Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

Securing medical image privacy in cloud using deep learning network

Gayathri S[1*] and Gowri S[2]

Abstract

The worldwide usage of Internet of Things (IoT) applications enhanced the utilization of consumer devices, such as smartphones, computers, screening equipment used in hospitals that merely rely on imaging techniques. Numerous images got generated over the cloud platform in a daily basis ad create storage complexity. On the other hand, securing the data stored in the cloud is important. Instead of storing large amount of data into the cloud, lightweight dynamic processing of data suppresses the complex issues in cloud security. Here secure cloud-based image processing architecture is discussed. Privacy preserving medical data communication is considered as the specific research scope. Cryptographic technique used to encode the original data and decode the data at the other end is currently in usage as conventional design. Providing privacy to the medical records through adding noise and denoising the same records is the proposed idea. The proposed work is keenly focused on creating a light weight cloud architecture that communicates the medical data effectively with privacy perseverance using deep learning technique. In the proposed system, the design of an efficient image denoising scheme with a hybrid classification model is created to ensure reliable and secure communication. Deep learning algorithms merged to form a Pseudo-Predictive Deep Denoising Network (PPDD). The proposed system's benefit is ensuring added security in Dark Cloud using a newly structured algorithm. The original data is packed in the Deep cloud using the Gaussian noise act as a key. The complete packing and unpacking of medical data is encapsulated by the transformed images. Over the cloud premise, the data is highly secured and invisible to the malicious users. To reduce the storage complexity, the dynamic data is unpacked and denoise process is applied at the edge devices. During the authorized access period alone, the data is decrypted and accessible at the edge nodes. The maximum process is dynamically happen in the cloud without depending on the storage boundary. The performance of proposed PPDD network model is evaluated through Signal to noise ratio (SNR), Similarity index (SI),Error Rate(ER) and Contrast to noise ratio(CNR). The proposed architecture is comparatively validated with existing state-of-art approach.

Keywords Denoising, Image processing, Deep learning, Privacy preserving, Cryptography

Introduction

Several digital devices are in use in recent days such as smart mobiles, Screening equipment in medical industry, Recording cameras etc. have increased in numbers as part of the growth of Internet of Things (IoT) technologies. These reason the mass age of pictures over various innovations commonly alongside the quickly developing innovation. Medical imaging devices are IoT-based processes that can generate images frequently in multimedia healthcare applications using IoT [1]. The capacity of the device is larger and stationary [2]. It must be portable, lightweight, and handheld [3]. With rapid development comes high demands on image management, processing, and storage. Cloud computing has made these services more beneficial [4]. Image denoising plays a crucial role

*Correspondence:
Gayathri S
srinigayu77@gmail.com
[1] Research Scholar, Sathyabama Institute of Science and Technology, Chennai, India
[2] School of Computing, Sathyabama Institute of Science and Technology, Chennai, India

in the production of denoise image noise reduction from noisy input. Let's take real-time applications, where it is nearly impossible to remove noisy images at the beginning. There are two types of image noise sources: internal devices and external environment. By removing noise from images, it made its way into other applications like image segmentation, image registration, and super resolution, among others, in order to produce content that is effective and of high quality. Deep neural networks (DNNs) are used in image denoising methods in the literature. Using a well-trained DNN model, the noisy input images are mapped to demised output images [5]. Large DNN models, which have many hidden layers and thousands of neurons in each one, produce high-quality images [6]. It has unique characteristics like a high workload for computation, extensive use of cost-effective cloud computing resources, and concern for privacy preservation. The first stage of image generation ought to be unique and distinct from other applications, such as medical and facial images.The practice of the DNN model is the next step.It contains data of the model proprietor and hole data of delicate preparation pictures.Images and the DNN model must be protected using cloud computing-based service flow for the entire valuable operation.

Deep neural networks

Deep neural network is one of the robust techniques utilized in most of the conventional pattern matching applications. The neural network toolbox consists of input layer, followed by number of hidden layers which is reconfigurable based on the complexity of the input features. If the features falls on the neural network input layer has less combinations then the number of iterative process are degraded. Neural network is utilized in complex feature analysis models. In certain cases the input features are randomly distributed with probabilistic functions. The random distribution of features enable the DNN model to continue the iteration till maximum. The conventional neural network holds maximum of 1000 epochs, evaluation using cross-entropy and error tolerance is provided by error histograms. The neural network performs pattern recognition process and evaluate the results with respect to confusion matrix.

Denoising framework

The concept of secure computing with deep learning based image denoising is discussed. Performing the task on the cloud was explained in this architecture. By maintaining secret information between images are retrieved through Deep Neural Network (DNN) model. Neural network based image denoising is performed on-premises of cloud. Cipher texts collected from both noisy image and clear image using DNN model are known and updated only to the cloud all over the complete service flow. Theoretically, homomorphic encryption [7] allows entire flow to be good in security and functionality. But practically it is not possible because it has large runtime and high computation cost on both local server and client premise. The system face a lot of difficulties to improve DNN based image denoising model such as privacy, high local cost efficiency, security, better cloud performance with good quality of denoising effect. To solve all these issues, the system has to develop connection between secure image hiding and image filtering in order to operate the system in effective and secured conditions. Data securing process and reliable benefits can be achieved by lightweight cryptographic technique such as adaptive secret keys to encrypt unprocessed images. In the cloud side, encrypted DNN based image denoising is processed using same secret shares. In our design, cloud is split into two servers independent of cloud service providers. In modern days, secure based applications are developed by two-server model. Each server can have secret shares individually and it is considered to be more trendy towards the two-server model. A highly customized secure protocol offers unique code word of denoise input images between the two cloud servers [8].

A kind of prototype solution like the Straw man solution is directly used in garbled circuits to achieve secure protocol, which is known very well about secure two-party computation protocols, is to enable two parties to cooperatively secure evaluation of arbitrary functions. Here, enabling secure computing enabled DNN architecture for image denoise is used to share the secret on the cloud based on performance in evaluation. In order to attain the target pattern, robust neural network is established for getting the denoise area. is directly applied to the garbled circuits and offers a practical choice for security. The model provides complex processing performance overhead. The expanded gate size offers complexity in a circuit and leads to the simple function of garbled circuits. Using a hybrid approach to recent security work, fixed frameworks are under practice. For analysis these approaches can be mostly motivated. The system need to be designed with reconfigurable protocol model with user specific application task because of embedded together with more complex circuits and many secure computation techniques [9].

In this paper the system have to follow the same blueprint techniques used provide a highly configurable model for secure computing system using neural network. In fact, the usage of garbled circuits in our work is very selectively used. Limitation of DNN based image denoising is to perform better than other techniques that need a very large amount of data. In the future, The system will work to design and support various types

of neural network models such as convolutional neural networks(CNN), Transfer learning (TL), Generalized adversial network (GAN) etc.

Deep analysis of image denoising technique through automated frameworks is discussed here. Considering various existing frameworks in machine learning and deep learning, the automated techniques are classification and feature extraction are studied. Multiplayer perceptron are commonly used techniques for image classification. Multi-layer perceptron act as the state of art model for image denoising systems discussed in [6]. The internal logics adopted within the neural networks are exclusive or operation between the features, addition, and multiplication even more. The characteristic function shows the relativity between the input pattern and the target pattern. For generating secure encryption schemes, exponential operations are included. In real time applications, more complex data and the combination of data are present. It is difficult to make correlation analysis when the data is acquired in exponential manner [10].

The usage of deep learning architecture consumes more GPU (Graphical processing unit) space. Hence the system expects less number of computations, with reduced dimensions of input pattern. When utilizing neural network architectures, the benefit existing with the cross validation process assigned. The repeated analysis of pattern through cross validation is encouraged [6, 11–18]. Dee learning enabled boosting technique is utilized in certain cases of denoise applications. Gaussian noise in real images are difficult to remove. The coarse noise map of the existing real time images are treated well with the boosting algorithms [19].

Figure 1 Shows the general processing steps considered for secure privacy preserving cloud denoising process.

Cloud storage is kept on increasing these days. Medical image storage is increasing. Hence processing and storage of medical data need an optimized system.

The evaluated prototype is used to implement the process for getting comprehensive estimation.

Medical images are preprocessed and encrypted using predictable pseudorandom noise data. On the other side, encrypted images in the cloud storage are retrieved through the denoising process.

A deep learning network-enabled denoising process is developed here, in which predictive pseudorandom noise data at the decryption phase need to be validated.

Predictable noise level is utilized to create a lightweight model to maintain the privacy of medical records.

The remainder of the paper consists of a comprehensive discussion of previously published scholarly articles in Section II. Section III discusses the solution statement and system tool identification for existing problem resolution. In Section IV, the system design architecture and specific system implementation steps are discussed. The remainder of the paper concludes with suggestions for improvement.

Literature survey

Removal of Gaussian noise

Denoising application for real time images considers the noise removal process as an important constraints. Gaussian noise in the real time images are very difficult to handle. Deep boosted residual learning network are utilized to enhance the performance of denoise process. Various deep learning algorithms available, in that Deep belief network handle the denoise process effectively.

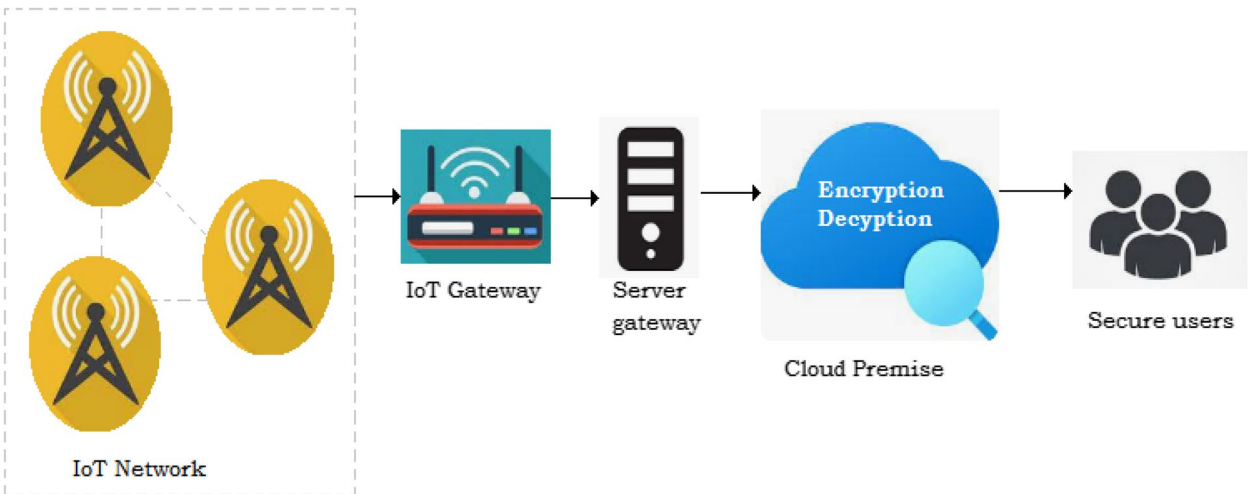


Fig. 1 General architecture of Secure cloud computing

In addition the boosting technique enhance the quality of image features. The major drawback persist with the existing denoise process includes the size of the image directly impact the processing time. The response rate of the deep belief network get degraded [19].

Removal of impulse noise

The image impulse noise removal is focused through adaptive switching enabled median filter. To reduce the impulse noise present in the gray-scale images, the adaptive technique is used The system demonstrated in which detection of noise is the first processing block which detects amount of member noise pixel based on the intensity value. In the second processing block, local noise density is calculated. In third processing block, filtration of degenerated pixel image is done based on the selection of filters with predefined size and local noise density. Next to these operations, updating of noise coverage is done carefully in upcoming blocks. At last, fifth processing block possesses size adaptive filter which is used to process noise residuals noted in third processing block. It has been experimentally verified that adaptive switching technique can undergo image restoration to maximum of 99% on impulse noise association is removed. The proper estimation is carried out to analyze the noise removal quality [20].

Removal of random noise

Salt and pepper noise, random patch noise are commonly occurring noise in image processing.A novel image denoising system for removing grey, salt and pepper noise in two stages. At first, patches are the crucial component which acts as basic unit where the generative models are built. Better clustering reports are obtained by locating image noise within the patches and are described by this algorithm. At next, patches classification is done by algorithm using generative clustering method. It has three functionalities. It suppresses the noise interference, rejects the process belonging to smaller number of patches and finally provides more identical data for noise repairing. Mostly, salt and pepper noise are removed by building non-local switching filter in this algorithm. The existing system greatly denoise the grey noise, salt-pepper noise, Gaussian noise of different densities whose simulation results are described effectively [21].

Removal of High density noise

High density noise factors accumulate at one place and interrupt the image processing quality.The high level of Gaussian noise are detected and removed by weighted adaptive mechanism (AWM). Initially, the author determines the adaptive window size for each pixel. Based on the image under test, the adaptive window size is being selected. The maximum and minimum values of the window size are tunable. The successive windows are said to be noise free after the patch restoration. The weights are getting updated to match the normalized value of the comparative image. Thus, the filter used in the proposed system has very low level of detection scheme with reduced error rate and high image pixel replacing quality which are experimentally demonstrated and compared for high-level noise [22].

Removal of patch noise

A certain patches of noise present in the pixels of the images impact the quality of visualization. Noise pixels are scattered in the image here and there. Denoising is applied through median filters, Integral filters [23]. Simple pixel bias adjustable technique remove the noise by rounding off the pixel values which are not relevant to the existing region pixel values. Further equivalent weights are assigned to the pixels. The proposed system is developed using thresholding based noise removal process. The presented process includes edge identification, structural element extraction, filtering of noise etc. [24].

System design

In existing frameworks a safe cloud-based image service framework that produces high-quality image content by allowing privacy-preserving and effective cloud-based image denoising. For a variety of image-centric applications, a key ensures quality [25–28]. Deep neural networks (DNN) have shown very promising results for a variety of image denoising techniques. Hence it is also used to perform denoise operations. This is due to the fact that deep neural networks are widely utilized in computer vision projects. Deep learning act as the cutting edge technique for secure noise removal, secure computing of image hiding is employed. Deep neural network with customized neuron blocks hold the unique pattern of the images, which act as a key factor for correlation metrics. A light weight cryptography technique with noise pattern act as shielding factor is innovated here. To evaluate the denoising quality and improving the performance of the network model, system interpretation is done. The proposed approach is developed for the purpose of iterative analysis of DCNN as Deep DarkNet. The experimental results demonstrated with prediction accuracy and denoise quality. The reconstruction of a deep learning image serves as the foundation for the iterative neural network.

Figure 2 Shows the system interpretation. The user interface is developed with the PC in which MATLAB tool is being configured. The medical images are stored into the backend local memory. Using read command these images are fetched inside the MATLAB simulator.

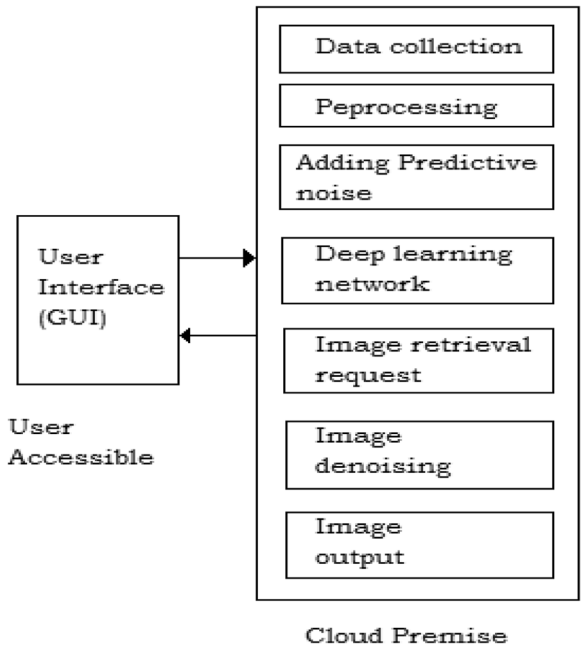


Fig. 2 System Interpretation

Proposed PPDDN is developed inside the tool, utilized for iterative training and testing.

Design methodology

In the proposed system, to ensure reliable and secure communication, design of efficient image denoising scheme, with classification model using Deep learning algorithms enrolled together to form a new algorithm named as Pseudo-Predictive Deep denoising network (PPDDN) is evaluated. The benefit of proposed system is to ensure added security in Dark Cloud using newly structured deep learning algorithm. Creating iterative model of DCNN as Deep Denoising network to ensure denoising quality and better performance of the Network model.

Figure 3 Shows the system architecture of proposed Pseudo-Predictive Deep denoising network (PPDDN) for secure medical data transfer application in the cloud platform.

Data preparation

Because the Self-Organizing Map is an unsupervised machine learning algorithm that organizes itself without any instruction from others, it is one of the most popular

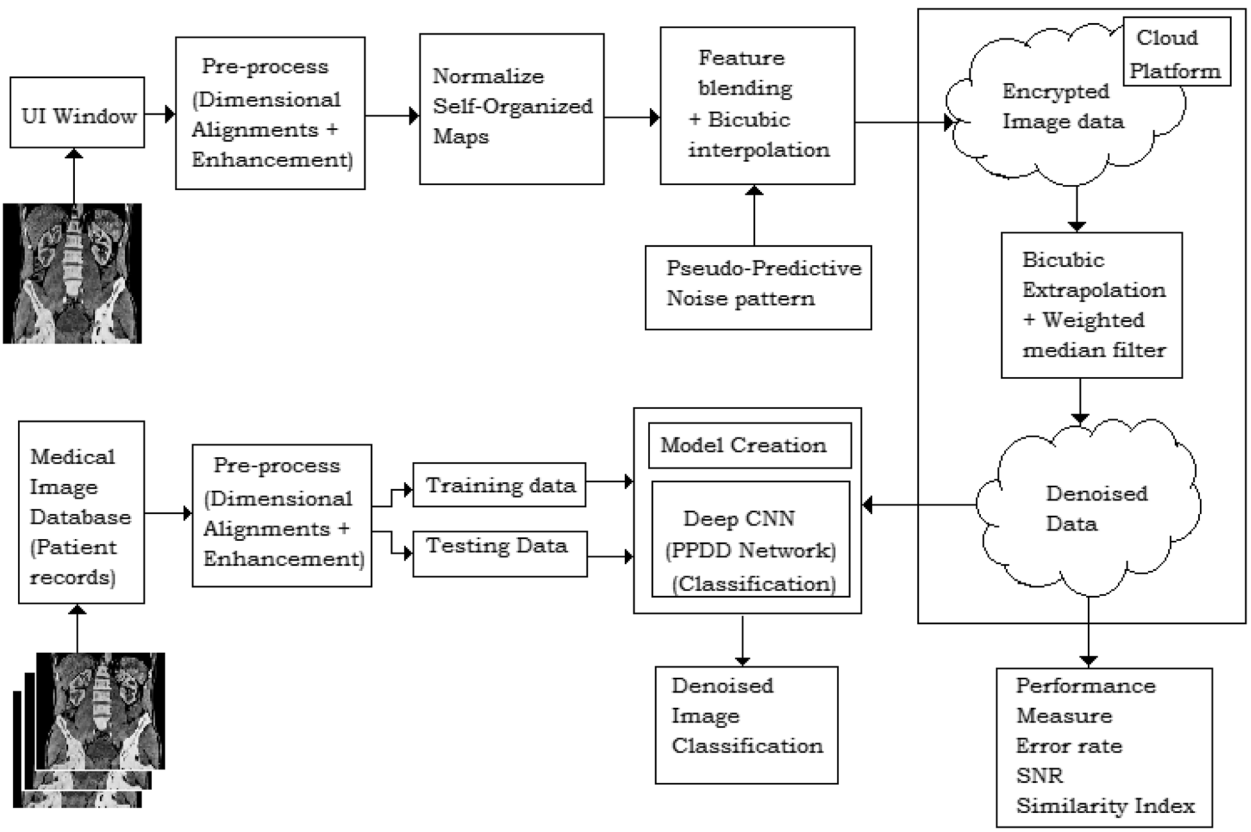


Fig. 3 System Design of Proposed Pseudo-Predictive Deep denoising network (PPDDN) Process

neural models. This module is used to load the original image, convert it into a grayscale image, and normalize the image using the SOM (Self Organizing Mapping system) model. The key function of image pre-processing, which is the operation of image quality, is to improve the image in the most meaningful ways, which increases the chances that the other processes will succeed. Enhancing contrast, removing noise, and isolating regions whose texture suggests the presence of alphanumeric information are typical aspects of preprocessing.

- Image enhancement is the process of enhancing an image's information and quality so that the final image is of a higher quality than the original for a particular application.
- The process of recovering or reconstructing an image that has been damaged by some knowledge of the degradation function is known as image restoration. The function of the restoration method is comparable to that of the enhancement method for enhancing image quality.

The SOM learning calculation is generally clear. It comprises of introducing the referenced loads, repeating over the information, viewing as the "triumphant" neuron for each information and changing loads in light of area of that "triumphant" neuron.

The proposed SOM model organizes the Euclidean distance between the specific neurons *'n'* and further validates the sample input *vi* minimized the given equation as,

The Covariate neuron is given by-

$$N_c = \sqrt{\sum_{i=0}^{d} (n_i - v_i)^2} \quad (1)$$

The neurons consider the initial condition as the first data present in it.

Reducing dimensionality

The raw data is fetched into the PPDDN model after making the dimensionality reduction process. Self-organized mapping model is utilized here to reduce the dimensionality of the data. the normalized samples are splitted up into 1×1000 values as one frame. the whole data is then converted into sequential frames of normalized data. hence at every iterative process 1×1000 samples are fetched inside the PPDD network.

Normalization

The fundamental benefit of utilizing a SOM is that the information is effortlessly interpreted and perceived. SOM assigns weighted constants to transform the original image data. The purpose of applying SOM to the original image is to secure the originality of the image pixels. Further the transform process normalizes the input data before entering into the cloud computing process.

De-noising the image

The user interface is provided within which the test image will be read. The image is further applied to denoise function through bicubic interpolation (BI) and noise removal through weighted Median filtering (WMF). Deep learning algorithm is used to rearrange the image pixels after denoising. On the other side, bicubic extrapolation(BE) is utilized. BI is a compression matrix of the original image without disturbing the original pixel quality. BE is the decompression matrix expand the encrypted image.

Deep learning model

Deep learning algorithms are subset of artificial intelligence frameworks (AI) that is induced to train the computers to provide automated task processing and provides solution to various problems occurring in it. Deep learning models are derived from neural networks to make feature correlations through pattern recognition technique. Deep learning algorithms are applied in smart applications in real time for object recognition, fault identification systems and various classification models. Utilization of transfer learning with pre-trained networks create high impact on object recognition. Image denoising techniques required deep learning principles to iteratively perform the noise elimination process, identification of noisy patches in the images, identification of similar occurrences of noise patterns etc.

For each neuron, various neurons having independent variables associated with it. Based on the bias weights, the neurons are organized. The generic neural network equation is expressed as below.

$$\boldsymbol{Z_{Network} = W_{Bias} + \sum W_n X_n}$$

Where,

$Z_{Network}$ = Graphical representation for ANN.

W represents the weights of the neurons.

X act as the input variables.

W_{Bias} represents the bias intercept.

Neural networks (NN) is processed in to different steps.

1. Consider the input variable X, the linear equation is expressed as $Z_{Network} = W_0 + W_1X_1 + W_2X_2 + \ldots + W_nX_n$ can perform the neural network process and predict Y values represented as Y_{pred}.

2. Basedon the number of iterations, the loss functions and error functions are evaluated. The error rate is identified as the difference between the expected results from neural analysis with predicted results from the developed Dark-Net model.
3. The quality of analysis is determined by the reduced error rate, loss function after the complete iterations.

At first, to understand the methods for the output calculation of neural network and then learn several techniques to get the optimum solution of the minimum error term.

The output layer nodes are dependent on hidden layers (L3, L2, L1) and input variables which is present immediate next to the preceding layer. The features are created automatically in the middle hidden layers of the network. These features are failed to derive explicitly. Hereby, deep learning model generate the features which are much differ from machine learning algorithms.

Train classifiers using extracted features

Feature extraction permits you to utilize the force of pretrained networks without putting time and exertion into preparing. The medical images from the database are processed and splitted into training images 70%, testing images 15% and validation images 15%. To create a PPDD network using convolutional neural network, the training data is utilized. Once the model performs better with low error rate, the model act as a benchmark for making the testing process. After the cloud process get completed the classification of images are done to validate the quality of cloud denoising.

PPDDN architecture formation

Preparing deep organizations is computationally escalated and can require numerous long stretches of figuring time; be that as it may, brain networks are innately equal calculations. You can utilize Parallel Computing Toolbox™ to exploit this parallelism by running in equal utilizing elite execution GPUs and PC bunches. To get more familiar with deep learning in equal, in the cloud, or utilizing a GPU, see Scale up Deep Learning in Parallel, on GPUs, and in the Cloud.

Figure 4 Shows the derived architecture of PPDDNet. The input images are assigned into the input layer, here the Pseudo-Predictive creation of input layer act as normalization and transformation layer. Self-organized mapping model (SOM) with Bayesian neural network is hybrid together to make the transformation. The transformed image pixels are considered as the features for the input layer. The novel architecture is derived from Convolution network, that contains input layer as the foremost one, convolution layer, followed by max-pooling layer and classification layer.

Deep learning interpretability

The integrity of deep learning network acts like a black box, since the connections are automated and further logical decisions are not depends upon certain known perspective. Based on the complexity of the data input, the structure is getting varied. The number of hidden layer is getting varied. The proposed PPDDN derived from the incorporation of Bayesian network with Self organized mapping model with Deep learning network. The input layers are tuned in the Pseudo-Predictive

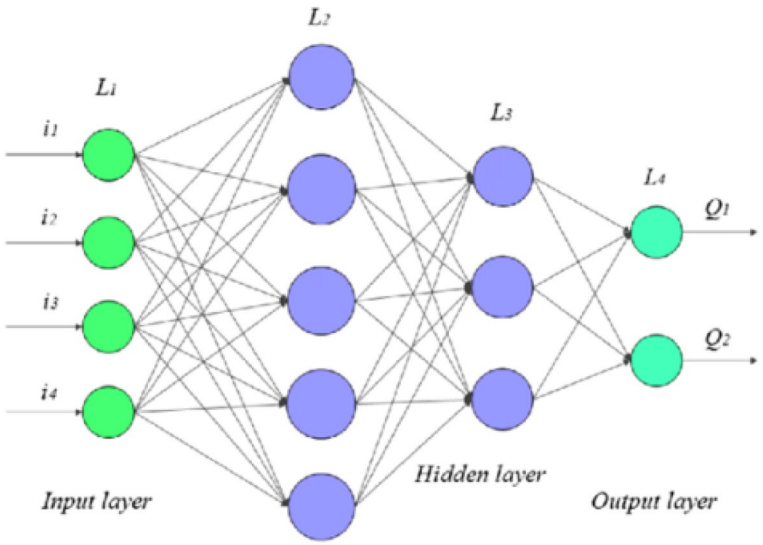


Fig. 4 Structure of Pseudo-Predictive deep denoising network Model

methodology where the features are unique covariate points present in the test images. These features are unique points collected randomly from the test images. The structure of PPDDN is explained in the Fig. 5 The feature mapped input points are fetched to input layer of 100×100 of image size. The down sampled image is filtered with Convolution 2D layer of 10×4 Stride channel. The filter undergoes all the areas of the input and further the filtered points are fetched into the Max-pooling layer. 2×2 smoothening operation is implemented there. The fully connected layer contains the unique neuron data of the input that acts as the authentication key for the decoder section. The deep learning model validates the points with the input features and correlates the test image with respect to the class result obtained. Further the decision at the end is fetched as output to a small web based user interface as discussed in section IV.

Cloud interfacing

The test image which is denoise is being fetched back to the cloud to show the denoise output after the analysis iterations done by the algorithm. Further the cloud output is displayed if the inputs are having authentication keyword matches, then the resultant will be given for access. The GUI window is implemented using MATLAB web toolbox with GUIDE toolbox for showing the results as a prototyping simulation.

The algorithm Pseudocode is given below.

Algorithm	**Pseudo predictive deep denoising network (PPDDNet)**
Input	*Image_db=database, lb_noise=labels, w_noise=attributes I=test image*
Output	***Di=denoised_image_class***
Let	*w_noise the extracted noise attribute of the input*
for	*intial* ***index****=0*
	Step 1:*Ik=Self_organized_map(I)*
	Step 2:*Ik2=Bicubic_Interpolation(Ik)*
	Repeat step 1, 2 for Image_db and Save ***Image_training****[1:N(Image_db)]*
Let	***Image_testing****=Ik2*
	j_index in I do
	if(authentication_code=PASS)
for	***M=PPDD(Image_training, Image_testing)***
Append	***Index*** *end*
	Test Dynamic Data I_new
	*apply PPDD(****Image_training****,* ***Image_New, M****)*
	Evaluation : Score=[Accuracy, SNR, SI]
Return	*Score*

The simulated results and discussions are given in section V.

Results and discussions

Input images

Figure 6 Shows the sample test images utilized for denoising process. The medical images are highly sensitive data used for diagnosing various diseases. The test samples are collected from TCIA open access medical image forum.

GUI front-end design

Figure 7 Shows the GUI front-end developed. Using MATLAB GUIDE tool the front end design is developed. The GUI control extracts the data from the backend. The GUI contains three buttons such as *Fetchinp*, *Denoise*, and *analyze*. The figure shows the analyzed result of enhanced image with obtained accuracy.

Performance measure

Figure 8 Shows the performance measure of PPDDNet architecture, the maximum epochs allowed are till 1000. The best performance score happened at the intermediate points between the 1000 epochs. The training and testing performance is shown in the Fig. 6.

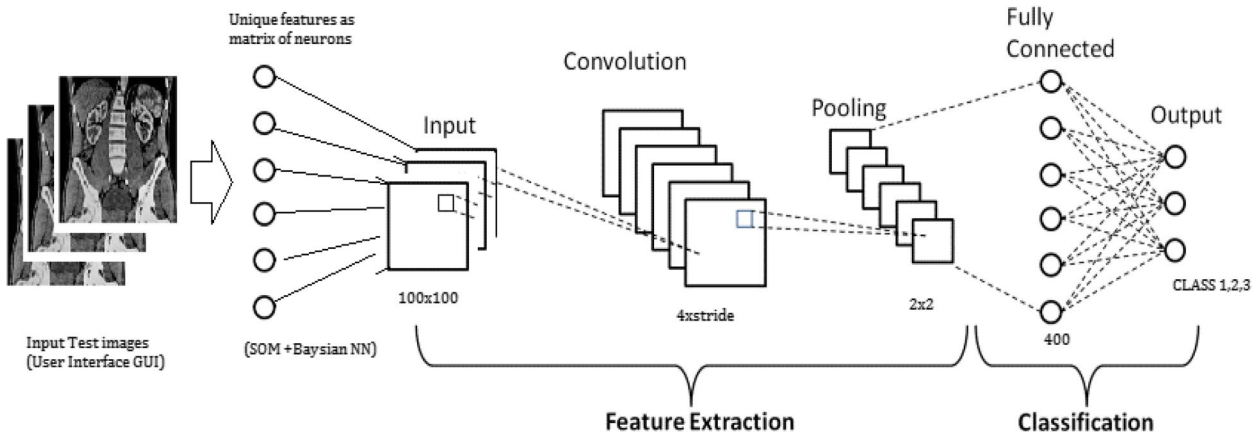


Fig. 5 Organization of Deep neurons (Zhang et al. 2019)

Neural configurations

Figure 9 Shows the neural configurations of the proposed neural network configurations. The total numbers of epochs allowed are maximum of 1000. The time chart is shown that provides the duration of process being computed. The minimum and maximum performance is scaled over here. These configurations are not manually done. Depends on the complex connections between the neurons on the input data, the configurations are automated. The lower the number of epochs, then lower will be the number of combinations.

Regression scores

Figure 10 Shows the Regression score of proposed analysis. The regression is assigned for training, testing. As per the best fit obtained at the training pattern and test pattern, then the fit line exactly lies within the data spots. The difference between the training and testing outcome need to be lower as possible.

Comparative analysis

Figure 11 Shows the Correlation analysis of input image vs. output image. The differences in various samples

Fig. 6 Sample test images

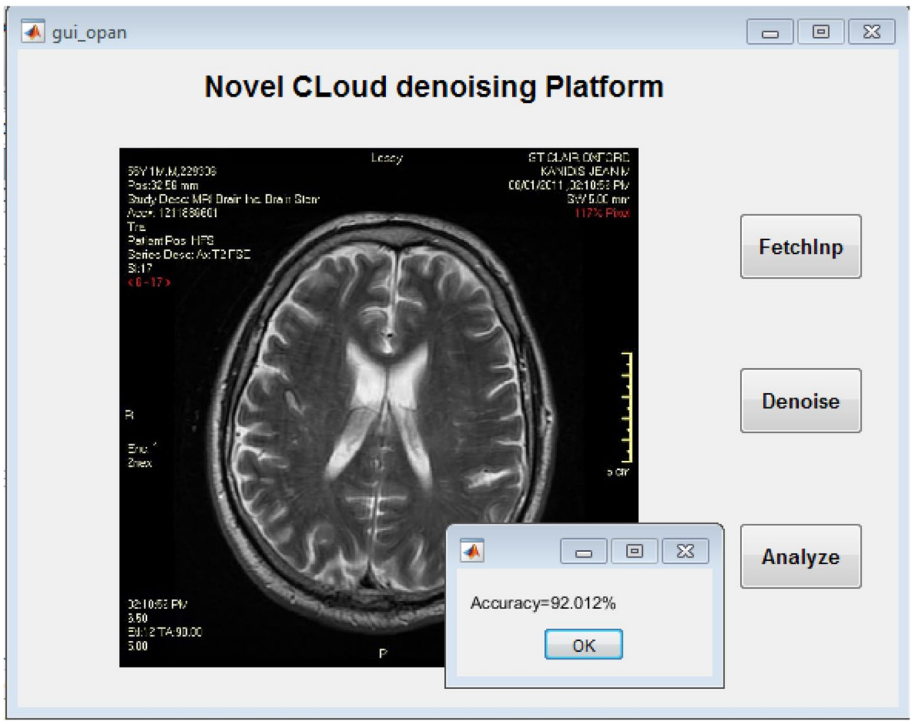


Fig. 7 GUI frontend for image collection

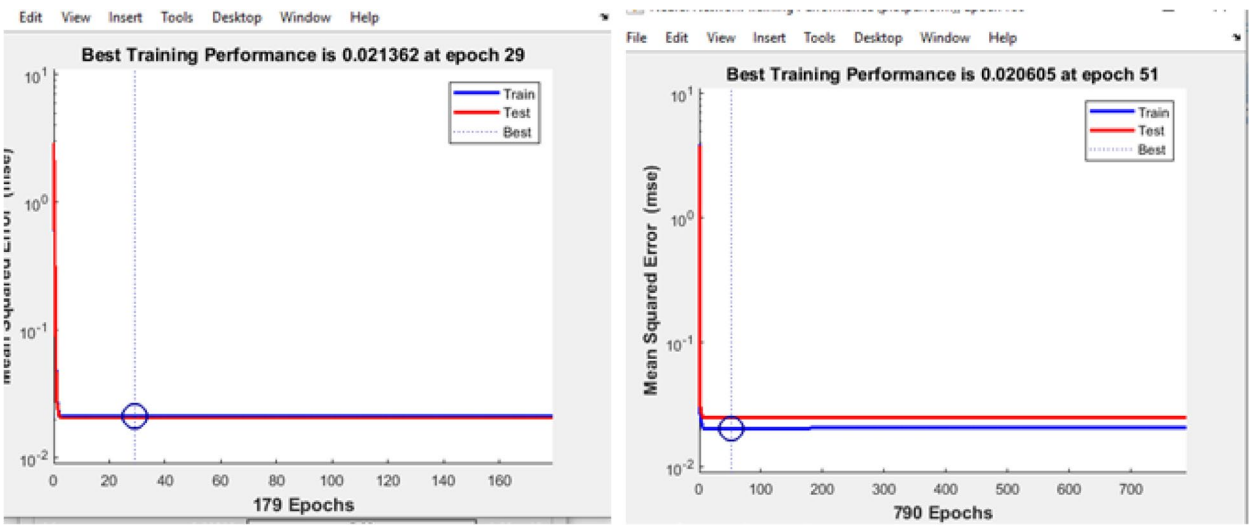


Fig. 8 Performance measure of Pseudo-Predictive Deep denoising network model

are displayed as the error spots over here. The error differences denote the mean outcome of the complete iterations computed by the Deep neural network architecture.

Figure 12 Shows the Mean, Standard Deviation of various inputs with respect to image quality. The various standard deviation (SD) of each color channels are scattered as graphical plot here. The image quality is

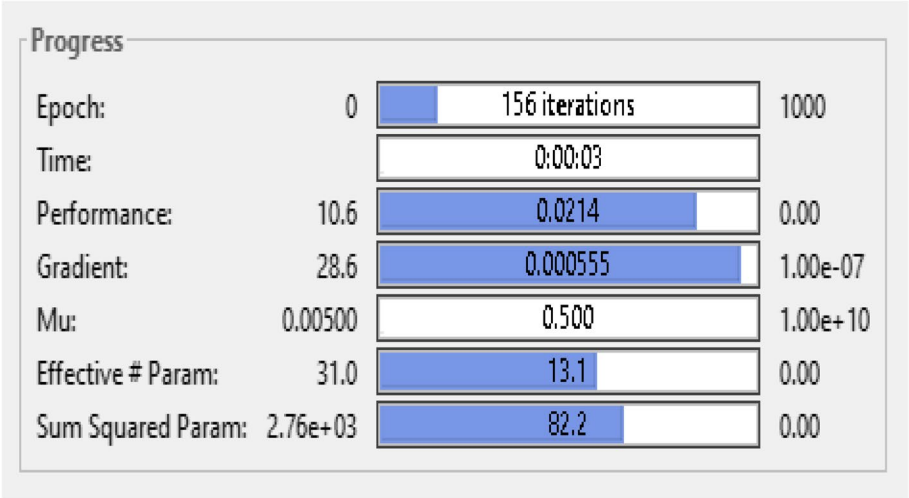


Fig. 9 Neural Configurations

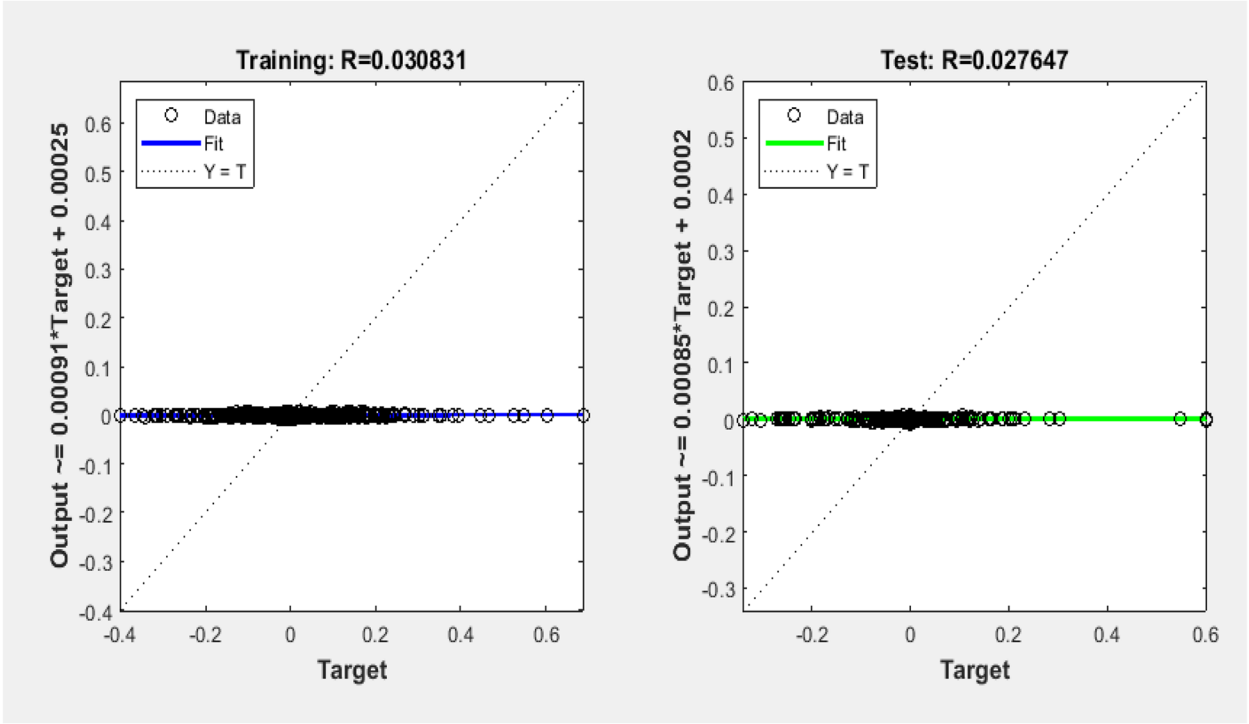


Fig. 10 Regression score of proposed analysis

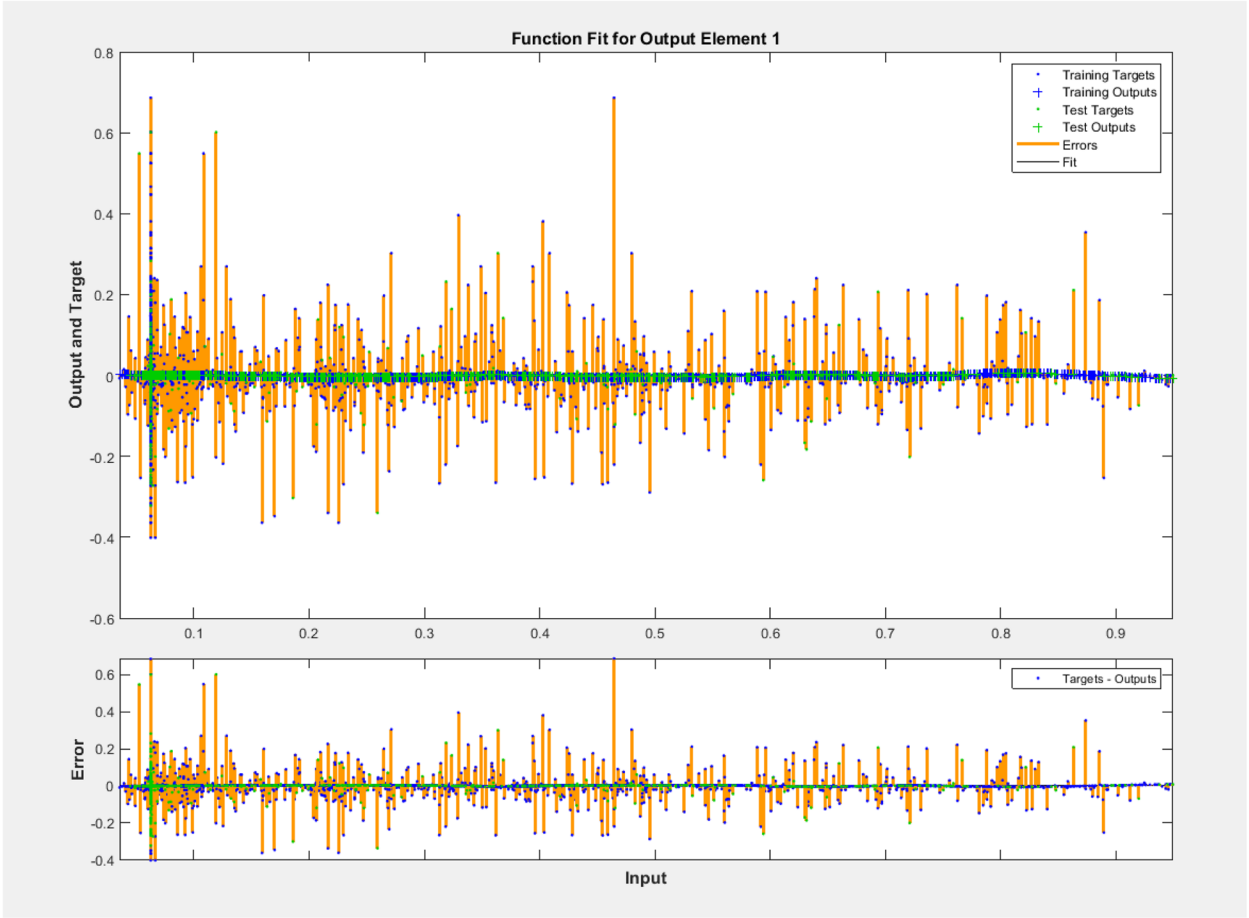


Fig. 11 Correlation analysis of input image vs. output image

altered by gradually varying the each pixel parameters within the image. The overall image quality is identified through SNR, SI etc. Various levels of values obtained with the experiments conducted here are shown in Table 1.

Table 1 Shows the comparative results of selective input images under test with respect to denoised output images obtained in terms of SNR, Structural Similarity index (SI), and corresponding error rate etc. The SNR obtained for the test images say SNR = 23.44, 24.55, 24.15, and 25.125 etc. The SI obtained in the range of SI = 0.948, 0.984, 0.962, 0.998 etc. The Error rate (ER) obtained in the range of ER = 0.00125, 0.00147, 0.00114, 0.00024 etc.

Table 2 depicts the comparative analysis of existing frameworks with Pseudo-Predictive proposed model PPDDNet. Through Deep Decoder, CNR = 53.35% is obtained as maximum. Y.Zheng et al., (2018) achieved SSIM = 0.002 range while utilizing the denoise process for Chest X-Rays. Using Berkeley dataset4, SNR = 0.179db is achieved. SSIM = 0.004 etc. The Pseudo-Predictive proposed PPDDN achieved SNR = 24.3165, SI = 0.973, ER = 0.001, CNR = 42.2% approximately.

Challenges

The major challenge behind the proposed computations rely on the different resolution of image data. The amount of transformation process getting varied for different image quality, further the common transformation of images need further enhancement. The Computation time is extended for the large images, complex images etc. the GPU utilization is higher

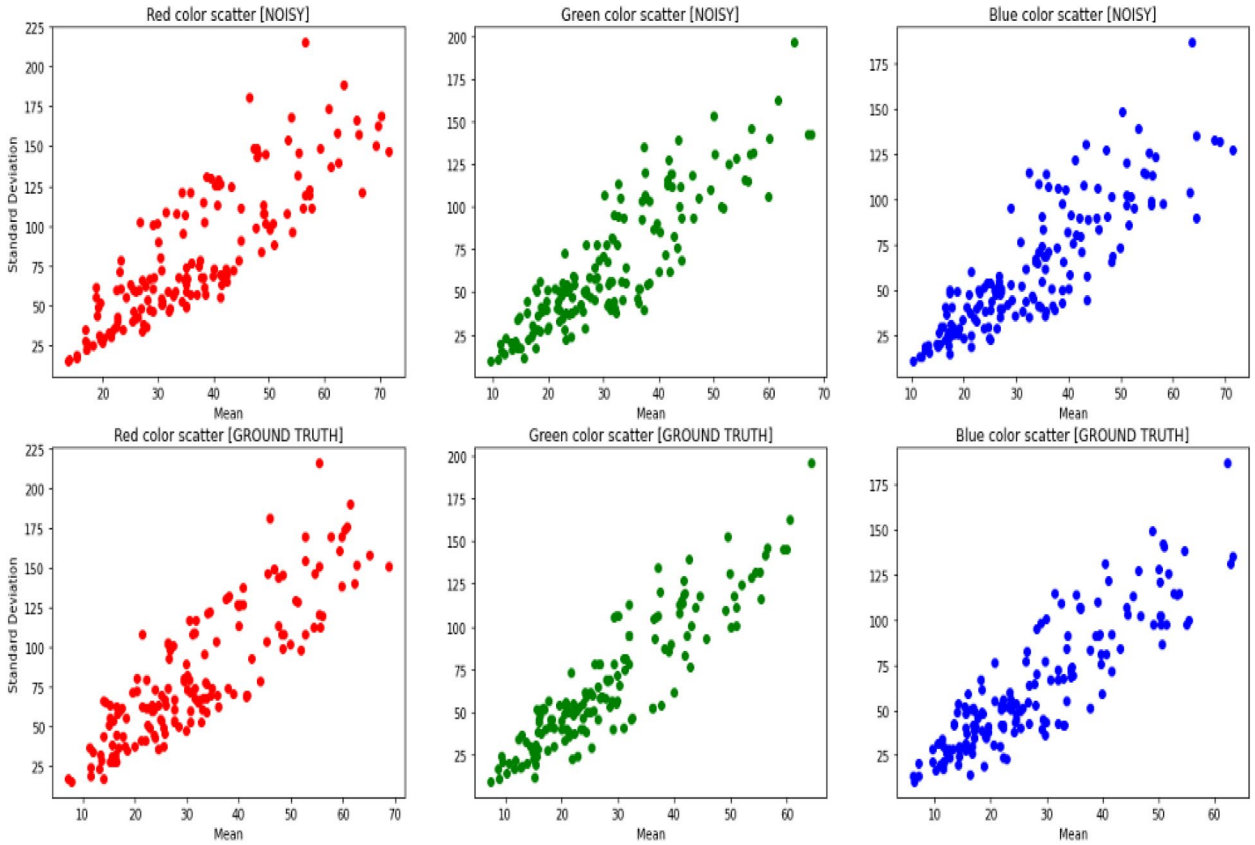


Fig. 12 Mean, Standard Deviation of Input test images

during the training process. These constraints are required to get overcome through Pseudo-Predictive enhancement of analysis model using Hybrid networks.

Conclusion

Real time privacy preserved data transfer is more important and used for the safe transaction of personal data. The proposed framework focused on implementing the deep learning based medical image denoising system with authenticated code words for privacy preserving. Thus the proposed model is clearly implemented and shown in the MATLAB backend and JAVA front end effectively. The proposed system considers various user providing input CT images and consider as the input images with respect to the patient information which is being encrypted using the noise data in the cloud. the system with PPDD as a Pseudo-Predictive methodology with respect to Deep neural network using Bayesian network and self-organized mapping model enabled the system to extract unique features from the given input image and further convert that feature information as noise and proceed with the deep learning network. The classified outputs compared the test images and the provided image in the database and finalize the result with respect to correlation ratio in terms of signal to noise ratio (SNR), error rate and the correlation noise ratio. The PPDDN achieved SNR = 24.3165, SI = 0.973, ER = 0.001, CNR = 42.2% approximately, further improved by evaluating hybrid deep learning algorithms in spite of improving the accuracy of de-noising process, also reducing the prediction time. Handling large sized

Table 1 Comparative analysis of error rate, SNR, SI using PPDDN method

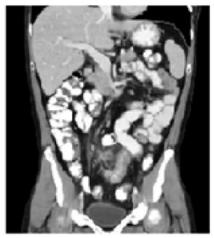
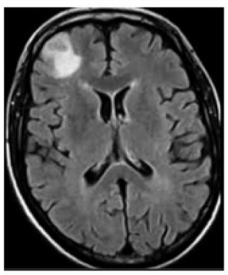
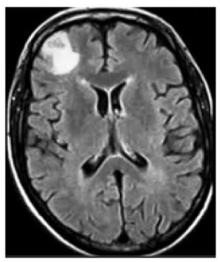
Test Image	Denoised Image	SNR	SI	ER
		23.44	0.948	0.00125
		24.55	0.984	0.00147
		24.15	0.962	0.00114
		25.125	0.998	0.00024

Table 2 Comparison of existing implementations and proposed work

REFERENCE	DATASET	MODEL	STATISTICAL EVALUATIONS
Cui et al., (2019) [10]	Ga-PRGD2 PET/CT	Deep Decoder	CNR = 53.35% ± 21.78%
Y. Zheng et al., (2021) [5]	Real time CHEST X-Rays	Deep Neural Network	SSIM = 0.002
Y. Zheng et al., (2017) [29]	Berkeley dataset4	SSE-LSH symmetric encryption	SNR = 0.179db, SSIM = 0.004
Proposed work	Real time CT images	Pseudo-Predictive deep Denoising network	SNR = 24.31625, SI = 0.973, ER = 0.001, CNR = 42.2% ± 15.44%

images need configurable model selection based on the image quality. System complexity increases in terms of complex images. Hence deep learning algorithm with configurable layers need to be developed in future model to adaptively vary the model process according to the input.

Conflict of interest
The authors declare that they have no conflict of interest

Authors' contributions
The work done by corresponding author. And it has been supervised by co author. The author(s) read and approved the final manuscript.

Funding
This declaration is not applicable (No funding received by the author).

Availability of data and materials
Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Ethics approval and consent to participate
Not applicable.

Competing interests
The authors declare no competing interests.

Received: 28 November 2022 Accepted: 11 March 2023
Published online: 21 March 2023

References

1. Wang G, Gehrke J, Xiao X (2011) Differential Privacy via Wavelet Transforms. IEEE Transactions on Knowledge Data Engineering 23(08):1200–1214. https://doi.org/10.1109/TKDE.2010.247
2. Ni J, Zhang K, Xia Q, Lin X, Shen XS (2020) Enabling strong privacy preservation and accurate task allocation for mobile Crowdsensing. IEEE Trans Mob Comput 19(6):1317–1331. https://doi.org/10.1109/TMC.2019.2908638
3. Ruwei H, Xiaolin G, Si Y, Wei Z (2011) Study of privacy-preserving framework for cloud storage. Comput Sci Inf Syst 8(3):801–819
4. Sahu HK, Verma RK, Sahu SK. Fuzzy logic based soft filters for removing noise and preserving edge. Int J Eng Res Tech. (IJERT) ISNCESR. 2015;3(20)
5. Zheng Y, Duan H, Tang X, Wang C, Zhou J (2021) Denoising in the Dark: Privacy-Preserving Deep Neural Network-Based Image Denoising. IEEE Trans Dependable Secure Comput 18(3):1261–1275. https://doi.org/10.1109/TDSC.2019.2907081
6. Saxena VK, Pushkar S (2013) Anonymization approach for privacy preserving in cloud computing. Proc. International Conference on Cloud, Big Data and Trust, 2013, Nov 13–15, RGPV. pp 179–82
7. Li JS, Liu IH, Tsai CJ, Su ZY, Li CF, Liu CG (2020) Secure Content-Based Image Retrieval in the Cloud With Key Confidentiality. IEEE Access 8:114940–114952. https://doi.org/10.1109/ACCESS.2020.3003928
8. Wang T, Zheng Z, Rehmani MH, Yao S, Huo Z. Privacy Preservation in Big Data From the Communication Perspective—A Survey. IEEE Communications Surveys & Tutorials. ;21(1)
9. Samie F, Bauer L, Henkel J (2019) From cloud down to things: an overview of machine learning in internet of things. IEEE Internet Things J 6(3):4921–4934. https://doi.org/10.1109/JIOT.2019.2893866
10. Cui J, Gong K, Guo N, Wu C, Meng X, Kim K, Zheng K, Wu Z, Fu L, Xu B, Zhu Z, Tian J, Liu H, Li Q (2019) PET image denoising using unsupervised deep learning. Eur J Nucl Med Mol Imaging 46(13):2780–2789. https://doi.org/10.1007/s00259-019-04468-4
11. Dawoud M, Turgay Altilar D (2014) Privacy-preserving search in data clouds using normalized homomorphic encryption. In: Lopes L et al (eds) Euro-Par 2014 Workshops, Part II, LNCS 8806. Springer, Switzerland, p 6272
12. Dunning LA, Kresman R (2013) Privacy preserving data sharing with anonymous id assignment. IEEE Trans Inf Forens Security 8(2):402
13. Guo S, Zhong S, Zhang A (2013) A privacy preserving Markov model for sequence classification. Bioinformatics, Computational Biology and Biomedicine: Proc. the International Conference on Bioinformatics, Computational Biology and Biomedical Informatics, BCB'13, September 22 – 25, 2013, Washington, DC, USA. ACM, New York, pp 561–68
14. Zhou M et al (2011) A privacy-preserved access control for cloud computing. Proc. IEEE 10th International confere.nce on Trust, Security and Privacy in Computing and Communications: TrustCom, 16- 18 Nov. 2011. IEEE, Changsha, pp 83–90
15. Darrie H (1965) Sturms problem of the number of roots. 100 Great Problems of Elementary Mathematics: Their History and Solutions. Dover, New York, p 112116
16. Lin P, Candan KS, Access-private outsourcing of Markov chain and random walk based data analysis applications, in Proc. 22nd International Conference on Data Engineering Workshops (ICDEW06)
17. Li W, Song H, Zeng F (2018) Policy-based secure and trustworthy sensing for internet of things in smart cities. IEEE Internet Things J 5(2):716–723. https://doi.org/10.1109/JIOT.2017.2720635
18. Saini P, Singh H, Iain S, Soni S (2016) Image retrieval in cloud computing environment with the help of fuzzy semantic relevance matrix. 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). pp 3205–210
19. Ma J, Peng C, Tian X, Jiang J (2012) DBDnet: a deep boosting strategy for image denoising. IEEE Trans Multimedia 24:3157–3168. https://doi.org/10.1109/TMM.2021.3094058
20. Ibrahim H (2019) Reduction of Salt-and-Pepper Noise from Digital Grayscale Image by Using Recursive Switching Adaptive Median Filter. Symposium on Intelligent Manufacturing Mechatronics. Springer, Singapore, pp 32–47
21. Fu B, Zhao X, Song C, Li X, Wang X (2019) A salt and pepper noise image denoising method based on the generative classification. Multimedia Tools and Applications 78(9):12043–12053
22. Zhang C, Yao H, Liu Q, Zhang P, Yuan YO, Feng J, Fang L (2018) Linear array ambient noise adjoint tomography reveals intense crust-mantle interactions in North China Craton. J Geophys Res Solid Earth 123(1):368–383
23. Thakur D, Singh S, Mittal N, Singh H, Oliva D, Demin A. Nature and biologically inspired image segmentation techniques. Archives of Computational Methods in Engineering. 2021;1–28.
24. Othman A, Iqbal N, Hanafy SM, Waheed UB (2021) Automated event detection and denoising method for passive seismic data using residual deep convolutional neural networks. IEEE Trans Geosci Remote Sens 60:1–11
25. Shokri R, Shmatikov V (2015) Privacy-preserving deep learning, 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton). pp 909–10. https://doi.org/10.1109/ALLERTON.2015.7447103
26. Wang T, Zheng Z, Rehmani MH, Yao S, Huo Z (2019) Privacy preservation in big data from the communication perspective—a survey. IEEE Commun Surv Tutorials 21(1):753–778. https://doi.org/10.1109/COMST.2018.2865107. Firstquarter 2019
27. Wang Y, Zhang A, Zhang P, Wang H (2019) Cloud-assisted EHR sharing with security and privacy preservation via consortium Blockchain. IEEE Access 7:136704–136719. https://doi.org/10.1109/ACCESS.2019.2943153
28. Yang X, Wang M, Wang X, Chen G, Wang C (2020) Stateless cloud auditing scheme for non-manager dynamic group data with privacy preservation. IEEE Access 8:212888–212903. https://doi.org/10.1109/ACCESS.2020.3039981
29. Zheng Y, Cui H, Wang C, Zhou J (2017) Privacy-Preserving Image Denoising From External Cloud Databases. IEEE Trans Inf Forensics Secur 12(6):1285–1298. https://doi.org/10.1109/TIFS.2017.2656824

Publisher's Note