Image Encryption and Compression Based on Auto Encoder for Real Time Using IoT Technique

Abdelmoty M. Ahmed*[1], Belgacem Bouallegue [2], Hassan A. Youness[1], and Hammam M. Abdelaal[3]

[1]Department of Computers and Systems Engineering, Faculty of Engineering, Minia University, Egypt
[2]College of Computer Science, King Khalid University, Abha, Saudi Arabia
[3]Department of Information Technology, Faculty of Computers and information, Luxor University, Egypt

Abstract
Machine Learning has completely transformed health care system, which transmits medical data through IoT sensors. So it is very important to encrypt them to protect patient data. Encrypting medical images from a performance perspective consumes time; hence the use of an auto encoder is essential. An auto encoder is used in this work to compress the image as a vector prior to the encryption process. The digital image passes across decryption function and a decoder to get back the image. In the proposed work, various experiments are carried out on hyp er parameters to achieve the highest outcome of the classification. The findings demonstrate that the combination of Mean Square Logarithmic Error as the loss function, ADAgrad as an optimizer, two layers for the encoder, and another reverse for the decoder, RELU as the activation function generates the best auto encoder results. The combination of Mean square error (lose function), RMSprop (optimizer), three layers for the encoder and another reverse for the decoder, and rely (activation function) has the best classification result. All the experiments with different hyper parameter have run almost very close to each other even when changing the number of layers. The running time is between 9 and 16 second for each epoch.

Keywords:
Auto encoder, IoT, Image encryption, Artificial Neural Network

1. Introduction

Health care systems use IoT sensors to collect patient's data from the cloud to analyse the data for giving useful recommendation. Unfortunately, IoT servers suffer from hacking [1][2][3] regularly, hence encryption is needed for such type of data [4][5]. Several techniques are developed for image encryption [6] using different algorithms like Chaotic Based Artificial Neural Network which has a complex design and neural network-based stream image encryption which is expensive in run time.

Data set: Our dataset is extracted from the clinical PACS database within the National Institutes of Physical fitness Clinical Center and consists of ~60% of all informed chest x-rays in the particular hospital. **Auto encoders**: Auto encoders are basic learning circuits aimed at transforming inputs into outputs with the least amount of possible distortion.Figure1 shows AEs that consist of an input layer and a layer of output that are connected by one or more hidden layers. AEs have the same number of units for input and output. The goal of this network is to recreate the input by converting inputs into outputs in the simplest way possible so that the input is not very distorted. In AEs, the training method requires minimising reconstruction errors, i.e. the output and input showing the minimal difference. The structure of a standard AEE is described in Figure 1[16].

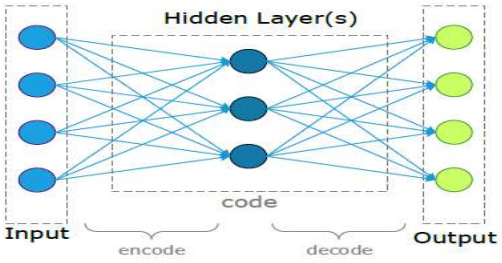

Fig.1 Structure of auto encoder

Transfer data on the IoT network is unsecure practice that needs a lot of effort to be done to secure all the stages of transferring data. Machine learning or deep learning is a very powerful tool in the field of security. The image encryption transforms an original image to the encrypted image in which people cannot recognize contents in the original image.

In this work, we focus on decreasing the amount of time needed for training and testing the model. Simply this can be accomplished by designing the neural network as an auto encoder to solve that issue. This paper used auto encoder [7][8] which is a convolution neural network to compress the x-ray image, after which a specific function is executed for encryption to secure the sent image. On the other side for decryption the reverse of the encryption function is used and decoding is also required to get the original image back with some accepted loss in its features. In this paper we will discuss the effect of the hyper parameter [9] of the auto encoder also the encryption function on the image loss and how can it be accepted through classification algorithm. The classification algorithm used is a Convolution Neural Network [10][11]. The rest of the paper is organized as follows: Section 2 gives

Manuscript received May 5, 2025
Manuscript revised May 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.5.7

related work. Section 3 introduces the proposed methodology. Section 4 focuses on the results that have been achieved in this paper. And finally, conclusions are drawn in Section 5.

2. Existing Methods

In previous studies [12], using Stacked Auto-Encoder (SAE) and chaotic logistic map, an application of image compression and encryption is suggested. Experiments show that this application is viable and successful. It can be used simultaneously on the internet for picture transmission and picture safety. It has established a five-layer SAE model. In [13] a method of X-ray image compression is presented based on a Recurrent Neural Networks Convolution (RNN-Conv). During implementation, the proposed architecture can provide variable compression rates while requiring each network to be trained only once for a particular X-ray image dimension. In [14] a learning-based method of image compression that uses wavelet decomposition is provided as a pre-processing stage. The proposed convolution auto encoder is trained end-to-end to achieve a target bitrate smaller than 0.15 bits per pixel across the complete CLIC2019 test range.

A new method of representation learning is proposed in [15] which describe unknown attacks more predicatively, enabling supervised methods of identification of learning-based anomalies. Specifically, to learn a latent representation from the input data, the author created three regularized versions of Auto Encoders (AEs). The bottleneck layers of these regularized AEs will then be used as the new classification algorithm input features, trained in a controlled way using normal data and known IoT attacks. A proposed new method of representation learning to more predicatively "describe" unknown attacks, allowing supervised methods of learning-based anomaly detection. Specifically, the author developed three regularised versions of Auto Encoders (AEs) to learn a latent representation from the input data. They also conduct experiments to explore the features of the models proposed and the effect on their output of hyper parameters.

3. Proposed Works

Figure 2 shows the block diagram of the modified auto encoder. The input is a 200 X 200 image to the encoder. The result feature vector from the encoder represents the input to the encryption block and gives the output as an encrypted feature vector which is used by the decryption and makes decryption to it and then decoded to retrieve the original image. After retrieving the original image two layers CNN are used to see how the change in modified auto encoder hyper parameters can affect the results of the classification stage.

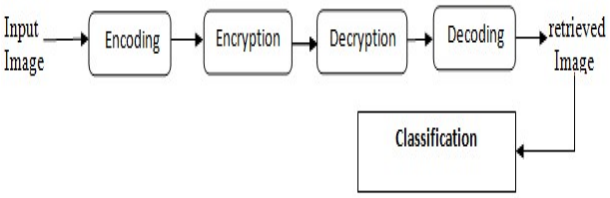

Fig.2 Proposed System Model

The proposed system consists of three layers (three convolutions and two max pooling) as an encoder and another three for the decoder. The first layer in the encoder is the input layer which has 200 X 200 input image, (3, 3) filter, each image has the same padding and 32 nodes. The second layer is MaxPooling 2D layer with (2, 2) pool size. It uses (3,3) filter, relu activation function, using the same padding for the image, and 64 nodes. The third layer is the Conv2D layer with the same criteria of the convolution layers but has 128 nodes.

The decoder consists of three layers also which is the reverse to the encoder. The first layer is the input layer of the decoder. The second layer is the conv2D layer with the same criteria in the convolution layer in the encoder with 128 nodes. Then there is UpSampling2D layer with (2, 2) filter. The third layer is the convolution layer with 64 nodes. The final layer is the convolution layer with one node and sigmoid activation function.

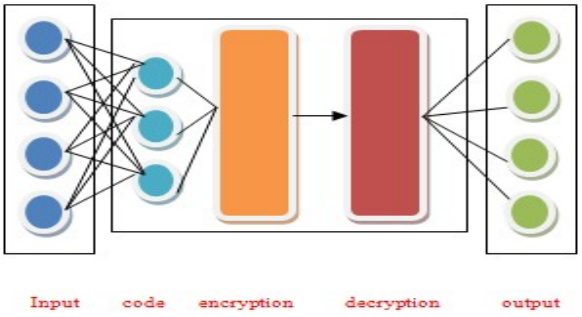

Fig.3 Modified Auto Encoder

Figure 3 shows the update in the auto encoder. The result feature vector from the encoder is handled by the encryption as an input. In this stage, an encryption mechanism used is by adding another image to the sent image and takes the square of the feature vector as follows.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \end{pmatrix} + \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \end{pmatrix}^{1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \end{pmatrix}$$

In the decryption step, the encrypted image is used and subtracted the added image from it then takes the square root of it to get the feature vector to be fed to the decoder to retrieve the original image.

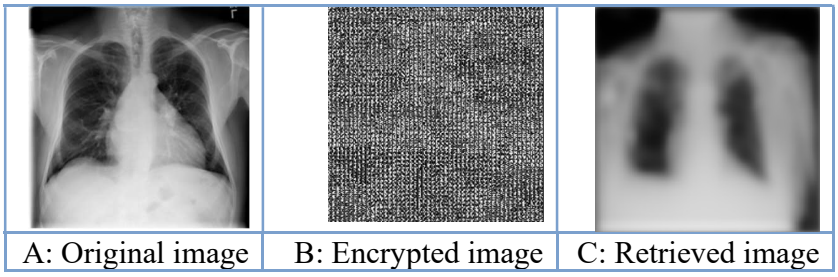

Fig. 4 A is the original image B is the encrypted image C is the retrieved image

Figure 4 shows the original image - B is the encrypted image after applying encoding and encryption - C is the retrieved equation after applying the decryption and decoding.

3. Proposed Algorithm

Our algorithm for the x-ray image can be summarized as follow:

1. The x-ray image is decoded using a CNN auto encoder.
2. The encoder output which is encoded matrix is then encrypted by adding it to another image then uses the power function on the feature vector.
3. In the decryption step the power function is reversed using the square root function.
4. The decrypted image is then decoded to retrieve the original image.

4. Simulation Results

The data set consists of 9000 images for training the auto encoder and for the prediction and training of the classifier. Figure 5 shows the number of negative cases is 5800 and positive cases are 3200.

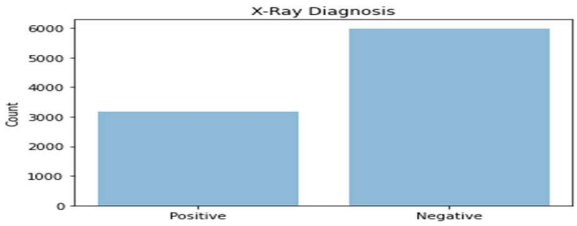

Fig.5 Comparison of Positive and Negative X-Rays

The effect of different hyper parameters like lose function, optimizer, number of layers, number of nodes, number of epochs, and activation function is examined on the auto encoder. Some different measure matrices are calculated.

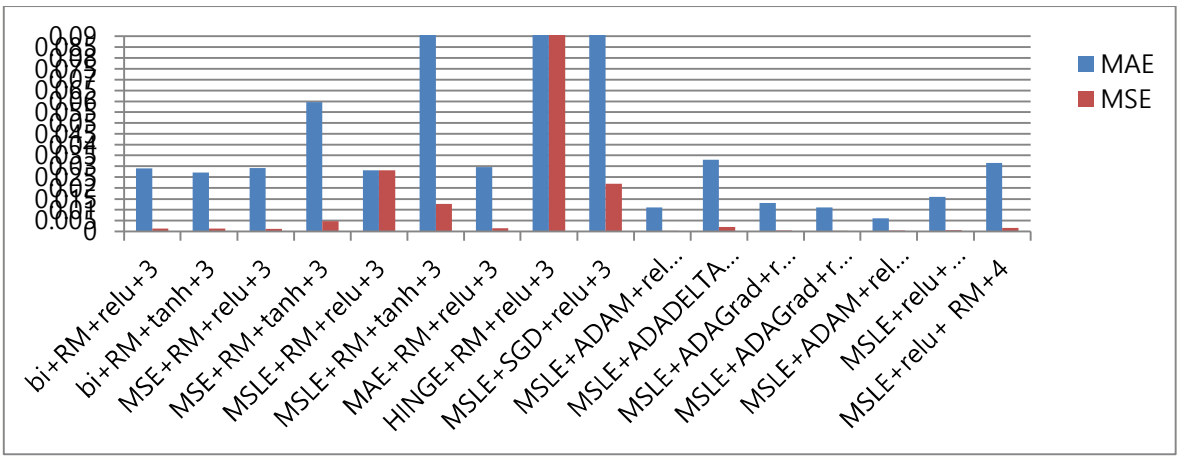

Fig.6 The mean square error (MSE) and the mean absolute error (MEA) for the different hyper parameter combination in the auto encoder

Figure 6 shows the different matrices in evaluating the auto encoder like the mean square error (MSE) and the mean absolute error (MAE). In the different parameter used by this research, the combination of the loss function (mean square logarithmic error), optimizer (ADAM), activation function (relu) and 3 layers in auto encoder model have given the less MSE and MAE which mean the best result.

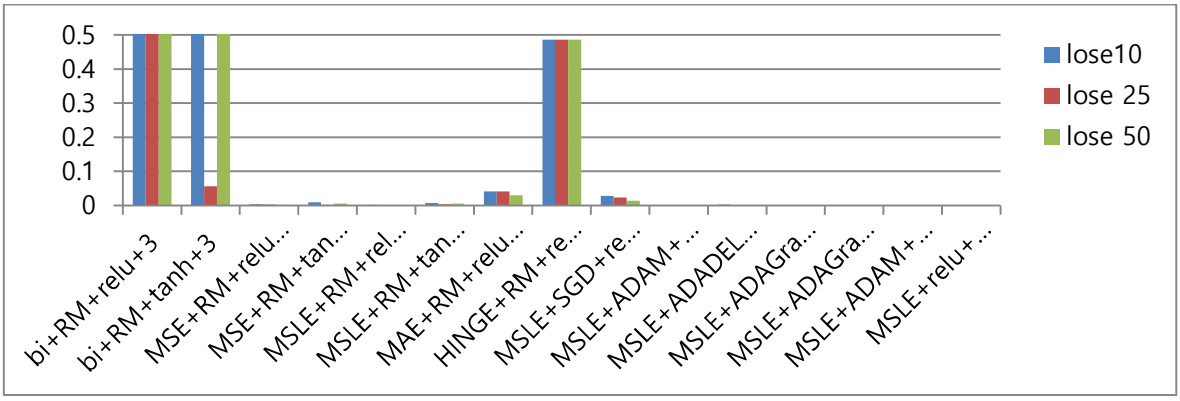

Fig7: The loss function in different number of epochs (10, 25, 50) for the different hyper parameter combination in the auto encoder

Figure 7 shows the loss function of the auto encoder with different hyper parameters. This loss function is in 10, 25, and 50 epochs. As shown in the graph more than one combination gives a little loss function as the last five combinations from the right.

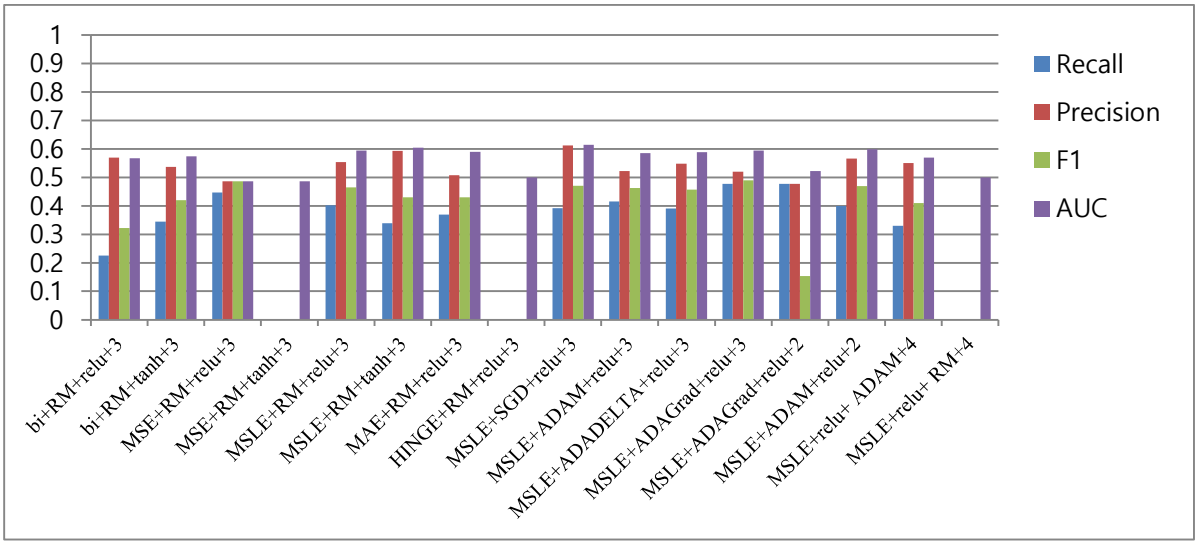

Fig 8 The recall, precision.F1 measure and area under the curve (AUC) for the classifier on the retrieved images after applying different hyper parameter combination in the auto encoder

Figure 8 shows the different matrices like recall, precision, F1, and AUC of the classification algorithm after applying different hyper parameters on the auto encoder. In other words, applying different hyper parameters' on the auto encoder and save the retrieved images from the auto encoder then try to classify it using another CNN classifier to see the effect of the different hyper parameters on the classification step.

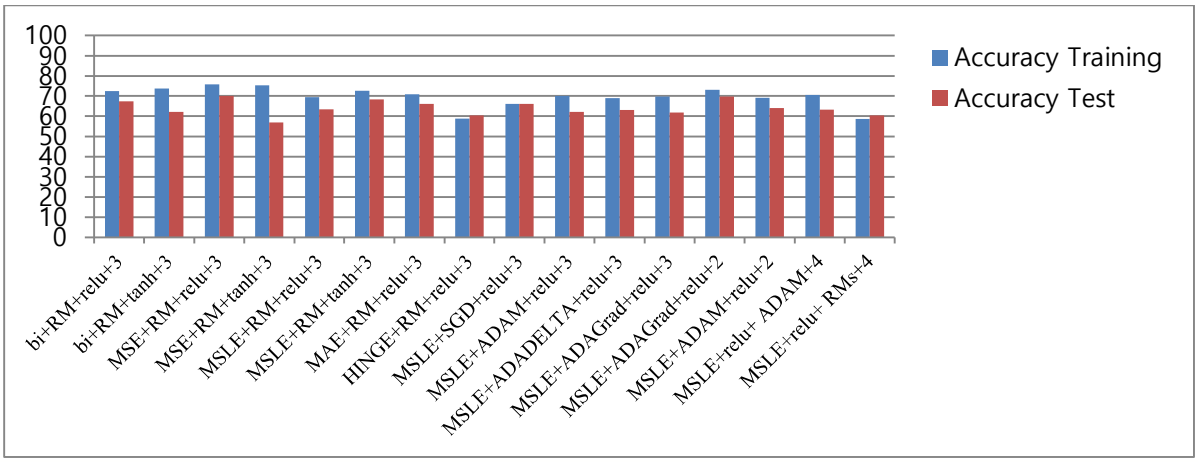

Fig 9 the training accuracy and the test accuracy of the classifier on the retrieved images after applying different hyper parameter combination on the auto encoder

Figure 9 shows the training and the test accuracy of the classification algorithm on the images from the auto encoder also for different hyper parameters.

The Figure shows the combination with the best auto encoder results. The upper row shows the matrices of the auto encoder. The second row shows the matrices of the classification. **A** shows the loss parameter of the training and validation iterations the loss in the training is decreasing by increasing the epochs also in the validation set. **B** shows the mean square error is getting decrease when increasing the epoch's number also the loss and the mean absolute error getting decrease. In the second row, **C** shows the different parameters of the classification (which is not the best one). **D** shows the confusion matrix of the classification stage which shows the performance of the classification model and the relation between the predicted and the actual values. **E** shows the iterations in the classification step.

Figure 10 shows the roc curve which shows the classification algorithm with reflects of different hyper parameters on the classification result. The mean square logarithmic error lose function, ADAGRAD optimizer, relu activation function and two CNN (MSLE+ADAGrad+relu+2 layers) have the best curve mean square logarithmic error lose function, ADAM optimizer, relu activation function and two CNN (MSLE+ADAM+relu+2 layers) and mean square logarithmic error lose function, ADAM optimizer, relu activation function and five CNN (MSLE+ADAM+relu+3 layers).

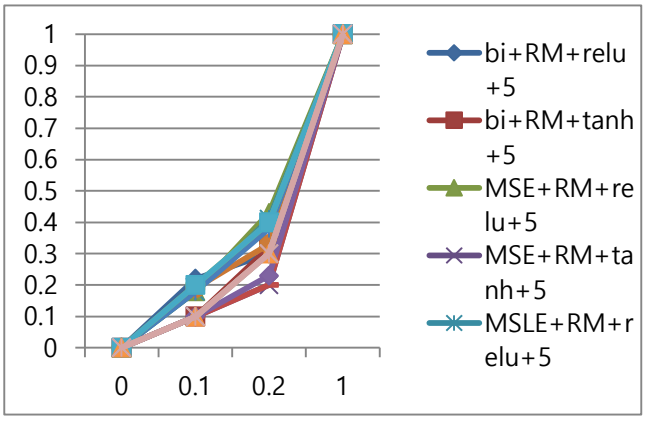

Fig 10 the roc curve of the classifier on the retrieved images

5. Conclusion

Simulation of the proposed Auto encoder for real time IoT systems by Combining Hyper parameter is validated and the effect of different parameters on the auto encoder and the matrices of the classification algorithm is done. From this investigation, we conclude that changing the algorithm hyper parameters may affect the algorithm matrices and the number of epochs also. The results shows that by increasing the number of epochs decrease the loss function but by increasing the number of layers does not increase the evaluation matrices. The optimizer (ADAM and ADAGrad) gives the best results when applying on the auto encoder with relu activation function and loss function Mean Square Logarithmic error. An early stopping can gives good results also.

References

[1] Mahmudul Hasan, Md. Milon Islam, Md Ishrak Islam Zarif, and M.M.A. Hashem," Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches ", Internet of Things,2019.

[2] Tie Luoand Sai G. Nagarajan, "Distributed Anomaly Detection using Auto encoder Neural Networks WSN for IoT", IEEE International Conference on Communications, 2018.

[3] Lirong Chen, Qingfeng Guan, Bin Feng, HanqiuYue, Junyi Wang, and Fan Zhang, A Multi-Convolutional Auto encoder Approach to Multivariate Geochemical Anomaly Recognition", Minerals, 2019.

[4] Hany F. Atlam, Robert John Walters, and Gary Wills," Internet of Things: State-of- the-art, Challenges, Applications, and Open Issues ", International Journal of Intelligent Computing Research, 2018.

[5] Sagar Bhat, Omkar Bhat, and Pradyumna Gokhale, " Applications of IoT and IoT: Vision 2020 ", IEEE Internet of Things Journal, 2018.

[6] Sangeetha S and Haseena P," Image Encryption using Deep Neural Networks based Chaotic Algorithm", International Research Journal of Engineering and Technology (IRJET),2020.

[7] Dor Bank, Noam Koenigstein, and Raja Giryes,"Auto encoders", arXiv: 2003.05991v1, 2020.

[8] Pierre Baldi," Auto encoders, Unsupervised Learning, and Deep Architectures", JMLR Workshop on Unsupervised and Transfer Learning, 2012.

[9] Marc Claesen and Bart De Moor," Hyper parameter Search in Machine Learning", arXiv:1502.02127v1,2015

[10] Sotiris Kotsiantis, I. D. Zaharakis, and P. E. Pinellas," Machine learning: A review of classification and combining techniques", Artificial Intelligence Review, 2006.

[11] Xiaofei Yang, Xiaofeng Zhang, Yunming Ye, Raymond Y. K. Lau, Shijian Lu, Xutao Li, and Xiaohui Huang," Synergistic 2D/3D Convolutional Neural Network for Hyper spectral Image Classification", remote sensing,2020.

[12] Minal Chauhan and Rashmin Prajapati," Image Encryption Using Chaotic Based Artificial Neural Network ", International Journal of Scientific & Engineering Research, Volume 5, Issue 6, 2014

[13] Asif Shahriyar Sushmit, Shakib Uz Zaman, Ahmed Imtiaz Humayun, Taufiq Hasan, and Mohammed Imamul Hassan Bhuiyan," X-Ray Image Compression Using Convolutional Recurrent Neural Networks", arXiv:1904.12271v2,2019.

[14] Pinar Akyazi and Touradj Ebrahimi," Learning-Based Image Compression using Convolutional Auto encoder andWavelet Decomposition", IEEE Transactions on Multimedia, 2019

[15] Van LoiCao, Diep N. Nguyen, Quang Uy Nguyen, and Hoang Dinh Thai," Learning Latent Representation for IoT Anomaly Detection", IEEE TRANSACTIONS ON CYBERNETICS,2020.

[16] Mehdi Mohammadi, Sameh Sorour, and Ala Al-Fuqaha," Deep Learning for IoT Big Data and Streaming Analytics: A Survey", IEEE Communications Surveys & Tutorials, 2017.