Healthcare Technology Letters

IET The Institution of Engineering and Technology | WILEY

LETTER

Secure medical image transmission using deep neural network in e-health applications

Ala Abdulsalam Alarood[1] | **Muhammad Faheem[2]** | **Mahmoud Ahmad Al-Khasawneh[3]** | **Abdullah I. A. Alzahrani[4]** | **Abdulrahman A. Alshdadi[5]**

[1]College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia

[2]School of Technology and Innovations, University of Vaasa, Vaasa, Finland

[3]School of Information Technology, Skyline University College, University City Sharjah, Sharjah, United Arab Emirates

[4]Department of Computer Science, Collage of Science and Humanities in Al Quwaiiyah, Shaqra University, Shaqra, Saudi Arabia

[5]Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia

Correspondence

Muhammad Faheem, School of Technology and Innovations, University of Vaasa, Vaasa 65200, Finland.
Email: muhammad.faheem@uwasa.fi

Funding information

University of Vaasa and the Academy of Finland

Abstract

Recently, medical technologies have developed, and the diagnosis of diseases through medical images has become very important. Medical images often pass through the branches of the network from one end to the other. Hence, high-level security is required. Problems arise due to unauthorized use of data in the image. One of the methods used to secure data in the image is encryption, which is one of the most effective techniques in this field. Confusion and diffusion are the two main steps addressed here. The contribution here is the adaptation of the deep neural network by the weight that has the highest impact on the output, whether it is an intermediate output or a semi-final output in additional to a chaotic system that is not detectable using deep neural network algorithm. The colour and grayscale images were used in the proposed method by dividing the images according to the Region of Interest by the deep neural network algorithm. The algorithm was then used to generate random numbers to randomly create a chaotic system based on the replacement of columns and rows, and randomly distribute the pixels on the designated area. The proposed algorithm evaluated in several ways, and compared with the existing methods to prove the worth of the proposed method.

1 | INTRODUCTION

In our current era of information technology, the rapid growth of the Internet, especially in electronic health care, has made electronic health care feasible and widespread. Electronic health care is considered one of the systems based on the Internet in a way that makes the patient able to contact the specialist doctor who is able to diagnose. Medical images are stored and sometimes processed, and then sent to the Internet later. During storage, some secret data can be added. The addition of secret data is often necessary but is sensitive for both parties. Therefore, the best way to preserve the privacy of patients, whose information may be highly confidential and sensitive, is to encrypt the data in a way that it is available only to authorized persons [1]. There are some characteristics that distinguish

medical images, including redundancy, high correlation between image pixels, and huge size of data. Unlike the ordinary images, encryption in medical images requires a special effort related to the speed and accuracy in extracting data. However, it is sometimes not suitable for securing large medical images. It is therefore necessary to secure the algorithms that process medical images against attacks [2]. A random number generator is usually used to generate a string of numbers in a schematic sequence rather than a logical one used for encryption. The more random the number that is generated, the more it helps in encryption, and is more feasible. In this regard, chaos systems are used to generate and design pseudo-random numbers in order to generate a strong encryption key [3]. Some of the techniques are distinguished from other technologies in several aspects, including in terms of the power of generating initial

random numbers, the reactions of the numbers, the amount of their sensitivity to the initial conditions, the long frequency, and the availability of space for the large encryption keys. Accordingly, this paper attempted to combine two methods of chaotic system and key optimization which will provide great performance in terms of security and speed. In addition to the rigor and strength of the algorithm, the contribution to an efficient algorithm must be the encryption process. Most of the algorithms are not efficient in real time because of the length of the algorithm sequence and the performance is not efficient to be online [4]. Algorithms are often vulnerable to attacks from external programs, especially in the case of online transmission. With regard to the development of the current devices and their wonderful performance, it contributed to the improvement of algorithms, especially in terms of random generation of numbers. In general, the performance of the devices is in two main aspects: increasing the frequency of the device (processor) speed and optimizing the use of a specific processor. In terms of hardware implementation, there are two options, ASIC and FPGA; the first is somewhat costly, and the second is a promising solution. FPGI is efficient in that it allows the designer to use basic programmable logic elements in designing and creating intelligent algorithms, but they are generally expensive in terms of design in general. As for the other type, it can be developed to be the same type of performance at a lower cost, but with tremendous efforts. The first type is capable of executing at the required speed and means processing hardware more than software.

Deep Learning (DL) and Artificial Intelligence (AI) have advanced rapidly in recent years. Artificial intelligence techniques have played very important roles in the field of medical images [5], such as processing and diagnosis by computer, and performance of all operations on images such as interpretation, merging, recording, and segmentation. Most of the images come from directed devices with radiation, and therefore, they are retrieved and analyzed using deep learning to extract information from the image, and the information is represented effectively. Deep learning algorithms help doctors make accurate decisions in diagnosing diseases quickly and efficiently, and this could prevent diseases in a timely manner. Artificial intelligence techniques help doctors understand how to analyze images, the differences between them, and the real causes of the disease. Artificial intelligence techniques include a lot of methods such as support vector machine (SVM) [6, 7], neural networks (NN) [8], K-nearest neighbor (KNN) [9], and other algorithms related to deep learning like convolutional neural networks (CNN), recurrent neural networks (RNN), and long short term memory (LSTM) [10], and the extreme learning model (ELM) and generative adversarial networks (GANs), which are limited in processing natural images and require a long time for analysis and more time for processing features. These algorithms are fed with raw data in analyzing the data as a whole, followed by the required classification. Learning algorithms try to learn many levels of abstraction and representation, and glean information from a large set of images that often exist in a standard database. These images show the desired behaviour of the data. Despite the discovery that was made in diagnosing diseases through medical imaging according to traditional methods, which showed accuracy in diagnosis over decades of time. Therefore, the development of deep learning has made a breakthrough in the performance of algorithms and the accuracy of work. At present time, speed and accuracy have been among the most sought-after important factors. Meanwhile, deep learning algorithms have proven their efficiency in many areas such as speech recognition, lip reading, text recognition, accurate computer diagnosis, face recognition and effective drug discovery.

The motive of this study was to develop a method for processing medical images using deep learning technology, controlling the number of hidden layers in the neural network using the highest effect factor, and processing and classifying the extracted features in a new way to diagnose diseases and heal the image in a way that protects the information from threats such as hacking.

The contribution of this manuscript is to find a chaotic system that is not detectable using DNN algorithm and adaptation of the deep neural network by the weight that has the highest impact on the output, whether it is an intermediate output or a semi-final output.

The remainder of the manuscript has been arranged as follows: Section 2 is related to previous studies related to the subject and the most important studies in this field. The subject methodology is presented in Section 3. Then, the results are presented in Section 4. Finally, the conclusions are presented in Section 5 of this research.

2 | RELATED WORK

Many previous studies have dealt with Security images in general [11], and medical images in particular [12]. The security of data and images is related to the strength of the proposed algorithm. Many algorithms have been proposed in the literature and often rely on robust random key generation [13]. A method of generating a secure key with reduced latency and based on the cardiogram in encryption [14] has been proposed. An improved method was proposed by [15] to heal the medical image using Fibonacci, which had the effect of scattering and hiding the information of the medical image [16]. The AES algorithm method was used to generate random numbers [17] from electrical impulse generators to increase the security of the resulting image. A dynamic cipher system based on state estimation has been proposed by [18] which is the basis for cipher key generation. The level of challenge was raised in relation to generating the highest randomness in relation to the initial key, which constantly changes with work and time [19], and it had an effective impact on the security of the medical image transmitted between the parties.

Exploring the chaotic system had an impact on the safety of the medical image [20] and the exploration of the usefulness of linear systems, which deals with the basic elements of coding such as sensitivity, predictability, pseudo-randomness and certainty [21]. Seed generation by the artificial intelligence system is a method proposed in order to increase the randomness of the
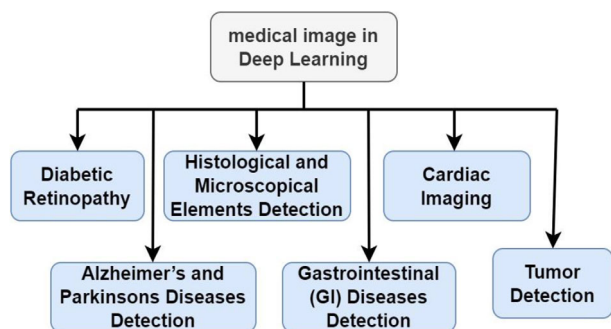
FIGURE 1 type of medical image detection by deep learning technique.

data distribution in medical images, which is difficult to trace the data [22], and it is a method based on complete randomness and has proven its effectiveness through graphing and linear results. A method adopted by current researchers [23] depends on a new method that has proven its worth through evaluation, which relies on a hybrid algorithm to generate chaos in the pixel distribution of the image again [24], and the chaotic sequences are difficult to track inside the image, only through the encryption key through which it is retrieve data [25].

Other researchers worked to cancel the relationship of pixels in the image that were preserved by certain equation, and this equation works to track the effect of pixels in the image and build a path that can be traced by the encryption key. Artificial intelligence techniques were used in the encryption of medical images in order to increase the security of data in them [26], and many researchers obtained unexpected results when using algorithms based on artificial intelligence such as ANN, CNN, and SVM, decision tree, NN, and others such as KNN [27]. Many medical image diagnostic tasks require research and new ways to identify abnormalities and changes to images over time. Deep learning algorithms came to open up many horizons in this regard. Many image resources are processed in deep learning techniques, which are sourced from three main types (X-rays—CT—and MRI scan). Most of the types of diseases diagnosed using deep learning are shown in Figure 1.

i. Diabetic retinopathy: The manual process of diagnosing and detecting diabetic retinopathy (DR) is difficult and takes a long time, as this disease does not show early symptoms, and so, the doctor needs a picture of the bottom of the retina. Accordingly, deep learning has proven its accuracy in working on this type of image. A deep learning algorithm was used in the Deep Convolutional Neural Network (DCNN) from the eye image archive to classify the signals of the moderation [27]. The deep learning algorithm was trained on standard dataset (EyePACS-1) collected from 847 patients, and the accuracy and sensitivities exceeded 95% [28]. And another study used DNN on different dataset (Kaggle fundus) to diagnose bleeding, secretions and aneurysms [29].

ii. Histological and microscopical elements detection: In histological analysis, the cell and surrounding tissues are studied. The changes that occur in it reflect the characteristics and features through which the disease can be diagnosed. Imaging and colouring of cells in dermatology give a clear picture of the disease. Therefore, to increase the accuracy of diagnosis, artificial intelligence algorithms such as DNN are used. Recently, many researches related to this type of disease have been published, and DNN applications have been used to diagnose cancer cells in the colon [30, 31]. Another study was conducted on thoracic lymph nodes and interstitial lung disease using CNN algorithm. There are many studies that used CNN in the early diagnosis of breast cancer by classifying features extracted from medical pictures [32]. A standard dataset was used to train the RNN algorithm by 75%, and the results showed its effectiveness in detecting the disease early and in limiting its spread.

iii. Gastrointestinal (GI) diseases detection: Mock processing through deep learning plays a vital role in analyzing diseases and in helping doctors in providing accurate and efficient treatment, owing to the advancement of computer science, computer analysis and the science of image processing, which are obtained from X-rays or magnetic resonance imaging (MRI). Accordingly, the DCNN method was used to detect haemorrhage in images from capsule endoscopy [33]. Additionally, a study was carried out using fully supported and fully stacked FCN networks compatible with LSTM by dividing big data into small data for ease of obtaining characteristics [34]. In another study, a set of features was extracted by the hybrid method and classified using CNN to detect digestive diseases in the image of MRI [35]. In a related study, a rapid feature extraction method using CNN technique was presented to detect inflammatory gastrointestinal diseases in WCT videos, and the extracted features were classified using SVM [36].

iv. Cardiac imaging: Deep learning provided an excellent method for imaging the heart, and in particular for measuring calcium scores. MRI images are common in this field [37]. SVM was used to classify the features extracted from the image and find the appropriate diagnosis [38, 39]. The diagnosis of the heart was done using features that enter into more than one of the hidden layers, which in turn gives an output and a line that is taken into account in choosing the accuracy of the result in the NN algorithm [40].

v. Tumour detection: Abnormal cell growth in one place is called a tumour. There are two types of tumour; one is non-cancerous (benign tumour) and the other is cancerous (malignant tumour). A study by [41] employed a method for diagnosing a tumour from a mammogram in a database containing 482 images, after removing noise using a median filter. Many researchers in the literature have used the famous SVM classifier to classify the features extracted from mammograms to diagnose benign or malignant tumours. The CNN algorithm was fed with specifications extracted from radiographic images, measuring the amount of clustering in each part of the image, and relying on it in the classification to diagnose the disease [42].

vi. Alzheimer's and Parkinson's diseases detection: This disease is considered a neurological disorder associated with

a pro-faulty decrease in motor accuracy. This disease is associated with the breakdown or death of dopaminergic neurons. Alzheimer's disease can be diagnosed by clinical images and by measuring the shift in the fixed features in the CT image. The deep Boltzmann machine (DPM) was used to measure the additional features and find out the distortions of the 3D magnetic resonance images [43]. 3D image was explored by [44] to investigate Alzheimer's disease by extracting good features of the image and classifying them using CNN. A dataset was used CAD Dementia for MRI and satisfactory results were obtained for people over the age of 75 years. Also, another group of authors used RMI brain images to detect whether the brain is healthy or of Alzheimer's, and the result was 98% in accuracy for training the data on images of basal standard data [45].

3 | PROPOSED METHOD

The work methodology in general consists of two main parts, whereby the first is to maintain data security in the medical image by improving its encryption method, and the second is to classify the features extracted from the image using deep learning and DNN algorithm. In encryption in general, there are two stages, the contribution to the proposed method lies in the two main parts of the work: confusion and diffusion. For confusion we choose pixel position and sub-blocks randomly by helping of DNN algorithm in additional to changing the value of pixels controlled also by the same algorithm. Encryption is the process of hiding image information so that it is secure and no one can see it without the encryption key. The encryption is based on the irregular scattering of data in relation to the outside world, and it cannot be rearranged except with the presence of the encryption algorithm. The proposed method is based on a chaotic system that extends in two stages: The region of interest (ROI) and the pixels in that region. First, the random key is generated, and chaos systems are very useful in this case. The entropy of the image as well as its statistical behaviour in randomness are handled. The Henon Map method was used to generate the key because of the ideal behaviour of this algorithm as well as it is scalable and compatible with many methods. The following Equation (1) can define the key generation:

$$\text{initial key} = \begin{cases} x_{n+1}, & 1 - ax_n^2 + y_n \\ y_{n+1}, & bx_n \end{cases} \qquad (1)$$

where x and y are two variables and a and b are two parameters that satisfy the chaotic behaviour such as $a = 1.4$ and $b = 0.3$, while n is iteration numbers, in Henon initial state that starts with x_0 and y_0 to initialize the key.

The system in general starts with generation of key of 128, followed by the formation of bit stream of random sequence, and then the initiation of encryption with variable iterations as shown in Figure 2.
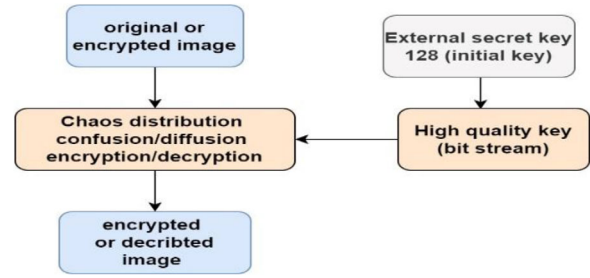

FIGURE 2 General illustration of proposed encryption system.

ALGORITHM 1 General proposed stage for image encryption using DNN.

1- **Read** images from dataset
2- **For** all image **do**
    2.1 **Preprocessing** given image
    2.2 **Extract** features from image
    2.3 **Creat**e Neural Network
    2.4 **Determine** effective parameters in the network
3- **Update** hidden layers and nodes according certain parameters
4- Confusion process
    4.1 **Use** DNN to select partition of image
    4.2 **For** each partition use DNN to scrambling
    4.3 **Update** cypher key
5- Diffusion process
    5.1 **While** not EOI Do
    5.1 **Move** pixels into vector
    5.2 **Use** DNN to change pixel value (vertically and horizontally)
    5.3 **Update** cypher key
6- Save the encrypted image to a file or transmit it through a secure channel for storage or further processing
7- Return to step 2

The deep learning algorithm uses the proposed method in the process of encryption the medical image from the process of reading the images from the standard dataset and then applying all the procedures to it from segmenting it into blocks and then changing the pixel values. As explained in Algorithm 1

In order to generate a high-quality key, which is the basis for the encryption process, some variables can be suggested; these variables are in the form of parts that can be interlocked with deep learning. The variables can be described as follows:

$$X\ h_0 = \frac{(k_1 \oplus k_2, \oplus \dots, \oplus k_8)}{2^8} \qquad (2)$$

$$Y\ h_0 = \frac{(k_9 \oplus k_{10}, \oplus \dots, \oplus k_{16})}{2^8} \qquad (3)$$

where $K_i = k_1\ |k_2|k_3, \dots, |k_{16}$ are the sequence of iteration for each layer in neural system. The encryption key uses itself in the initial cycles as soon as the hidden layers are changed in deep learning. The value of key 16 is better than its analogues to create a chaotic context added to the design of nodes in the proposed layers in the neural network system. Then, the statistic behaviour of the random system can be described in Figure 3.

The random number remains in constant change with each cycle in random sequence. This allows the conversion of the
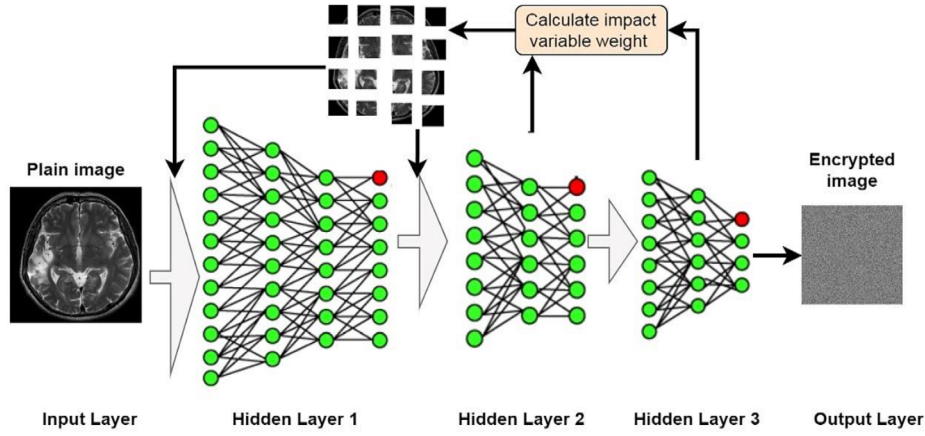
FIGURE 3 Behaviour of proposed image encryption within deep learning algorithm.

number to the appropriate chaotic state of the system. A key consisting of 128 works on a highly random statistical behaviour can be described by the following equations:

$$XH = \left(Xh_i \times 10^{12}\right) \bmod 2^{16} \tag{4}$$

$$YH = \left(Yh_i \times 10^{12}\right) \bmod 2^{16} \tag{5}$$

In encryption in general, there are two stages. The first stage is the confusion stage, in which the locations of the pixels in the image are changed. In this regard, the locations are of two types. First, changing the columns according to certain equation and second is changing the rows to increase the randomness of secret image. The process of changing, with respect to rows and columns, increases the security of the medical image, in addition to changing the dependence of parts of the images cut from the original image through deep learning. Figure 4 can be referred.

The second stage of image encryption is called diffusion, and through it, the pixel values of the image are changed, and thus noise is generated. To achieve encrypted image, the OR operation is performed between the pixel value, the K key, and the scrambled image vector.

One of the most random operations that take place in the image encryption process is the process that accompanies the random division and segmentation of the image, in addition to the random distribution of pixels in the image through deep learning, consisting of several stages in the formation of the hidden layers of the neural network and the feedback process that allows reprogramming each of the hidden layers according to the infectiousness of each iteration. The well-known standard neural network components are the main parts such as the input layer, the hidden layer, and the output layer. Deep learning contributes and interferes with the components of the hidden layer depending on the input layer, which is the main interest of the work. Several parameters control the deep neural network, and some of them are variables that can be changed according to the desired result, while some are fixed parameters that can only be changed by changing the structure of certain layer in the neural network. These parameters will be illustrated in details during the discussion of design neu-

ral network. Figure 5 shows the adaptive design of deep neural network.

where w considers the weight of neural network derived from each hidden layer such as hidden layer got variable length (number of nodes) from certain layer into next layer can get by:

$$y_m = w_{nm} \cdot x_m \tag{6}$$

This function is called transection function from layer to another layer (except for recursive flow), and source node is given by $x_m = x_{m-1} \bmod x_m$ and destination node is given by $y_m = y_m + y_{m+1}$. The most important thing is how to control the recursive function that will be discussed in the next paragraph.

Output layer is considered the final result reflecting the complexity with desired results. Relevantly, hyperbolic equation reflects the result after many iterations in neural stage to achieve good prediction. Furthermore, neural machine can give many encryptions, and it is crucial to automatically to choose the best one to increase the efficiency of the proposed system. Hence, deep learning, namely machine learning was proposed. The next section will detail the contribution in this issue.

Many variables control the neural network and by training the network with these variables, the best possible prediction result can be controlled. Several features are extracted from the medical image in the algorithm. The feature that has the highest impact on the result is chosen, and the least effect is ignored, and then the work cycle is repeated. If the result continues to increase, the system automatically increases one hidden layer. If the result is stable, increment one node in the specified hidden layer, and so on. The main interests of parameters are weight, transection, recursive number and flow, number of iteration ratio with feedback, and acknowledgement from each neuron and layer. In order to find the high impact parameter, the structure of neural network must be integrated, and the network must be fully connected to achieve result of each stage with flow of information through these stages.

- The standard enclosure of neural system is represented by infinite weighted summation with two samples present and
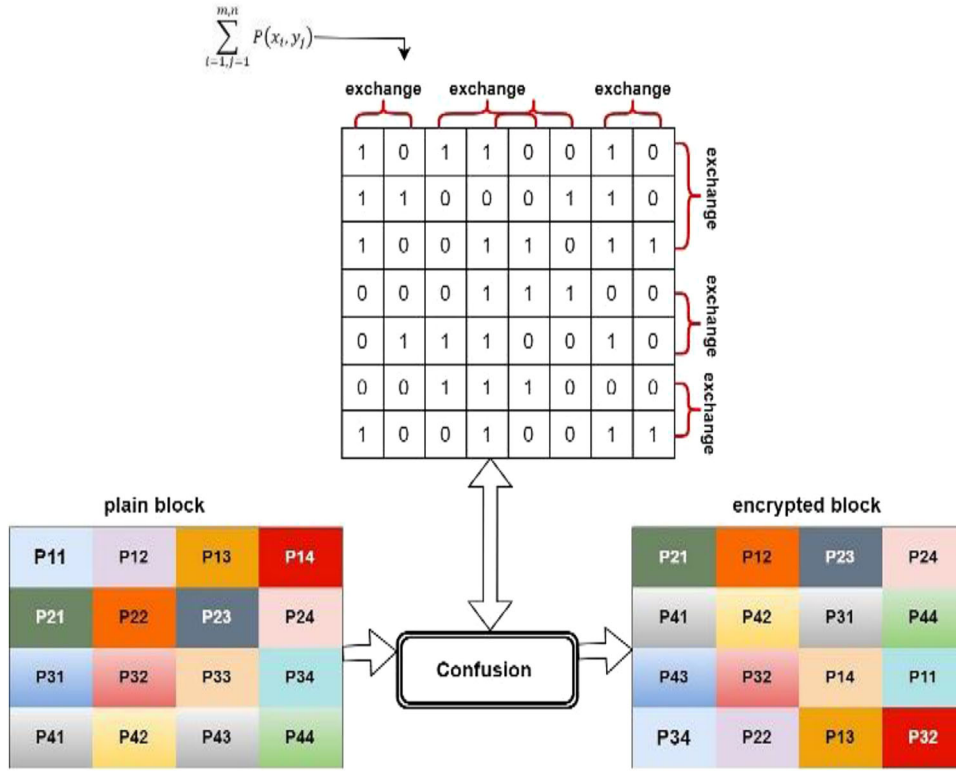
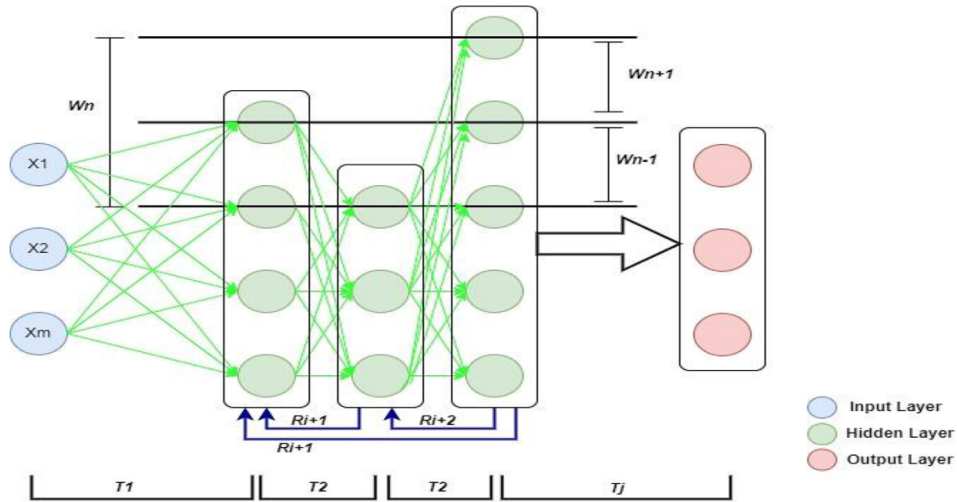**FIGURE 4** Confusion process in proposed method.

FIGURE 5 Proposed structure of neural network.

past for input signal $(x_j(n))$ and delayed one is $(x_j(n-1))$ represent delay by *1* time and the output signal $y_j(n)$ can be expressed with Equation (7):

$$y_k\ (n) = \sum_{i=0}^{\infty} w^{i+1} x_j\ (n-1) \qquad (7)$$

where w is the weight that controls the flow of data within the network, and i is the number of ' for training network. The structure is as illustrated in Figure 6.

In this regard, the weight derived from the structure achieves three cases distinguished as follows: (a) $|w| < 1$ represents the output signal of $y_k(n)$ exponentially which means that the system
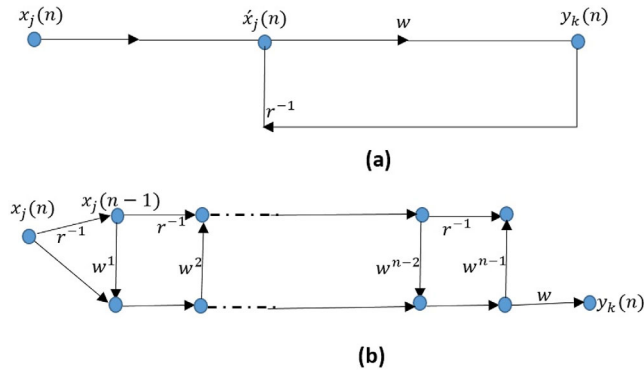
FIGURE 6 (a) signal flow graph of one stage in neural system; (b) flow graph with recurrent data flow of corresponding weight.

FIGURE 7 Strategy of node structure created and derivation.

is stable; (b) $|w| = 1$ represents the linear behaviour; (c)$|w| > 1$, represents negative exponential.

Now, for power N, the factor $|w|$ will be small enough to achieve neglecting case asw^N, and for practical purpose, the situation produces the finite sum of y_k.

$$y_k(n) \approx \sum_{l=0}^{N-1} w^{l+1} x_j(n-1) \tag{8}$$

This means that the suggested weight will be:

$$y_k(n) = wx_j(n) + w^2 x_j(n-1)$$
$$+ w^3 x_j(n-2) + \cdots + w^N x_j(n-N+1) \tag{9}$$

Then derived weight (w) will store in vector for next classification. Thus, in deep neural network, the weight will be changed according the behaviour of the system, whether it will increase or decrease for each iteration. In this study, weight parameter is classified in addition to other parameters to obtain the best prediction in the deep learning system.

- The flow of the system is the second parameter considered in the proposed system due to its direct effects on the result of next stage. There are many cases in the data flow such as when one input to the node produces one input, or two inputs from different nodes produce one output of the node, and many other cases for different iterations in the system. If input will classify into Boolean number such accepted or not in certain stage, and weight w consider the bias or control to the system in one stage and in one node.

This step will estimate the neurons in the next step based on the output function and bias that controls the weight at each stage.

Figure 7 illustrates the behaviour of neural when updating multiple layers in deep neural system whither forwarding or feedback data. XOR operation is implemented during iterations and in several ways. Direction of data flow comes from inherent node or not, and sometime from recurrent flow. All these give
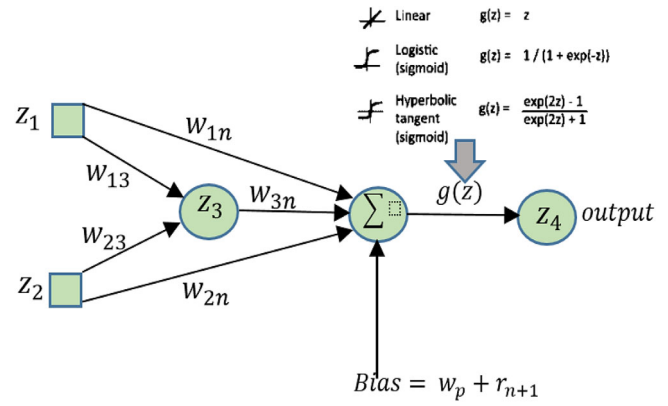
the factor for node to direct the new flow to the appropriate node.

The last pattern must give achieve if $(w_n + w_{n+1}) > 0$ then $x_{n+2} = 1$ and if $(x_n \oplus x_{r(n+2)}) = 1$ then new nod created. Two patterns at the same layer cannot achieve the same result function because of the consistent update and control of data flow by predicted bias.

All transaction flow will store in certain vector to classify later as a deep learning system for better prediction.

- Recurrent network is the third parameter that can be used for deep neural network to increase accuracy. Recurrent network can be defined as the flow distinguishes from other feed-forward neural layers and represented as at least one feedback loop.

4 | RESULT AND DISCUSSION

In this section, the proposed algorithm for encryption and securing medical images was evaluated and tested. Two types of images namely colour and grey medical images were used in our study, and the test was also done on images from a standard dataset in order to benchmark and find out the strength of the proposed method. The image resolution was 512×512, and the result was simulated using MATLAB 2015a, a laptop computer equipped with CPU of Core i9, 3.9 speed, 32 GB memory, and Fedora 32 operating system. Among the information used in the algorithm is the size of the blocks in the partition which was 32 (and $n = 4$) which was repeated 10,000 times. The proposed method is adapted to images with different dimensions, because it works on any distribution of pixels and any partition of the sub-blocks. As for the segmentation process, it is not affected in any way, and the deep neural network works in the same way in different types of images.

4.1 | Simulation results

Simulated results on image security refer to the use of computer simulations to evaluate the effectiveness of different
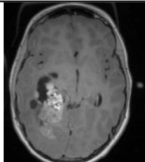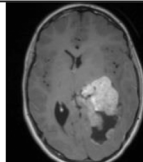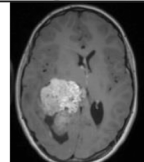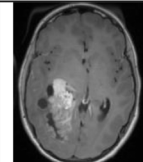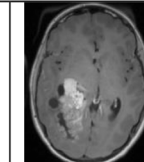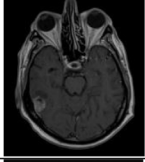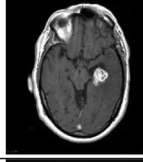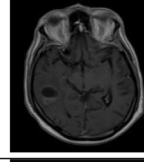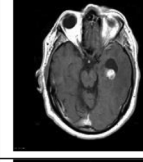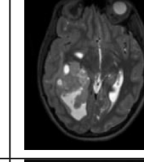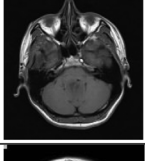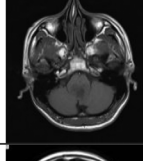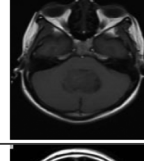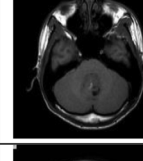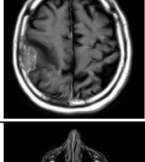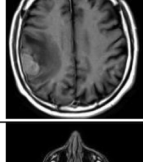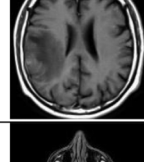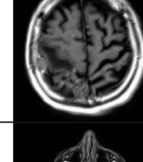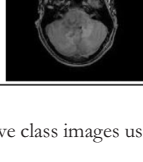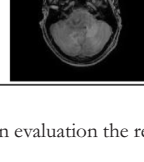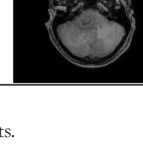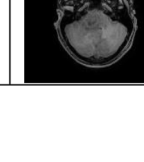
Image samples					Label	Description
					Image 1	Flat tomography of the brain
					Image 2	Upper cerebral tomography
					Image 3	Lower cerebral tomography
					Image 4	Imaging of the cerebral hemispheres
					Image 5	Imaging of the eye socket and hindbrain

FIGURE 8   Labels of five class images used in evaluation the results.

techniques and algorithms for securing digital images. This process involves creating a digital image and then testing it against various attacks that can compromise its security, such as tampering, copying, or alteration. There are several techniques used in simulated image security testing, including watermarking, steganography, and encryption. In proposed method we consider encryption between two sides. Encryption is a technique that involves transforming the image data into a form that can only be decrypted by authorized parties. This can help to protect the image from being accessed or altered by unauthorized individuals.

Simulated results on image security are an important tool for evaluating the effectiveness of image security techniques and algorithms. They can help to improve the security of digital images and protect them from unauthorized access and tampering. Many images were considered in this study and most of these images are from a standard brain tomography dataset. Figure 8 depicts image labels that used in evaluation through proposed method within five classes.

In encryption, there are many evaluation criteria achieved such as:

i. information entropy

The randomness of the image can be measured in information entropy and is defined by the following equation:

TABLE 1   Entropy of proposed algorithm.

Tested images	Entropy
Image 1	7.9992
Image 2	7.9994
Image 3	7.9993
Image 4	7.9984
Image 5	7.9989

$$H\ (m) = \sum_{i=1}^{w} P\left(m_i\right) \log_2 \frac{1}{P\left(m_i\right)} \qquad (10)$$

For instance, $P(m)$ considers the probability of the appearance m, to grey scale image where the max entropy will be 8. When the entropy reaches 8, it means that the randomness of the image is large and good, that is, the distribution of pixels on the image is more random. Table 1 shows the randomness of the encrypted medical image, where the entropy is close to 8.

In this regard we can conclude that the proposed method is worthy in generated randomness of encrypted image.
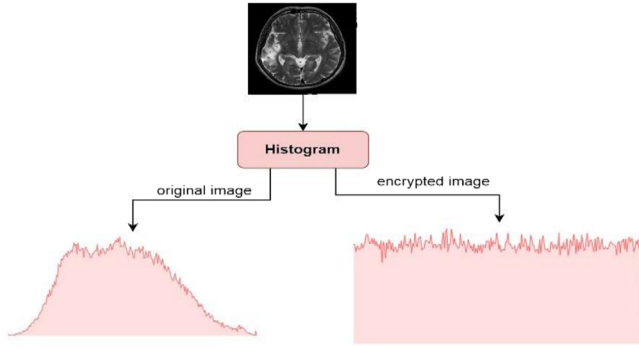
FIGURE 9 Histogram of pain image and encrypted image.

TABLE 2 Analysis of Chi-Square of encrypted image.

Given image	Encrypted image
Image 1	260.9
Image 2	241.1
Image 3	231.5
Image 4	270.5
Image 5	212.8

TABLE 3 Correlation coefficient of proposed method.

Image	Direction	Original image	Encrypted image
Image 1	V	0.987	−0.011
	H	0.976	0.019
	D	0.962	0.014
Image 2	V	0.991	0.005
	H	0.991	−0.007
	D	0.976	−0.041
Image 3	V	0.987	−0.022
	H	0.976	0.006
	D	0.962	0.008
Image 4	V	0.977	−0.041
	H	0.981	0.009
	D	0.976	0.004
Image 5	V	0.981	0.062
	H	0.973	0.081
	D	0.942	0.062

ii. Image Histogram

The histogram reflects the behaviour and distribution of the pixels in the image. In the encrypted image, the histogram should prevent attackers from guessing the image information. The histogram of the encrypted image should not be the same as the original image. In Figure 9, the graph shows a medical image before and after encryption.

The experiment further confirmed the histogram calculations of the encrypted image, which depend on the square test calculated as follows:

$$X^2 = \sum_{i=1}^{256} \frac{(O_i - EV)^2}{EV} \qquad (11)$$

where O_i is the recurrent rate for grey value i, and EV is $O/256$ is the expected frequency of the grey scale. Accordingly, the chi-square of the encrypted image is illustrated in Table 2.

Among the tests and evaluations of the encryption algorithm, Chi-Square is used, which is considered one of the most important statistical tests to determine the similarity between the original and the encrypted image. This is because the expected image should be as close as possible to the original image, and the best measure for this prediction is the Chi-Square algorithm. The application of this type of standard because it is the only one capable of distinguishing between noise and an encrypted image, because noise degrades the loss of image data, but an encrypted image cannot lose any type of data. It is considered one of the most important measures of randomness.

iii. Correlation coefficient

Neighbouring pixels in a normal image have a coherent correlation. On this basis, the low correlation between adjacent pixels can reflect the strength of encryption in the image. Mathematically, the correlation between two adjacent pixels is determined by the following equations:

$$r\ (A, B) = \frac{E\left((A - E\ (A))\ (B - E\ (B))\right)}{\sqrt{D\ (A)\ D\ (B)}} \qquad (12)$$

$$\mathrm{E}\ (A) = \frac{1}{s} \sum_{i=1}^{s} A_i \qquad (13)$$

$$D\ (A) = \frac{1}{s} \sum_{i=1}^{s} (A_i - E\ (A))^2 \qquad (14)$$

From the above: A and B are considered as the values of two adjacent pixels, where s is the number of selected pairs (A and B). The values of the correlation coefficient for the encrypted medical image are in the form of vertical V, horizontal H and diagonal D directions. The correlation coefficient in the images is close to zero and the correlation coefficient values are presented in Table 3. The evaluation also includes the benchmarking with existing method in literature as shown in Table 4.

iv. Differential attack

Differential attack depends mainly on guessing information about the medical image by making a small change in the normal image and the encrypted image using the same method. The change should be so slight so that it does not arouse suspicion. To assess the performance, it is necessary to find the number of pixel change rate (NPCR) and the unified

TABLE 4 Benchmarking of the correlation coefficient values with existing methods.

Method(s)	H	V	D
Proposed	−0.007	0.005	−0.041
[46]	−0.001	0.009	−0.003
[47]	0.002	0.001	0.001
[48]	0.002	−0.001	0.000
[49]	0.094	0.005	0.006
[17]	0.009	−0.007	0.018

TABLE 5 Performances of NPCR and UACI.

Images	NPCR	UACI
Image 1	99.60	33.41
Image 2	99.61	33.40
Image 3	99.63	33.44
Image 4	99.61	33.45

TABLE 6 Performances of NPCR and UACI.

Methods	NPCR	UACI
Proposed	99.61	33.42
[46]	99.61	33.26
[47]	99.53	33.45
[48]	99.51	33.39
[49]	99.79	33.16
[17]	99.60	33.49

average changing intensity (UACI). Then, the Equation below is used:

$$NPCR = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\% \quad (15)$$

$$D(i,j) = \begin{cases} 0 & if \ E_1(i,j) = E_2(i,j) \\ 1 & if \ E_1(i,j) \neq E_2(i,j) \end{cases} \quad (16)$$

$$UACI = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|E_1(i,j) - E_2(i,j)|}{255} \times 100\% \quad (17)$$

E_1 and E_2 are considered as two encrypted images of the plain and modified one (when changing one pixel in the plain image), while M is the width of image, and N is the height. Different attacks can be recognized by NPCR and UACI values as shown in Tables 5 and 6, respectively.

v. Key space

The key space is an important statistical standard and is used to measure the encrypted image, and it must be at least 2100, because key space lower than the aforementioned would

mean that the algorithm is weak and can be broken using brute force attack. The initial condition Y_0 can be a support for this method, while a is the control parameter, with iteration number N_0 in chaotic map. Hence, the accuracy of Y_0 will be 10^{16} while the $N_0 = 10^3$, and so, the total key space will be 10^{35}. This will give the proposed algorithm the strength to stand against brute force attack.

5 | LIMITATION

Each algorithm has limitations, including our proposed algorithm. These limitations can be summarized as follows: Computational load. Encryption algorithms, especially those that are concerned with images, are powerful, but require significant implementation time and effort, which constitutes a challenge in itself. Key management is considered important, especially after the development of information technology and the experiences gained by hackers and intruders. In the event that the encryption key is lost or cannot be accessed, it becomes impossible to decrypt the image, so in the future a recovery must be developed for such cases. Among the limitations is the incompatibility with compression or reduction and enlargement. In this case, the data that is inside the image may be lost and cannot be returned to. This creates a lot of complexity in such cases.

6 | CONCLUSION

Medical images have recently become the subject of interest to many researchers, especially in keeping them secure. This has led to the need to use AI algorithms, in order to move away from the traditional methods to obtain better results. The deep neural network method was used to segment medical images, distribute the small parts randomly, and then distribute the pixels to certain areas randomly. Using the deep neural network technique, the randomness that was used in confusion and diffusion was increased. The deep neural network was developed by calculating the high weights that have an effect on each hidden layer of the system and returning the useful feedback to the nodes in those layers. One of the most important elements that have been taken care of in the proposed method is the process of distributing and dividing the image blocks according to the most impact variables in the result of the deep neural network. And in both stages, confusion, diffusion, and randomness of pixels in the image in additional to scrambling bits of pixels for changing pixel value. When evaluating the proposed algorithm by several criteria, as well as when benchmarking the results with previous research, the proposed method has been proven.

REFERENCES

1. Hasan, M.K., Islam, S., Sulaiman, R., et al.: Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access 9(6), 47731–47742 (2021)
2. El-Shafai, W., Khallaf, F., El-Rabaie, E.S.M., El-Samie, F.E.A.: Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. J. Ambient Intell. Hum. Comput. 12(10), 9007–9035 (2021)
3. Avudaiappan, T., Balasubramanian, R., Pandiyan, S.S., Saravanan, M., Lakshmanaprabu, S.K., Shankar, K.: Medical image security using dual encryption with oppositional based optimization algorithm. J. Med. Syst. 42(11), 1–11 (2018)
4. Uetama, T.R., Setiawan, W., Sofyan, E.: Performance comparison of real time image processing face recognition for security system. Proc. Conf. Manage. Eng. Ind. 2(1), 21–25 (2020)
5. Fourcade, A., Khonsari, R.H.: Deep learning in medical image analysis: a third eye for doctors. J. Stomatol. Oral Maxillofac. Surg. 120(4), 279–288 (2019)
6. Balasubramaniam, V.: Artificial intelligence algorithm with SVM classification using dermascopic images for melanoma diagnosis. J. Artif. Intell. Capsul. Netw. 3(1), 34–42 (2021)
7. Sulong, G., Mohammedali, A.: Human activities recognition via features extraction from skeleton. J. Theor. Appl. Inf. Technol. 68(3), 67 (2014)
8. Shahid, N., Rappon, T., Berta, W.: Applications of artificial neural networks in health care organizational decision-making: a scoping review. PLoS One 14(2), e0212356 (2019)
9. Kamal, M.S., Northcote, A., Chowdhury, L., Dey, N., Crespo, R.G., Herrera-Viedma, E.: Alzheimer's patient analysis using image and gene expression data and explainable-AI to present associated genes. IEEE Trans. Instrum. Meas. 70, 1–7 (2021)
10. Yue, Z., Ding, S., Zhao, W., Wang, H., Ma, J., Zhang, Y., Zhang, Y.: Automatic CIN grades prediction of sequential cervigram image using LSTM with multistate CNN features. IEEE J. Biomed. Health. Inf. 24(3), 844–854 (2019)
11. Li, C., Zhang, Y., Xie, E.Y.: When an attacker meets a cipher-image in 2018: A year in review. J. Inf. Secur. Appl. 48(3), 102361 (2019)
12. Elhoseny, M., Shankar, K., Lakshmanaprabu, S.K., Maseleno, A., Arunkumar, N.: Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Comput. Appl. 32(15), 10979–10993 (2020)
13. Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A.K., Yang, P., Huang, H., Hou, G.: Secure and robust fragile watermarking scheme for medical images. IEEE Access 6(8), 10269–10278 (2018)
14. Ghafoor, R., Saleem, D., Jamal, S.S., Ishtiaq, M., Ejaz, S., Jamal Malik, A., Khan, M.F.: Survey on reversible watermarking techniques of echocardiography. Secur. Commun. Network 2021, 8820082 (2021)
15. Salem, N., Elnaggar, F.: RIFD fibonacci zeckendorf hybrid encoding and decoding algorithm for medical image compression and reconstruction. In: *2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA)*. Valencia, Spain, pp. 66–73 (2020)
16. Guo, C., Liu, J., Li, W., et al.: Imaging through scattering layers exceeding memory effect range by exploiting prior information. Opt. Commun. 434, 203–208 (2019)
17. Hua, Z., Yi, S., Zhou, Y.: Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process. 144, 134–144 (2018)
18. Biswas, M., Kuppili, V., Saba, L., et al.: State-of-the-art review on deep learning in medical imaging. Front. Biosci. 24(3), 380–406 (2019)
19. Abd-El-Atty, B., Iliyasu, A.M., Alaskar, H., Abd El-Latif, A.A.: A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. Sensors 20(11), 3108 (2020)
20. Vaseghi, B., Mobayen, S., Hashemi, S.S., Fekih, A.: Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption. IEEE Access 9, 25911–25925 (2021)
21. Sangavi, V., Thangavel, P.: An exotic multi-dimensional conceptualization for medical image encryption exerting Rossler system and Sine map. J. Inf. Secur. Appl. 55, 102626 (2020)
22. Ye, C., Chen, C.: Secure medical image sharing for smart healthcare system based on cellular neural network. Complex Intell. Syst. 9(2), 1653–1670 (2023)
23. Ebrahim, S.M.A.: Hybrid chaotic method for medical images ciphering. arXiv:2012.02865 (2020)
24. Jain, K., Aji, A., Krishnan, P.: Medical image encryption scheme using multiple chaotic maps. Pattern Recognit. Lett. 152, 356–364 (2021)
25. Swaraja, K., Meenakshi, K., Kora, P.: An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. Biomed. Signal Process. Control 55, 101665 (2020)
26. Liu, J., Li, J., Chen, Y., Zou, X., Cheng, J., Liu, Y., Bhatti, U.A.: A robust zero-watermarking based on SIFT-DCT for medical images in the encrypted domain. Comput. Mater. Contin. 61(1), 363–378 (2019)
27. Stolte, S., Fang, R.: A survey on medical image analysis in diabetic retinopathy. Med. Image Anal. 64, 101742 (2020)
28. Zhou, Y., He, X., Huang, L., Liu, L., Zhu, F., Cui, S., Shao, L.: Collaborative learning of semi-supervised segmentation and classification for medical images. In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. Long Beach, CA, pp. 2079–2088 (2019)
29. Tariq, M., Palade, V., Ma, Y.: Transfer learning based classification of diabetic retinopathy on the Kaggle EyePACS dataset. In: *The 3rd International Conference on Medical Imaging and Computer-Aided Diagnosis*. Leicester pp. 261556 (2022)
30. Shadab, S.A., Ansari, M.A., Singh, N., Verma, A., Tripathi, P., Mehrotra, R.: Detection of cancer from histopathology medical image data using ML with CNN ResNet-50 architecture. In: Computational Intelligence in Healthcare Applications, pp. 237–254. Academic Press, Cambridge, MA (2022)
31. Razzak, M.I., Naz, S., Zaib, A.: Deep learning for medical image processing: Overview, challenges and the future. In: Classification in BioApps: Automation of Decision Making, pp. 323–350. Springer, Berlin (2018)
32. Soffer, S., Morgenthau, A.S., Shimon, O., Barash, Y., Konen, E., Glicksberg, B.S., Klang, E.: Artificial intelligence for interstitial lung disease analysis on chest computed tomography: a systematic review. Acad. Radiol. 29(1), S226–S235 (2022)
33. Öztürk, Ş., Özkaya, U.: Gastrointestinal tract classification using improved LSTM based CNN. Multimed. Tools Appl. 79(39), 28825–28840 (2020)
34. Min, J.K., Kwak, M.S., Cha, J.M.: Overview of deep learning in gastrointestinal endoscopy. Gut Liver 13(4), 388 (2019)
35. Charfi, S., El Ansari, M., Ellahyani, A., El Jaafari, I.: Ulcer and red lesion detection in wireless capsule endoscopy images using CNN. In: Convolutional Neural Networks for Medical Image Processing Applications, pp. 91–108. CRC Press, Boca Raton, FL (2022)
36. Naz, J., Sharif, M., Yasmin, M., Raza, M., Khan, M.A.: Detection and classification of gastrointestinal diseases using machine learning. Curr. Med. Imaging 17(4), 479–490 (2021)
37. Lalitha, S., Sanjana, T., Bhavana, H.T., Bhan, I., Harshith, G.: Medical imaging modalities and different image processing techniques: State of the art review. In: Disruptive Developments in Biomedical Applications, pp. 17–36. CRC Press, Boca Raton, FL (2022)

38. Gupta, S., Kalaivani, S., Rajasundaram, A., Ameta, G.K., Oleiwi, A.K., Dugbakie, B.N.: Prediction performance of deep learning for colon cancer survival prediction on SEER data. Biomed Res. Int. 2022, 1467070 (2022)

39. Sulong, G., Mohammedali, A.: Recognition of human activities from still image using novel classifier. J. Theor. Appl. Inf. Technol. 71(1) (2015)

40. Chavero-Pieres, M., Viola, M.F., Appeltans, I., et al.: Magnetic resonance imaging as a non-invasive tool to assess gastric emptying in mice. Neurogastroenterol. Motil. 35(2), e14490 (2023)

41. Özyurt, F., Sert, E., Avci, E., Dogantekin, E.: Brain tumor detection based on Convolutional Neural Network with neutrosophic expert maximum fuzzy sure entropy. Measurement 147, 106830 (2019)

42. Tiwari, P., Pant, B., Elarabawy, M.M., Abd-Elnaby, M., Mohd, N., Dhiman, G., Sharma, S.: Cnn based multiclass brain tumor detection using medical imaging. Comput. Intell. Neurosci. 2022, 1830010 (2022)

43. Noor, M.B.T., Zenia, N.Z., Kaiser, M.S., Mamun, S.A., Mahmud, M.: Application of deep learning in detecting neurological disorders from magnetic resonance images: a survey on the detection of Alzheimer's disease, Parkinson's disease and schizophrenia. Brain Inf. 7, 1–21 (2020)

44. Katako, A., Shelton, P., Goertzen, A.L., et al.: Machine learning identified an Alzheimer's disease-related FDG-PET pattern which is also expressed in Lewy body dementia and Parkinson's disease dementia. Sci. Rep. 8(1), 13236 (2018)

45. Bhat, S., Acharya, U.R., Hagiwara, Y., Dadmehr, N., Adeli, H.: Parkinson's disease: Cause factors, measurable indicators, and early diagnosis. Comput. Biol. Med. 102, 234–241 (2018)

46. Chai, X., Gan, Z., Yuan, K., Chen, Y., Liu, X.: A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Comput. Appl. 31(5), 219–237 (2019)

47. Chandrasekaran, J., Thiruvengadam, S.J.: A hybrid chaotic and number theoretic approach for securing DICOM images. Secur. Commun. Network 2017, 6729896 (2017)

48. Wang, X., Liu, C.: A novel and effective image encryption algorithm based on chaos and DNA encoding. Multimed. Tools Appl. 76(3), 6229–6245 (2017)

49. Kumar, S., Panna, B., Jha, R.K.: Medical image encryption using fractional discrete cosine transform with chaotic function. Med. Biol. Eng. Comput. 57, 2517–2533 (2019)