Intelligent Automation & Soft Computing

Tech Science Press

DOI: 10.32604/iasc.2023.038243
Article

DeepGan-Privacy Preserving of HealthCare System Using DL

Sultan Mesfer Aldossary*

Prince Sattam Bin Abdulaziz University, Wadi Ad Dawaser, 11990, Saudi Arabia
*Corresponding Author: Sultan Mesfer Aldossary. Email: s.aldossary@psau.edu.sa

Received: 03 December 2022; Accepted: 17 April 2023; Published: 23 June 2023

Abstract: The challenge of encrypting sensitive information of a medical image in a healthcare system is still one that requires a high level of computing complexity, despite the ongoing development of cryptography. After looking through the previous research, it has become clear that the security issues still need to be looked into further because there is room for expansion in the research field. Recently, neural networks have emerged as a cost-effective and effective optimization strategy in terms of providing security for images. This revelation came about as a result of current developments. Nevertheless, such an implementation is a technique that is expensive to compute and does not handle the huge variety of different assaults that may be made on pictures. The primary objective of the system that has been described is to provide evidence of a complex framework in which deep neural networks have been applied to improve the efficiency of basic encryption techniques. Our research has led to the development and proposal of an enhanced version of methods that have previously been used to encrypt pictures. Instead, the generative adversarial network (GAN), commonly known as GAN, will serve as the learning network that generates the private key. The transformation domain, which reflects the one-of-a-kind fashion of the private key that is to be formed, is also meant to lead the learning network in the process of actually accomplishing the private key creation procedure. This scheme may be utilized to train an excellent Deep Neural Networks (DNN) model while instantaneously maintaining the confidentiality of training medical images. It was tested by the proposed approach DeepGAN on open-source medical datasets, and three sets of data: The Ultrasonic Brachial Plexus, the Montgomery County Chest X-ray, and the BraTS18. The findings indicate that it is successful in maintaining both performance and privacy, and the findings of the assessment and the findings of the security investigation suggest that the development of suitable generation technologies is capable of generating private keys with a high level of security.

Keywords: Healthcare; cryptography; deep learning; adversarial network; privacy

1 Introduction

One of the key resources that must be effectively protected for every business is data. When data are stored, transferred, and processed through any kind of network system, there is cause for concern over the protection of the data. There have been a great number of algorithms that are used for data security nowadays; nevertheless, each one has its own unique set of possible uses, benefits, and disadvantages. The implementation of data security measures depends on the kinds and structures of the data, as well as on whether they are used in centralized or decentralized systems. Recent years have seen a significant increase in the use of Wireless Communication and the implementations that use it for many enterprise applications hosted on decentralized internet infrastructures. In recent years, the business has witnessed an increase in wireless technologies and the applications that make use of them. The increase in data computation, information sharing, configurability, and interface capabilities of the network as well as those of the applications themselves can be seen in respect of data computation, information sharing, configurability, and interface capabilities. As a result of these technological advances as well as advances in broadband connections, unlicensed spectrum, and electromagnetic spectrum identification, IoT has been able to establish a strong foundation. In 1999, the concept of the Internet of Things was introduced, and it was initially discussed in the context of supply chain management. It presents a new world in which all objects are interconnected via the internet [1]. Considering the significant progress made in the IoT [2], smart objects have become a common type of device that can be used for a variety of inventive, intelligent, and novel applications. Some of these applications include smart agriculture, smart cities, smart healthcare, crowdsourcing, and crowd sensing. It is now possible, with the use of technologies such as artificial intelligence, network technology, and smart sensors, to successfully manage healthcare by interacting with one another and exchanging information with one another. Other applications of IoT include access control, intelligent identification, and data processing. The establishment of this arrangement sets the way for a healthcare system that is bolstered in terms of its safety, effectiveness, and real-time capabilities. Various security measures are in place to help assist in fighting attacks on images, but they aren't entirely successful in balancing security requirements with requirements for image quality. Most recently, it was discovered that deep neural networks performed better even when unstructured data was present, with total independence from data labeling. In addition to this, the unpredictability of the chaotic graph's behavior also offers a substantial level of safety. Therefore, combining chaotic behavior with deep learning can provide a more effective encryption solution for ages. Because DNN models are getting more complicated in architectural designs to improve their routine, more computational possessions are required to train such models.

One of the most important ways to provide a lot of computational power for those complex DNN models to be trained is through the use of a cloud server. Because anyone with access to the server can alter any image that has been delivered to it, the cloud server itself is only deemed to be somewhat honest. In contrast to other datasets, transferring medical data is therefore extremely difficult and complex. Because of this circumstance, we feel compelled to devise a solution to this problem, which would be a method by which data could be sent to a cloud server for the training of models while still preserving the confidentiality of the data. Because of issues like these, researchers came up with the idea of "trainable image encrypting," which seeks to develop a cryptography approach that enables deep neural network models to directly learn from encrypted images without first needing to decrypt them. Authors [3–5] have recently introduced state-of-the-art encryption algorithms for privacy-preserving deep learning. These techniques are dubbed the Tanaka scheme and the Sirichotedumrong Kinoshita, and Kiya (SKK) scheme, respectively. Tanaka's scheme and SKK's scheme, both of which may be utilized in medical research that makes use of DNNs, are given their names and are known, respectively, as the Tanaka scheme and the SKK system.

As a result, the work that was proposed presents a model that makes use of deep learning and chaotic maps to carry out better optimization in the interest of enhancing the encryption performance of a medical image. In the present study, deep neural networks were applied to improve the efficiency of basic encryption techniques to provide evidence of a complex framework for implementing deep neural networks. Through our research, we have developed and proposed an enhanced version of methods previously used to encrypt pictures. In place of this, the generative adversarial network (GAN), also known as GAN, will be used as the learning network that generates the private key. In addition to reflecting the one-of-a-kind style of the private key to be formed, the transformation domain also serves to guide the learning network in developing the private key. An excellent Deep Neural Network (DNN) model may be developed by using this scheme while maintaining the instantaneous confidentiality of the medical images being used for training. The proposed DeepGAN approach was tested on open-source medical datasets and three sets of data: the Ultrasonic Brachial Plexus, the Montgomery County Chest X-ray, and the BraTS18.

The remaining sections are arranged as follows: Along with a discussion of research issues and a solution in Section 3, Section 2 reviews the existing literature and the various strategies for encryption systems utilized in picture transmission lines. In Section 4, we will discuss the experimental setup and the dataset, and in Section 5, we will discuss the analysis of the results. The functionality of prior models is analyzed in Section 6, which you may see here. In Section 7, the article is concluded. The work's future scope is also discussed.

2 Literature Review

This section provides a summary of the previous research that is relevant to our study. Previous research on medical image encryption, machine learning applicable to the area of medicine, and trainable picture encryption served as our primary sources of information for this work. These investigations were carried out in several subspecialties within the medical profession. Wang et al. [6] used classical machine learning on the dataset provided by the Tumor Hospital of Liaoning Province to successfully identify malignancy in mammography. The dataset was obtained from the Liaoning Province Tumor Hospital. The two approaches to Machine learning that are put into practice are the standard support vector machine, as well as the single-layered neural network. Even though this research did not make use of an Algorithms technique, it did pave the way for the idea of employing deep learning models to conduct autonomous mammograms. Image encryption has been researched extensively, which has led to the development of a wide variety of potential methods [7–10]. An innovative method for the encryption of medical metaphors has been suggested by Lima et al. [7]. This method is based on the cosine number transform, which just requires modular arithmetic to operate. This attribute prevents errors caused by rounding off and makes it possible for the image to be retrieved after the encryption and decryption process in a manner that is identical to the image that corresponds to the original. The system that has been proposed is adaptable and may be used with images that comply with the Digital Imaging and Communications in Medicine (DICOM) standard. This standard is commonly utilized in applications that are related to medicine. For multi-frame DICOM medical images, Natsheh et al. [8] suggest a straightforward and efficient encryption method. Using the Advanced Encryption Standard can shorten the time used to scramble and decrypt these photos (AES). Because the Blowfish Algorithm is quicker and the least significant bit (LSB) approach is utilized for picture concealment, Mukhedkar et al. [9] demonstrate shows how image encryption can be accomplished.

A method for medical image encryption founded on a grouping of messy neural networks was introduced by Dridi et al. [11]. The major goal of the suggested solution is to protect medical photographs using a less complicated algorithm than the ones now used. The results of the experiments validated the performance and efficacy of the suggested approach, and it is to the requirements of both the Electronic Image database and the Publications in Medicine. The work of Gilad-Bachrach et al. [12] has a practical machine learning methodology for a delinquent involving medical, financial, or other sorts of delicate data, which not solitary calls for precise prophecies but also close consideration of upholding data privacy and security. This makes it possible for a sender to send their data securely to the network's cloud service. Encryption assures that the data will remain confidential because the cloud provider does not have access to the keys that are necessary to decipher the information. A similar idea was presented by Hu et al. [13] for the encryption of batches of images by using created feature representations that were encoded using stacked auto-encoder networks. To learn a mapping from input photos to output images, Yi et al. [14] employ a probabilistic generative adversarial network. It has been shown that this technique can effectively colorize photos, rebuild objects from edge maps, and create synthetic photographs from label maps. According to DualGAN [15] method allows for the training of an image interpreter with two independent sets of unlabeled pictures. By learning two reliable image translators from one domain to the other from two sets of unlabeled input photographs at the same time, DualGAN can effectively perform a broad range of picture translation tasks. Zhu et al. [16] created the CycleGAN framework for translating pictures using unpaired training data. It concurrently trains two sets of GAN models that map from class A to class B and back again to achieve this.

The combined mapping, which places all the pictures in the same class, serves as the foundation for the loss formula. The effectiveness of GANs depends on the perception of an adversarial loss, which makes it possible to distinguish produced pictures from target images. Adversarial loss is used to determine how to convert the source photos to the given dataset pictures, which refers to picture translation. A branch of deep learning called the Generative Adversarial Network, or GAN [17], was developed. The main parts of a GAN algorithm are typically the generator and the discriminator. The discriminator must decide if the input is real data or a made-up sample, and the generator must record the dispersion of the data sample. Numerous GAN-based algorithms have been created for a variety of applications since the ground-breaking work that was done by [17,18].

3 Proposed Method DeepGAN

Goodfellow and his colleagues have developed a method that uses adversarial neural networks to protect data from other neural models. This method lies between anonymization techniques and homomorphic encryption. A, B, and E were the three parties involved in the GAN cryptography setup. E usually wants to eavesdrop on A and B's conversations, while A and B typically want to communicate safely. Thus, secrecy (rather than integrity) is the desired security attribute, and the adversary is a "passive attacker" with only a very restricted set of capabilities aside from the ability to intercept communications. A wants to send B a single, private message (P) in the scenario shown above. A receives the message P. This input is processed by A, and output C is created. "P" stands for "plaintext" and "C" for "ciphertext," respectively. B and E both get C, digest it, and try to get back P. Let's use PB and PE to symbolize these computations, respectively. With a shared secret key K, person A, and person B have an edge against E. As an additional input to A and B, that secret Key [K] is employed. Fig. 1, shows the encryption model incorporated in the proposed model.

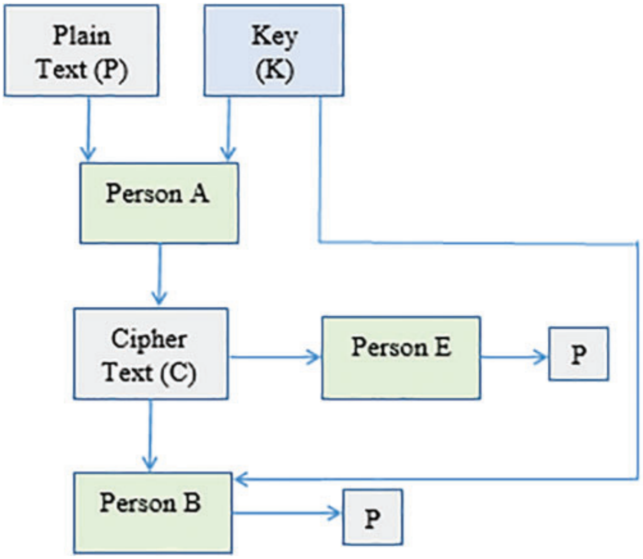


Figure 1: The encryption model used in the proposed solution

The following goals of the participants are stated informally. Simple reconstruction of P is E's objective (in other words, to minimize the error between P and PE). The goal of A and B's conversation is to be as explicit as possible (to reduce the chance of a mistake between P and PB), while also keeping E from overhearing it. B and A were collaboratively trained to effectively interact while discovering E's weaknesses using generative adversarial network techniques. The real kicker is that neither A nor B has any preconceived ideas about the strategies that En will employ, let alone the cryptography algorithms that they will utilize to achieve their aim. A and B receive training to overcome the best E rather than a fixed E, by technique of the GAN principles. The outcomes of the GAN studies in cryptography were astounding. B and E start to be able to piece together the original message after about 8000 training steps, as shown in Fig. 2. The A and B networks appear to grasp this at 10,000 training steps in, and E's mistake rate starts to increase once more. To put it another way, B was able to take what he had learned from E's actions and safeguard the communication while still enhancing its effectiveness.

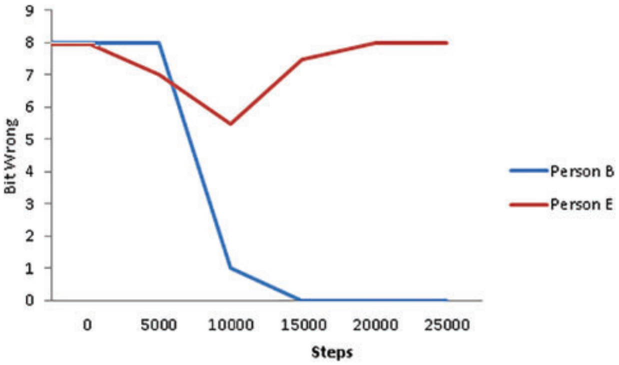


Figure 2: Errors in image encryption caused by uncertainty that result in a high mistake rate

The discriminator and the generator make up the generating countermeasure network. The generator tries to produce a randomly produced output (such as a facial image, a digital image, etc.), while the discriminator tries to tell the output apart from the actual sample. The two models are trained using the Dropout and Back Propagation algorithms. It is anticipated that while the two networks compete with one another, the network will continue to optimize, improving the output and eventually creating a generator network that can create realistic output as shown in Fig. 3.

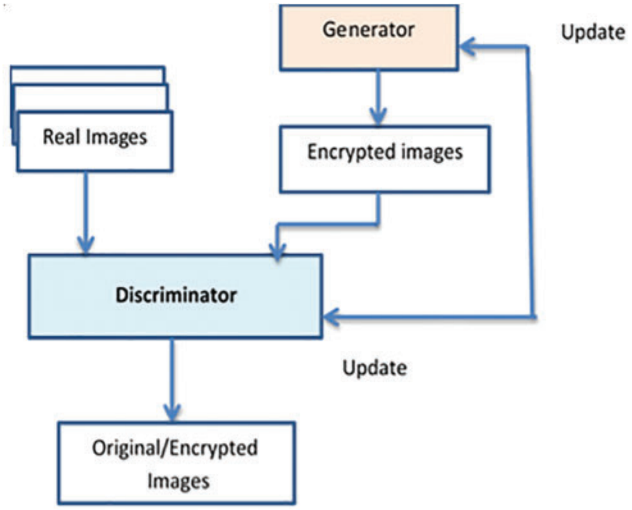


Figure 3: The flow chart of the proposed GAN model for image encryption

Utilizing leaky ReLU like an activation function in the hidden layers and sigmoid in the final layer, we employ a few Dense, Flattened, and Dropout layers. Because the discriminator's task is to do binary classification, as illustrated in Fig. 4, Adam is employed as an optimizer, and binary cross-entropy is utilized as just a loss function. The following benefits are now available to our network as a result of our participation in the Dense Block: The Dense Block increases feature reuse and reduces the model size by enabling the learned feature map to be received by all succeeding layers. The images that are produced as a result of this have a higher image-generating quality and greater generality. This is one of the advantages of this. In a word, the Dense block describes a situation where each layer's input originates from the output of all earlier layers.

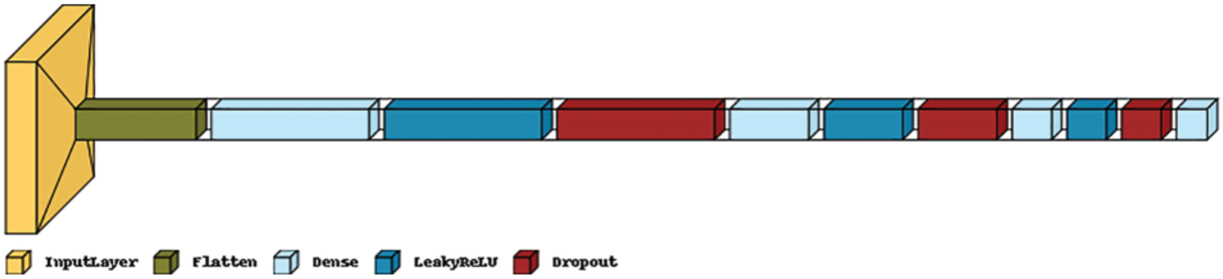


Figure 4: A GAN's discriminator is a classifier that is used to distinguish real data from those generated by the generator

The Dense block also has the advantage of lowering the number of parameters, which results in a more compact network. As opposed to other networks' hundreds or thousands of widths, the Dense block's output feature maps for each convolution layer are few (less than 100). The simultaneous impact of this connection is to make the transfer of features and gradients more efficient, as well as to make it simpler to train the network. When a network is deeper, there is a greater possibility that the gradient disappearance problem will arise. The reason is that gradient and input data are exchanged through numerous levels. This dense connection now equates to each layer directly connecting input and loss, alleviating the gradient disappearance phenomenon and making the deeper network unproblematic.

To train the generator, it first creates latent points and then creates labels that are equal to 1 to trick the discriminator. The function then reports the model's performance after a few steps. Table 1, depicts the generator of the GAN. The Leaky ReLUs, are activation functions that are based on ReLUs but have a modest slope for negative values as opposed to a flat slope. It is not learned during training; rather, the slope coefficient is chosen before training. This kind of activation function is common in situations where sparse gradients may be an issue, such as when training generative adversarial networks.

Table 1: Discriminator setup

Layer (Type)	Output shape	Param#
input_7 (InputLayer)	[(None, 100)]	0
dense_17 (dense)	(None, 256)	25856
leaky_re_lu_6 (LeakyRLU)	(None, 256)	0
dense_18	(None, 512)	131584
leaky_re_lu_7 (LeakyRLU)	(None, 512)	0
dense_19 (dense)	(None, 1024)	525312
leaky_re_lu_8 (LeakyRLU)	(None, 512)	0
dense_20 (dense)	(None, 1024)	803600
reshape (Reshape)	(None, 256)	0

Note: Total Param = 1486352, Trainable param 1,486352, Non trainable Param = 0.

Generally speaking, deeper neural network architectures can increase the system's capacity for learning. The complexity and length of training will also rise with an increase in the number of layers, though, and occasionally there is little to no obvious improvement in the model's optimization as a result of layer addition. This paper suitably designs the DeepGAN network structures based on trials. Consequently, the system will operate more efficiently and training will be consistent and timely. Fig. 5, lists the parameters that match the network structure.

$$f\,(k) = \{\; k\;\; k > 0\;\; ak\;\; k \leq 0\; \} \tag{1}$$

Leaky ReLUs is one attempt to address the issue of "dying ReLUs" by having a slight negative slope (of 0.01, or so).

4 Experiments

There are often 2 types and two outputs in picture steganography techniques. The datasets that are employed are typically vast as well. A powerful graphics card and GPU-based PC are required for the training and testing. The trained model can then be used in a standalone computer or CPU for deployment. All experiments were conducted using Python 3.5 and later versions, as well as Pytorch.

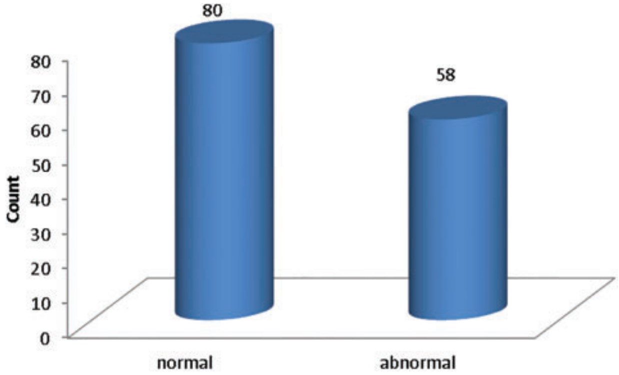


Figure 5: Data distribution of Montgomery county chest x-ray

On open-source medical datasets, including the Ultrasonic Brachial Plexus, the Montgomery County Chest X-ray, and the BraTS18, we tested our suggested technique DeepGAN. The assessment findings and security analysis show that the proposed key generation network can create private keys with a high degree of security. The results are expected to show that it is successful in maintaining performance and privacy. This collection of 138 posterior-anterior radiographs includes 80 normal images and 58 images that are abnormal and show signs of tuberculosis as revealed in the figure. Every image is de-identified and offered in DICOM format. The package includes effusions and military patterns among the many abnormalities it covers. Fig. 5 shows the data distribution of normal and abnormal data in the dataset. Fig. 6 shows the sample x-ray images from the Montgomery county chest x-ray dataset. The X-ray pictures that are counted in this data set were obtained from the tuberculosis control program.

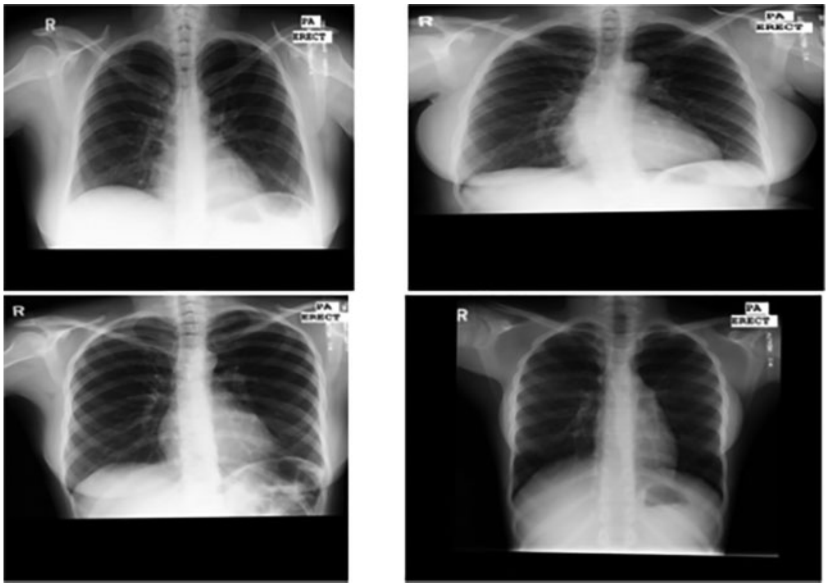


Figure 6: Montgomery county chest x-ray samples

The dataset BraTS 2018 provides heterogeneous 3D brain MRIs with documented tumor segmentations for each unique patient, each of whom has four distinct MRI scans. The necrotic and non-enhancing tumor core, the enhancing tumor, and the peritumoral edema are the three distinct sub regions of the tumor that are described in the annotations. Combining the annotations produced three different types of tumors: the whole tumor, the tumor core, and the enhancing tumor. The information came from 19 universities and was collected using a variety of MRI scanners. The example photos from the BraTS18 dataset are displayed in Fig. 7.

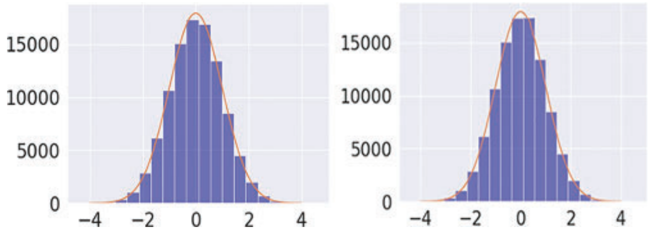


Figure 7: Key distribution

When optimizing DeepGAN during training, we utilize the Adam optimizer, and the learning rate (LR) is set to 0.0001 as exposed in Table 2. The Beta value is set as 0.9 and 0.999. The Epsilon value is chosen as 1e-08 and the weight decay is 0.

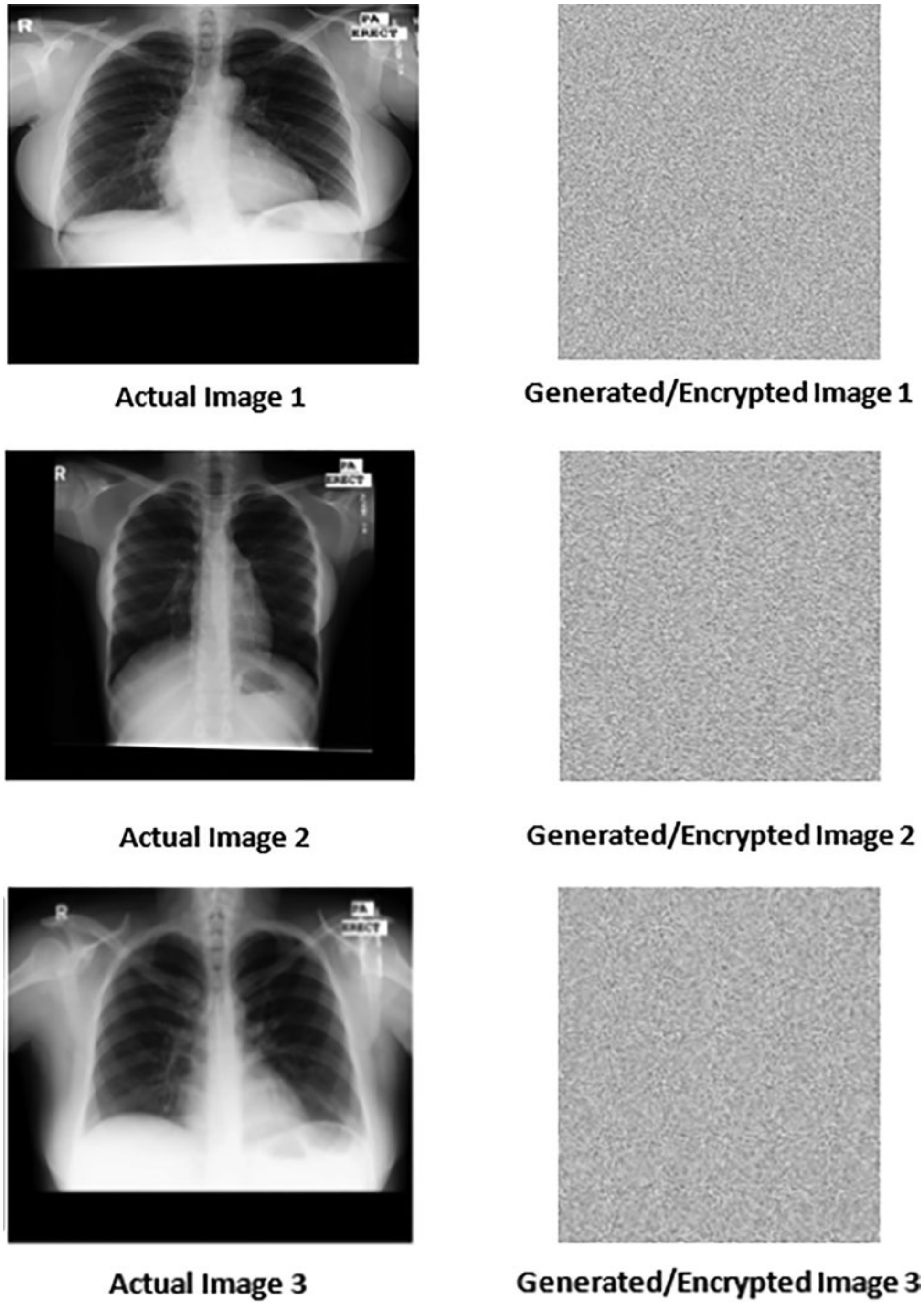
Table 2: Parameter fine-tuning

Parameter	Value
Optimizer	Adam
Betas	0.9 and 0.9999
Epsilon	1e-08
Learning rate	0.0001
Weight-decay	0

5 Result and Discussion

This section uses simulation experiments to demonstrate the proposed DeepGAN-based symmetric encryption communication system's capacity for encrypted transmission of messages of any length and generality. The findings reveal that DeepGAN is extremely adaptable and trustworthy in producing keys when used to generate different types of keys, as illustrated in Fig. 7. It is likely that GAN cryptography will play a pivotal role in mainstream AI applications. By using GAN cryptography, datasets can theoretically be shared with data scientists without revealing sensitive information. In addition, neural models can be applied to GAN-encrypted data without fully decrypting it.

When evaluating the safety and sturdiness of various systems, precision or bit accuracy is the parameter that is most frequently utilized. Accuracy in steganography is measured by how well a suggested method can determine if a picture contains steganography. This is referred to as “accurate identification.” Four terms are used to calculate accuracy: False Positive (FP), True Positive (TP), and True Negative (TN), False Negative (FN). The model's accurate positive and negative predictions are referred to as true positive and true negative, respectively, while the inaccuracies in the model's predictions are referred to as false positive and false negative. Fig. 8 shows the encrypted images generated from the original medical image.



Actual Image 1

Generated/Encrypted Image 1

Actual Image 2

Generated/Encrypted Image 2

Actual Image 3

Generated/Encrypted Image 3

Figure 8: Encrypted images

The number of accurate predictions the model has made across all classes are used to determine accuracy. Although correctness is a straightforward and widely used metric, it is not a suitable one when the data is unbalanced. That means the price for false positives and false negatives is the same. The performance of the model is properly assessed using assessment metrics other than accuracy.

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \tag{2}$$

When adopting a superior steganography approach, a lower steganography accuracy value equates to more security. How successfully the utilized steganalysis model was tested is described using a new word called the detection rate. Thus, the confidentiality of the suggested approach is assessed. Findings demonstrate that encrypted pictures may preserve the privacy of patients in medical imaging while being completely distinct from the original medical image. To complete the decryption process, the ciphertext picture can also be changed back to its original state. The experimental results demonstrate that the suggested DeepGAN is a reliable key generation method to encrypt and decode medical pictures with high security, which streamlines the process of safeguarding the private information of medical images. The suggested DeepGAN may also be utilized to encrypt multimodality medical pictures from various inspection tools, according to observation. You can see that the plaintext picture and the private key are incompatible. Any plaintext images may be encrypted with the newly acquired private key using a variety of encoding methods. Fig. 9, depicts the loss and the accuracy of the proposed model based on the medical image dataset.

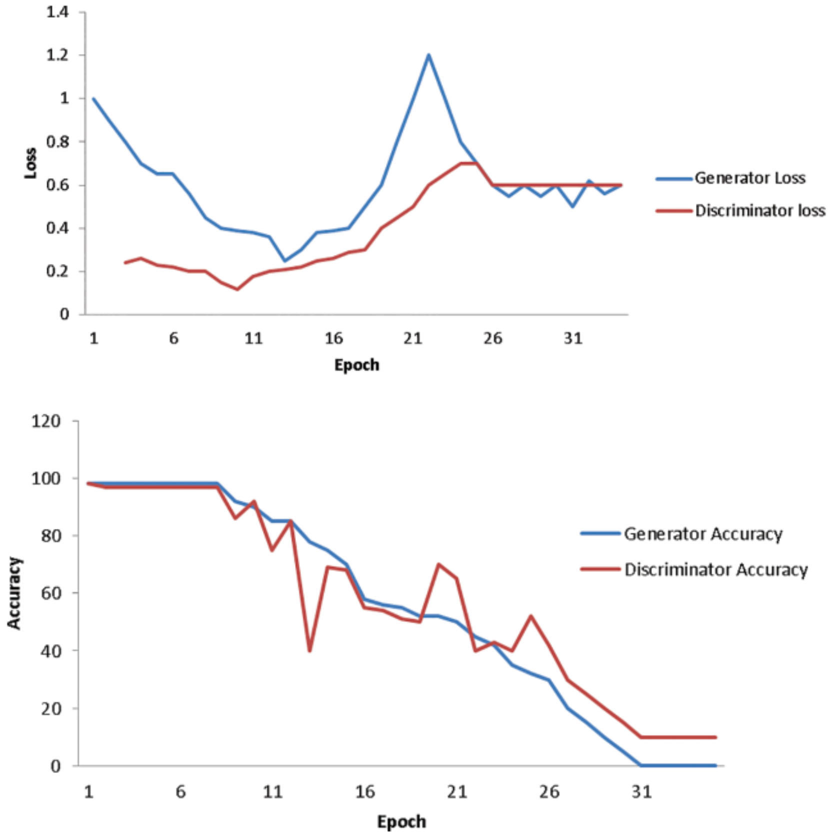


Figure 9: Model loss and accuracy

Fig. 9, shows the processing speed of the encryption operations and decryption operations on medical images of various resolutions is assessed to gauge the effectiveness of the suggested network. The proposed model architecture can encode or decrypt 16.18 medical images per second for 256 × 256 resolution, but only 4.23 medical images per second for 512 × 512 resolution. The efficiency requirements in clinical practice can essentially be met by this encryption/decryption speed.

6 Comparison

A comparison of the various steg-analysis algorithms' accuracy for stego images created by widely used techniques is depicted in Table 3. The model proposed by Qiu et al. produced an accuracy of 95% and the 94% accuracy was achieved by the Li et al. This article presents a method for generating intricate texture-like images of any size by exploiting the generative network, using a modified deep convolutional generative adversarial network (DeepGAN). It then demonstrates that it is possible to add a second image to the created texture while retaining a degree of visual similarity that is virtually undetectable to the human eye, as shown in Table 3.

Table 3: Parameter fine-tuning

Model	Accuracy (%)
Qiu et al. [4]	95
Shi et al. [5]	50
Zhu [6]	72
Ke [18]	94
Zhang [19]	50
Liu [20]	50
Arjovsky [21]	59
Li et al. [22]	94

7 Conclusion and Future Work

The learning network for encrypting and decrypting the medical picture will be the Deep-GAN network. To make the procedure easier, this choice was selected. The learning model is oriented toward the target domain to execute the encryption procedure. By using the reconstruction network to decrypt the encrypted picture, the original image may be seen (plaintext). Our analysis of chest X-ray datasets shows that the proposed technique can encrypt/decrypt medical pictures more quickly than other comparable state-of-the-art methods while still providing high-level security protection. This was proved by our capacity to secure medical picture data to a high degree. To further improve DeepGAN's performance, researchers plan to focus their attention shortly on the development of portable deep learning networks similar to MobileNet and Xception. To evaluate DeepGAN's generalizability, we plan to test not only its accuracy but also its safety and how well it performs in a variety of application settings. In addition to this, we will release the source code for our prototype as well as other relevant information (such as software). Research on GAN-based steganography is something we plan to keep up with in a couple of different ways. To begin, it is currently unknown what the architecture for adversarial training will entail. Within the context of GAN networks, we will investigate the interaction that occurs between the generator and the discriminator to increase the performance of our safety framework. Second, the design that is being offered is built over space.

Funding Statement: The author received no specific funding for this study.

Conflicts of Interest: The author declare that they have no conflicts of interest to report regarding the present study.

References

[1] F. Liu, L. Jiao and X. Tang, “Task-oriented GAN for PolSAR image classification and clustering,” *IEEE Transaction on Neural Network. Learning System*, vol. 30, no. 9, pp. 2707–2719, 2019.

[2] H. Hong, X. Li and M. Wang, “GANE: A generative adversarial network embedding,” *IEEE Transaction on Neural Network. Learning System*, vol. 31, no. 7, pp. 2325–2335, 2020.

[3] N. Zheng, J. Ding and T. Chai, “DMGAN: Adversarial learning based decision making for human-level plant-wide operation of process industries under uncertainties,” *Transaction on Neural Network. Learning System*, vol. 32, no. 3, pp. 1–5, 2020.

[4] A. Qiu, X. Chen, X. Sun, S. Wang and W. Guo, “Coverless image steganography method based on feature selection,” *Journal of Information Hiding and Privacy Protection*, vol. 1, no. 2, pp. 49, 2019.

[5] H. Shi, J. Dong, W. Wang, Y. Qian and X. Zhang, “SSGAN: Secure steganography based on generative adversarial networks,” *Multimedia*, vol. 1, no. 1, pp. 534–544, 2017.

[6] Z. Yue, S. Ding, L. Zhao, Y. Zhang, Z. Cao *et al.,* “Privacy-preserving time-series medical images analysis using a hybrid deep learning framework,” *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–21, 2021.

[7] H. A. Abdallah and S. Meshoul, “A multilayered audio signal encryption approach for secure voice communication,” *Electronics*, vol. 12, no. 1, pp. 1–26, 2022.

[8] A. Ihsan and N. Doğan, “Improved affine encryption algorithm for color images using LFSR and XOR encryption,” *Multimedia Tools and Applications*, vol. 1, no. 17, pp. 1–17, 2022.

[9] M. S. Alshehri, S. Almakdi, M. A. Qathrady and J. Ahmad, “Cryptanalysis of 2d-scmci hyperchaotic map based image encryption algorithm,” *Computer Systems Science and Engineering*, vol. 46, no. 2, pp. 2401–2414, 2023.

[10] J. C. Dagadu, J. P. Li and O. A. Emelia, “Medical image encryption based on hybrid chaotic DNA diffusion,” *Wireless Personal Communications*, vol. 108, no. 1, pp. 591–612, 2019.

[11] M. Dridi, M. A. Hajjaji, B. Bouallegue and A. Mtibaa, “Cryptography of medical im-ages based on a combination between a chaotic and neural network,” *IET Image Process*, vol. 10, no. 1, pp. 830–839, 2016.

[12] J. Qin, Z. He, X. Xiang and N. N. Xiong, “Reversible data hiding in encrypted images based on adaptive prediction and labeling,” *Computers, Materials & Continua*, vol. 73, no. 2, pp. 3613–3628, 2022.

[13] F. Hu, J. Wang, X. Xu, C. Pu and T. Peng, “Batch image encryption using generated deep features based on stacked autoencoder network,” *Mathematical Problems in Eng.*, vol. 2017, no. 12, pp. 1–15, 2017.

[14] D. Arroyo, R. Rhouma, G. Alvarez, L. Shujun and F. Veronica, “On the security of a new image encryption scheme based on chaotic map lattices,” *Chao an Interdisciplinary Journal of Nonlinear Science*, vol. 18, no. 1, pp. 1–8, 2008.

[15] Z. Yi, H. Zhang, P. Tan and M. Gong, “DualGAN: Unsupervised dual learning for image-to-image translation,” in *Proc. IEEE ICCV*, Venice, Italy, pp. 2868–2876, 2017.

[16] J. Zhu, T. Park, P. Isola and A. A. Efros, “Unpaired image-to-image translation using cycle-consistent adversarial networks,” in *Proc. IEEE ICCV*, Venice, Italy, pp. 2242–2251, 2017.

[17] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, F. Warde *et al.,* “Generative adversarial networks,” *Communications*, vol. 63, no. 11, pp. 139–144, 2020.

[18] J. Zhu, R. Kaplan, J. Johnson and L. Fei-Fei, “Hidden: Hiding data with deep networks,” in *Proc. ECCV*, Munich, Germany, pp. 201–210, 2016.

[19] Y. Ke, M. Zhang, J. Liu, T. Su and X. Yang, *Generative Steganography with Kerckhoffs' Principle Based on Generative Adversarial Networks*, Henderson, NV, USA: arXiv Press, 2017. [Online]. Available: https://arxiv.org/abs/1711.04916

[20] Z. Zhang, G. Fu, J. Liu and W. Fu, "Generative information hiding method based on adversarial networks," in *Proc. ICCEN*, Shanghai, China, pp. 261–270, 2018.

[21] C. Liu and H. Wechsler, "Gabor feature based classification using the enhanced fisher linear discriminant model for face recognition," *IEEE Transactions on Image Processing*, vol. 11, no. 4, pp. 467–476, 2018.

[22] C. Li, M. Hu, Y. Li, H. Jiang, N. Ge *et al.,* "Analogue signal and image processing with large memristor crossbars," *Nature Electronics*, vol. 1, no. 1, pp. 52–59, 2018.