Journal of Information Systems Engineering and Management
2025, 10(13s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secure Transmission of Images Based on Chaos Encryption and Deep Neural Network

Rishav Gusain[1], Ashwani Kumar[2], Xiaochun Cheng[3], Raj Shekhar[2] Avinash Kumar Sharma[1]
[1]*Department of CSE, Sharda School of Computing Science and Engineering (SSCSE), Sharda University, Greater Noida, India*
[2]*School of Computer Science Engineering & Technology, Bennett University, Greater Noida, UP India*
[2]*Department of Computer Science, Swansea University, Bay Campus, Fabian Way, Swansea, SA1 8EN Wales, UK*
* *Corresponding Author:* Avinash Kumar Sharma Email: *avinashsharma2006@gmail.com*

ARTICLE INFO

Received: 01 Dec 2024

Revised: 15 Jan 2025

Accepted: 29 Jan 2025

ABSTRACT

In today's world of digital media, digital images are the most frequently used method of transmitting images, and therefore, their protection is significant. As it has been seen, the technology keeps on changing and thus, though there have been improvements in encryption of images, the problem of secure transmission is not completely solved. Therefore, the process must be made continuous and refined to protect data privacy and integrity, as well as transmission and storage reliability. This work focuses on the application of cryptography together with neural networks employing Python with Keras for secure image transfer. The proposed method involves image encryption through pixel shuffling, logistic-map chaotic values, and XOR operations to produce encrypted images. The neural network layer decodes the encrypted images and measures the quality of the decrypted images dependent on PSNR, MSE, and Correlation Coefficients. Thus, by comparing these metrics for the original and reconstructed images, the project will improve security and determine the effectiveness of the encryption-decryption method. The combination of the chaotic maps and neural networks gives a strong foundation for image encryption. The chaotic values bring in randomness into the encryption process, thus increasing the level of security while the neural network helps in perfect reconstruction and image quality. This approach is advantageous as it addresses both the issues of data security and, after decryption, image quality and so it offers a midway point for secure image transmission in this technology-driven world.

Keywords: Secure transmission, Cryptography, Neural networks, Shuffling, Chaotic values, Encrypted image, Reconstructed image.

INTRODUCTION

As internet technologies has emerged as a significant trend, multimedia has surfaced as a main form of communication. Graphics is among the numerous forms of multimedia useful in relaying information because it has the capacity to present intricate information in an enthralling and comprehensible way. Digital images have found many uses in many fields, such as business, teaching, scientific research, aviation, defence, and the government. Using computers or mobile devices, the Internet lets us share visuals in a matter of seconds. Still, anybody can get that image and, as we all know, unauthorized cryptanalysis is a nightmare for the information in the communication of images [4]. These changes in pictures can mask significant information and change the quality of a picture to convey wrong information [5]. Therefore, the concept of image security has extended its significance [7]. Medical pictures contain sensitive information and cannot just go through the process of computation. It seems to me highly confidential if a fraction of it is altered, can lead to misdiagnosis of patients. Maintaining patient confidentiality is important because sometimes the records of patients are exceedingly sensitive. Analysing picture data and limiting the availability of that data only to personnel who are approved is one of the most effective techniques [18]. A technique for safeguarding medical pictures reduces the chances of unauthorized access while preserving patient anonymity. This is a definitive strategy of preventing unauthorized access and ensures that any and all medical data remains protected for the duration of its existence. Medical pictures are dissimilar to ordinary pictures with reference to measure of effectiveness, particularly high spatial co-relation and large data measurement. The process of securing a picture in healthcare is overly challenging, particularly in terms of data gathering, speed and dependability. Consequently, integrity and origin authentication of digital pictures is also a problem among researchers in the image processing field. That is why image security raised the concept in mind of researchers for encrypting. It may be

important to use traditional encryption techniques to secure these large datasets in healthcare organizations. One should prevent the computing processes necessary for analyzing healthcare pictures from possible risks [11]. This mainly involves generating random numbers and these are used in form the keys for encryption. Randomly generated numbers prove to be of immense importance when it comes to enhancing the performance of encryption algorithms. Existing solutions for image security employ various cryptographic algorithms, including AES and RSA, for protecting the picture data. Despite the effectiveness of these approaches, they have particular drawbacks and cannot always be adequate to address the dynamic nature of threats in cyberspace. Leading to an escalating interest in learning about new methods that may offer better protection against threats [24]. To raise image security, deep learning algorithms incorporate multiple levels of abstraction using neural networks, making it difficult for attackers to attack the system. The overall system thus becomes more robust and the process of image encryption becomes faster. Most of the traditional practices of encrypting data may not be very efficient in securing large dataset of medical photos. Therefore, it is crucial to mitigate the risks in algorithms used in the processing of medical images. There are multiple ways to encrypt the pictures, for example, high-speed scrambling, bit-wise XOR diffusion, chaos and logistic mapping and so on. Applying measures, such as the use of watermarks, can go along way to enhancing image security and minimise unauthorised use or breaches. However, deep learning can improve patients' privacy and avoid scams while providing confirmed healthcare image analytics [25]. Image security is improved with deep learning since the process involves neural networks at various levels of abstraction. Chaotic maps are often used in cryptographic methods due to their pseudo random behaviour. It generates the pseudo random numbers to generate the key for encrypting purpose. Some minor changes in primary setting can lead to significant change in output. Chaotic maps are deterministic but appear random. They feature properties like as ergodicity, sensitivity to beginning circumstances, and topological mixing that make them appropriate for cryptography applications [9]. Deep neural networks (DNNs), with their robust capabilities in pattern recognition, classification, and transformation, offer innovative solutions for secure image transmission. By leveraging the strengths of DNNs, it is possible to develop advanced encryption techniques that not only secure images against unauthorized access but also ensure their seamless transmission across various networks [24]. These networks can be trained to perform complex transformations on images, including encryption and decryption tasks. The primary advantage of utilizing DNNs in encryption lies in their ability to learn and adapt to intricate patterns within the data, enabling the creation of highly secure and efficient encryption schemes [12]. **Figure 1** depicts an overview of the overall proposed methodology in the paper. It also shows how data will flow in the algorithm.

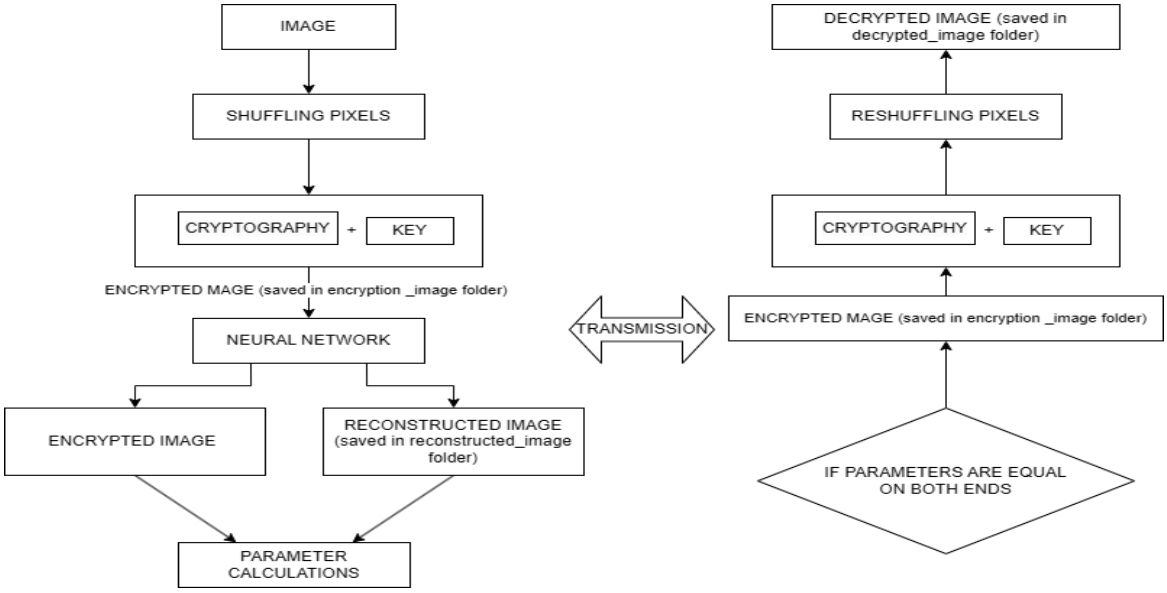

Fig.1: Overall methodology of the paper

The paper is organised into six sections. Section I provides a full introduction to picture security, cryptography, and deep learning approaches. Section II provides key objectives for this investigation. Section III is a related work of the studies. Section IV discusses the proposed methodology of the paper. Section V shows the results of the paper and a table of parameters having PSNR, MSE & Correlation coefficient of individual images taken as an input image. Section VI shows the conclusion, followed by the future scope.

The primary motivation for this paper is to propose an algorithm to secure transmission of medical images. Key points include:

- Ensuring the security of image data from attackers is crucial, especially in medical diagnoses, to hold the confidentiality, integrity, and availability of transferred data.
- Combining cryptographic techniques with deep learning enhances the encryption method, leading towards more secure and faster due to neural networks' multiple levels of abstraction to secure transmission process of images.
- To make a system have capabilities to handle the secure transmission process.

d aliquet risus feugiat in. In iaculis nunc sed augue lacus viverra vitae congue eu. Ipsum a arcu cursus vitae congue

LITERATURE REVIEW

In this section, the literature is reviewed and discussed on the basis of picture security adopting Neural network and cryptographic related techniques:- Seethalakshmi et al. [1] presented an algorithm of integration of Visual Cryptography and Data hiding by Image Steganography to make data security system more secured. This approach involves adding steganography to cryptography with the aim of improving the encryption algorithm and to make the algorithm strong enough to resist attacks. Moreover, for enhancement of the efficiency and security of the encryption process, there is also a tendency to use neural networks in order to define better places for the implantation of the stealth data. Thus, the proposed method has an added advantage of combining the strength of visual cryptography and steganography to make it harder for the enemy to get through the layered barriers. Cai et al. [3] have used tent map, Chebyshev map and the piecewise linear chaotic map for encryption. Their work mainly concentrates only on PRRABPM uses the permutation technique for encrypting and decrypting the plain text. This method raises the complication degree of the encrypting process; the latter is now based on plain text. In this way, the use of the chaotic maps leads to the high sensitivity to primary environment. Coutinho et al. [4] described the application of the NNs in Cryptography, especially the Adversarial Neural Cryptography (ANC). The author also details how neural networks can be used in cryptographic systems to enhance securities against adversarial actions. The method increases the security of the learned encryption algorithms through proposed adversarial training. This point of view trains neural networks in developing of the encryption/decryption algorithms that are nearly impossible to attack with the help of adversarial methods; it reveals a novel method of data protection against threats. Kalsi et al. [6] propose DNA Cryptography integrated with deep learning for the purpose of secure data transfer. The algorithm used in their approach includes key generation with the aid of a GA coupled with the Needleman-Wunsch algorithm. Data is encoded in DNA and then protected with additional layers of security through deep learning algorithms. DNA Deep Learning Cryptography can provide significant storage capacity and perform multiple operations simultaneously, thus being suitable for secure data encryption. This technique combines the high capacity of DNA sequences with a deep learning model to secure and efficient encryption method. Separable reversible data hiding in encrypted signals using cryptographic solutions is discussed by Tai and Chang et al. [8]. Their work compares the outcome of the suggested scheme with other methods of encryption, that proves their solution can be efficient and secure. This hide data technique gives recovery after decrypting, hence allowing an extra level of security and functionality to the encryption. The fractional-order hyper-chaotic system is discussed by Wen et al. [14] for chaotic image encryption. They evaluated entirely a proposed method of color image encryption and pointed out the weakness that can allow CPTA on such approach. Their works show the importance of having proper chaotic systems to help improve the strength of encryptions. As a result of using fractional-order hyper-chaotic systems, the proposed method has a higher degree of complexity and a more difficult to predict pattern than other methods, which will make it harder for the attackers to break into the encrypted images. Zakaria et al. In [15], the two-dimensional mKdV map is used in cryptographic encoding algorithms for images. They further explore briefly the mathematical ideas and algorithms behind these methods by comparing it with Sine-Gordon and Arnold's cat maps for encryption. Their work plays an important role in how different chaotic maps can be implemented for image encryption. The results provide few original insights other than that image encryption with chaotic systems may be less secure and fast in many methods. Zhang et al. To address this issue the authors of [16] suggest an approach where Convolutional Neural Networks (CNN) are combined with chaotic systems for secure image encryption. The study has been validated through an extensive performance evaluation, illustrating that this schema indeed provides a strong security against known-plain-text and chosen plain text attacks. Our method shows good robustness to cropped attack tests, which guarantees the integrity and security of encrypted images with partial data loss. Because of the ability to give chaotic

behavior, it employs deep convolutional neural networks and integrates them with CNNs, which makes this algorithm secure in terms of image encryption. Padinjappurathu Gopalan et al. [18] Privacy-preserving disease prediction in current modern healthcare systems are addressed using Logistic Regression with Error-Correcting Code (LR-ECC) and). In practice, we propose a learning framework that seamlessly works with logistic regression anomaly component over error correcting codes and ensure both robustness and accuracy so necessary for noisy healthcare data all while not giving away patient's health status to any untrusted party. Deep Learning with Genetic Algorithms (EHGA-DLNN) EHGA-DLNN is a technique that uses genetic algorithms for optimizing parameters while enhancing deep learning, hence together it produces an effective predictive model. This model has outperformed SVM, DLNN, ANN and KNNBased traditional classifiers having accuracy: 98.35%, sensitivity: 97.33% & specificity 96.36%. Nevertheless, the superior performance of EHGA-DLNN indicates its potential to predict diseases in an accurate and reliable manner whilst maintaining patient privacy. Alsafyani et al. [19] introduced a unique technique for safe image encryption based on DL and optical chaotic maps, with a special emphasis on facial image encryption. The approach combines deep learning's robust feature extraction capabilities with the unpredictability of chaotic maps to improve encryption security while maintaining image quality. This approach achieved impressive performance measures, including peak signal-to-noise ratio (PSNR) at 92%, a root mean squared error (RMSE) of 85%, and a structural similarity index (SSIM) of 68%. These results show that encrypted images still well retain the vivid quality but have very minimal distortion from the original images. Furthermore, this proposed model is performing better than the other existing models in terms of PSNR, RMSE, and SSIM, as well as encryption speed, making it a highly efficient and effective method for secure image communication. This security technology holds a firm defense against probable attacks and is formulated with deep learning coupled with optical chaotic maps, underlining that this technology is perfectly applicable in secure image communication systems. Lata and Cenkeramaddi et al. [21] explore DL techniques enhance the security of the medical images and also provides insights into research challenges and future aspects of the field. S & S et al. [25] propose the PPDD network for improving security in the Dark Cloud environment. This network uses deep learning to ensure the dependable and safe transfer of medical data. An effective picture denoising approach, along with a hybrid classification model, ensures high-quality image processing. The strategy emphasises secure, cloud-based image processing while maintaining privacy, utilising powerful deep learning techniques. The PPDD network's lightweight architecture is specifically built for medical data exchange, and it includes additional security mechanisms to secure sensitive information. Tamba et al. [30] provide a new Hopfield neural network model that employs multistable memristors. Their research looks on equilibrium states, dynamic behaviours, and the model's effectiveness in encoding biological imagery. Their study, which was implemented using a microcontroller and empirically confirmed, demonstrates a secure biomedical picture encryption technique that takes advantage of neural network instability. This method improves AI applications for recognition, encryption, and cognitive architectures. The paper emphasises the practical application of Hopfield networks across a variety of hardware platforms for effective biomedical image processing, representing important advances in the field.

METHODS

The proposed methodology is divided into two parts which can be taken as two ends. The first end is the sender's end, where the images are encrypted by using scrambling the pixels method and logistic map is used to create the keys. In code there are two functions for creating the random sequence of numbers they are indexgen and keygen both are creating different random sequence of numbers for encryption and then layer of neural network is created for reconstructing the image taking encrypted image as an input. The second end is the receiver's end, where the parametric values are evaluated first on an individual basis. If values are found to be the same, then it allows for the process of decryption. The encryption process is reversed during the decryption step. After these processes, the image is securely transmitted from one end to another end. Dataset: Brain MRI images were taken as a dataset of a total of 14715 images. From Kaggle. **Figure 2** shows the algorithm of the sender's side, where images are encrypted by shuffling and cryptographic method. After encryption, encrypted images are considered as input into a neural network to develop a reconstructed image from that encrypted image. Then parameters i.e., PSNR, MSE and correlation coefficient are calculated. After that, encrypted image and reconstructed image and parameters are sent to the receiver's end for the diagnosis of healthcare image. **Figure 3** shows the algorithm of the receiver's side, where the parameter values are calculated, and those values are compared with the sender's side parametric evaluation. If both are found to be equal, then the encrypted image will be decrypted otherwise the message will be displayed that "Your image has been interrupted. Please resend the image". Then the decrypted image is ready for the patient's diagnosis.

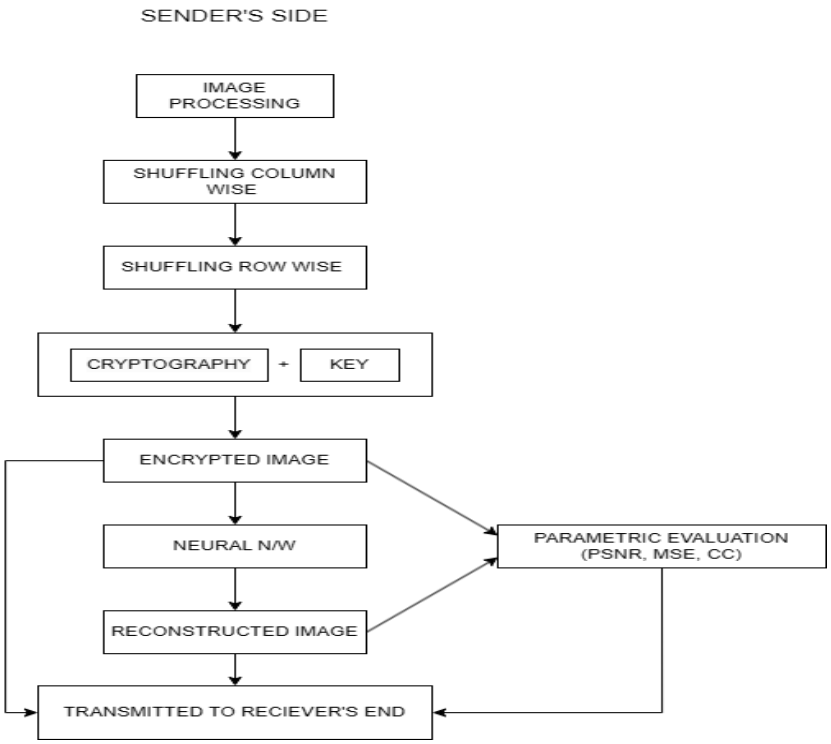

Fig.2: Sender's side algorithm

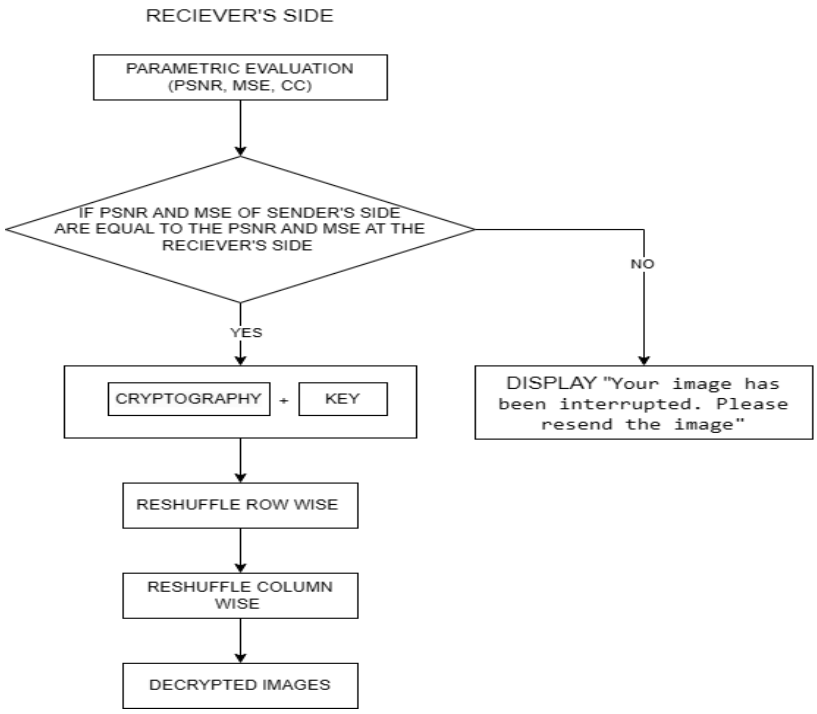

Fig.3: Receiver's side algorithm

Pseudo Code for the Algorithm

1 Process the image.
2 Perform scrambling by using indexgen function using logistic map column wise then row wise to get a shuffled image.
3 Perform XOR on image with a key by generating chaotic (Random) key values by using keygen function.
4 Save the encrypted image into the "encrypted_image" folder.
5 Create a neural network to construct the reconstructed image from the encrypted image by using.

6 Check the parametric values.
7 Transfer the image to the receiver's end.
8 Compare the parametric values.
9 If values at sender's end = = values at receiver's end.
10 Then only decrypt the image using decryption process by reversing the encryption process.
11 else display "Your image has been interrupted. Please resend the image".
12 Save the decrypted image in the "decrypted_image" folder.

Neural Network Creation: Imagine that there is a special layer of neural network developed only for the task of reconstructing the encrypted images as well as measuring accuracy. This later applies dense connections to efficiently and carefully process each feature input for images, eventually giving way to exact output production. The operation is primarily facilitated by the Rectified Linear Unit (ReLU) activation function [31] that enhances the network in learning detailed details and patterns from the encrypted input. Nodes contribute optimally to the reconstruction of the original image from the encrypted state through ReLU activation. This has to be determined regarding the quality of fidelity of images after decryption using encryption techniques, and it is vital for the safe transmission of such information. Figure 4 depicts general structure for a neural network contains an input layer that feeds data into this setup, followed by one or more connected hidden layers wherein neurons execute computations with activation functions modelling the nonlinearity of the neuron interactions. Neurons in each layer are densely connected to other neurons in the layer and during learning, the connection between neurons have their weights adaptively adjusted to reduce the gap between the predictions obtained in the output layer. Special architectures exist, such as convolutional or recurrent layers, that are suited for sequences. This means that in turn, data types like images or sequences improve the effectiveness of the network. **Figure 4** below gives the structure visually for how input is passed through layers to yield final predictions. It is critical in deep learning applications, such as image categorization, and sequence prediction.

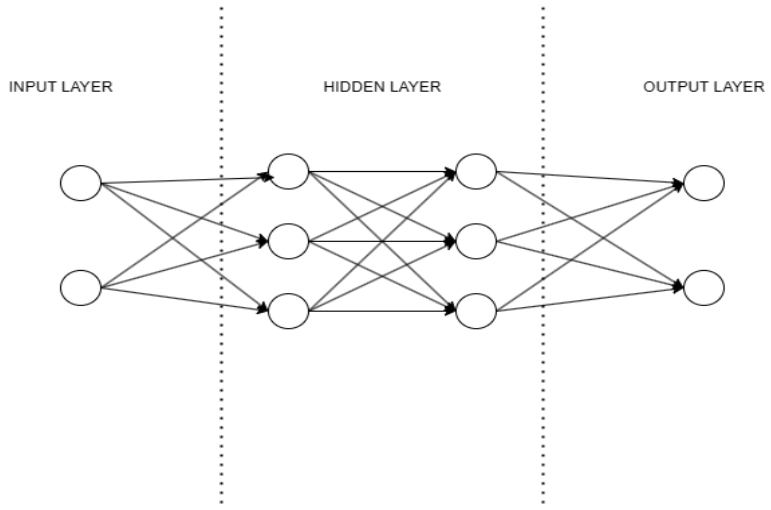

Fig 4: Layers of neural networks

Parametric Calculations: The performance metric variables used for evaluation of the images are PSNR, MSE and CC. These are compared at both ends ie., sender's end and receiver's end. The description and formulae for these are given below.

MSE is a used measure to determine the squared gap, between the original values and the predicted values. In image processing, MSE helps in gauging the disparity between the image and a distorted or reconstructed version. The formula for calculating MSE is:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)] \qquad \text{(i)}$$

PSNR is a metric utilized to evaluate the quality of reconstruction by compression techniques like those used in image and video compression. It compares the data with the compressed data, providing insights into how the compression process retains information. PSNR is calculated in terms of the Mean Squared Error between the original and the compressed image and can be obtained as follows:

$$\text{PSNR} = 10 \log_{10} \frac{(\text{MAX\_i})\text{^}2}{\text{MSE}} \qquad \text{(ii)}$$

Where MAX_i shows maximum possible pixel of the image which is 255 for an 8-bit image.

Correlation Coefficient (CC) are measures employed to show how well and in what direction there is an association between two variables. In image processing and data analysis, these coefficients play a role in assessing how connected or similar two datasets or images are, to each other. The Pearson correlation coefficient (r) determines the linear relationship between two variables. For two image matrices X and Y, where each matrix describes the pixel intensity of two images:

$$\text{CC(r)} = \frac{\sum_{i=1}^{n}(\text{X\_i}-\bar{\text{X}})(\text{Y\_i}-\bar{\text{Y}})}{\sqrt{\sum_{i=1}^{n}(\text{X\_i}-\bar{\text{X}})\text{^}2 \ \sum_{i=1}^{n}(\text{Y\_i}-\bar{\text{Y}})\text{^}2}} \qquad \text{(iii)}$$

Where X_i and Y_i presents the value of the pixel at position i of the images X and Y respectively. $\bar{X}$ and $\bar{Y}$ are the mean pixel values of the image X and Y, respectively. The n shows the number of pixels in the image.

RESULTS

Outcome was measured in python & matplotlib versions 3.11.7 & 3.8.0 respectively. Input images were taken from https://www.kaggle.com/datasets/ashfakyeafi/brain-mri-images, brain images were taken. It was in the form of RGB ie. 3 channelled images. A total of 14715 images were taken as a dataset for the process of encryption and decryption. Five images were taken for the test set.

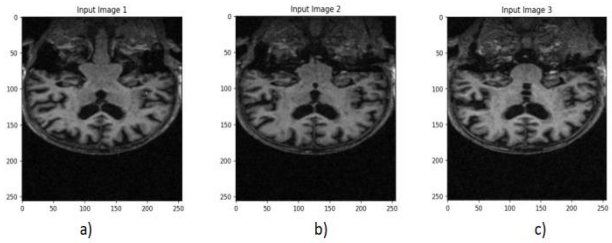

Fig 5: Input images taken for encryption.

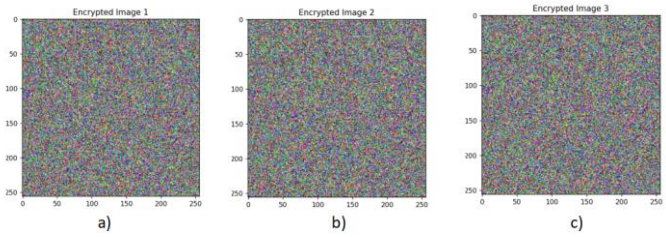

Fig 6: Encrypted images using chaotic map and scrambling.

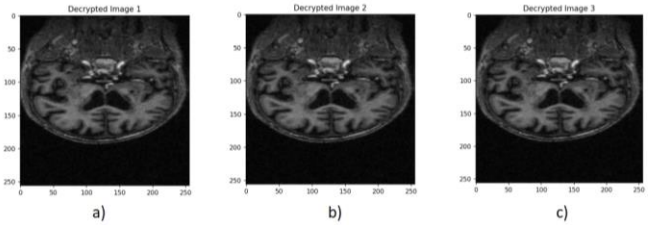

Fig 7: Decrypted images by reversing the process of encryption.

Figure 5 Input images at the start of an encrypted communication technique. Panel a) first input image, panel b) second input image, and panel c) third input image, all set up for encryption followed by decryption at the transmitting end to ensure security of the information during transmission. **Figure 6** depicts the encrypted photos obtained from the encryption procedure. Pixel shuffling is used to conceal the original image structure before encryption. A logistic map function generates chaotic numbers, which serve as cryptographic keys. Each pixel value is XOR encrypted with these chaotic numbers to create encrypted versions of the images. The first, second, and third

encrypted photographs are presented sequentially, demonstrating how encryption can be used effectively to protect image content. **Figure 7** depicts the decrypted images at the receiver's end, following parameter verification on both ends. Panels a, b, and c show the first, second, and third decrypted images, respectively. These images are obtained after authentication of the identical settings on both sides, thereby ensuring the decryption process to be sound and secure. Encryption and decryption techniques play a very important role in safe data transfer of confidential information, such as medical images and secret documents. The technique uses chaotic mapping and XOR encryption, for example, to prevent interception and unauthorized access during communication over possibly insecure communication lines. However, parameter validation at the transmitter and receiver ends is strong enough to ensure that images transmitted are valid and well in integrity besides providing secrecy and reliability in digital communication.

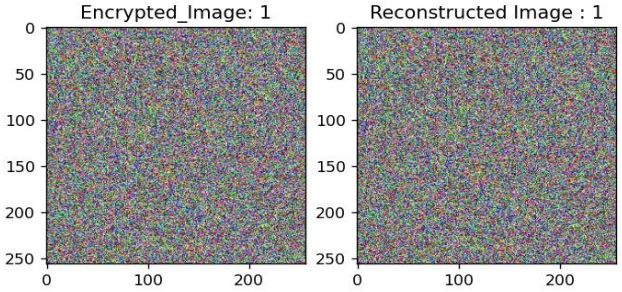

Fig 8: Reconstructed first image using neural network.

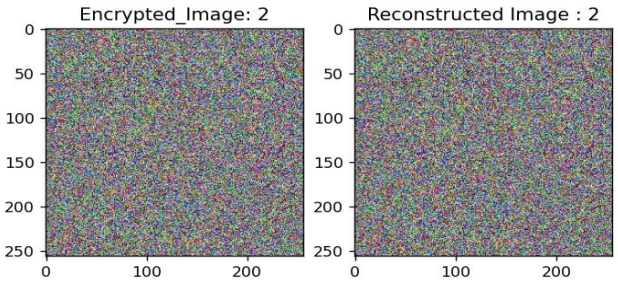

Fig 9: Reconstructed second image using neural network.

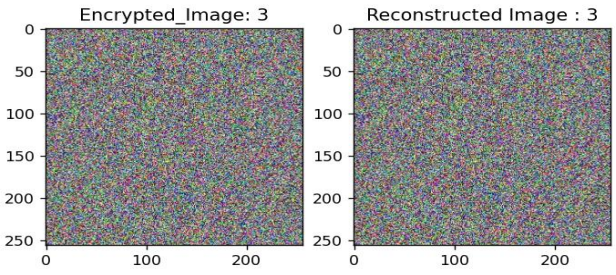

Fig 10: Reconstructed third image using neural network.

Figures 8, 9, and **10** show the reconstructed images for the encrypted versions of the first, second, and third photographs, respectively. These figures depict the successful decryption process, in which encrypted images are restored to their original form following transmission. It is evident in Table 1 that five test images are used to evaluate the PSNR, MSE, and CC values of the reconstructed images. These are measures that compare the quality and fidelity of reconstruction images to their encrypted images. Higher PSNR values imply higher image quality, lower MSE values show greater image similarity, and higher CC values denote a stronger linear relationship between encrypted and reconstructed images, which is critical for assessing the success of the encryption-decryption process. **Table 1:** Showing the parametric evaluation of 5 different test images.

Image	PSNR	MSE	Correlation Coefficient
Image 1	18.60	90.71	0.81
Image 2	19.07	89.85	0.83

Image 3	20.00	84.75	0.87
Image 4	19.82	85.91	0.86
Image 5	19.77	86.57	0.86

Figure 11 depicts the relationship between the loss and the number of epochs used during neural network training. As indicated, the loss function gradually reduces as the number of epochs grows. This pattern illustrates that the model learns and refines its parameters with each successive epoch, resulting in better performance and fewer errors. As a result, as the model progresses through epochs, the reconstructed image becomes clearer and more accurate. This happens because, with each epoch, the model modifies its weights using the back-propagation algorithm, lowering the difference between the projected output and the actual target. Initially, the loss is rapidly reduced as the model learns the basic patterns in the data. The rate of loss decrease slows during succeeding epochs, indicating that the model's parameters are being fine-tuned to capture more intricate data. Thus, watching the loss curve aids in selecting the best number of epochs to obtain a high-quality reconstructed image while preserving generalization.

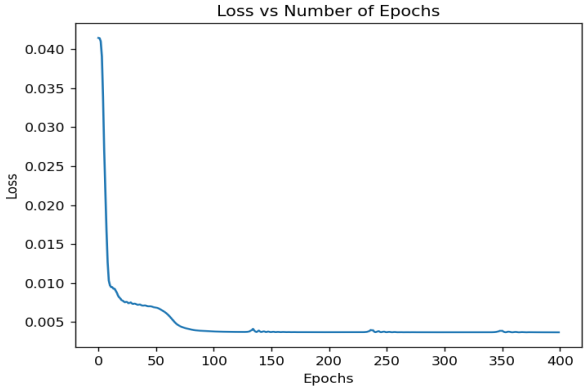

Fig 11: Graph between loss and number of epochs.

Conflicts of Interest: The authors declare that they have no conflict of interest

DISCUSSION

Concerning picture security, integrating deep learning and encryption provides a strong technique to safeguard confidential data, particularly patient information that is critical for medical diagnosis. The procedure starts with encrypting images with pixel scrambling and chaotic functions like the logistic map. These approaches incorporate randomization into the picture, rendering it illegible to unauthorised users unless they possess the decryption key. A neural network is then used to reconstruct the images. This neural network is made up of dense layers that use the ReLU activation function. This is accomplished through training on encrypted data in the form of images, in which the network learns to decode the patterns back into their initial state. This means that only the rightful owners of the decryption key may restore and correctly interpret these photographs. To ensure the accuracy of the above-mentioned reconstruction method above parameter are used. These measurements reflect how precisely the reconstructed images mimic the real ones, which is used to determine correctness during the encryption and decryption operations. Once the metrics have suggested a certain level of similarity between the original and reconstructed images, decryption is done to bring the images back to their original state for the patient's diagnosis. The average PSNR, MSE & CC values are found to be 19.4565263828188, 87.56405741373698 & 0.8524252964031132 respectively. The encryption process could be more secure in further research so that it can't be decrypt easily in the transmission process by the unauthorised person. Further face authentication can be added to the receiver end to confirm the doctor's identity for diagnosis purposes to make the process confidential between the patient and the healthcare provider, so that other third parties cannot access the patient information or pictures to maintain the confidentiality of the healthcare data. This neural network check can be integrated into further research to check the parametric evaluation of the images.

REFRENCES

[1] Seethalakshmi, K.S., Usha, B.A. and Sangeetha, K.N., 2016, October. Security enhancement in image steganography using neural networks and visual cryptography. In 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) (pp. 396-403). IEEE.
[2] Chandrasekaran, J. and Thiruvengadam, S.J., 2017. A hybrid chaotic and number theoretic approach for securing DICOM images. Security and Communication Networks, 2017(1), p.6729896.
[3] Cai, S., Huang, L., Chen, X. and Xiong, X., 2018. A symmetric plaintext-related color image encryption system based on bit permutation. Entropy, 20(4), p.282.
[4] Coutinho, M., de Oliveira Albuquerque, R., Borges, F., Garcia Villalba, L.J. and Kim, T.H., 2018. Learning perfectly secure cryptography to protect communications with adversarial neural cryptography. Sensors, 18(5), p.1306.
[5] Hua, Z., Yi, S. and Zhou, Y., 2018. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Processing, 144, pp.134-144.
[6] Kalsi, S., Kaur, H. and Chang, V., 2018. DNA cryptography and deep learning using genetic algorithm with NW algorithm for key generation. Journal of medical systems, 42, pp.1-12.
[7] Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A.K., Yang, P., Huang, H. and Hou, G., 2018. Secure and robust fragile watermarking scheme for medical images. IEEE access, 6, pp.10269-10278.
[8] Tai, W.L. and Chang, Y.F., 2018. Separable reversible data hiding in encrypted signals with public key cryptography. Symmetry, 10(1), p.23.
[9] Chai, X., Gan, Z., Yuan, K., Chen, Y. and Liu, X., 2019. A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Computing and Applications, 31, pp.219-237.
[10] Chowdhary, C.L., Patel, P.V., Kathrotia, K.J., Attique, M., Perumal, K. and Ijaz, M.F., 2020. Analytical study of hybrid techniques for image encryption and decryption. Sensors, 20(18), p.5162.
[11] Salem, N. and Elnaggar, F., 2020, October. RIFD fibonacci zeckendorf hybrid encoding and decoding algorithm for medical image compression and reconstruction. In 2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA) (pp. 66-73). IEEE.
[12] Wang, Y., Li, Y. and Lu, X.N., 2020, September. Evaluation criteria for visual cryptography schemes via neural networks. In 2020 International Conference on Cyberworlds (CW) (pp. 289-292). IEEE.
[13] Priyadharshini, A., Umamaheswari, R., Jayapandian, N. and Priyananci, S., 2021, February. Securing medical images using encryption and LSB steganography. In 2021 international conference on advances in electrical, computing, communication and sustainable technologies (ICAECT) (pp. 1-5). IEEE.
[14] Wen, H., Zhang, C., Huang, L., Ke, J. and Xiong, D., 2021. Security analysis of a color image encryption algorithm using a fractional-order chaos. Entropy, 23(2), p.258.
[15] Zakaria, L., Yuliani, E. and Asmiati, A., 2021. A two-dimensional mKdV linear map and its application in digital image cryptography. Algorithms, 14(4), p.124.
[16] Zhang, R., Yu, L., Jiang, D., Ding, W., Song, J., He, K. and Ding, Q., 2021. A novel plaintext-related color image encryption scheme based on cellular neural network and Chen's chaotic system. Symmetry, 13(3), p.393.
[17] Lawnik, M., Moysis, L. and Volos, C., 2022. Chaos-based cryptography: Text encryption using image algorithms. Electronics, 11(19), p.3156.
[18] Padinjappurathu Gopalan, S., Chowdhary, C.L., Iwendi, C., Farid, M.A. and Ramasamy, L.K., 2022. An efficient and privacy-preserving scheme for disease prediction in modern healthcare systems. Sensors, 22(15), p.5574.
[19] Alsafyani, M., Alhomayani, F., Alsuwat, H. and Alsuwat, E., 2023. Face image encryption based on feature with optimization using secure crypto general adversarial neural network and optical chaotic map. Sensors, 23(3), p.1415.
[20] Ibrahim, D., Sihwail, R., Arrifin, K.A.Z., Abuthawabeh, A. and Mizher, M., 2023. A novel color visual cryptography approach based on Harris Hawks Optimization Algorithm. Symmetry, 15(7), p.1305.
[21] Kusum, L. and Cenkeramaddi, L.R., 2023. Deep Learning for Medical Image Cryptography: A Comprehensive Review.
[22] Nazir, S. and Kaleem, M., 2023. Federated learning for medical image analysis with deep neural networks. Diagnostics, 13(9), p.1532.
[23] Nitaj, A. and Rachidi, T., 2023. Applications of neural network-based AI in cryptography. Cryptography, 7(3), p.39.

[24] Palanisamy, P., Urooj, S., Arunachalam, R. and Lay-Ekuakille, A., 2023. A Novel Prognostic Model Using Chaotic CNN with Hybridized Spoofing for Enhancing Diagnostic Accuracy in Epileptic Seizure Prediction. Diagnostics, 13(21), p.3382.

[25] Gayathri, S. and Gowri, S., 2023. Securing medical image privacy in cloud using deep learning network. Journal of Cloud Computing, 12(1), p.40.

[26] Cui, G., Zhou, X., Wang, H., Hao, W., Zhou, A. and Ma, J., 2024. Optical Color Image Encryption Algorithm Based on Two-Dimensional Quantum Walking. Electronics, 13(11), p.2026.

[27] Lin, Y.R. and Juan, J.S.T., 2024. RG-Based Region Incrementing Visual Cryptography with Abilities of OR and XOR Decryption. Symmetry, 16(2), p.153.

[28] Oladipupo, E.T., Abikoye, O.C. and Awotunde, J.B., 2024. A Lightweight Image Cryptosystem for Cloud-Assisted Internet of Things. Applied Sciences, 14(7), p.2808.

[29] Panigrahy, A.K., Maniyath, S.R., Sathiyanarayanan, M., Dholvan, M., Ramaswamy, T., Hanumanthakari, S., Vignesh, N.A., Kanithan, S. and Swain, R., 2024. A faster and robust artificial neural network based image encryption technique with improved ssim. IEEE Access.

[30] Tamba, V.K., Biamou, A.L.M., Pham, V.T. and Grassi, G., 2024. Multistable Memristor Synapse-Based Coupled Bi-Hopfield Neuron Model: Dynamic Analysis, Microcontroller Implementation and Image Encryption. Electronics, 13(12), p.2414.

[31] Chhabra, M., Sharan, B., Elbarachi, M. and Kumar, M., 2024. Intelligent waste classification approach based on improved multi-layered convolutional neural network. Multimedia Tools and Applications, pp.1-26.