. 57, no. 4, pp. 2343–2356, 2018.
- [14] G. Swain, "Adaptive and non-adaptive PVD steganography using overlapped pixel blocks," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7549–7562, 2018.
- [15] G. Swain, "A data hiding technique by mixing MFPVD and LSB substitution in a pixel," *Information Technology and Control*, vol. 47, no. 4, pp. 714–727, 2018.
- [16] G. Swain, "Two new steganography techniques based on quotient value differencing with addition-subtraction logic and PVD with modulus function," *Optik*, vol. 180, pp. 807–823, 2019.
- [17] S. Arunkumar, V. Subramaniaswamy, V. Vijayakumar, N. Chilamkurti, and R. Logesh, "SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images," *Measurement*, vol. 139, pp. 426–437, 2019.
- [18] E. S. B. Hureib and A. A. Gutub, "Enhancing medical data security via combining elliptic curve cryptography with 1-LSB and 2-LSB image steganography," *International J Comp Sci Network Security (IJCSNS)*, vol. 20, no. 12, pp. 232–241, 2020.
- [19] A. Anees, A. M. Siddiqui, J. Ahmed, and I. Hussain, "A technique for digital steganography using chaotic maps," *Nonlinear Dynamics*, vol. 75, no. 4, pp. 807–816, 2014.
- [20] Z. Xia, X. Wang, X. Sun, Q. Liu, and N. Xiong, "Steganalysis of LSB matching using differences between nonadjacent pixels," *Multimedia Tools and Applications*, vol. 75, no. 4, pp. 1947–1962, 2016.
- [21] M. Sajjad, K. Muhammad, S. W. Baik et al., "Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3519–3536, 2017.
- [22] A. Elhadad, A. Ghareeb, and S. Abbas, "A blind and high-capacity data hiding of DICOM medical images based on fuzzification concepts," *Alexandria Engineering Journal*, vol. 60, no. 2, pp. 2471–2482, 2021.
- [23] S. Kaur, S. Bansal, and R. K. Bansal, "Steganography and classification of image steganography techniques," in *Proceedings of the International Conference on Computing for Sustainable Global Development*, pp. 870–875, IEEE, New Delhi, India, March 2014.
- [24] V. Thanikaiselvan and P. Arulmozhivarman, "High security image steganography using IWT and graph theory," in *Proceedings of the IEEE International Conference on Signal and Image Processing Applications*, pp. 337–342, IEEE, Melaka, Malaysia, October 2013.
- [25] A. Abdelaziz, M. Elhoseny, A. S. Salama, and A. M. Riad, "A machine learning model for improving healthcare services on cloud computing environment," *Measurement*, vol. 119, pp. 117–128, 2018.
- [26] A. Arya and S. Soni, "Performance evaluation of secret image steganography techniques using least significant bit (LSB) method," *International Journal of Computer Science Trends and Technology*, vol. 6, no. 2, pp. 160–165, 2018.
- [27] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy, and A. Ghoneim, "Secure quantum steganography protocol for fog cloud internet of things," *IEEE Access*, vol. 6, pp. 10332–10340, 2018.
- [28] A. S. Anwar, K. K. A. Ghany, and H. E. Mahdy, "Improving the security of images transmission," *International Journal of Bio-Medical Informatics and E-Health*, vol. 3, no. 4, pp. 7–13, 2015.
- [29] M. Jain, R. C. Choudhary, and A. Kumar, "Secure medical image steganography with RSA cryptography using decision tree," in *Proceedings of the 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 291–295, Noida, India, December 2016.
- [30] S.-J. Horng, S.-F. Tzeng, Y. Pan et al., "b-SPECS+: batch verification for secure pseudonymous authentication in VANET," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.
- [31] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'," *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.
- [32] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, "Medical JPEG image steganography based on preserving inter-block dependencies," *Computers & Electrical Engineering*, vol. 67, pp. 320–329, 2018.
- [33] M. Elhoseny, G. Ramirez-Gonzalez, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.
- [34] H. E. Rostam, H. Motameni, and R. Enayatifar, "Privacy-preserving in the Internet of Things based on steganography and chaotic functions," *Optik*, vol. 258, Article ID 168864, 2022.
- [35] R. Eswaraiyah and E. Sreenivasa Reddy, "Robust medical image watermarking technique for accurate detection of tamper inside region of interest and recovering original region of interest," *IET Image Processing*, vol. 9, no. 8, pp. 615–625, 2015.
- [36] N. Sahu, D. Peng, and H. Sharif, "Diagnosis-steganography-transmission: an innovative integrated paradigm for ECG healthcare," *SN Computer Science*, vol. 2, no. 4, pp. 1–22, 2021.
- [37] S. Al-Refai and M. M. Al-Jarrah, "Secure data hiding technique using batch video steganography," in *Proceedings of the 2nd International Conference on Information Hiding and Image Processing*, pp. 1–4, ACM, London, United Kingdom, September 2019.
- [38] S. Li and X. Zhang, "Toward construction-based data hiding: from secrets to fingerprint images," *IEEE Transactions on Image Processing*, vol. 28, no. 3, pp. 1482–1497, 2018.
- [39] A. I. Taloba, A. A. Sewisy, and Y. A. Dawood, "Accuracy enhancement scaling factor of Viola-Jones using genetic algorithms," in *Proceedings of the 14th International Computer Engineering Conference (ICENCO)*, pp. 209–212, Giza, Egypt, December 2018.
- [40] A. I. Taloba and S. S. Ismail, "An intelligent hybrid technique of decision tree and genetic algorithm for e-mail spam detection," in *Proceedings of the 9th International Conference on Intelligent Computing and Information Systems (ICICIS)*, pp. 99–104, Cairo, Egypt, December 2019.