[1]Tao Sun

Advancements in Communication Systems: From Image Compression Techniques to Deep Learning Applications

Journal of Electrical Systems

Abstract: **-** With the advancement of medical technologies, it is now crucial to diagnose illnesses using medical imaging. Medical pictures frequently travel from one end of the network to the other via its branches. Thus, a high degree of security is needed. Unauthorised usage of the image's data causes issues. The significant expansion of the Internet of Things (IoT) in healthcare sector has raised serious concerns about security and integrity of medical data for applications that provide healthcare services. The aim of this research is to transmit the secure compressed medical image using communication system utilizing DL model. Input image has been compressed using convolutional equalizing quantizer with Gaussian scale encoder mixture model. then the secure image has been transmitted using Elliptic Curve wavelet transform based on cloud IoT model. the experimental analysis has been carried out for various input medical image compression and transmission in terms of data throughput, end-end delay, QoS, training accuracy, average precision. The proposed technique attained End-end delay of 61%, Data Throughput of 96%, QOS of 93%, training accuracy of 97%, average precision of 94%.

Keywords: : Communication system, deep learning, image compression, secure image transmission, cloud IoT model

1. Introduction:

Information technology and medical services have recently attracted a lot of attention in a related way, which has led to certain improvements in the medical field. on the data-centric therapeutic field of telehealth, massive amounts of data are created and accessed regularly on a distributed cloud. Medical image processing is the main activity in telehealth, where sharing X-ray, CT, MRI, other imaging data can be used to treat and diagnose disorders. As patient data is transferred across a dispersed environment for processing and storing, this ease of transmission raises concerns about data privacy as well as security. Cryptographic techniques are well recognised as a means of ensuring confidentiality as well as validity of medical picture data in a bilateral transmission setting [1]. In e-Healthcare, medical records and imaging data are sent to a distant healthcare provider so that patients can be monitored remotely. The transfer of medical photographs and other medical data is being made easier by developments in IoT and cloud-based storage, which offer enormous storage capacity and powerful processing power. People are being forced to switch to cloud-based storage due to the rise in multimedia material since it offers enormous storage capacity and powerful processing power. The cloud computing technology shares resources and data with other devices through data outsourcing. All that is needed to utilise these resources is to submit requests or multimedia files to cloud servers for processing [2]. The information can be retrieved by the user once the process is complete. As a result, there is a great deal of risk associated with cloud-based design, including insider threats and single points of failure. Reports of data breaches and service disruptions have surfaced in recent years, even though Cloud Service Providers (CSPs) have been built to be fully and potently connected in order to guarantee user information confidentiality. Multi-cloud computing has become more popular as a result of all these problems and difficulties with cloud security. Image compression is now crucial for uses like transmission and database storage due to advancements in image sensor hardware [3]. Using the widest range mobile phone as an example, popular mobile phones currently on the market have over 20 million image pixels, with each image having a file size of approximately 3MB. The size of image data has increased, putting more demands on physical storage devices and network bandwidth for transmission. The image's compression procedure not only enhances the surrounding environment but is also essential for processing, transmission, and storage. When an image is compressed, unnecessary information is removed, leaving only the valid information intact so that the image may be recreated using that valid

[1] School of Electronic and Information Engineering, JiuQuan Vocational Technical College, JiuQuan,735000, China

Corresponding Author: Tao Sun

E-mail: pipicool032@163.com

information. Artificial Intelligence (AI) and Deep Learning (DL) have advanced quickly in last several years. In the realm of medical imaging, AI approaches have been instrumental [4]. These include computerised diagnosis and processing, execution of all image activities, including segmentation, recording, fusion, interpretation. Since directed devices produce the majority of the images, deep learning techniques are used to retrieve and analyse the images in order to extract information that is effectively represented. Numerous techniques are used in artificial intelligence, including support vector machines (SVM), neural networks (NN), K-nearest neighbour (KNN), other deep learning algorithms like generative adversarial networks (GANs), convolutional neural networks (CNN), recurrent neural networks (RNN), long short-term memory (LSTM). However, these techniques are limited in their ability to process natural images and take a long time to analyse and process features. When analysing the data overall, these algorithms are supplied raw data, which is then followed by necessary classification. Learning algorithms extract information from a vast collection of images, many of which are found in a typical database, and attempt to learn several levels of abstraction and representation [5].

2. Related works:

The majority of studies on object detection from picture data do not consider lossy compression and image quality simultaneously, or how they affect object detection performance. Nonetheless, some research has been done on the performance of deep CNNs in various scenarios, such as when input data reduction leads to a decline in quality. Another intriguing study field is compressing CNNs and developing resource-efficient deep models; for these purposes, our goal is to produce compact models that require less memory and infer more quickly, ideally without compromising algorithmic performance. Author [6] looked on how image quality affected image classification performance, which is like object detection but doesn't need localization. JPEG and JPEG2000 lossy picture compression was one technique used to degrade quality. Based on 10,000 photos selected from the ILSVRC 2012 validation set, the study used the ImageNet 2012 1000-class dataset. Because derivative of rounding function is zero almost everywhere, in [7], autoencoder's quantization is replaced by a smooth approximation in backpropagation. However, quantization is still used in the backpropagation's forward pass to prevent decoder from learning to invert smooth approximation. In [8], a soft relaxation of entropy as well as quantization was created. Instead of providing a precise quantized output, the developed network outputs the weight and a quantization level. A strong and adaptable technique, generative adversarial networks (GANs) [9] have also been used in image reduction. In [10], a discriminator was used to teach a decoder to produce realistic visuals. Perceptual loss based on a pretrained AlexNet's feature map is used to quantify similarity. In order to finish image segmentation or image classification, feature maps were taken out of learning-based image compression in [11]. The study [13], which was based on the work in [12], trained the discriminator of GAN using segmentation map-based image synthesis. This method employed synthesised images for non-important regions as well as produced extremely good performance at low bite rates. In order to provide a quantitative justification for revision of ISO/IEC IS 19794-6, author [14] examined current image compression techniques and compared JPEG and JPEG2000. He examined three different formats: cropped (IREX K3), masked and cropped (IREX K7), an unsegmented polar format (IREX K16). Utilizing commercial version of Daugman "iris2pi" method with JPEG-2000 compression, work [15] examined impact of picture compression on recognition system performance and connected it to image quality. Author [16] assessed the effects on the iris images of many general-purpose file compression schemes, lossless versions of lossy codecs, specialised lossless image codecs. Work [17] studied impact of utilizing pre-compressed data in iris segmentation as well as calculated relation between iris segmentation performance as well as general image quality metrics. In their research, they looked at how various iris segmentation techniques performed when subjected to extreme image compression, specifically utilising the JPEG, JPEG 2000, JPEG-XR methods. With exception of the loss function, which considers the diffused image provided as input to the encryption network, the encryption model is comparable to [18]. The effective encryption approach in [19] is a result of the deep neural network's immediate generation of cypher pictures without the need for network training. The network's weights are managed using DCT coefficients that are jumbled. The encryption technique is secure against attacks because of its nonlinearity, which is a result of numerous layers and activation functions.

3. Proposed image compression model

We outline the top-level model architectures that we looked into. Further information about the various recurrent network elements in our studies is given in the subsections. Our compression networks are made up of a decoding network (D) with recurrent network components, an encoding network (E), binarizer (B). After encoding, the input images are converted into binary codes that are sent to decoder or stored. Based on incoming binary code, decoder network estimates original input image. We repeat this process using residual error, which is discrepancy between decoder's reconstruction as well as original image. Proposed image compression model is shown in figure-1.

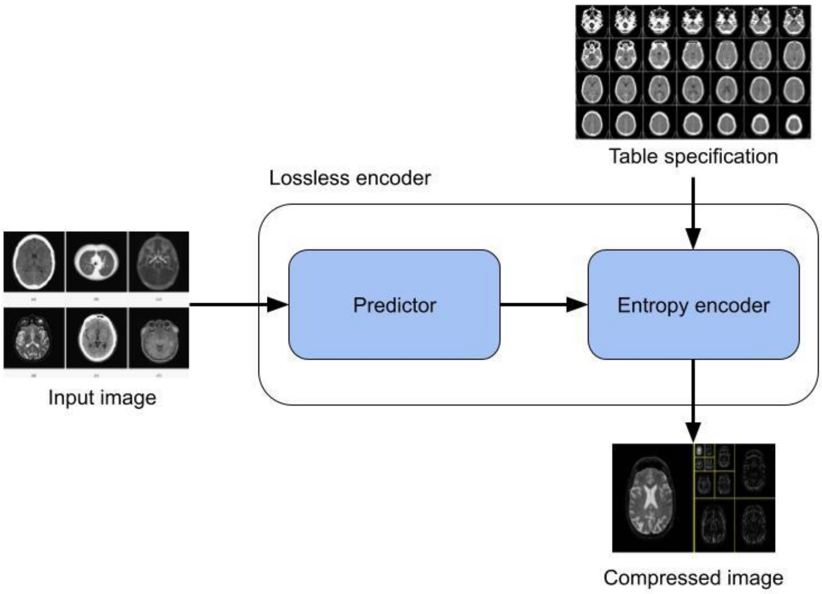


Figure-1 proposed image compression model

The method of disguising picture data so that it is safe and unreadable by anybody without encryption key is known as encryption. Based on asymmetric distribution of data with respect to external environment, the encryption cannot be changed unless the encryption technique is present. The suggested approach is predicated on a two-stage chaotic system that encompasses the pixels within the area of interest (ROI) and the ROI itself. First, a random key is created; in this situation, chaotic systems come in very handy. Both the image's entropy and its statistical unpredictability behaviour are taken care of.

4. Convolutional equalizing quantizer with Gaussian scale encoder mixture model (CEQ-GSEM):

The convolutional neural network architecture consists of many layers, including max pooling, ReLu, and convolutional layers. Its six levels are Max-pooling, ReLu, Conv2D, and a fully connected layer. To increase training performance, the network incorporates additional layers, like dropout. You can only activate the dropout layer during training. During forward pass, dropout layer randomly removes a certain number of neurons and remembers neurons that remain. only during backward pass updates non-dropped. One feature that contributes to regularisation is dropout. Dropout layer prevents overfitting during the training phase by helping the model learn robust features that are independent of the neurons. Convolutional layer output is typically down- or sub-sampled to produce a condensed set of feature maps. The pooling layer is typically computed right after the convolutional layer. The most popular and extensively used pooling layer, max-pooling, allows feature maps to have just their maximal values retained. Max-pooling is thought to be a CNN's primary function. It dramatically reduces the spatial size of feature maps and, as a result, the amount of computing required to process the following layers. The following equation can be used to summarise the primary functions of any CNN by eqn (1)

$$O^I = P\left(\sigma(O^{I-1} \times W^I + b^l)\right) \tag{1}$$

where the lth layer's previous layer's output feature map is represented by the Ol−1, the layer's weights and biases are indicated by the Wl and b l, respectively, and the non-linearity function outside the convolutional layer is indicated by the σ(•). A pooling process, denoted by P in Equation (1), frequently occurs after these phases. Low-luminance pixels undergo fine quantization steps to ensure that their inaccuracy is constrained to the same degree as that of high-luminance pixels. Several quantization tables are created in order to achieve this, and they are adaptively altered pixel by pixel based on the associated brightness level of each pixel. the scalar quantization is applied to them, where a quantization table corresponding to each pixel is used for every coefficient. In order to perform inverse quantization, every pixel should bring the label of its quantization table as additional information, which can be replaced by a value of a quantization step as only linear quantization is used by eqn (2)

$$\mathbf{y}_i = \mathbf{w}_i + \mathbf{n}_i = \mathbf{x}_i + (-1)^{b+1}\gamma\mathbf{x}_i + \mathbf{n}_i \; b = 0{,}1 \tag{2}$$

where the terms "yi" and "ni" stand for the attack noise and the received coefficient, respectively. In order to construct an ML decoder, we need to know the yi distribution for b = 0; 1. Using GMM with M component to model the low frequency coefficients of the original image (xi), we obtain the following from eqn(3):

$$\mathbf{x}_i \sim GM(\vec{p},\vec{\mu},\vec{\sigma}) \Rightarrow f_{\mathbf{w}_i}(\mathbf{w}_i) = \sum_{j=1}^{M} \frac{p_j}{\sqrt{2\pi}C_b\sigma_j} \exp \frac{-\left(\mathbf{x}_i - C_b\mu_j\right)^2}{2C_b^2\sigma_j^2} \tag{3}$$

The distribution of watermarked coefficients wi is easily obtained by eqn (4)

$$\mathbf{w}_i \sim GM(\vec{p},C_b\vec{\mu},C_b\vec{\sigma}) \Rightarrow f_{\mathbf{x}_i}(\mathbf{x}_i) = \sum_{j=1}^{M} \frac{p_j}{\sqrt{2\pi}\sigma_j} \exp \frac{-\left(\mathbf{x}_i - \mu_j\right)^2}{2\sigma_j^2}$$

$$\text{where } C_b = 1 + (-1)^{b+1}\gamma \text{ for } b = 0.1 \tag{4}$$

The 256x256 input images are first split up into separate blocks, normalised, then reshaped into vectors before being organised into a 64x1024 matrix to train network. The neural network compresses input images during training such that they are smaller in size and then decompresses them back to their original size. 64 neurons are present in both the input and output layers to recover compressed input image. In terms of applied compression operation, the hidden layers have less neurons than the input layer. Here, lossless entropy coding systems are fully convolutional, processing binary codes in progressive order as well as raster-scan order for a particular encoding iteration. c(y, x, d) is a binary code of size H × W × D produced by each of our image encoder architectures. We assume a normal lossless encoding system where actual compression is performed by an arithmetic coder, in conjunction with a conditional probabilistic method of present binary code c(y, x, d). We disregard slight cost associated with employing a practical arithmetic coder that necessitates a quantized representation of Pˆ(c | T).

5. Secure image transmission model using Elliptic Curve wavelet transform (ECWT) based on cloud IoT model:

The output layer is seen as the completed product that combines the intended outcomes with the complexity. Importantly, the hyperbolic equation represents the outcome of numerous neural stage iterations required to obtain accurate prediction. Additionally, a neural network can provide a multitude of encryptions; therefore, it is essential to automatically select the optimal one in order to maximise the effectiveness of the suggested system. Thus, machine learning, or deep learning, was proposed. The contribution to this issue is described in depth in the following section. NN is controlled by a multitude of variables, and the optimal prediction outcome can be achieved by training network with these variables. System extracts multiple features from the medical image. The feature with the greatest influence on the outcome is selected, the factor with the least impact is disregarded, and the process is then repeated. System automatically raises one hidden layer if result keeps rising. One node should be added to the designated hidden layer if the outcome is steady. The neural network's structure must be integrated, it is fully connected to achieve every stage's results with data flowing through them to determine high impact parameter. Models with improved diffusion properties feed an encrypted network with a diffused picture as input. When the output deviates from the desired output, the encryption network is penalised since it creates a cypher image and the discriminator detects the difference between the output and desired picture. As seen in figure 2, the decryption network similarly produces a recovered plain image.

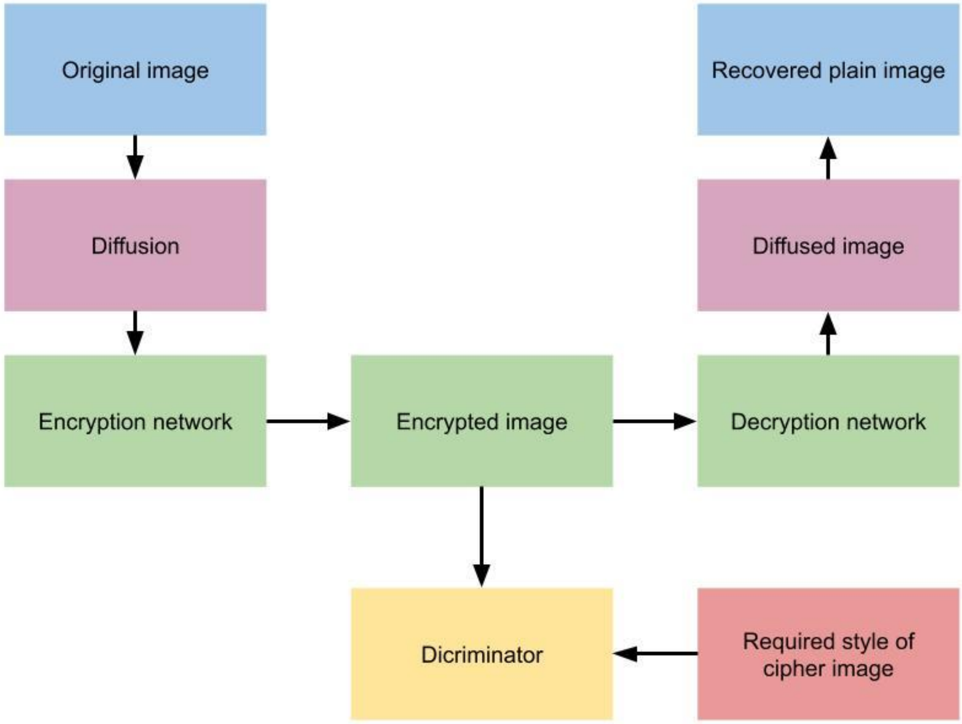


Figure-2 secure image transmission model using ECWT

Following Equation (5) can define key generation:

$$\text{initial key } = \begin{cases} x_{n+1}, \ 1 - ax_n^2 + y_n \\ \qquad bx_n \end{cases} \tag{5}$$

where n represents number of iterations in Henon starting state, which begins with x0 and y0 to initialise key, x and y are 2 variables and a and b are 2 specifications that satisfy chaotic behaviour, such as a = 1.4 and b = 0.3. Generally speaking, the system begins with the generation of a 128-bit key, which is followed by creation of a random bit stream and start of variable-iteration encryption. A few factors can be proposed to build a high-quality key, which forms foundation of encryption process; these variables take the form of pieces that are interlocked using DL. Following is a description of the variables by eqn (6)

$$Xh_0 = \frac{(k_1 \oplus k_2, \oplus \dots, \oplus k_8)}{2^8}$$

$$Yh_0 = \frac{(k_9 \oplus k_{10}, \oplus \dots, \oplus k_{16})}{2^8} \tag{6}$$

where the series of iterations for every layer in the neural system is represented by $Ki=k1|k2|k3,\dots,|k16$. Deep learning hidden layers are modified, encryption key is used once. When it comes to adding a chaotic context to node designs in suggested layers of NN method, key 16 performs better than its equivalents. Set of solutions to an equation of type is known as an elliptic curve by eqn (7)

$$y^2 = x^3 + ax + b, \tag{7}$$

where 4 = 4a 3 + 27b 2 , 0, is equivalent to condition that cubic polynomial x 3 + ax + b has no repeated roots. To prevent the encrypted image's ultimate grayscale expansion, we reduce the size of the colour image and apply grayscale to the whole field E(Fp). Next, in order to better match third encryption stage, we use proposed 4D cat map to make expanded grey values uniformly distribute in field E(Fp). We disseminate the encrypted image globally after EC has encrypted it in order to prevent known-plaintext and chosen-plaintext assaults. We will now go over each of these encryption procedures in detail. quantum grayscale representation, in which a number of quantum operations are performed after original image pixel values are transformed into their corresponding binary numbers by eqn (8)

$$|I\rangle = \frac{1}{2n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|f(y,x)\rangle|YX\rangle \quad (8)$$

By creating a solid connection between header, pixel, generated security data, this improves algorithmic security. However, as hashing is a computationally demanding operation by nature, hashing the pixel data and the header's secret attributes to generate keys and initialization vectors may result in computational overhead. Therefore, by supplying encryption keys and initialization vectors externally, second approach presented here removes this overhead. Traditional techniques like key distribution centres or public-key techniques like Diffie-Hellman key exchange can be used to supply the keys. An alternative method for exchanging external keys and initialization vectors involves encrypting them at the sender's end and decrypting them at the recipient's end using the DICOM header. Diffusion is the second stage of picture encryption. It modifies the image's pixel values and produces noise as a result. OR operation is carried out between pixel value, K key, scrambled picture vector to produce encrypted image.

One of the most random procedures that takes place throughout image encryption method is procedure that goes along with image's random division as well as segmentation, random distribution of pixels in image through DL. The fundamental components of a NN, such as input layer, hidden layer, output layer, are well-known standard components. Primary focus of work is on how deep learning affects and influences hidden layer's components based on input layer. DNN is controlled by a number of specifications, some of which are variables that may be altered to achieve the desired outcome and others of which are fixed parameters that can only be altered by altering the architecture of a specific neural network layer. A detailed illustration of these parameters will be provided throughout the design neural network discussion.

6. Results and discussion:

Using the GforceGTX 770 and CUDNN 5110 devices, we conducted all of our tests using Python 2.7 with the Spyder Integrated Development Environment (IDE), Keras, and TensorFlow frameworks. Using the standard dataset and a learning rate of 0.5, we evaluate the performance of our watermarking framework. Our method was trained over several epochs. It consistently yields nearly same accuracy as well as error rate.

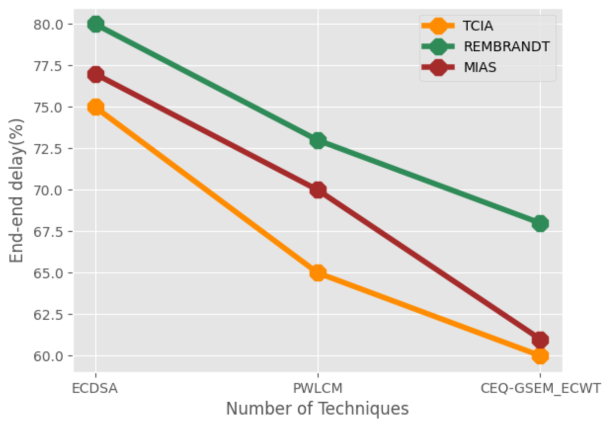
Dataset description: Two different datasets are used in this investigation. The first was acquired from Nanfang Hospital and General Hospital, Tianjing Medical University, China, between 2005 and 2010. It was then made available online in several editions, with the most recent edition being uploaded in 2017. The first was obtained between 2015 and 2010. Collection contains T1-weighted, contrast-enhanced images from 233 patients who had pituitary tumours, gliomas, and meningiomas. The size, shape, and location of brain tumours might vary depending on their types and grades. Three distinct perspectives are included in the dataset: sagittal, coronal, and axial views. The second dataset can be accessed through the public access repository of Cancer Imaging Archive (TCIA). Thirty-one patients with a variety of disorders, grades, ages, races have MRI multisequence pictures available in Repository of Molecular Brain Neoplasia Data (REMBRANDT). Images on T1-weighted contrast-enhanced that show various glioma grades (Grades II, III, and IV) were chosen. The mammograms are from the Free Mammography Database patient files (MIAS). Ten mammograms were also utilised to train classifier. Of the 46 mammograms, 10 benign and 15 malignant masses are located in dense areas with glandular tissues, ducts, breast boundaries, blood vessels, glandular tissues in different breast areas.

Table-1 Comparative based various medical images

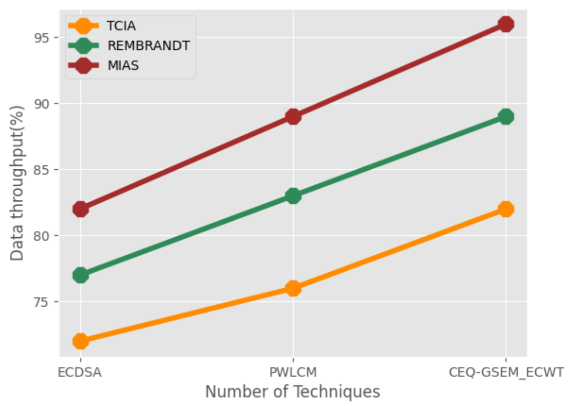
Dataset	Techniques	End-end delay	Data throughput	QOS	Training accuracy	Average precision
TCIA	ECDSA	75	72	70	74	73
	PWLCM	65	76	77	79	78
	CEQ-GSEM_ECWT	60	82	85	83	84
REMBRANDT	ECDSA	80	77	75	82	72
	PWLCM	73	83	81	87	75

	CEQ-GSEM_ECWT	68	89	86	92	85
MIAS	**ECDSA**	77	82	85	89	81
	PWLCM	70	89	88	94	85
	CEQ-GSEM_ECWT	61	96	93	97	94

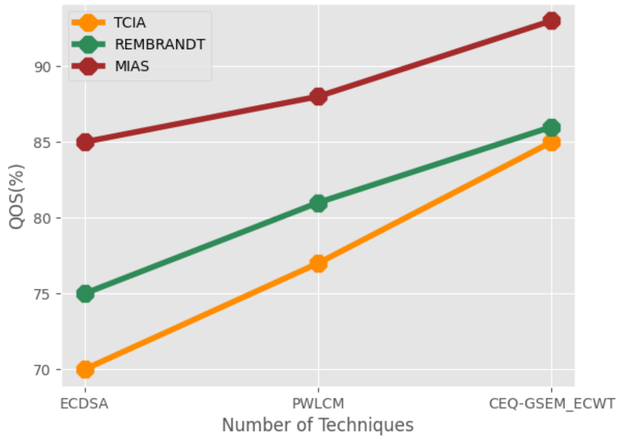
Based on a variety of medical imaging, Table 1 compares the suggested and current techniques. Dataset analysed are TCIA, REMBRANDT, MIAS dataset. The parameters analysed are End-end delay, Data Throughput, QOS, training accuracy, average precision. Training and testing has been carried out based on end-end delay of epochs. Plaintext sensitivity is a crucial factor to consider while calculating the efficacy of a suggested picture encryption technique, in addition to key sensitivity. Stated differently, the one-bit modification requires the encryption system to be extremely sensitive to the raw image. Suggested method employs plain image-related keys for encryption, meaning that iterating the chaotic map and using the resulting sequence for the pixel confusion phase is done using plain image-related initial conditions. In order to further improve security, the suggested approach does diffusion across a permuted picture by introducing a plaintext related key image $|Id\rangle$. The input image is represented quantum mechanically by the $|Id>$, where a single bit difference significantly alters the key image.



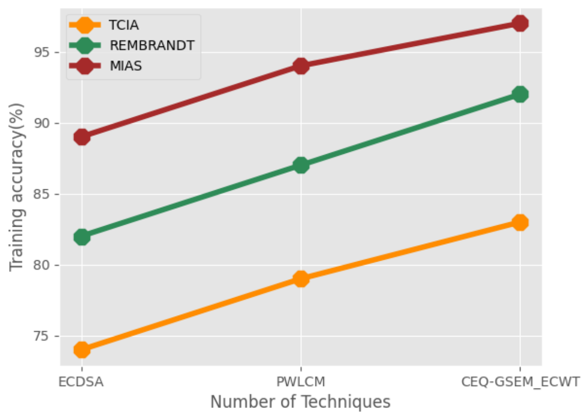
(a) End-end delay



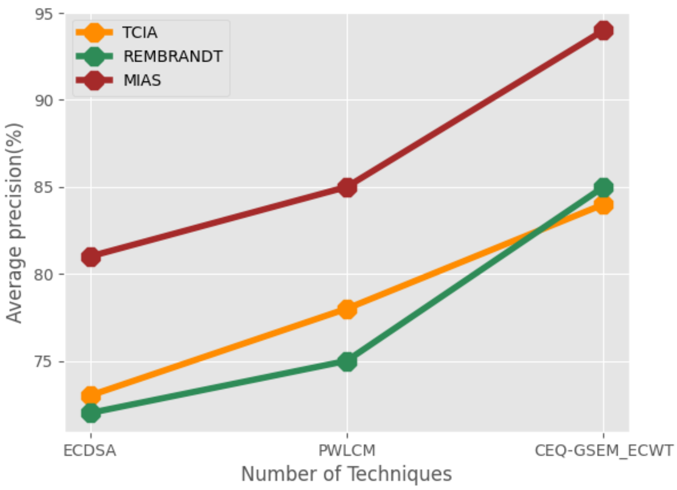
(b) Data throughput



(c)QOS



(d) Training accuracy



(e) Average precision

Figure-3 Comparative for TCIA dataset in terms of (a) End-end delay, (b) Data Throughput, (c) QOS, (d) training accuracy, (e) average precision

Figure-3 (a)- (e) shows comparative for TCIA dataset. Proposed technique End-end delay of 60%, Data Throughput of 82%, QOS of 85%, training accuracy of 83%, average precision of 84%; ECDSA attained End-end delay of 75%, Data Throughput of 72%, QOS of 70%, training accuracy of 74%, average precision of 73%, PWLCM attained End-end delay of 65%, Data Throughput of 76%, QOS of 77%, training accuracy of 79%, average precision of 78%. for REMBRANDT dataset The proposed technique attained End-end delay of 68%, Data Throughput of 89%, QOS of 86%, training accuracy of 92%, average precision of 85%; ECDSA attained End-end delay of 80%, Data Throughput of 77%, QOS of 75%, training accuracy of 82%, average precision of 72%, PWLCM attained End-end delay of 73%, Data Throughput of 83%, QOS of 81%, training accuracy of 87%, average precision of 75% The proposed technique attained End-end delay of 61%, Data Throughput of 96%, QOS of 93%, training accuracy of 97%, average precision of 94%; ECDSA attained End-end delay of 77%, Data Throughput of 82%, QOSof 85%, training accuracy of 89%, average precision of 81%, PWLCM attained End-end delay of 70%, Data Throughput of 89%, QOS of 88%, training accuracy of 94%, average precision of 85% for MIAS dataset.

One of the most random procedures that takes place throughout image encryption process is procedure that goes along with image's random division and segmentation, random distribution of pixels in image through DL. The neural network's hidden layers are formed over a number of stages, and a feedback mechanism allows for the reprogramming of each hidden layer in response to the degree of virality of each iteration. Input layer, hidden layer, output layer are well-known examples of the basic elements of a neural network. The main focus of the work is on how components of hidden layer are affected and influenced by deep learning depending on the input layer. DNN is controlled by a number of specifications, some of which are variables that may be altered to achieve the desired outcome and others of which are fixed parameters that can only be altered by altering the architecture of a specific neural network layer. A detailed illustration of these parameters will be provided throughout the design neural network discussion.

7. Conclusion:

Using a deep learning model in a communication system, the research aims to send medical images that are securely compressed. In this case, the input image was compressed using a mixture model of Gaussian scale encoder and convolutional equalising quantizer. then, based on the cloud IoT paradigm, the secure image was communicated using an Elliptic Curve wavelet transform. The trials also demonstrated that, in most circumstances, a higher compression level leads to a lower recognition performance. The analysis of the real and fake scores revealed that objects introduced by compression change the distinctive biometric features of the iris that are present in real samples, making compressed photos more dissimilar. Applying encryption algorithm's inverse yields decrypted image data. The algorithm is used to produce good encryption and decryption results for grayscale photos. The simultaneous execution of chaotic key creation, permutation, and diffusion is the reason it is faster. The suggested cypher framework is suitable for embedded systems that respect resource constraints and real-time performance, as demonstrated by the results. The security analysis is carried out well, outcomes of the experiments demonstrate that the proposed method serves as the foundation for cryptography.

Funding：

This work is co-funded by the 2023 Gansu Provincial Vocational Education Teaching Reform Research Project (2023gszyjy-054) and the 2023 Gansu Provincial College Teachers Innovation Fund Project (2023B-448).

Reference:

[1] Khandelwal, J., & Sharma, V. K. (2023). W-VDSR: Wavelet-based secure image transmission using machine learning VDSR neural network. *Multimedia Tools and Applications*, *82*(27), 42147-42172.

[2] Alarood, A. A., Faheem, M., Al-Khasawneh, M. A., Alzahrani, A. I., & Alshdadi, A. A. (2023). Secure medical image transmission using deep neural network in e-health applications. *Healthcare Technology Letters*, *10*(4), 87-98.

[3] Ye, G., Liu, M., Yap, W. S., & Goi, B. M. (2023). Reversible image hiding algorithm based on compressive sensing and deep learning. *Nonlinear Dynamics*, *111*(14), 13535-13560.

[4] Singh, M., Baranwal, N., Singh, K. N., Singh, A. K., & Zhou, H. (2023). Deep learning-based biometric image feature extraction for securing medical images through data hiding and joint encryption–compression. *Journal of Information Security and Applications*, *79*, 103628.

[5] Yang, Y. G., Niu, M. X., Zhou, Y. H., Shi, W. M., Jiang, D. H., & Liao, X. (2024). A visually secure image encryption algorithm based on block compressive sensing and deep neural networks. *Multimedia Tools and Applications*, *83*(10), 29777-29803.

[6] Kumar, P., Rahman, M., Namasudra, S., & Moparthi, N. R. (2023). Enhancing security of medical images using deep learning, chaotic map, and hash table. *Mobile Networks and Applications*, 1-15.

[7] Zhang, M., Li, Y., Zhang, Z., Zhu, G., & Zhong, C. (2023). Wireless image transmission with semantic and security awareness. *IEEE Wireless Communications Letters*, *12*(8), 1389-1393.

[8] Wang, Y., Chen, L., Wu, G., Yu, K., & Lu, T. (2023). Efficient and secure content-based image retrieval with deep neural networks in the mobile cloud computing. *Computers & Security*, *128*, 103163.

[9] Sultan, L. R. (2023). Deep learning approach and cover image transportation: a multi-security adaptive image steganography scheme. *Smart Science*, *11*(4), 677-694.

[10] Liang, Y., Zhao, M., Liu, X., Jiang, J., Lu, G., & Jia, T. (2024). An adaptive image compression algorithm based on joint clustering algorithm and deep learning. *IET Image Processing*, *18*(3), 829-837.

[11] Padhy, S., Dash, S., Shankar, T. N., Rachapudi, V., Kumar, S., & Nayyar, A. (2024). A hybrid crypto-compression model for secure brain mri image transmission. *Multimedia Tools and Applications*, *83*(8), 24361-24381.

[12] Xu, J., Ai, B., Chen, W., Wang, N., & Rodrigues, M. (2023). Deep joint source-channel coding for image transmission with visual protection. *IEEE Transactions on Cognitive Communications and Networking*.

[13] Zhang, W., Bai, K., Zeadally, S., Zhang, H., Shao, H., Ma, H., & Leung, V. C. (2023). Deepma: End-to-end deep multiple access for wireless image transmission in semantic communication. *IEEE Transactions on Cognitive Communications and Networking*.

[14] Rohhila, S., & Singh, A. K. (2024). Deep learning-based encryption for secure transmission digital images: A survey. *Computers and Electrical Engineering*, *116*, 109236.

[15] Chai, X., Song, S., Gan, Z., Long, G., Tian, Y., & He, X. (2024). CSENMT: A deep image compressed sensing encryption network via multi-color space and texture feature. *Expert Systems with Applications*, *241*, 122562.

[16] Garcia-Nonoal, Z., Mata-Mendoza, D., Cedillo-Hernandez, M., & Nakano-Miyatake, M. (2024). Secure management of retinal imaging based on deep learning, zero-watermarking and reversible data hiding. *The Visual Computer*, *40*(1), 245-260.

[17] Pandey, B. K., Pandey, D., Alkhafaji, M. A., Güneşer, M. T., & Şeker, C. (2023). A reliable transmission and extraction of textual information using keyless encryption, steganography, and deep algorithm with cuckoo optimization. In *Micro-Electronics and Telecommunication Engineering: Proceedings of 6th ICMETE 2022* (pp. 629-636). Singapore: Springer Nature Singapore.

[18] Baranwal, N., Singh, K. N., & Singh, A. K. (2024). Using chaos to encrypt images with reconstruction through deep learning model for smart healthcare. *Computers and Electrical Engineering*, *114*, 109089.

[19] Panwar, K., Kukreja, S., Singh, A., & Singh, K. K. (2023). Towards deep learning for efficient image encryption. *Procedia Computer Science*, *218*, 644-650.