A Novel Chaos-based Privacy-Preserving Deep Learning Model for Cancer Diagnosis

Mujeeb Ur Rehman*†, Arslan Shafique†, Yazeed Yasin Ghadi‡, Wadii Boulila§¶, Sana Ullah Jan‖, Thippa Reddy Gadekallu **, Maha Driss¶††, and Jawad Ahmad‖

* James Watt School of Engineering, University of Glasgow, UK † † Department of Electrical Engineering, Riphah International University, Islamabad, Pakistan. ‡ Department of Computer Science and Software Engineering, Al Ain University, Abu Dhabi, 122612, UAE. § Robotics and Internet of Things Lab, Prince Sultan University, Riyadh, Saudi Arabia. ¶ RIADI Laboratory, University of Manouba, Manouba, Tunisia. ‖ School of Computing, Edinburgh Napier University, Edinburgh, EH10 5DT, United Kingdom. ** School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632014, India. †† Security Engineering Lab, CCIS, Prince Sultan University, Riyadh, Saudi Arabia.

Abstract—Early cancer identification is regarded as a challenging problem in cancer prevention for the healthcare community. In addition, ensuring privacy-preserving healthcare data becomes more difficult with the growing demand for sharing these data. This study proposes a novel privacy-preserving non-invasive cancer detection method using Deep Learning (DL). Initially, the clinical data is collected over the Internet via wireless channels for diagnostic purposes. It is paramount to secure personal clinical data against eavesdropping by unauthorized users that may exploit it for personalized interests. Therefore, the collected data is encrypted before transmission over the channel to prevent data theft. Various security measures, including correlation, entropy, contrast, structural content, and energy, are used to assess the proposed encryption method's efficiency. In this paper, we proposed using the Convolutional Neural Network (CNN)-based model and Magnetic Resonance Imaging (MRI) with different techniques, including transfer learning, fine-tuning, and K-fold analysis cancer detection. Extensive experiments are carried out to evaluate the performance of the proposed DL techniques with regard to traditional machine learning approaches such as Decision Tree (DT), Naive Bayes (NB), Random Forest (RF), and Support Vector Machine (SVM). Results show that the CNN-based model has achieved an accuracy of 98.9% and outperforms conventional ML algorithms. Further experiments demonstrate the efficiency of both encryption schemes, achieving entropy, contrast, and energy of 7.9999, 10.9687, and 0.0151, respectively.

1 Introduction

Cancer is notoriously difficult to identify in its early stages. Furthermore, cancer becomes more prone to growing back after treatment if detected after specific stages. Commonly, medical imaging analysis is used for detecting abnormalities in human body, for instance, blood cancer [1], [2], [3], skin cancer [4], brain tumours [5], lung cancer [6], breast cancer [7]. Cancer is actually a tumour developed from organ disorders and is considered one of the leading causes of death worldwide [8]. Statistics indicate that around 18.1 million cancer cases were diagnosed in the single year of 2018, resulting in 9.6 million deaths [9]. These studies report that lung cancer is the leading cause of death with (18.4%) of all deceased. Other causes include colon cancer with (5.8%), breast cancer resulting in (6.6 %), skin cancer (melanoma and non-melanoma) with (1.3%), and prostate cancer causing (3.8%) of all deaths [10].

Early cancer detection has a higher chance of responding to therapy, resulting in a better likelihood of survival, less morbidity, and less expensive treatment [11]. There are different screening ways to detect abnormalities in the body indicative of cancer or pre-cancer (cancer before they develop symptoms), for example, Hepatitis B Virus (HPV) testing, visual examination with acetic acid (VIA), and mammography screening. Main symptoms of cancer include fatigue or extreme tiredness, eating problems, swelling, thickening or lumps in a body part, pain, jaundice, cough or hoarseness, fever, headache, and vision or hearing problems [12]. Furthermore, reliable and definite predictions of cancer prognosis are very challenging. Certain types of cancer are more challenging for early diagnosis because their symptoms are ambiguous, and their tell-tale indications on mammograms and scans are imprecise. Therefore, it is critical to improve prediction models in clinical cancer research by using multivariate data and high-resolution diagnostic methods [13].

Most of the classification models that have been developed in the last few decades are based on supervised learning, in which datasets play a vital role [14]. These datasets are either in the form of images or consent forms that can be corrupted by attackers or eavesdroppers. Intuitively, a set of accurate data enhances the accuracy of the supervised learning-based models. Therefore, data security is a crucial aspect that can be achieved through image encryption in the case of image data. There is a plethora of image encryption methods designed to secure digital images that bring along encryption, computer, or security issues [15], [16], [17], [18], [19], [20], [21]. Moreover, it is essential to design an encryption scheme that is able to offer a certain level of security to the digital images with low computation complexity.

This paper contributes in two ways toward the privacy-

preserving cancer detection paradigm. First, clinical data security is enhanced by employing chaos, DWT, and bit-plane extraction methods. Secondly, the cancer diagnosis model is developed using a CNN-based deep learning model. The clinical data in terms of MRI images are acquired at one diagnostic centre (centre A ($\hat{A}$)). This data is then transmitted via an Internet-aided wireless channel to another diagnostic centre that lacks a non-invasive diagnostic machine (centre $\hat{B}$Data may be transmitted by email, which is safe in and of itself but is insufficiently secure to assure data privacy. Therefore, image encryption is adopted for the secure transmission of MRI images. These images are decrypted using the inverse version of the proposed encryption algorithm at the receiver end. Moreover, the patient's report at the receiver end is also encrypted before being sent to the other end. Initially, the patient's report is in text format, but before sending it to the transmission end, it must be scanned and converted into an image form. Therefore, the patient's report can also be encrypted using the proposed encryption algorithm.The data is then fed to the proposed non-invasive model for classification into normal or cancer-positive patients. The result is encrypted and sent back to the centre A ($\hat{A}$), where it will be decrypted for consultation. A flowchart of the pictorial view of the proposed methodology is displayed in Figure 1.

The rest of the paper is organized as follows: Section 2 provides a literature review of the encryption schemes and disease diagnosis methodologies along with vulnerabilities and potential solutions. Section 3 illustrates the proposed encryption scheme to secure the data, and Sections 4 and 5 present the theoretical fundamentals and the proposed diagnosis methodology of the CNN-based cancer diagnosis model, respectively. In section 6, the experimental results are discussed, and finally, section 7 concludes the paper.

2 Related Works

Conventional encryption schemes such as Advanced Encryption Standard (AES) [22] and Data Encryption Standard (DES) [23] are not suitable for securing the images against cyber attacks due to highly correlated data and a large number of encryption rounds. As a result, these schemes increase computational time, a situation not suitable for real-time applications. Furthermore, machine learning has been widely used for disease detection over the last few decades [24], [25], [26], [27], [28], [29], [30]. This section provides an overview of the existing image encryption and disease diagnosis methodologies in the recent literature, along with solutions given in the subsequent subsections.

2.1 Data Encryption Techniques

Multi-round image encryption, proposed by Romi et al. [31], is considered a secure multi-channel approach. Specifically, this approach is designed to handle a small amount of data or images. Large computational time and weak security of images with highly correlated data present a risk that needs to be overcome. Selective encryption can be used to speed up overall encryption computations while keeping an eye out for these flaws. In order to address these issues, Yinan et al. [32] presented DNA origami cryptography (DOC) as a security technique for secure communication. However, the small key size makes it vulnerable to brute force attacks, but this strategy works effectively and offers a sufficient amount of integrity throughout the communication. In order to withstand a brute force assault, Alvazari [33] suggested a key-space of 2^{100} to resist the brute force attack. As a result, the key size should be raised to improve security.

In [34], Li et al. introduced an image encryption technique based on chaos that incorporates dynamic variable selection and orbit perturbation processes. To obtain random numbers, logistic and chaotic sine maps are utilized to expand the keyspace enough to withstand a brute force attack. While the security level is maintained, both chaotic maps [35], [36] are implemented sequentially rather than in parallel. As a result, the execution time is quite lengthy, which is inconvenient for real-time applications. In [37], Sivakumar et al. used scan patterns and real random streams, which are generated using chaos theory, to present a chaos-based image encryption scheme. The scan pattern is used to permute the image pixels. Moreover, a random key is created using a photonics-based technique and is then utilized to execute an XOR operation which is performed bit-by-bit to generate the final encrypted image. Because the authors reduced the time complexity of their suggested encryption technique only via permutation operations, the security level is compromised for two primary reasons. Firstly, their suggested approach makes use of just a few elementary mathematical operations. Second, no diffusion operation is included. According to Claud Shannon's confusion and diffusion criteria [38], an encryption system must have both confusion and diffusion operations in order to be secure. In [39], Kaur et al. proposed a chaos-based image encryption scheme in which piecewise linear chaotic maps (PWLCM) is used to generate a random number for permutation and confusion purposes. Unlike one-dimensional chaotic maps such as chaotic logistic maps [40], PWLCM is a high-dimensional chaotic map that performs better than all other one-dimensional chaotic maps [41], [42], [43], [44]. Kamrani et al. [45] proposed an encryption system based on confusion and diffusion operations utilising two chaotic logistic maps. To strengthen the security of their suggested encryption algorithm, the authors fulfilled Shannon's criteria for a confusion-diffusion mechanism. However, since both processes are implemented sequentially, completing all of the mathematical operations in their proposed work takes a long time.

An image encryption scheme for medical imaging like MRI and X-ray suggested in [46] by Rehman et al. has a tiny key-space and lack of security issues. Chaos and substitution boxes (S-boxes) are used to tackle both of these problems. For enlarging the key-space, multiple chaotic maps are used, in which six key parameters and the key sensitivity of each are 10^{15}, which means that the total key-space will be at least 2^{200} which is large enough to resist a brute force attack. In addition, S-boxes, which substitute image pixels according to the substitution algorithm, enhance the security of encrypted images. Guodong et al. [47] developed an image encryption scheme based on frequency and spatial encryption. The Discrete Cosine Transform is used for frequency-domain encryption, whereas a substitution-permutation procedure is used for spatial domain encryp-

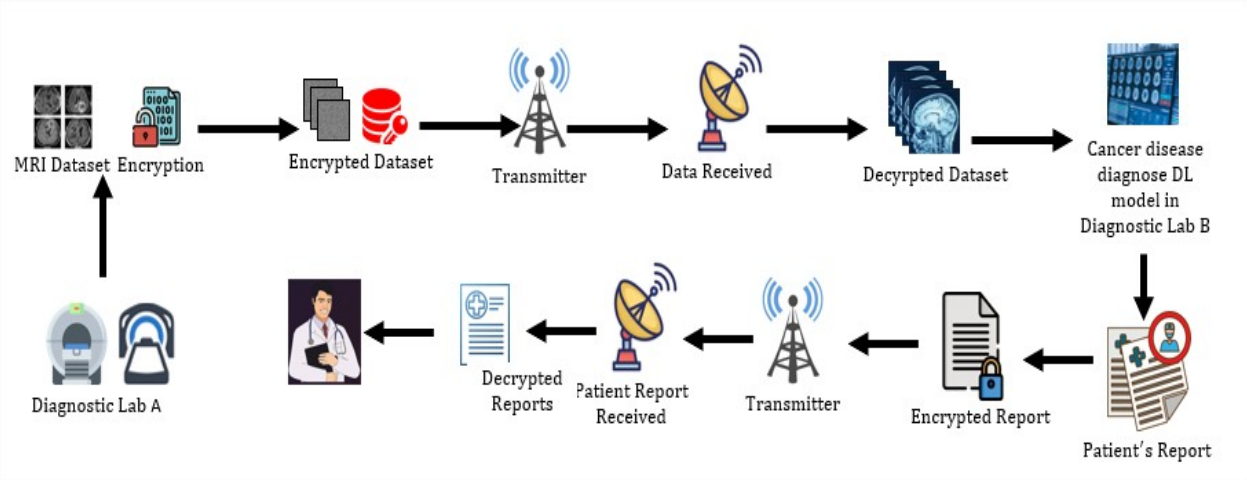


Fig. 1: Overview of the proposed research

tion. This method is capable of encrypting digital images quickly and securing them at a higher level. Statistical analyses, such as correlation, entropy, contrast, and energy analysis, are used to demonstrate a level of security. This method provides convincing results. However, it is not robust against noise or cropping attacks. In [48], a method for encrypting multiple images using the Lyapunov, phase, and bifurcation diagrams is proposed. In this scheme, to ensure the integrity of the original image, numerous grayscale photos are fused together. Using a hyperchaotic system with numerous encryption rounds, a random sequence is created for scrambling, resulting in a higher encryption computation time.

2.2 Machine Learning-based Disease Detection

In [49], Onur et al. proposed a three-dimensional convolutional neural network-based nodular lung disease detection and diagnosis method where a publicly accessible dataset on Kaggle is used to train the model. While the detection and diagnosis systems are developed individually, it has been discovered that linking the detection and diagnostic components is critical. By leveraging this connection, an end-to-end system is created that performs better and is more durable, obviating the need for a false positive reduction phase during nodule identification. The systems' overall accuracy is 95%, which is insufficient for swearing instances, such as those involving patients who are swearingly suffering from a lung illness. In [50], Rishav et al. discussed unbalanced datasets to highlight their associated problems. They found, for example, that if the overall number of cases for a specific class is significantly high than the acceptable number, this may result in inaccurate classifications. A transfer learning-based image classification can be used to address this problem.

A well-known VGG-19 is also being considered to increase the system's efficiency. VGG-19 is a convolutional neural network and has 19 layers [51]. This is accomplished by using an ImageNet dataset and applying machine learning techniques to identify various subjects, such as a breast cancer patient or a normal subject. To maintain nearly one to one ratio of images from normal subjects and patients in the collection, 277,524 images are taken. When the various methodologies are compared, the methodology provided in [50] outperforms, with an accuracy of 90.3%. In [52], a Stacked Sparse Autoencoder (SSAE)-based deep learning approach for efficiently detecting nuclei in high-resolution histopathology images of breast cancer is proposed. In order to determine the nuclei's distinguishing features, the SSAE learns high-level features from pixel intensities alone. Image patches are represented by high-level features derived from the autoencoder, which are then input to a classifier that classifies each patch as either nuclear or nonnuclear. Although the methodology proposed in [52] is able to classify them, the overall accuracy is 78.83%, which is not acceptable in sensitive medical decisions. In [14], Yi et al. proposed a methodology to detect breast cancer using Automated Breast Ultrasound (ABUS), in which a 3D convolutional neural network is incorporated. Specifically, a supervision method is presented in which a classification of cancer patients and healthy subjects is performed using multilayer architecture. The dataset is composed of 899 cases, of which 754 are from cancer patients and 144 are from healthy persons. The system performance is tested using several metrics such as accuracy, precision, F1-score, and recall. The experimental results show that this system can classify with an accuracy of up to 95%.

Apart from CNN, several different deep learning models such as Deep Belief Networks (DBN), recurrent neural networks (RNN), and deep Boltzmann machines (DBM) have also been used in medical applications such as disease diagnosis. In [53], Altan et al. proposed a methodology to detect breast cancer using DBN in which different medical images are used as a dataset. To detect breast cancer, statistical and physiological features are extracted from the images used in the dataset. The accuracy of his proposed model is 96.4% which is quite good yet insufficient for effectively detecting malignant disorders. In [54], Patil et al. used image processing, segmentation, and RNN to detect breast cancer from medical images. Moreover, to enhance the proposed work, an optimized hybrid classifier is also incorporated. Original medical images contained a lot of noise. So, a median filter is used on the images in the dataset to remove the noise,

which makes the model more optimized and accurate. Li et al. [55] developed a future forecasting system that detects an early cancer disease in which DBM are used. There is no segmentation or noise reduction, which reduces the accuracy of their suggested model, which is unacceptable for real-time cancer illness diagnosis. Antropova et al. [56] proposed a technique for breast lesion classification based on recurrent and convolutional neural networks. The training phase is used to develop long-term, short-term memory (LSTM). To capture local variations in lesion enhancement, features from numerous pre-trained CNNs are retrieved. Additionally, the performance of the LSTM is compared to that of the CNN, with the LSTM outperforming the CNN. Their planned work is 93% accurate.

Keeping in mind the challenges pointed out in the literature, this paper proposed novel data encryption and disease diagnosis techniques. The major contributions of this work are summarized in the following subsection.

2.3 Contributions

According to the WHO report, efficient cancer detection and diagnosis are paramount to reducing the resulting rate of casualties [57]. The contributions of this work are as follows.

- To enhance the security of medical data, a chaos-based image encryption technique is presented and compared with existing schemes to demonstrate the proposed encryption scheme's efficiency.
- Primary clinical data has been collected from three hospitals in Rawalpindi and Islamabad, Pakistan.
- We devised a method for accurately predicting the occurrence of cancer that may be deployed using a smartphone application. The suggested technique makes use of CNN as a classification algorithm.
- Additionally, a K-fold analysis and voting technique are utilized to select a particular subset of the data, and as a result, the proposed model provides higher accuracy.
- Various performance metrics like precision, recall, and F1 score are used to validate the proposed model in addition to the commonly used accuracy measure. Furthermore, transfer learning and fine-tuning techniques are performed for further performance enhancement.

3 Proposed Data Encryption Scheme

The proposed algorithm for data security contains four main ingredients: (a) Bit-plane extraction, (b) Discrete Wavelet Transform (DWT), (c) Confusion (Permutation); and (d) Diffusion (Substitution using substitution box (S-box). As mentioned in the literature, chaos-based encryption schemes offer several benefits, including their sensitivity to initial conditions, difficult-to-predict, and huge keyspace, which leads to better outcomes than frequency-based encryption [58], [59], [60]. Thus, chaos-based encryption is employed to secure the medical data used in the proposed work to an appropriate degree of security. Numerical analysis of the chaos-based and frequency-based encryption schemes is performed in [61], and it is clearly stated that chaos-based encryption schemes may generate more random enciphered images than frequency-based encryption schemes.

To generate random sequences, a Cubic Logistic chaotic map (CLCM) is used, which is one-dimensional. It is worth mentioning here that high-dimensional chaotic maps are more secure, but it also takes more time to execute. Therefore, for time reduction, a low-dimensional chaotic map is considered in the proposed encryption algorithm. However, to enhance the security level of encrypted medical images, multiple encryption methodologies such as bit-plane extraction, chaos theory, confusion, and diffusion are used.

To reduce the time complexity of the proposed encryption schemes. Only low-frequency bands and the most significant bit plane are considered. Because the low-frequency bands and most significant bits contained most of the plaintext information. The block diagram of the proposed encryption technique is given in Figure 2, and Figure 3 illustrates four encrypted images corresponding to the original images.

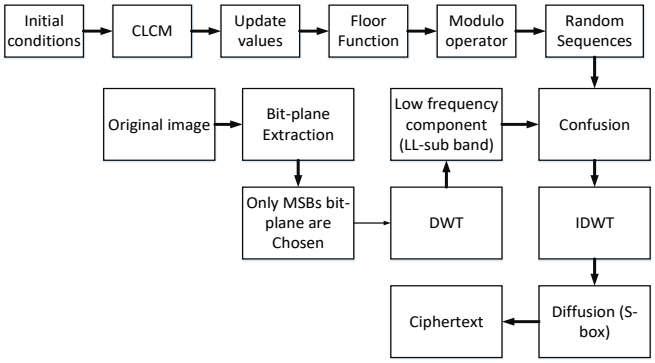


Fig. 2: Block diagram of proposed encryption technique

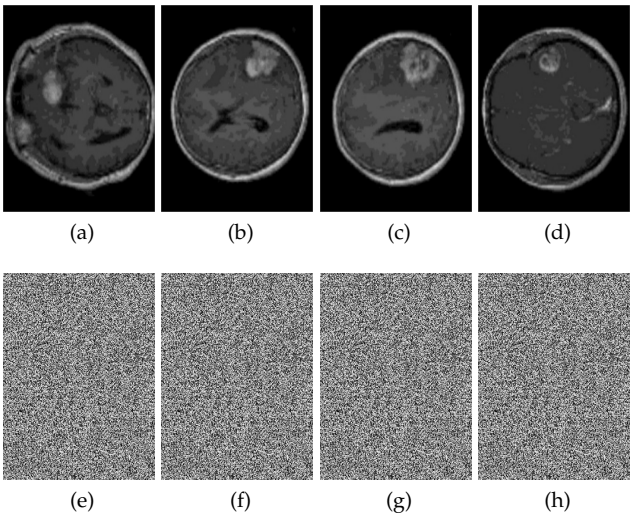


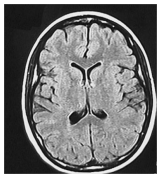
Fig. 3: Original images and their corresponding encrypted images

(a) Bit-plane extraction: The process of extracting binary planes from original image is known as bit plane extraction. The theoretical representation of bit-plane extraction is given in Equation 1:

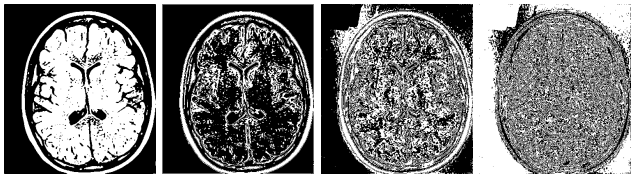
$$\mathbf{I} = \frac{1}{2^{\mathbf{L}}} \sum_{a=0}^{2^{\mathbf{L}}-1} \sum_{b=0}^{2^{\mathbf{L}}-1} I_{a,b}^{\mathbf{L}} \times 2^{\mathbf{L}} \tag{1}$$

Where $\mathbf{L}$ represents the total number of binary bit-planes and its values in range: $\{\ \mathbf{L} |\ \mathbf{L} \in \mathbf{W} \wedge 0 \leq \mathrm{n} \leq 7\ \}$. The individual bit plane can be extracted as: $\mathbf{I}_{a,b}^{'7} \times 2^7$, $\mathbf{I}_{a,b}^{'6} \times 2^6$, $\mathbf{I}_{a,b}^{'5} \times 2^5$, $\mathbf{I}_{a,b}^{'4} \times 2^4$, $\mathbf{I}_{a,b}^{'3} \times 2^3$, $\mathbf{I}_{a,b}^{'2} \times 2^2$, $\mathbf{I}_{a,b}^{'1} \times 2^1$, and $\mathbf{I}_{a,b}^{'0} \times 2^0$. Where, $\mathbf{I}_{a,b}^{'7} \times 2^7$ represents the 8^{th} bit-plane and so on. The amount of plaintext information in the individual bit plane may vary, as can be seen in Figure 4.

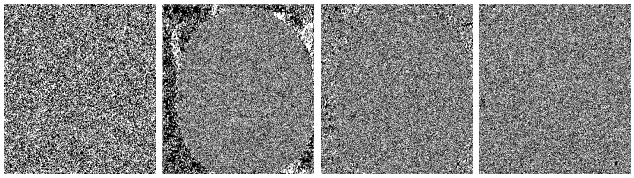
The 8^{th} contains the highest percentage of plaintext information, and the 1^{st} contains the least amount of plaintext information.



(a) Original image



(b) 8^{th} bit plane (c) 7^{th} bit plane (d) 6^{th} bit plane (e) 5^{th} bit plane



(f) 4^{th} bit plane (g) 3^{rd} bit plane (h) 2^{nd} bit plane (i) 1^{st} bit plane

Fig. 4: Binary Plane extracted form original image

The percentage amount of information present in an individual bit plane is displayed in Table 1 and it can be determine using Equation 2 [62].

$$\mathbf{I} = \frac{2^{\mathbf{L-1}}}{\sum_{\mathbf{L=0}}^{7} 2^{-1}} \tag{2}$$

TABLE 1: Percentage amount of information in individual binary bit planes

Bit plane index	Percentage amount of information	Bit plane index	Percentage amount of information
0	0.3000	4	6.2500
1	0.7900	5	12.2300
2	1.4200	6	25.7000
3	3.1200	7	50.2000

The original image form all the extracted binary bit planes can be reconstructed as follows:

$$\mathbf{I}_{a,b} = \mathbf{I}_{a,b}^{'7} \times 2^7 + \mathbf{I}_{a,b}^{'6} \times 2^6 + \mathbf{I}_{a,b}^{'5} \times 2^5 + \mathbf{I}_{a,b}^{'4} \times 2^4 + \mathbf{I}_{a,b}^{'3} \times 2^3 + \mathbf{I}_{a,b}^{'2} \times 2^2 + \mathbf{I}_{a,b}^{'1} \times 2^1 + \mathbf{I}_{a,b}^{'0} \times 2^0 \tag{3}$$

Most of the information from the original image is present in the 8^{th} binary bit plane. Therefore, for enhancing the image security, only the most significant binary bit-planes (8^{th}, 7^{th}, 5^{th} and 4^{th} bit-plane) are considered for the rest of the encryption steps.

(b) Discrete Wavelet Transform: The wavelet components of the signals may be extracted using a wavelet transform. An audio signal's precise features may be separated using wavelets [63]. For example, a wavelet may be used to separate fine details (edges) from low-frequency components. For this, small and enormous wavelets are used to isolate fine and coarse details, respectively.

The plaintext is transformed into various frequencies using the Haar wavelet in the proposed encryption technique. Sub-bands such as the LL, LH, HL, and HH may be extracted using the decomposition of plaintext image by applying DWT.

The Haar waveltes can be expressed as $W = HOH^T$. Where O represents the original image having same numbers of rows (R) and columns (C), H express the haar transform matrix equal to the size of the original image and W represents the transformation matrix which holds haar basis function $h_f(z)$ in which $z \in [01]$ and b may defined as $b|b \in N \wedge 0 \leq b \leq C-1$. Uniquely, it can be decomposed using Equation 4.

$$b = 2^e + s \tag{4}$$

Here, e and s represents the greatest power of 2 and the reminder ($s = 2^e$) respectively. According to Equation 5, haar has a basis function.

$$h_b(z) = \frac{1}{\sqrt{C}} \begin{cases} 1 & \text{if } b = 0 \quad \& \quad 0 \leq f < 1 \\ 2^{e/2} & \text{if } b > 0 \quad \& \quad s/2^e \leq f < \frac{s+0.5}{2^e} \\ -2^{e/2} & \text{if } b > 0 \quad \& \quad (s+0.5)/2^e \leq f < \frac{s+1}{2^e} \\ 0 & \text{anywhere} \end{cases} \tag{5}$$

Equation 6 provides the inverse version of the transformation kernel, which may be substituted to produce a 2D Discrete Haar Wavelet Transform (DHWT).

$$h'(z,b) = \frac{1}{\sqrt{C}} h_b(z/M) \qquad for\ \ z = 0, 1, 2, ..., C-1 \tag{6}$$

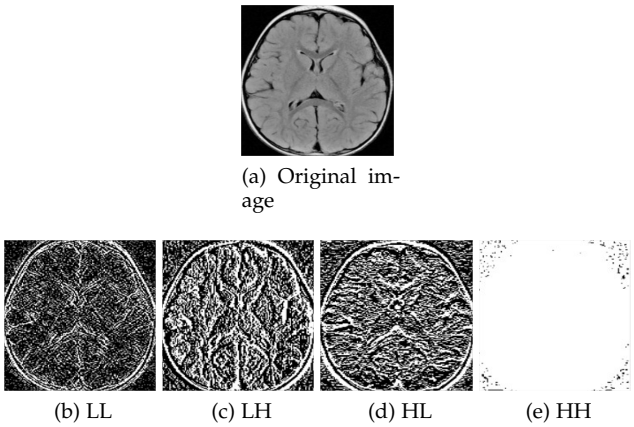
Where, $h_a(w)$ is defined as:

$$h_b(z) = H' = \begin{Bmatrix} h_0(\frac{0}{C}) & h_0(\frac{1}{C}) & ....h_0(\frac{C-1}{C}) \\ h_1(\frac{0}{C}) & h_1(\frac{1}{C}) & ....h_1(\frac{C-1}{C}) \\ h_2(\frac{0}{C}) & h_2(\frac{1}{C}) & ....h_2(\frac{C-1}{C}) \\ . & . & . \\ . & . & . \\ . & . & . \\ h_{C-1}(\frac{0}{C}) & h_{C-1}(\frac{1}{C}) & ...h_{C-1}(\frac{C-1}{C}) \end{Bmatrix} \tag{7}$$

Finally, the transformation matrix for $b = 0, 1, 2, \cdots, C-1$ will be given as:

$$H = \frac{1}{\sqrt{C}} H' \tag{8}$$

High and low-pass filters are used to evaluate each pixel row in the horizontal direction in the case of 2-D signals (images of $I(R, C)$).The result is an image of L_r and H_r with a size of $\frac{R}{2^1} \times \frac{C}{2^1}$. After that, the new images (L_r and H_r) are analyzed in the vertical direction using high-pass and low-pass filters called $\alpha(C)$ and $\beta(C)$. This results in the LL_1, LH_1, HL_1, and HH_1 frequency subbands. Figure 5 shows the four frequency sub-bands generated after applying 2DHWT.

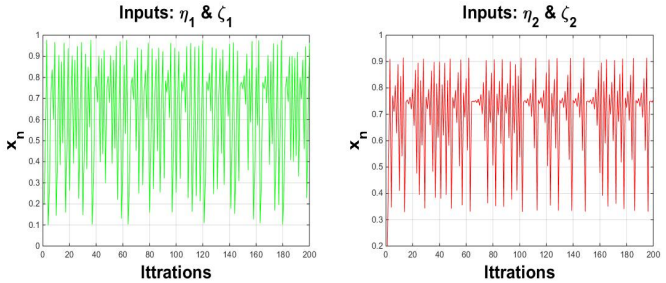


(a) Original image

(b) LL (c) LH (d) HL (e) HH

Fig. 5: Frequency bands extracted from the cameraman image using DWT

(c) Confusion process: As shown in Figure 5, the low-frequency sub-band ($LL\ sub-band$) contains the majority of the information in the original image. As a result, in the proposed encryption scheme, the confusion process is performed only on this sub-band to reduce the overall computational time required for encryption. The confusion process is applied according to a random sequence generated using chaos by incorporating Algorithm 1.



(a) (b)

Fig. 6: Random sequences generated using CLCM

(d) Substitution process: As the scrambled bit-planes consist of several frequencies, it is necessary to convert them into eight-bit integer values using the inverse discrete wavelet transform (IDWT) for the substitution process. Such integer values are replaced by S-box values given in Table 2. The S-box used in the proposed work is proposed by Hussain et al. [64]. The substitution process is explained in Example 1:

Algorithm 1 Random sequence generation module

1: **Input** CLCM and seed values (η_1, ζ_1 (For creating confusion in rows), η_2 and ζ_2 (For creating confusion in columns) where, $\zeta \in$ (0 1) and [1.41 1.63]). The CLCM equation is given as:

$$\zeta_{i+1} = \eta * \zeta_i(1 - \zeta_i) * (2 + \zeta_i) \tag{9}$$

2: **Output**: τ = mod (σ, 256)
3: Using the inputs, generate the random values equal to the number of rows present in the $LLsub-band$.
4: Store the random values in an array, lets say K
5: Update K as follows:

$$\varrho = K_i \times D_{num}$$

D_{num} can be any large number i.e, 999.
6: To convert the decimal values into the real integer numbers, apply the floor function.
7: To restrict the the values in range [0 255], take modulo of the values generated after applying the floor function. Save the integer values in an array (σ).
8: Apply τ sequence to create confusion in the rows and columns of the $LLsub-band$. The random sequence for row and columns scrambling is shown in Figure 6.
9: **End**

Example 1: Lets take a small portion of an image generated after taking IDWT is:

$$I = \begin{bmatrix} 80 & 156 & 205 \\ 246 & 90 & 50 \\ 183 & 120 & 165 \end{bmatrix}$$

Convert the pixel values of the image I into binary values:

$$\begin{bmatrix} 01010000 & 10011100 & 11001101 \\ 11110110 & 01011010 & 00110010 \\ 10110111 & 01111000 & 10100101 \end{bmatrix}$$

Convert all the eight bits of each pixel into two groups containing four bits each.

$$\begin{bmatrix} \{(0101), (0000)\} & \{(1001), (1100)\} & \{(1100), (1101)\} \\ \{(1111), (0110)\} & \{(0101), (1010)\} & \{(0011), (0010)\} \\ \{(1011), (0111)\} & \{(0111), (1000)\} & \{(1010), (0101)\} \end{bmatrix}$$

$$\begin{bmatrix} \{R:5, C:0\} & \{R:9, C:12\} & \{R:12, C:13\} \\ \{R:15, C:6\} & \{R:5, C:12\} & \{R:3, C:2\} \\ \{R:11, C:7)\} & \{R:7, C:8\} & \{R:10, C:6\} \end{bmatrix}$$

Replace the values with the corresponding S-box values to create diffusion in the input values. The encrypted matrix will be:

$$\begin{bmatrix} 198 & 71 & 79 \\ 83 & 104 & 82 \\ 251 & 174 & 73 \end{bmatrix}$$

The purpose of choosing low-frequency bands and the most significant bit plane in the proposed encryption

TABLE 2: S-box

254	132	255	222	122	15	53	115	145	150	225	175	78	64	184	93
87	19	27	95	246	252	113	59	228	207	101	180	161	154	152	149
238	85	229	91	89	37	26	143	114	123	0	190	51	164	75	237
249	240	82	28	196	209	230	203	105	6	31	217	72	118	226	176
42	253	116	108	163	120	80	131	221	16	97	8	88	153	169	170
198	34	11	21	46	247	67	20	125	36	76	155	104	102	128	179
139	214	148	50	121	12	158	216	189	210	185	232	197	110	231	146
5	109	244	127	77	3	1	107	174	117	181	61	142	124	168	172
41	62	239	29	10	58	25	66	151	47	52	43	212	79	191	173
200	65	39	242	7	166	233	201	219	74	177	144	71	183	63	171
137	2	204	24	14	248	73	135	81	17	178	136	157	167	156	165
9	35	130	235	90	40	133	251	182	140	193	100	55	79	220	162
86	213	23	70	111	194	245	38	186	4	224	147	22	223	98	159
250	112	84	141	18	57	160	205	60	199	99	211	13	92	94	187
40	56	241	234	54	68	33	126	45	138	32	48	206	208	96	188
202	69	30	106	134	227	83	236	192	129	103	215	243	218	119	195

scheme is to reduce the overall encryption computational time. The low-frequency bands and most significant bits contained most of the plaintext information. Therefore, there is no need to encrypt all the sub-bands and bit-planes except the LL sub-band and the most significant bit-planes.

There will be no information loss on the receiving end while the original information is being recovered because both the DWT and bit-plane extraction methods have inverse processes that have the ability to recover the exact pixel values of digital images.

4 Convolutional Neural Networks (CNN)

Several methodologies for detecting a tumour using machine learning (ML) algorithms have been proposed in recent years [65], [66], [67]. From the literature, the accuracy achieved via using ML algorithms is not acceptable. Therefore, a deep learning algorithm known as CNN is used to enhance the performance of the proposed classification task.

CNN has dominated the machine vision area in recent years. A CNN comprises multiple layers: hidden, input, and output. CNN often uses convolutional, pooling, fully connected, and normalizing layers as hidden layers. Additional layers may be used for more advanced models. Figure 7 illustrates examples of a conventional CNN [68].

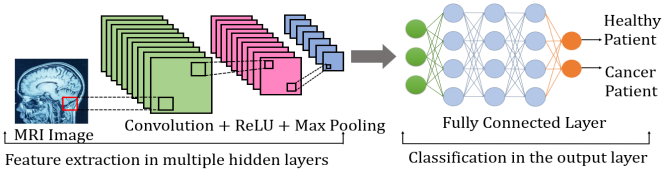


Fig. 7: CNN architecture

The vector calculus and chain rule may be applied in the CNN learning process.

Take $x \in R^X$ and S as a vector and any scalar $(i.eS \in R)$ respectively. The partial derivative of S with respect to w will be:

$$\frac{\partial S}{\partial w} = \frac{\partial S}{\partial w_i} \tag{10}$$

w and $\frac{\partial S}{\partial w}$ will be same in size and $\frac{\partial S}{\partial w}$ is the i^{th} element. Moreover, an assumption is made i.e $\mathbf{N} \in R^L$ and $\frac{\partial S}{\partial w^R} = \frac{\partial S}{\partial w})^R$. For this scenario, the partial derivative of S will be as under:

$$\left[\frac{\partial w}{\partial \mathbf{N}^R}\right]_{il} = \frac{\partial w_i}{\partial \mathbf{N}_i} \tag{11}$$

Whereas, $\frac{\partial S}{\partial \mathbf{N}^R}$ can be determined using the chain rule as defined in Equation 12.

$$\frac{\partial S}{\partial \mathbf{N}^R} = \left[\frac{\partial S}{\partial \mathbf{N}^R}\right]\left[\frac{\partial w}{\partial \mathbf{N}^R}\right] \tag{12}$$

The difference between the outcomes $u, \mathbf{N}^1 \rightarrow L^1, \mathbf{N}^2 \rightarrow L^1, \cdots \mathbf{N}^L \rightarrow T^L = S$ and $CNN's$ $\mathbf{N}^M$ may determine using the loss function i.e $S = |u - \mathbf{N}^M|^2$. Therefore, the convolution is stated that:

$$w_{i^{k+1}.l^{l+1},c} = \sum_{i=0}^{Q}\sum_{l=0}^{L}\sum_{c=0}^{\mathbf{E}} h_{i.l.c} \times \mathbf{N}^M_{i^{k+1}+i,l^{k+1}+l,c} \tag{13}$$

The convolution size depends on the size of filter. i.e, if filter (h) size is $(O \times L \times \mathbf{E}^k)$, the size of the convolution will be: $(O - O + 1) \times (L^k - L + 1)$ with $\mathbf{E}$ slices that means $z(w^{k+1})$ in $Q^{O^{k+1} \times L^{k+1} \times \mathbf{E}^{k+1}}$, O^{k+1} = O^k - O + 1, L^{k+1} = L^k - L + 1, $\mathbf{E}^{k+1}$ = $\mathbf{E}$.

Equation 14 can be used to calculate the probability of each symbol is $T \in \{1, 2, 3, \cdots T\}$ that occurs in each training event.

$$O(T|\mathbf{N}) = \frac{exp(ST)}{\sum_i^T exp(S_i)} \tag{14}$$

Here, the non-normalized log probability is represented by S. Whereas the cross-entropy for the proposed model can be determined using as follows:

$$Entropy = \sum_{T=1}^{T} log(p(T)q(T)) \tag{15}$$

Gradient training deep models are achievable due to the cross-entropy loss as it is differentiable in logistics, S_T. The gradients vary from -1 to +1, and the fundamental aspect of the gradients is $\frac{\partial k}{\partial S_T}$. If the cross-entropy is kept as low as possible, the chance of a correct classification increases. Overfitting can be avoided by examining the distribution of over labels independent of the training examples $v(t)$ with a smooth parameter eta, where $p(T|\mathbf{N})$= $\sigma T, \mathbf{N}'$ is modified as follows:

$$p'^{T|\mathbf{N}} = (1 - \eta)\varpi_{T,\mathbf{N}} + \eta \mathbf{\Xi}(T) \tag{16}$$

$p^{'T|\mathbf{N}}$ is the combination of of $q^{S|N}$ and stable distribution $\Xi(T)$ having weights (1 - η) and η respectively. When label-smoothing regularization is performed with $\Xi(T) = \frac{1}{T}$, the $p^{'T|\mathbf{N}}$ becomes:

$$p^{'T|\mathbf{N}} = (1-\eta)\varpi_{T,\mathbf{N}} + \frac{\eta}{S} \tag{17}$$

Equation 17 can be expressed in the function of entropy as follows:

$$q(p^{'}, r) = -\sum_{t=1}^{J} log(p(t))p^{'(t)} = (1-\eta)q(p^{'}, r) + \eta P(u, q) \tag{18}$$

In other words, the label-smoothing regularisation is equivalent to computing the Kullback–Leibler divergence by replacing a single cross-entropy loss with two losses, one for each of $\mathbf{G}(p, r)$ and $\mathbf{G}(s, r)$.The second loss penalises the predicted label distribution r for deviating from the prior distribution s by an amount equal to $\frac{\eta}{(1-\eta)}$. In [69], [70], other mathematical formulations of CNN architecture can be found.

4.1 Transfer Learning

Predictive tasks such as brain tumours, liver and lung disorders, and other diseases may be predicted by using transfer learning. It means that data from one context may be utilized to enhance performance in another one. Transfer learning is often used when the new dataset on which the pre-trained model is trained is smaller than the original one. Repurposing an Inception-v3 model trained on ImageNet to learn features for training on a new dataset is the goal of this project (CIFAR-10 and Caltech Faces) [71]. Starting with the features acquired on ImageNet and adapting them to a new dataset or task rather than starting from the beginning with random weight initialization is an advantage of transfer learning [72].

4.2 Fine Tuning

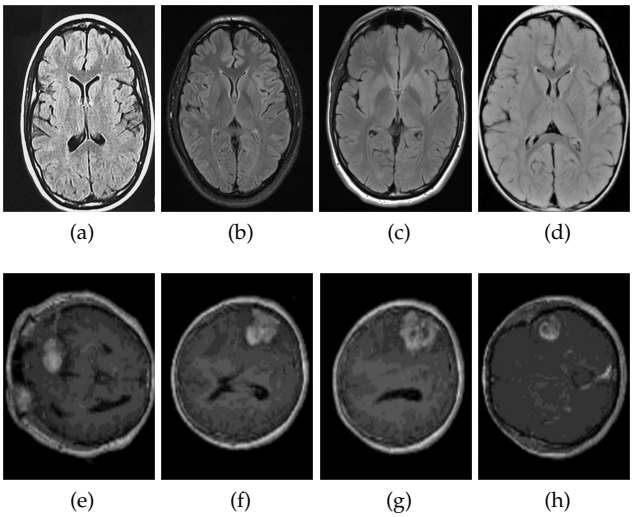
In order to identify the 1000 generic object classes in ImageNet, the proposed model has been modified. Transfer learning is the foundation of network fine-tuning. We can train a CNN to learn features for a wide range of domains by strengthening the classification function for error reduction [73]. The network is then fine-tuned to reduce errors in a more narrowly defined region when the classification function is updated. The network's functions and characteristics are assigned to the specialised domain in this configuration.

The CNN classification function, commonly known as "softmax," is used while computing the likelihood of each of the ImageNet dataset's 1000 classes. To begin the fine-tuning process, old values in the softmax classifier are removed and replaced with new random values. A new softmax classifier is then trained from the start using the back-propagation technique and a huge dataset of cancer patient data.

The learning rates of each layer must be correctly calibrated before the back-propagation process for fine-tuning can be initiated, and this is critical. For the purpose of this research, we increased the learning rate of the top classification layer to 10 and decreased it to 0.1 for the following seven classification layers. The back-propagation technique was used to optimise the network parameters, with a total of five thousand rounds being completed using stochastic gradient descent (SGD) [74].

5 Material and Method

The suggested non-invasive methodology for cancer diagnosis complements existing diagnostic tools and mechanisms and helps medical practitioners diagnose cancer more reliably and precisely. The dataset contains 4,800 authenticated MRI images that will be utilized in the planned research. The MRI images of the normal patient are different from such images in which tumour appears. The tumour in MRI images have different color intensities as it can be seen in Figure 8.



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig. 8: (a-d) Normal patient images (e-h) Cancer image patient

The images are grouped into training images and patient testing images. Before beginning to analyse MRI scans, all radiographs were checked for quality control, and any low-quality or unreadable scans were eliminated. Following that, two professionals appraised the images before they were accepted for use in the AI system. Finally, a third expert examined the assessment set to ensure no grading issues existed.

The proposed work aims to categorize healthy and cancer disease patients, therefore distinguishing them from one another. The classification performance is assessed in order to reach this categorization. Figure 9 depicts the proposed work's block diagram.

- The data is gathered using magnetic resonance imaging (MRI) scans. The sizes of various MRI scans vary; for instance, A and B signify the rows and columns of image pixels, respectively.
  Image Preprocessing : The imaging preprocessing stage is critical for producing clear and distinct images. The preprocessing of the image permits the classification phase. First and primarily, the data augmentation procedure was used. This procedure contributes

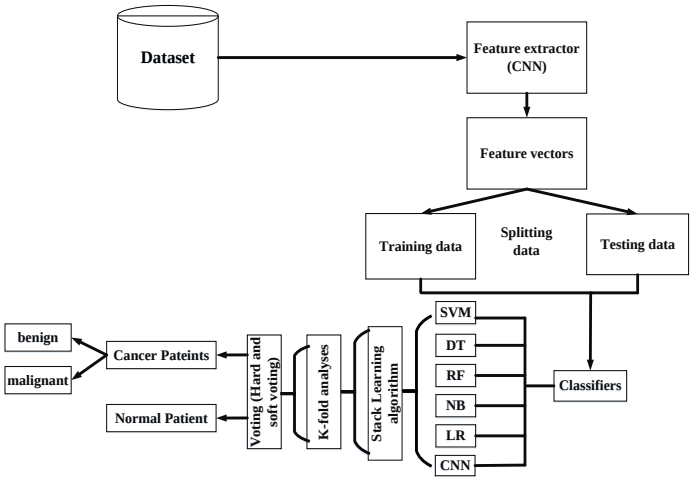


Fig. 9: Flowchart of the proposed model for cancer diagnosis

to the dataset's volume expansion by performing several conversions to the initial input. The input was duplicated using several conversion techniques, including translation, symmetry, and rotation. The stages involved in preprocessing and augmentation are mentioned below.

Translation: The images were resized to a particular pixel count and oriented in a specified direction.

Centering The rows and columns of each image were removed from their edges. Thus, images of various sizes might be obtained. Later, the whole row and column widths are clipped, and the total number of images is tallied.

Segmentation: It is required to extract and classify high-quality images. While segmenting the high-resolution pictures, spectral confusion occurred, delineation was compromised, and the images' precision was lowered. Moreover, to enhance this, the object-oriented image segmentation approach was used to remove salt and noise from the image while also increasing its precision via the use of object structure and spectral signatures.

Feature extraction: Features are retrieved by employing the filters provided in the various layers. Filters in the first layers (convolution and pooling) are used to extract low-level features, whereas high-level features are extracted in the upper convolutional layer.

- Distinct feature vectors (Z.Vs) for each X-ray image were made: $Z.V = Z_1, Z_2, Z_3 \cdots Z_{14}$.
- The provided matrix ($Z.Vs$) contains only vectors representing statistical features collected from MRI Scans. Such features may be represented in a single data set, as seen in Equation 19.

$$\begin{pmatrix} Z.V_1 = Z_1, Z_2, Z_3 ... Z_{14} \\ Z.V_2 = Z_1, Z_2, Z_3 ... Z_{14} \\ Z.V_3 = Z_1, Z_2, Z_3 ... Z_{14} \\ \vdots \\ Z.V_n = Z_1, Z_2, Z_3 ... Z_{14} \end{pmatrix} \tag{19}$$

- These retrieved features were then sent to the classifier for decision-making with the help of fully connected layers.

The dataset was divided into two portions for training and testing purposes. The training data set included a combination of healthy and pneumonia-infected patients, and the model was trained using CNN. As specified in Equation 20, nearly 80% of the dataset was randomly selected for training purposes, taking into account both healthy and contaminated data types. The precise allocation of data for training and testing purposes may vary.

Additionally, we used transfer learning and fine-tuning to increase the accuracy of the suggested model. The model's accuracy was determined to be 98% after fine-tuning. Furthermore, K-fold analysis and voting procedures were added to improve the suggested model's accuracy, which was successfully attained at 99.7 percent.

5.1 K-Fold Analysis

The K-fold validation purpose is used to test the proposed model by selecting various values of K ($K = 10$, $K = 15$, $K = 20$, $K = 25$, $K = 30$). Such a validation methodology uses the dataset to train the model by selecting different training data from the whole dataset. For instance, if the value of $K = 10$, a total of ten iterations will be performed in which ten percent of the whole data set is selected for testing purposes. i.e., for the first iteration, the first $1/10^{th}$ part of the dataset will be used for testing purposes. Similarly, in the second iteration, the second $1/10th$ will be used for testing, while the remaining data will be used for training. Mathematically, it can be written as:

$$\begin{cases} \text{if} & \\ \text{Total test instances} & \text{T= 5000} \\ \text{Training instances} & \text{(Total instances) - (5000)} \end{cases} \tag{20}$$

To evaluate the model when K is set at 10, divide the dataset into ten divisions. Each division will be used as a test dataset in each iteration.

5.2 Voting Techniques

It is a meta classifier that combines equivalent or excellent machine learning classifiers for classification and detection [75]. It is also known as an "ensemble voting classifier." The Ensemble Voting Classifier is used to carry out "hard" and "soft" voting, respectively.

5.2.1 Hard Voting

The simplest example of majority voting is hard ensemble voting, which is the most common kind of voting. This strategy is based on obtaining a majority of votes [76]. For example, in the suggested study, in order to improve the accuracy of the model, k-fold analysis is employed to classify the event into two categories depending on the majority of votes

received: A and B. Figure 10 shows the accuracy of all of the k-models, and it can be observed that the majority of the models prefer class A over class B. As a result, after applying rigorous voting, a forthcoming sample will be classified as class A. The detailed flow diagram of the hard voting applied to the proposed work is given in Figure 10.

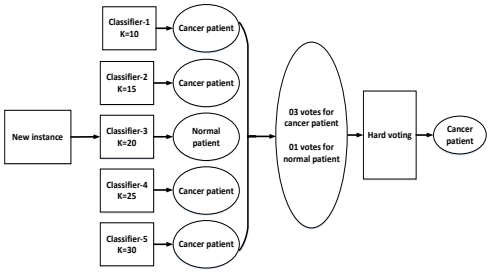


Fig. 10: Classification using hard voting

5.2.2 Soft Voting

A classifier's predicted probability, denoted by p, is used to anticipate which classes will be selected. Figure 11 depicts various probabilities of occurrences of a particular type based on the results of a single k-model [77]. Equation 21 can be used to determine the probability of each class occurring.

$$\text{Class cancer } (\mathbf{C}) = \frac{Po(\mathbf{C})_1 + Po(\mathbf{C})_2 + \cdots + Po(\mathbf{C})_N}{N} \tag{21}$$

$$\text{Class normal } (\mathbf{N}) = \frac{(\mathbf{N})_1 + Po(\mathbf{N})_2 + \cdots + Po(\mathbf{N})_N}{N} \tag{22}$$

$$\text{Class } (\mathbf{C}) = \frac{0.70 + 0.45 + 0.55 + 0.65 + 0.40}{5} \times 100 = 55 \tag{23}$$

$$\text{Class } (\mathbf{N}) = \frac{0.30 + 0.55 + 0.45 + 0.35 + 0.60}{5} \times 100 = 45\% \tag{24}$$

6 Results and Discussion

Different performance measurement parameters are explained below to evaluate the performance of both proposed models, including the encryption scheme for data security and the detection model for cancer diagnosis.

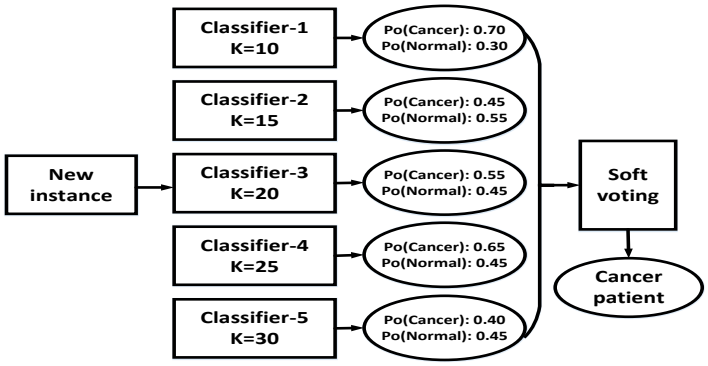


Fig. 11: Classification using soft voting.

6.1 Analysis of Proposed Encryption Scheme

To analyze and compare the proposed encryption scheme against existing techniques, security parameters such as entropy, energy, correlation, homogeneity, structural content (S.C), and histogram analysis are conducted. The mathematical representations and the relationship with strong security are given in Table 3. Further details of a similar analysis are given in [78], [79], [80], [81], [82]. From Table 3, it can be seen that the numerical values of the security analysis for the proposed work are much better than the existing ones. This is because numerous DWT, chaos, and bit-plane extraction approaches are used to improve the suggested encryption scheme's performance. In addition, the use of DWT and bit-plane extraction makes the proposed encryption process significantly faster by only encrypting the low-frequency band and the most important bits. . The results given in Table 4 show that the proposed scheme performs better than existing encryption schemes.

6.2 Histogram Analysis

A histogram shows pixel distribution over the image [88]. Figure 12 shows the histogram for an original picture with several histogram peaks. As shown in Figure 12, the pixels of the encrypted images are evenly distributed. Enciphered pictures' histograms must be near flat and distinct from the original image's histogram to provide a secure encryption process. As is evident from Figure 12, the proposed encryption scheme does provide satisfactory results and fulfills the minimum requirement of the histogram test. Performance measures to evaluate ML/DL detection systems include accuracy, specificity/precision, sensitivity, recall, F1 score, and AUC in detecting cancer. For such detection models, various performance criteria might lead to varying conclusions. For instance, in terms of accuracy, which is usually a primary assessment measure for any classification system, a model may provide excellent results if it is able to identify the patterns correctly. Different performance parameters and their corresponding mathematical equations are listed in Table 5.

In Table 5, Γ_P, Γ_N, F_P and F_N represent true positives, true negatives, false positives and false negatives, respectively. These terms are defined as follows:

True positives (Γ_P): The number represents the instances when a patient has cancer, and the model detects it correctly.

TABLE 3: Performance measuring parameters

Parameters	Mathematical equations	Relationship with strong security (S.S)	Variable explanation
Entropy	$Ent = -\sum O(p_i) log_2 en(c_i)$	Entropy $\propto$S.S	$O(p_i)$ is probability of occurrence
Energy	$Energy = \sum O(a,b)^2$	Energy $\propto \frac{1}{S.S}$	O(a,b) is an original image
Correlation	$Co = \frac{\frac{1}{L}\sum_{j=1}^{L}(x_i - En(a))(y_i - En(b))}{\sigma_a \sigma_b}$ $\sigma_a = \sqrt{VARa}, \sigma_b = \sqrt{VAR_b}$ $VAR(a) = \frac{1}{L}\sum_{j=1}^{L}(a_i - E(a))^2$ $VAR(b) = \frac{1}{L}\sum_{j=1}^{L}(b_i - E(b))^2$	Correlation $\propto \frac{1}{S.S}$	L: Total pixels, E(a) and E(b) is Encrypted image in horizontal and vertical direction
Contrast	$Cont = \sum \lvert a-b \rvert^2 O(a,b)\Big]$	Contrast $\propto$S.S	O(a,b) is gray-level co-occurrence matrices
Homogeneity	$\sum_a \sum_b \frac{O(a,b)}{1+\lvert a-b \rvert}\Big]$	Homogeneity $\propto \frac{1}{S.S}$	//
S.C	$Sc = \frac{\sum_{a=1}^{M}\sum_{b=1}^{N}[O(a,b)]^2}{\sum_{a=1}^{M}\sum_{b=1}^{N}[En(a,b)]^2}$	S.C $\propto \frac{1}{S.S}$	En is encrypted image

TABLE 4: Statistical security analysis.

	Proposed work						
Encrypted MRI images	Homogeneity	SC	Entropy	Correlation	Energy	Contrast	Execution time (sec)
Normal MRI image$_1$	258	18	7.9992	0.0001	0.154	9.2413	0.021
Normal MRI image$_2$	259	15	7.9991	-0.0054	0.0156	10.7891	0.020
Normal MRI image$_3$	260	16	7.9988	0.0010	0.0155	10.1584	0.025
Normal MRI image$_4$	251	16	7.9991	0.0001	0.0155	10.7914	0.027
Cancer MRI image$_1$	251	19	7.9991	-0.0035	0.0152	10.7341	0.029
Cancer MRI image$_2$	256	17	7.9997	0.0006	0.0151	10.7982	0.030
Cancer MRI image$_3$	251	16	7.9992	-0.0015	0.0155	10.1351	0.022
Cancer MRI image$_4$	260	15	7.9990	0.0004	0.0154	10.7546	0.025
Average	260	15	7.9990	0.0004	0.0154	10.7546	0.025
	Comparison						
Existing schemes	MSE	PSNR	Entropy	Correlation	Energy	Contrast	Execution time (sec)
Ref [83]	249	20	7.9953	-0.0015	0.0156	9.9882	1.361
Ref [84]	248	25	7.9959	0.0006	0.0155	9.9783	1.399
Ref [85]	249	23	7.9925	-0.0075	0.0160	9.9944	2.978
Ref [86]	248	26	7.9944	-0.0050	0.0159	9.6986	2.036
Ref [87]	247	21	7.9972	0.0009	0.0158	9.9973	2.971

TABLE 5: Performance evaluating parameters

Parameters	Mathematical equations
Parameters	Mathematical equations
Accuracy	$\frac{\Gamma_P + \Gamma_N}{\Gamma_P + F_P + \Gamma_N + F_N}$
Specificity /precision	$\frac{\Gamma_P}{\Gamma_P + F_N}$
Sensitivity /recall	$\frac{\Gamma_N}{\Gamma_N + F_P}$
F1-Score	$2 \times \left[\frac{\text{Sensitivity} \times \text{Specificity}}{\text{Sensitivity} + \text{Specificity}}\right]$

True negatives (Γ_N): The number represents the instances when a patient is actually not suffering from cancer, and the model correctly identifies it as healthy.

False positives (F_P): The number represents the instances when a patient is healthy, but the model identifies it as cancer affected.

False negatives (F_N): The number represents the instances when a patient has cancer, however, the proposed model identifies it as healthy.

The performance parameters given in Table 5 can be determined using the confusion matrix, a 2-D array which contain Γ_P, Γ_N, F_P and F_N. The confusion matrices for the proposed model with transfer learning and fine-tuning are given in Figure 13. Furthermore, the statistical values for the proposed and existing schemes are shown in Table 6, demonstrating that the suggested approach is significantly more reliable than the existing ones. Numerous existing models like CNN, RF, NB, and SCM are employed to determine which one performs the best. Several methodologies for tumour detection using machine learning (ML) algorithms have been proposed in recent years. According to the literature, the accuracy gained via machine learning algorithms is not satisfactory. As a result, a deep learning technique known as CNN is employed to improve the suggested classification task's performance. When CNN is used, the suggested work is 97.2 percent accurate, as shown in Table 6. While RF, NB, and SVM give accuracy of 98%, 90%, and 15%, respectively, that reflects that the CNN is the better option for the proposed model. Apart from CNN, several deep learning algorithms such as Recurrent Neural Networks (RNNs) [89], Deep Boltzmann Machines (DBMs) [90], and Deep Belief Networks (DBNs) [91] are also analyzed to compare their performance with that of CNN. Different statistical values corresponding to each parameter are given in Table 6, indicating that CNN has the highest accuracy among them. Additionally, accuracy and loss curves are shown in Figure 14 with the minimal loss indicating the capability of the proposed model in terms of predicting classes accurately.

TABLE 6: Performance comparison of the proposed work with the existing ones

Schemes	CNN	Tranfer Learninng	Fine Tuning	DBN	RNN	DBM	RF	NB	SVM (sigmoid kernel)	SVM (linear kernel)	SVM (rbf kernel)	SVM (polynomial kernel)
								Accuracy (Ac_y)				
Proposed	97.2	97.4	97.7	95.3	95.6	97.1	98	90	15	53	95	96
Ref [92]	91	81	89	88	87	85	90	90	92	91	84	86
Ref [93]	86	93	92	90	89	91	.92	91	92	92	91	92
Ref [94]	95	75	77	78	79	86	79	73	74	82	84	86
Ref [95]	85	83	82	90	92	88	89	92	93	91	92	97
Ref [96]	92	86	82	86	82	90	92	92	94	91	92	93
								Precision ($Prec_y$)				
Proposed	0.97	0.98	0.98	0.96	0.95	0.93	0.89	0.99	0.32	0.35	0.99	0.97
Ref [92]	0.84	0.92	0.900.	0.79	0.86	0.89	0.85	0.86	0.87	0.89	0.92	0.89
Ref [93]	0.92	0.95	0.93	0.90	0.90	0.89	0.96	0.93	0.93	0.95	0.98	0.99
Ref [94]	0.97	0.95	0.96	0.95	0.93	0.90	0.98	0.96	0.99	0.98	0.99	0.98
Ref [95]	0.89	0.88	0.87	0.88	0.90	0.93	0.84	0.92	.97	0.98	0.97	0.98
Ref [96]	0.89	0.88	0.87	0.88	0.91	0.93	0.84	0.92	.97	0.98	0.97	0.98
								sensitivity (Sen_y)				
Proposed	0.97	0.98	0.99	0.97	0.95	0.93	0.96	0.80	0.15	0.87	0.92	0.85
Ref [92]	0.89	0.92	0.93	0.91	0.90	0.93	0.95	0.91	0.94	0.95	0.94	0.92
Ref [93]	0.92	0.94	0.91	0.90	0.91	0.93	0.90	0.98	0.94	0.95	0.92	0.91
Ref [94]	0.91	0.92	0.90	0.89	0.90	0.92	0.89	0.96	0.92	0.93	0.91	0.92
Ref [95]	0.97	0.91	0.92	0.91	0.93	0.90	0.91	0.92	0.96	0.95	0.92	0.96
Ref [96]	0.91	0.92	0.94	0.93	0.90	0.91	0.96	0.96	0.92	0.92	0.91	0.91
								F1 Score				
Proposed	0.98	0.99	0.98	0.95	0.96	0.93	0.96	0.89	0.22	0.45	0.94	91
Ref [92]	0.86	0.92	0.81	0.85	0.81	0.83	0.88	0.85	0.97	0.93	0.94	0.92
Ref [93]	0.92	0.92	0.83	0.83	0.90	0.91	0.92	0.93	0.91	0.98	0.96	0.94
Ref [94]	0.96	0.97	0.92	0.89	0.90	0.89	0.91	0.91	0.96	0.95	0.92	0.91
Ref [95]	0.91	0.90	0.92	0.91	0.90	0.93	0.93	0.92	0.91	0.95	0.96	0.99
Ref [96]	0.91	0.90	0.92	0.89	0.91	0.93	0.93	0.92	0.91	0.95	0.96	0.99

7 Conclusion

In this study, two critical issues related to cancer detection are discussed: data privacy-preserving and cancer diagnosis. The sensitive medical images of patients used for cancer diagnosis are protected using an image encryption technique that employs DWT, chaos, and bit-plane extraction to send data without being manipulated by attackers or unauthorized accesses. Before being utilized for cancer diagnosis, the data is decrypted once received in encrypted form. The second part of this study focuses on cancer diagnosis utilizing deep learning models, namely CNNs, to perform feature extraction and classification. Furthermore, transfer learning and fine-tuning approaches are employed to enhance the overall accuracy of the suggested model. Several metrics, including precision, accuracy, F1 score, and recall, are used to evaluate the performance of the proposed cancer diagnosis model. A comprehensive comparison is also provided to demonstrate the efficacy of the proposed approach compared to existing techniques.

8 Future research directions

The proposed approach has a 97.2% accuracy using CNNs, which is relatively high, but it may be enhanced more by adopting the following future directions:

- Use different preprocessing techniques to clean the considered dataset, such as principal component analysis (PCA) [97] and linear discriminant analysis (LDA) [98].
- Investigate the concept of federated learning, which is an intriguing approach for introducing intelligence to diverse distributed systems and applications by allowing participating devices to autonomously train a global model initialized by a centralized system [99].
- Introduce a generative adversarial network-based technique to enhance image quality in the considered dataset, which can improve cancer diagnosis accuracy and resolve data imbalance distribution.
- The mobile application that can be used for detecting cancer at early stages can be developed. The patient will only need the MRI images as an input.

Acknowledgments

The authors would like to acknowledge the support of Prince Sultan University, Saudi Arabia.

References

[1] D. Tellez, G. Litjens, J. van der Laak, and F. Ciompi, "Neural image compression for gigapixel histopathology image analysis," *IEEE transactions on pattern analysis and machine intelligence*, 2019.

[2] T. Botterill, T. Lotz, A. Kashif, and J. G. Chase, "Reconstructing 3-d skin surface motion for the diet breast cancer screening system," *IEEE transactions on medical imaging*, vol. 33, no. 5, pp. 1109–1118, 2014.

[3] G. Litjens, O. Debats, J. Barentsz, N. Karssemeijer, and H. Huisman, "Computer-aided detection of prostate cancer in mri," *IEEE transactions on medical imaging*, vol. 33, no. 5, pp. 1083–1092, 2014.

[4] S. S. Mohamed and M. M. Salama, "Prostate cancer spectral multifeature analysis using trus images," *IEEE Transactions on Medical Imaging*, vol. 27, no. 4, pp. 548–556, 2008.

[5] A. Islam, S. M. Reza, and K. M. Iftekharuddin, "Multifractal texture estimation for detection and segmentation of brain tumors," *IEEE transactions on biomedical engineering*, vol. 60, no. 11, pp. 3204–3215, 2013.

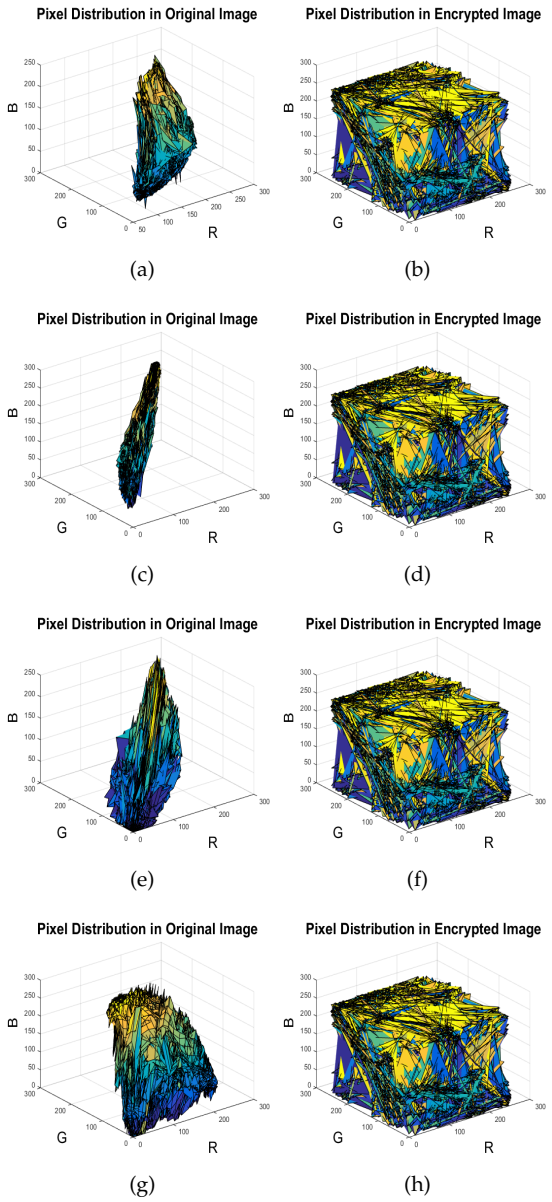


Fig. 12: Pixel distribution in original and encrypted images

Total No. of Patients: 5000	Predicted NO (Normal Patient)	Predicted Yes (Cancer disease)
Actual NO (Normal Patient)	TP: 4364	FP: 85
Actual yes (Cancer disease)	FN: 55	TN: 496

(a) Confusion matrix for CNN model

Total No. of Patients: 5000	Predicted NO (Normal Patient)	Predicted Yes (Cancer disease)
Actual NO (Normal Patient)	TP: 4379	FP: 133
Actual yes (Cancer disease)	FN: 85	TN: 491

(b) Confusion matrix for Transfer model

Total No. of Patients: 5000	Predicted NO (Normal Patient)	Predicted Yes (Cancer disease)
Actual NO (Normal Patient)	TP: 3986	FP: 53
Actual yes (Cancer disease)	FN: 62	TN: 899

(c) Confusion matrix for Fine Tuning model

Fig. 13: Confusion matrices for CNN, transfer learning and fine tuning based proposed model.

[6] X. Wang, H. Chen, C. Gan, H. Lin, Q. Dou, E. Tsougenis, Q. Huang, M. Cai, and P.-A. Heng, "Weakly supervised deep learning for whole slide lung cancer image analysis," *IEEE transactions on cybernetics*, vol. 50, no. 9, pp. 3950–3962, 2019.

[7] X. Feng, L. Song, S. Wang, H. Song, H. Chen, Y. Liu, C. Lou, J. Zhao, Q. Liu, Y. Liu, *et al.*, "Accurate prediction of neoadjuvant chemotherapy pathological complete remission (pcr) for the four sub-types of breast cancer," *IEEE Access*, vol. 7, pp. 134697–134706, 2019.

[8] F. Bray, M. Laversanne, E. Weiderpass, and I. Soerjomataram, "The ever-increasing importance of cancer as a leading cause of premature death worldwide," *Cancer*, 2021.

[9] S. H. Read and S. H. Wild, "Prevention of premature cardiovascular death worldwide," *The Lancet*, vol. 395, no. 10226, pp. 758–760, 2020.

[10] L. A. Habel, S. Shak, M. K. Jacobs, A. Capra, C. Alexander, M. Pho, J. Baker, M. Walker, D. Watson, J. Hackett, *et al.*, "A population-based study of tumor gene expression and risk of breast cancer death among lymph node-negative patients," *Breast Cancer Research*, vol. 8, no. 3, pp. 1–15, 2006.

[11] V. Gausman, D. Dornblaser, S. Anand, R. B. Hayes, K. O'Connell, M. Du, and P. S. Liang, "Risk factors associated with early-onset colorectal cancer," *Clinical Gastroenterology and Hepatology*, vol. 18, no. 12, pp. 2752–2759, 2020.

[12] A. Rizzo, M. Santoni, V. Mollica, F. Logullo, M. Rosellini, A. Marchetti, L. Faloppi, N. Battelli, and F. Massari, "Peripheral neuropathy and headache in cancer patients treated with immunotherapy and immuno-oncology combinations: the mouseion-02 study," *Expert Opinion on Drug Metabolism & Toxicology*, no. just-accepted, 2021.

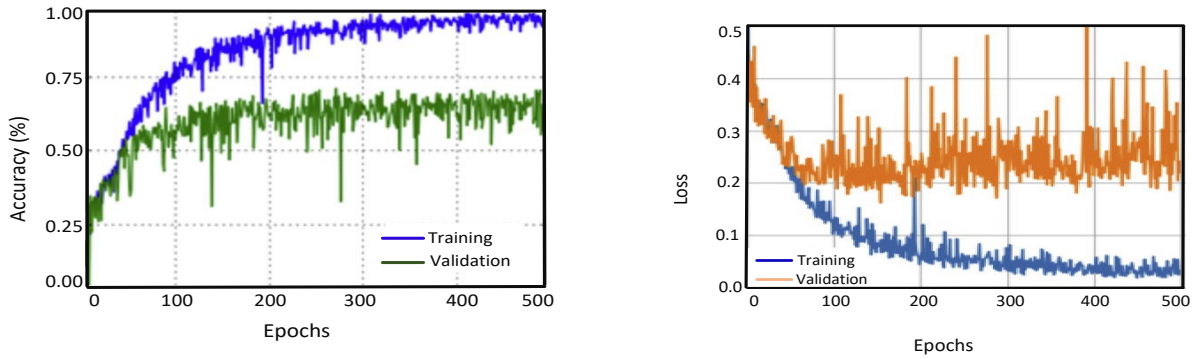
[13] A.-M. Yang, Y. Han, C.-S. Liu, J.-H. Wu, and D.-B. Hua, "D-tsvr recurrence prediction driven by medical big data in cancer," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3508–3517, 2020.

[14] Y. Wang, N. Wang, M. Xu, J. Yu, C. Qin, X. Luo, X. Yang, T. Wang, A. Li, and D. Ni, "Deeply-supervised networks with threshold loss for cancer detection in automated breast ultrasound," *IEEE transactions on medical imaging*, vol. 39, no. 4, pp. 866–876, 2019.

[15] A. Shafique and F. Ahmed, "Image encryption using dynamic s-box substitution in the wavelet domain," *Wireless Personal Communications*, vol. 115, no. 3, pp. 2243–2268, 2020.

[16] B. Bai, S. Nazir, Y. Bai, and A. Anees, "Security and provenance for internet of health things: A systematic literature review," *Journal of Software: Evolution and Process*, vol. 33, no. 5, p. e2335, 2021.

[17] A. Shafique and J. Shahid, "Novel image encryption cryptosystem



(a) Training and validation accuracy

(b) Training and validation loss

Fig. 14: Accuracy and loss curves

based on binary bit planes extraction and multiple chaotic maps," *The European Physical Journal Plus*, vol. 133, no. 8, pp. 1–16, 2018.

[18] T. A. Al-Maadeed, I. Hussain, A. Anees, and M. T. Mustafa, "A image encryption algorithm based on chaotic lorenz system and novel primitive polynomial s-boxes," *Multimedia Tools and Applications*, pp. 1–22, 2021.

[19] A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map," *The European Physical Journal Plus*, vol. 135, no. 2, pp. 1–13, 2020.

[20] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of cryptographic s-boxes based on mobius transformation and chaotic tent-sine system," *IEEE Access*, vol. 7, pp. 173273–173285, 2019.

[21] A. Anees and I. Hussain, "A novel method to identify initial values of chaotic maps in cybersecurity," *Symmetry*, vol. 11, no. 2, p. 140, 2019.

[22] J. Daemen and V. Rijmen, "Reijndael: The advanced encryption standard.," *Dr. Dobb's Journal: Software Tools for the Professional Programmer*, vol. 26, no. 3, pp. 137–139, 2001.

[23] D. E. Standard *et al.*, "Data encryption standard," *Federal Information Processing Standards Publication*, vol. 112, 1999.

[24] M. U. Rehman, S. Najam, S. Khalid, A. Shafique, F. Alqahtani, F. Baothman, S. Y. Shah, Q. H. Abbasi, M. A. Imran, and J. Ahmad, "Infrared sensing based non-invasive initial diagnosis of chronic liver disease using ensemble learning," *IEEE Sensors Journal*, 2021.

[25] M. U. Rehman, A. Shafique, S. Khalid, M. Driss, and S. Rubaiee, "Future forecasting of covid-19: A supervised learning approach," *Sensors*, vol. 21, no. 10, p. 3322, 2021.

[26] M. Safaei, E. A. Sundararajan, M. Driss, W. Boulila, and A. Shapi'i, "A systematic literature review on obesity: Understanding the causes & consequences of obesity and reviewing various machine learning approaches used to predict obesity," *Computers in biology and medicine*, vol. 136, p. 104754, 2021.

[27] M. Al-Sarem, A. Alsaeedi, F. Saeed, W. Boulila, and O. Ameer-Bakhsh, "A novel hybrid deep learning model for detecting covid-19-related rumors on social media based on lstm and concatenated parallel cnns," *Applied Sciences*, vol. 11, no. 17, p. 7940, 2021.

[28] S. Ben Atitallah, M. Driss, W. Boulila, A. Koubaa, and H. Ben Ghezala, "Fusion of convolutional neural networks based on dempster–shafer theory for automatic pneumonia detection from chest x-ray images," *International Journal of Imaging Systems and Technology*, vol. 32, no. 2, pp. 658–672, 2022.

[29] S. Ben Atitallah, M. Driss, W. Boulila, and H. Ben Ghezala, "Randomly initialized convolutional neural network for the recognition of covid-19 using x-ray images," *International journal of imaging systems and technology*, vol. 32, no. 1, pp. 55–73, 2022.

[30] M. U. Rehman, A. Shafique, K. H. Khan, S. Khalid, A. A. Alotaibi, T. Althobaiti, N. Ramzan, J. Ahmad, S. A. Shah, and Q. H. Abbasi, "Novel privacy preserving non-invasive sensing-based diagnoses of pneumonia disease leveraging deep network model," *Sensors*, vol. 22, no. 2, p. 461, 2022.

[31] R. Audhkhasi and M. L. Povinelli, "Generalized multi-channel scheme for secure image encryption," *Scientific reports*, vol. 11, no. 1, pp. 1–9, 2021.

[32] Y. Zhang, F. Wang, J. Chao, M. Xie, H. Liu, M. Pan, E. Kopperger, X. Liu, Q. Li, J. Shi, *et al.*, "Dna origami cryptography for secure communication," *Nature communications*, vol. 10, no. 1, pp. 1–8, 2019.

[33] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International journal of bifurcation and chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[34] H. Li, Y. Wang, and Z. Zuo, "Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms," *Optics and Lasers in Engineering*, vol. 115, pp. 197–207, 2019.

[35] W. Wang, Z. Han, M. Alazab, T. R. Gadekallu, X. Zhou, and C. Su, "Ultra super fast authentication protocol for electric vehicle charging using extended chaotic maps," *IEEE Transactions on Industry Applications*, 2022.

[36] C. Rupa, M. Harshita, G. Srivastava, T. R. Gadekallu, and P. K. R. Maddikunta, "Securing multimedia using a deep learning based chaotic logistic map," *IEEE Journal of Biomedical and Health Informatics*, 2022.

[37] T. Sivakumar and P. Li, "A secure image encryption method using scan pattern and random key stream derived from laser chaos," *Optics & Laser Technology*, vol. 111, pp. 196–204, 2019.

[38] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[39] G. Kaur, R. Agarwal, and V. Patidar, "Chaos based multiple order optical transform for 2d image encryption," *Engineering Science and Technology, an International Journal*, vol. 23, no. 5, pp. 998–1014, 2020.

[40] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 22023–22043, 2019.

[41] L. Liu and S. Miao, "A new simple one-dimensional chaotic map and its application for image encryption," *Multimedia Tools and Applications*, vol. 77, no. 16, pp. 21445–21462, 2018.

[42] M. Z. Talhaoui, X. Wang, and A. Talhaoui, "A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme," *The Visual Computer*, vol. 37, no. 7, pp. 1757–1768, 2021.

[43] B. Yosefnezhad Irani, P. Ayubi, F. Amani Jabalkandi, M. Yousefi Valandar, and M. Jafari Barani, "Digital image scrambling based on a new one-dimensional coupled sine map," *Nonlinear Dynamics*, vol. 97, no. 4, pp. 2693–2721, 2019.

[44] M. Kumar, A. Saxena, and S. S. Vuppala, "A survey on chaos based image encryption techniques," in *Multimedia security using chaotic maps: principles and methodologies*, pp. 1–26, Springer, 2020.

[45] A. Kamrani, K. Zenkouar, and S. Najah, "A new set of image encryption algorithms based on discrete orthogonal moments and chaos theory," *Multimedia Tools and Applications*, vol. 79, no. 27, pp. 20263–20279, 2020.

[46] M. U. Rehman, A. Shafique, S. Khalid, and I. Hussain, "Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps," *IEEE Access*, vol. 9, pp. 52277–52291, 2021.

[47] D. Hyun, L. Abou-Elkacem, R. Bam, L. L. Brickson, C. D. Herickhoff, and J. J. Dahl, "Nondestructive detection of targeted microbubbles using dual-mode data and deep learning for real-time ultrasound molecular imaging," *IEEE transactions on medical imaging*, vol. 39, no. 10, pp. 3079–3088, 2020.

[48] G. Carneiro, J. Nascimento, and A. P. Bradley, "Automated analysis of unregistered multi-view mammograms with deep learning," *IEEE transactions on medical imaging*, vol. 36, no. 11, pp. 2355–2365, 2017.

[49] O. Ozdemir, R. L. Russell, and A. A. Berlin, "A 3d probabilistic deep learning system for detection and diagnosis of lung cancer using low-dose ct scans," *IEEE transactions on medical imaging*, vol. 39, no. 5, pp. 1419–1429, 2019.

[50] R. Singh, T. Ahmed, A. Kumar, A. K. Singh, A. K. Pandey, and S. K. Singh, "Imbalanced breast cancer classification using transfer learning," *IEEE/ACM transactions on computational biology and bioinformatics*, vol. 18, no. 1, pp. 83–93, 2020.

[51] M. S. M. Khan, M. Ahmed, R. Z. Rasel, and M. M. Khan, "Cataract detection using convolutional neural network with vgg-19 model," in *2021 IEEE World AI IoT Congress (AIIoT)*, pp. 0209–0212, IEEE, 2021.

[52] J. Xu, L. Xiang, Q. Liu, H. Gilmore, J. Wu, J. Tang, and A. Madabhushi, "Stacked sparse autoencoder (ssae) for nuclei detection on breast cancer histopathology images," *IEEE transactions on medical imaging*, vol. 35, no. 1, pp. 119–130, 2015.

[53] G. Altan *et al.*, "Breast cancer diagnosis using deep belief networks on roi images," *Pamukkale University Journal of Engineering Sciences*, vol. 1000, no. 1000, pp. 0–0.

[54] R. S. Patil and N. Biradar, "Automated mammogram breast cancer detection using the optimized combination of convolutional and recurrent neural network," *Evolutionary intelligence*, vol. 14, no. 4, pp. 1459–1474, 2021.

[55] Y. Li, F. Fauteux, J. Zou, A. Nantel, and Y. Pan, "Personalized prediction of genes with tumor-causing somatic mutations based on multi-modal deep boltzmann machine," *Neurocomputing*, vol. 324, pp. 51–62, 2019.

[56] N. Antropova, B. Huynh, H. Li, and M. L. Giger, "Breast lesion classification based on dynamic contrast-enhanced magnetic resonance images sequences with long short-term memory networks," *Journal of Medical Imaging*, vol. 6, no. 1, p. 011002, 2018.

[57] W. H. Organization *et al.*, "Definition, diagnosis and classification of diabetes mellitus and its complications: report of a who consultation. part 1, diagnosis and classification of diabetes mellitus," tech. rep., World Health Organization, 1999.

[58] G. Ye and X. Huang, "Spatial image encryption algorithm based on chaotic map and pixel frequency," *Science China Information Sciences*, vol. 61, no. 5, pp. 1–3, 2018.

[59] L. Gao, L. Qi, and L. Guan, "The property of frequency shift in 2d-frft domain with application to image encryption," *IEEE Signal Processing Letters*, vol. 28, pp. 185–189, 2021.

[60] M. A. S. Hassan and I. S. I. Abuhaiba, "Image encryption using differential evolution approach in frequency domain," *arXiv preprint arXiv:1103.5783*, 2011.

[61] M. Guan, X. Yang, and W. Hu, "Chaotic image encryption algorithm using frequency-domain dna encoding," *IET image processing*, vol. 13, no. 9, pp. 1535–1539, 2019.

[62] F. Francis-Lothai and D. B. Bong, "A fingerprint matching algorithm using bit-plane extraction method with phase-only correlation," *International Journal of Biometrics*, vol. 9, no. 1, pp. 44–66, 2017.

[63] A. Shafique, M. M. Hazzazi, A. R. Alharbi, and I. Hussain, "Integration of spatial and frequency domain encryption for digital images," *IEEE Access*, vol. 9, pp. 149943–149954, 2021.

[64] I. Hussain, A. Anees, T. A. Al-Maadeed, and M. T. Mustafa, "Construction of s-box based on chaotic map and algebraic structures," *Symmetry*, vol. 11, no. 3, p. 351, 2019.

[65] J. Amin, M. Sharif, M. Raza, T. Saba, and M. A. Anjum, "Brain tumor detection using statistical and machine learning method," *Computer methods and programs in biomedicine*, vol. 177, pp. 69–79, 2019.

[66] D. N. George, H. B. Jehlol, and A. S. A. Oleiwi, "Brain tumor detection using shape features and machine learning algorithms," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no. 10, pp. 454–459, 2015.

[67] P. R. Kshirsagar, A. N. Rakhonde, and P. Chippalkatti, "Mri image based brain tumor detection using machine learning," *Test Engineering and Management*, pp. 3672–3680, 2020.

[68] R. Arandjelovic, P. Gronat, A. Torii, T. Pajdla, and J. Sivic, "Netvlad: Cnn architecture for weakly supervised place recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 5297–5307, 2016.

[69] J. Wu, "Cnn for dummies," *Nanjing University*, vol. 202, 2015.

[70] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 2818–2826, 2016.

[71] X. Xia, C. Xu, and B. Nan, "Inception-v3 for flower classification," in *2017 2nd International Conference on Image, Vision and Computing (ICIVC)*, pp. 783–787, IEEE, 2017.

[72] M. Alkhelaiwi, W. Boulila, J. Ahmad, A. Koubaa, and M. Driss, "An efficient approach based on privacy-preserving deep learning for satellite image classification," *Remote Sensing*, vol. 13, no. 11, p. 2221, 2021.

[73] E. C. Too, L. Yujian, S. Njuki, and L. Yingchun, "A comparative study of fine-tuning deep learning models for plant disease identification," *Computers and Electronics in Agriculture*, vol. 161, pp. 272–279, 2019.

[74] C. Käding, E. Rodner, A. Freytag, and J. Denzler, "Fine-tuning deep neural networks in continuous learning scenarios," in *Asian Conference on Computer Vision*, pp. 588–605, Springer, 2016.

[75] N. Khuriwal and N. Mishra, "Breast cancer diagnosis using adaptive voting ensemble machine learning algorithm," in *2018 IEEMA engineer infinite conference (eTechNxT)*, pp. 1–5, IEEE, 2018.

[76] R. Atallah and A. Al-Mousa, "Heart disease detection using machine learning majority voting ensemble method," in *2019 2nd international conference on new trends in computing sciences (ictcs)*, pp. 1–6, IEEE, 2019.

[77] J. Cao, S. Kwong, R. Wang, X. Li, K. Li, and X. Kong, "Class-specific soft voting based multiple extreme learning machines ensemble," *Neurocomputing*, vol. 149, pp. 275–284, 2015.

[78] I. Hussain, A. Anees, and A. Algarni, "A novel algorithm for thermal image encryption," *Journal of integrative neuroscience*, vol. 17, no. 3-4, pp. 447–461, 2018.

[79] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, "Construction of chaotic quantum magnets and matrix lorenz systems s-boxes and their applications," *Chinese Journal of Physics*, vol. 56, no. 4, pp. 1609–1621, 2018.

[80] 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.

[81] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 9, pp. 3106–3118, 2014.

[82] F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, "A noisy channel tolerant image encryption scheme," *Wireless personal communications*, vol. 77, no. 4, pp. 2771–2791, 2014.

[83] I. Hussain, A. Anees, A. H. Alkhaldi, M. Aslam, N. Siddiqui, and R. Ahmed, "Image encryption based on chebyshev chaotic map and s8 s-boxes," *Optica Applicata*, vol. 49, no. 2, 2019.

[84] S. Zhu, C. Zhu, Y. Fu, W. Zhang, and X. Wu, "A secure image encryption scheme with compression-confusion-diffusion structure," *Multimedia Tools and Applications*, vol. 79, no. 43, pp. 31957–31980, 2020.

[85] H. Liu, F. Wen, and A. Kadir, "Construction of a new 2d chebyshev-sine map and its application to color image encryption," *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 15997–16010, 2019.

[86] L. Guo, H. Du, and D. Huang, "A quantum image encryption algorithm based on the feistel structure," *Quantum Information Processing*, vol. 21, no. 1, pp. 1–18, 2022.

[87] Y. Luo, X. Ouyang, J. Liu, L. Cao, and Y. Zou, "An image encryption scheme based on particle swarm optimization algorithm and hyperchaotic system," *Soft Computing*, pp. 1–27, 2022.

[88] D. S. Malik and T. Shah, "Color multiple image encryption scheme based on 3d-chaotic maps," *Mathematics and Computers in Simulation*, vol. 178, pp. 646–666, 2020.

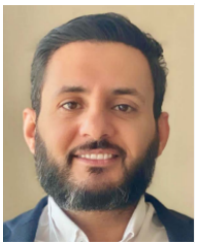
[89] R. Pascanu, C. Gulcehre, K. Cho, and Y. Bengio, "How to construct deep recurrent neural networks," *arXiv preprint arXiv:1312.6026*, 2013.

[90] Y. Zhang, R. Salakhutdinov, H.-A. Chang, and J. Glass, "Resource configurable spoken query detection using deep boltzmann machines," in *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 5161–5164, IEEE, 2012.

[91] A.-r. Mohamed, G. Dahl, G. Hinton, *et al.*, "Deep belief networks for phone recognition," in *Nips workshop on deep learning for speech recognition and related applications*, vol. 1, p. 39, 2009.
[92] P. Palimkar, R. N. Shaw, and A. Ghosh, "Machine learning technique to prognosis diabetes disease: random forest classifier approach," in *Advanced Computing and Intelligent Technologies*, pp. 219–244, Springer, 2022.
[93] R. Bharti, A. Khamparia, M. Shabaz, G. Dhiman, S. Pande, and P. Singh, "Prediction of heart disease using a combination of machine learning and deep learning," *Computational intelligence and neuroscience*, vol. 2021, 2021.
[94] T. M. Ghazal, S. Abbas, S. Munir, M. Khan, M. Ahmad, G. F. Issa, S. B. Zahra, M. A. Khan, and M. K. Hasan, "Alzheimer disease detection empowered with transfer learning," 2022.
[95] M. Elhoseny, M. A. Mohammed, S. A. Mostafa, K. H. Abdulkareem, M. S. Maashi, B. Garcia-Zapirain, A. A. Mutlag, and M. S. Maashi, "A new multi-agent feature wrapper machine learning approach for heart disease diagnosis," *Comput. Mater. Contin*, vol. 67, pp. 51–71, 2021.
[96] J. Rasheed, A. A. Hameed, C. Djeddi, A. Jamil, and F. Al-Turjman, "A machine learning-based framework for diagnosis of covid-19 from chest x-ray images," *Interdisciplinary Sciences: Computational Life Sciences*, vol. 13, no. 1, pp. 103–117, 2021.
[97] A. Maćkiewicz and W. Ratajczak, "Principal components analysis (pca)," *Computers & Geosciences*, vol. 19, no. 3, pp. 303–342, 1993.
[98] P. Xanthopoulos, P. M. Pardalos, and T. B. Trafalis, "Linear discriminant analysis," in *Robust data mining*, pp. 27–33, Springer, 2013.
[99] M. Driss, I. Almomani, J. Ahmad, *et al.*, "A federated learning framework for cyberattack detection in vehicular sensor networks," *Complex & Intelligent Systems*, pp. 1–15, 2022.

Mujeeb Ur Rehman (Professional Engineer) received the Ph.D. degree with distinction from the Faculty of Engineering and Applied Sciences, Riphah International University, Islamabad, Pakistan, in 2022; He is currently a Researcher with the James watt school of Engineering, University of Glasgow, Scotland. He is also a lecturer at Department of Electrical Engineering, Riphah International University, Islamabad, Pakistan. His research interests include Artificial Intelligence, Non-Invasive health care, IoT, Cyber Security, and Multimedia Encryption.

Arsalan Shafique received the B.E. degree in mechatronics engineering from the Wah Engi¬neering College, Wah Cantt, in 2014, and the M.S. degree in electrical engineering from Heavy Industries Taxila Education City (HITEC) Uni¬versity, Taxila, in 2017. He is currently pursuing the Ph.D. degree with the Faculty of Engineering and Applied Sciences, Riphah International Uni¬versity, Islamabad, Pakistan. He is also serving as a Research Associate for Riphah International University. His research interests include cryptography, secure communication, and machine learning.



Yazeed Ghadi (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from The University of Queensland. His dissertation on developing novel hybrid plasmonicphotonic on-chip biochemical sensors received the Sigma Xi best Ph.D. thesis award. He is currently an Assistant Professor in software engineering at Al Ain University. He was a Postdoctoral Researcher with The University of Queensland, before joining Al Ain University. He has published more than 25 peer-reviewed journals and conference papers and he holds three pending patents. His current research interests include developing novel electro-acousto-optic neural interfaces for large-scale high-resolution electrophysiology and distributed optogenetic stimulation. He was a recipient of a number of awards.

Wadii Boulila received the B.Eng. degree (1st Class Honours with distinction) in computer science from the Aviation School of Borj El Amri, in 2005, the MSc. degree in computer science from the National School of Computer Science (ENSI), University of Manouba, Tunisia, in 2007, and the Ph.D. degree in computer science conjointly from the ENSI and Telecom-Bretagne, University of Rennes 1, France, in 2012. He is currently an associate professor of computer science with Prince Sultan University, Saudi Arabia. Wadii received the award of the young researcher in computer science in Tunisia for the year 2021 from Beit El-Hikma. He participated in many research and industrial-funded projects. He has served as the Chair, a Reviewer, and a TPC member for many leading international conferences and journals. He is an IEEE Senior member and a Senior Fellow of the Higher Education Academy (SFHEA), U.K.

Sana Ullah Jan (S'17–M'19) received the B.S. degree in electronic engineering from International Islamic University, Islamabad, Pakistan, in 2012. He has completed a combined M.S./Ph.D. degree from the University of Ulsan, South Korea. Currently, he is a lecturer with Edinburgh Napier University, UK. He previously served as a Lab Engineer with the University of Lahore, Islamabad Campus, Islamabad, Pakistan, from 2012 to 2014. His research interests include wireless sensor networks (WSNs), visible light communications (VLCs), applications of Bluetooth Low Energy (BLE), and machine learning-based sensor fault detection, isolation, and diagnosis applications.

Maha Driss received the Engineering degree (Hons.) in computer science and the M.Sc. degree from the National School of Computer Science, University of Manouba, Tunisia, in 2006 and 2007, respectively, and the Ph.D. degree conjointly from the University of Manouba and the University of Rennes 1, France, in 2011. From 2012 to 2015, she was an Assistant Professor in computer science at the National Higher Engineering School of Tunis, University of Tunis, Tunisia. From 2015 to 2021, she was an Assistant Professor of computer science at Taibah University, Saudi Arabia. She is currently an Assistant Professor of computer science with Prince Sultan University, Saudi Arabia. She is also a Senior Researcher with the RIADI Laboratory, University of Manouba. She served as a reviewer in several world-leading high-impact journals and she has chaired tracks and participated as a reviewer at a number of international conferences.

Jawad Ahmad (Senior Member, IEEE) is currently an experienced researcher with more than ten years of cutting-edge research and teaching experience in prestigious institutes including Edinburgh Napier University, U.K., Glasgow Caledonian University, U.K., Hongik University, South Korea, and HITEC Univer¬sity, Taxila, Pakistan. He has coauthored more than 100 research articles, in international journals and peer-reviewed international conference proceedings. He has taught various courses both at undergraduate (UG) and postgraduate (PG) levels during his career. He regularly organizes timely special sessions and workshops for several flagship IEEE conferences. His research interests include cybersecurity, multimedia encryption, and machine learning and applications. He is an invited reviewer for numerous world-leading high-impact journals.