I.J. Image, Graphics and Signal Processing, **2024, 6, 72-86**
Published Online on December 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2024.06.06

A Novel GAN with DNA Sequences and Hash-based Approach for Improving Medical Image Security

Anita Murmu*
National Institute of Technology Patna, Department of Computer Science and Engineering, Patna, Bihar, India – 800005
E-mail: anitamurmu.cs@gmail.com
ORCID iD: https://orcid.org/0000-0002-2085-1131
*Corresponding Author

Piyush Kumar
National Institute of Technology Patna, Department of Computer Science and Engineering, Patna, Bihar, India – 800005
E-mail: piyush.cs@nitp.ac.in
ORCID iD: https://orcid.org/0000-0003-2065-3028

Received: 29 March, 2023; Revised: 30 June, 2023; Accepted: 10 August, 2023; Published: 08 December, 2024

Abstract: Medical imaging is a field of medicine where doctors use images of different body organs to treat or diagnose patients. Nowadays, medical image segmentation, compression, and security are currently relatively difficult issues for illness diagnosis. These medical pictures are being sent via the internet; thus data must be protected against cyberattacks. Medical images are extremely sensitive to even slight changes, and data volumes are dramatically increasing the amount of the data. To protect the confidentiality of digital images saved online, privacy and security must be ensured. In this paper, a novel DL-based Generative Adversarial Network (GAN) with tent map and hash-map utilized to generate a robust private key. The fake image is generated by using GAN. T It is suggested to use the 2D-Henon Sine Map (2D-HSM), DNA computing, chaotic maps, and a SHA-512-based strategy are proposed. The SHA-512 algorithm and the 2D-HSM are used to construct the key. The Henon map and the Mersenne Twister are used in a two-level encryption method that is shown (MT). After that, a DNA computing-based XOR operation is performed using the key. A decoding procedure based on DNA rules captures the encoded images. The comprehensive outcome is based on several security measures, such as key space, SSIM, information entropy, PSNR, and histogram analysis. The proposed technique performs better than the existing approaches.

Index Terms: GAN, Chaotic map, Security, Hash-map, Cryptography, Key generation

1. Introduction

Medical imaging uses physical phenomena such as light, radioactivity, electromagnetic radiation, nuclear magnetic resonance, and sound to produce visual representations and pictures of internal or exterior human body tissues or a portion of the human body either non-invasively or via an invasive process. The imaging techniques most often employed in clinical medical imaging include computed tomography (CT), X-ray, radiography, magnetic resonance imaging (MRI), digital pathology, and ultrasound. Medical images are huge and have high intensities, making them vulnerable to different types of attacks because of their low-security level [1]. To address these issues, different image encryption schemes have been proposed. Therefore, many techniques for securing these images from cryptographic attacks and efficient storage have been proposed. Some of them are image watermarking [1], image steganography [2], image encryption [3,4], and lossless compression [5]. However, encryption techniques for securing medical images have grown popular in recent years [3]. Encryption techniques are divided into two types, namely, stream and block ciphers. Stream ciphers are more efficient and faster than the block cipher encryption process, as stream cipher encrypt only one bit of data at a time [6]. The purpose of a stream cipher is to produce unpredictable and random sequences of

pixels. Stream ciphers are more efficient than block ciphers because stream cipher encrypts only one bit of the data at a time into individual symbols rather than entire blocks. Chaotic systems and feedback shift registers are two types, i.e., linear and nonlinear, are the most frequent stream ciphers generators [6].

Ravichandran et al. [7] have proposed a two-stage diffusion phase and shuffling phase. At the first step of diffusion, the pixels of the shuffled image are bitwise circularly moved to increase the systems defense against differential assault. DNA XOR operations and DNA coding provide the foundation of the diffusion operations second stage. Wu et al. [8] have suggested the encryption and decryption processes are carried out by a system that consists of a transmitter and a receiver. To provide a randomly generated DNA encoding and diffusion module and a content-aware permutation for the transmitter and receiver, respectively. However, the algorithm is not evaluated in the case of noise attacks. The modality of medical images is prescribed and costly, as we have seen during the COVID-19 situation, which was suffered by attackers. Therefore, the need for encrypted medical images greatly hides valuable information like biometric data, which will be difficult to extract or decipher for attackers. A new algorithm based on deep learning (DL)-based model, Generative Adversarial Network (GAN), is proposed to generate key streams [9]. Then, this key is used to perform XOR-based encryption to get the cipher image [8]. However, these methods still do not properly analyze various attacks. The approaches described above are about different techniques for the encryption process of medical images. All existing techniques have used a single method for generating encryption keys for medical image datasets, did not consider integrity and noise attack challenges in medical images, and provided less security. To overcome these issues, a unique method based on GAN, DNA, hash-map, chaos, and SHA-512 has been developed to effectively protect and preserve medical imaging in order to address the limitations of existing models. These methods are used to provide security for medical imaging. The proposed approach achieves information or security in network goals, including privacy, reliability, and also prevents from noise attacks during the time of encryption. Information that is protected and restricted from unlawful use remains confidential.

The secret key is produced in this proposed approach using a novel 2D Hénon-Sine Map (HSM-2D), DL-based GAN, and SHA-512. In order to enhance the encryption process, pixels of image are shuffled using the Hénon map. The secrets code is used in conjunction with the compressed image to execute XOR operations depending on the DNA sequence. The final encrypted image is created by combining the encrypted images using the Mersenne Twister (MT) technique. The MT is one of the most widely used and effective pseudo-random number generator techniques. MT has been used in various applications, including simulations and encryption. The MT generates high-quality number generators that are similarly distributed over the possible variation in values, which helps enhance the encryption process of medical images.

The proposed model's major contribution is given below:

1. The effective security techniques for medical imaging are limited by the existing models. A novel method is proposed for key generation and encryption of medical images to overcome these restrictions.
2. In the proposed model, design a strong key generation algorithm with the help of deep learning GAN, Tent map, and hash-based equation.
3. Mersenne Twister, DNA encoding, SHA-512, HSM-2D, and other algorithms are used to create keys and encrypt images.
4. The performance measure of the model is evaluated by using key space, PSNR, histogram analysis, SSIM, and entropy on the X-ray and malaria datasets.

There are four sections to the paper. In the next part, the proposed methodology is thoroughly explained. In section 2 literature survey is explained. In Section 3, the performance of the proposed model is evaluated. In Section 4, the article conclusion.

2. Literature Survey

The last few years, the GAN concept has undergone significant changes. This has been a positive trend for computer vision applications due to the rising computing capabilities of existing processors. Moreover, the accessibility of large volumes of data has assisted in these improvements. A chaotic map with DNA-based picture encryption has been proposed by Wu et al. [10]. A novel 2D-SHM for the key generation process has been suggested by the author. Then, DNA-based encoding and diffusion are used. The encrypted final image is then obtained using DNA-based decoding. The results are thoroughly examined while taking into account the various image resolutions. Akkasaligar and Birada [11] have suggested a new lightweight medical image encryption technique due to DNA-based computing and hyperchaos. In this case, a small number of pixels are chosen, DNA-based confusion is carried out, and the remaining pixels are encoded into the DNA sequence. Then, combine all of the pixels once more to create the cipher image. However, in the case of noise attacks, the procedure is not tested. Hosney et al. [12] have proposed a new method based on the confusion and diffusion process for colored picture encryption. The images are split into G, R, and B channels before zigzag-based permutation is applied at the block level. The final cipher image is then obtained by performing the diffusion process on the shuffled image after creating a private key using a 1D-logistic map. The outcome is assessed utilizing SIPI datasets.

Kumar et al. [13] have proposed a chaos-based substitution process to obtain a secure image. The substitution procedure is based on a zig-zag scan. The key generation procedure for the encryption process uses a 1D logistic map. Jeevitha and Prabha [14] proposed a DWT and edge map based on the encryption of medical images. The medical image in this case is originally segmented into a number of DWT planes. The encrypted image is then obtained after applying an edge map and DWT-bit level permutation. However, the technique has not demonstrated how to combine image compression and encryption to further cut storage costs. A new DNA, chaos, and Mersenne Twister (MT) algorithm based on medical imaging have been proposed by Rahman and Kumar [27]. A novel 2D chaotic map has been proposed by the authors to produce encryption private keys. The final encrypted form of the medical image is then created using MT confusion and DNA-based diffusion processes. The proposed scheme based on GAN, DNA, hash maps, chaos, and SHA-512 methods has been developed to effectively protect and preserve medical imaging. Moreover, the proposed scheme combines MT with encryption, which provides more security and reduces storage costs due to the use of MT techniques. However, the proposed approach shortcoming the limitation of [14]. The details of existing studies that discriminate between clinically significant and security are presented in Table 1.

Table 1. Literature survey

Ref.	Objective	Modality	Dataset	Techniques
[15]	Provide security to medical image	MRI, X-ray, CT, Ultrasound, ECG	Chest X-ray, ultrasound, Heart(ECG)	WBAN
[16]	Security of telemedicine and healthcare system	X-ray, CT	X-ray, Brain	DNA-chaos cryptosystem
[17]	Encryption of medical image	CT, MRI	Dicom	Chaos-DNA-IWT
[18]	Encryption and decryption of medical image	MRI	Brain	Chaotic map and DNA code
[19]	Medical image encryption and registration	CT, MRI	CT, MRI	SymReg-GAN
[20]	To improve the medical image security	MRI	Breast MRI	SVM, IWT
[21]	Protection of medical image	MNIST	MINST	DCGAN
[22]	Security of image	Lena jpg	Lena	Tent maps, and rectangular transformation
[23]	Medical image security with segmentation	X-ray	Chest X-ray	Resnet-50 and Cycle GAN
[24]	Healthcare image encryption and compression	X-ray	Chest X-ray	ANN, Levenshtein entropy encoding
[25]	Image encryption	2D image	Gray image and baboon image	Chaotic map and AES
[10]	Encryption and decryption image	Color image	SIPI dataset	Confusion, diffusion and 1D lodistic map

3. Proposed Methodology

Medical imaging is sent over the internet for research and patient care. However, it is essential to protect it against attacks and maintain its integrity. Therefore, effective encryption must be used before transferring the medical images over the internet in order to secure them. A new key generation system based on GAN, DNA, chaos, and SHA-512 encryption and decryption methods are being developed to effectively protect medical image modalities namely, MRI, Ultrasound, CT, X-ray, microscopic, and other than non-medical images. The notations used in this study are shown in Table 2 together with their descriptions.

Table 2. Notation with their definitions

Notations	Definitions
m, n	Width and height of image
x1, y1	Chaotic sequence by 2D-HSM
c	Control parameter
append()	Function to insert value in list array
encode()	Function to get hexdigest from given string
z	Index of pixels
S	Sum of all pixels of the images.
Key	Serect key for encryption
R_1	(Key[z]%8) + 1
R_2	(z%8) + 1
C_i	Cipher image
DNA_{Ri}	Pixel encode with rule Ri
$Decode_{Ri}$	Decode DNA with rule Ri
sequence1, sequence2	The sequence generated by Henon map, MT

3.1. Key generation

The proposed algorithm's initial step is to generate a strong encryption key. The proposed method uses the GAN, HSM-2d [10], SHA-512, input image, and DNA to generate a key stream having a key-value encoded in DNA sequences. To begin, generate the key using GAN with the MINST dataset. The key is generated using GAN along with a tent map and a hash-based equation. The generated key has high entropy and has a very large keyspace of size $(256)^{196608}$. The complete flow of the key generation server is given in Fig. 1.

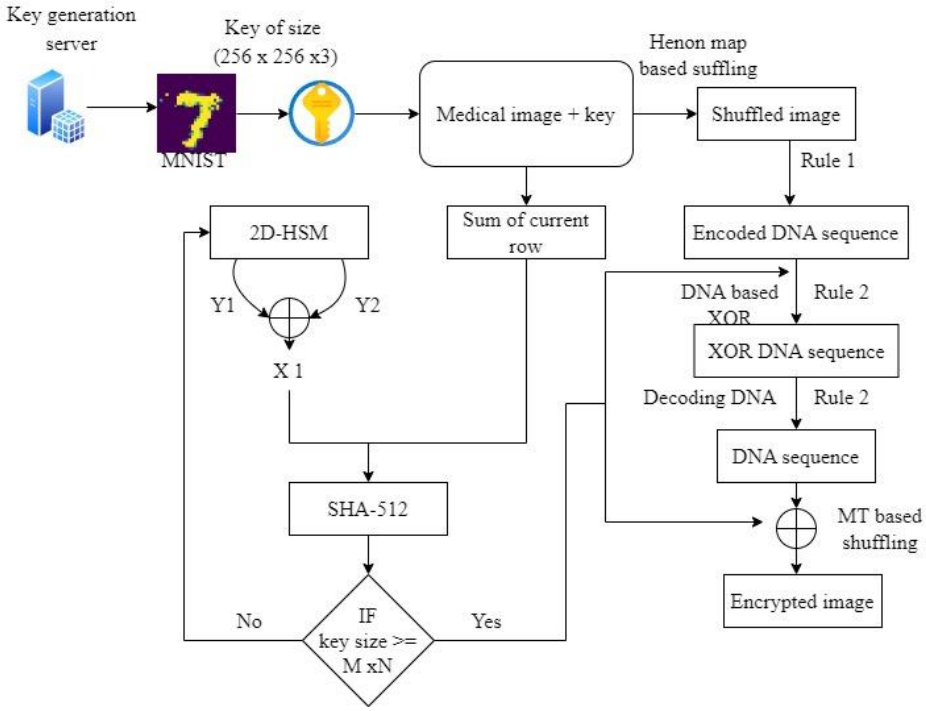

Fig. 1. Proposed model for key generation and encryption.

At first generate fake images from GAN based on the style (that is seed) is provide. The GAN [8] architecture is followed. In this GAN architecture, there are two networks, a discriminator and a generator The architecture of the generator and discriminator networks are shown in Fig. 2., and Fig. 3., respectively. The Generator's work is to create fake sample images from the initial input image (seed) given to the generator input and convert it into transformation domain images of that style provided to generate output. The generator's job is to create a fake image and fool the discriminator into discriminating between real and fake images as much as possible. The discriminator's task is to correctly distinguish between actual and fake images. Ideally, a good discriminator should be able to correctly distinguish if the given generator's output image is fake or real. For the Generator network, there are three downsampling layers in which the first layers have (7 x 7) convolution with a stride of 1, the second and third ones having (3 x 3) convolution layer with the stride of 2, and then 6 residual blocks with (3 x 3) convolution layer with the stride of 1, 2 transposed convolutional layers with (3 x 3) conv. and stride of 2, and 1 ordinary convolution layer having (7 x 7) convolution with stride 1. Instance normalization is done for every convolution layer. As seen in Eq. (1), the loss function is as follows:

$$L_G = min_G(E_{x\sim pdata(x)}\log(1 - D(G(x)))) \tag{1}$$

where, G denotes generator and D represents the discriminator.

Now, that it is on to the discriminator network to tell the difference between the actual image and fake image generated by each generator. The discriminator network consists of four convolutional layers and outputs a 1-D result. The discriminator's loss function is provided in Eq. (2):

$$L(G,D) = min_G max_D(E_{x\sim pdata(y)}\log(D(y)) + E_{x\sim pdata(y)}\log(1 - D(G(x))) \tag{2}$$

In GAN, both the generator and discriminator form the model architecture and they are in a balanced state when the discriminator has 50% accuracy. When discriminator accuracy becomes even less than 50%, the discriminator may start giving irrelevant information in back-propagation to generator, which may degrade the generator network's performance. In the first step of the key generation, the key image of size (256 x 256 x 3) is generated. Now the tent map is applied to generate the sequence by the following Eq. (3):

$$x_i = F(x_i, r) = \begin{cases} r * x_i & 0 < x_i < 0.5 \\ r * (1 - x_i) & x_i > 0.5 \end{cases} \quad (3)$$

from a sequence generated, the pixels of the key image are shuffled. Now, on this shuffled key image, apply a hash-based proposed Eq. (4).:

$$\text{key(i, j)} = \begin{cases} (key\ (i,j) + i + j)\%256 & if\ key(i,j) \in hash - table \\ dist\ [key(i,j)] < 1 & otherwise \end{cases} \quad (4)$$

where i, j is row and column number, respectively. After applying this hash-based modulo operation above, the final key image of size (256 x 256 x 3) as output is generated. This key image is now used for further encryption and decryption. Algorithm 1 shows the steps of key generation.

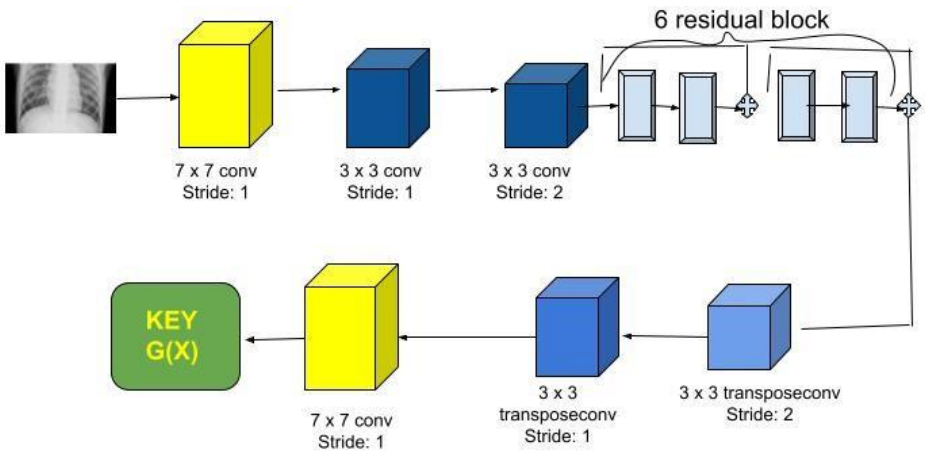

Fig. 2. Generator architecture.

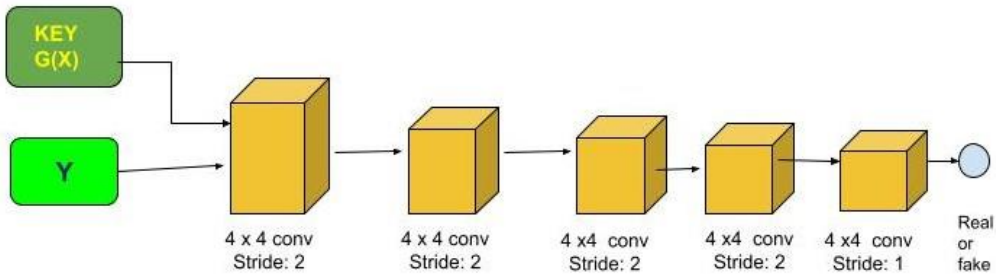

Fig. 3. Discriminator architecture.

Then use hsm-2d to generate two chaotic sequences, x1 and y1, by passing initial and control parameters a, b, x0, y0, as shown in Eq. (5).

$$\begin{cases} y_{m+1} = (1 - b\ sin^2\ (y_m) + x_m) mod\ 1 \\ x_{m+1} = a x_m\ mod\ 1 \end{cases} \quad (5)$$

where a, b $\in$ control parameter and x_n, y_n are initialization parameter for chaotic sequence.

Now obtain a new sequence X by performing modulo operation between x1 and y1 and appending the sum of pixels of the current row value of the input image.

$$X = (x1 \oplus y1) mod\ 256$$
$$X.append(S)$$

The encryption method key becomes sensitive to an input picture as a result. The SHA-512 algorithm should then be given the X sequence to produce a 64-byte result.

$$X_{encode} = X.encode()$$

Then append this value to the final secret key value by converting the bit stream generated using SHA-512 to an integer value. Repeat these steps until the key of the desired size is achieved. Finally, encode each value of the key stream into DNA sequences using Table 3.

Table 3. Encoding and decoding rule for DNA sequence

DNA base	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
T	11	11	10	10	01	01	00	00
A	00	00	01	01	10	10	11	111
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

Algorithm 1: Hash-based key generation process

Inputs: Image datasets $\boldsymbol{M_i}$, *where i= 1,2,3,…,n.*
Output: *Secret key for encryption. Key of size (512 * 512 * 3)*

```
function keyGenerator(M_i):
    Generate the transformed image from GAN of size (512 * 512 * ) key = MINST(M)
    From the initial condition applied on tent map get the key sequence k_seq using eq. (4)
    K_sequence = TentMap (x_i, r, size).
      // apply key shuffling based on sequence generated by the Tent map.
          for r in range(len(rows)) do
              for i in range(len(columns)) do
                  key(r,i) =key(r,i)[k_seq (r,i)]
              end
          end
            // apply hash-based eq. (5)
            for i in range(len(columns)) do
                  for i in range(len(columns)) do
                        if key(r,i) in hash-table then
                              (key(r,i) = key(r,i)+ r+i)%256
                        else
                              dict[key(r, i)] = 1
                        end
                  end
            end
end
```

3.2. Encryption

The key generated by the GAN server is now used to encryption of the medical image. The overall flow diagram of an encryption method is shown in Fig. 4. First of all, the pixels of the original image are shuffled. Split original image into three channels. Now, shuffle pixels of each individual channel using Mersenne Twister (MT) [26]. Once pixels from each channels matrix have been shuffled, merge them back together to form the RGB image. To achieve the final ciphertext image, conduct XOR-based encryption between the shuffled original image and the secret key generated, and the output is completely different from the actual original medical images. Now, after reshuffling, merge all the channels back together to get an RGB image again. In the process of decryption to get back the original image, to reverse the steps of encryption. At first, to split the cipher image into 3 channels. Then reshuffle each channel of the split image.

After that, XOR the cipher image with the key image used during encryption to get back to the original image. The Hénon map and DNA-based diffusion are all part of the image encryption process. Transform the $M_{M \times N}$ image into a MN-dimensional 1-dimensional array to start the encryption procedure. The Hénon map may be obtained by using Eq. (6):

$$HenonMap(a, b, r_m, k_m) = \begin{cases} r_{m+1} = 1 - a\, r_n^2 + k_n \\ k_{m+1} = b r_n \end{cases} \quad (6)$$

where r_{n+1}, s_{n+1} are pixels at (n+1)th position and r_n, s_n are pixel at nth position.

After that, encode the pixels of a shuffled image by the DNA rules [27] as shown in a Table 4. Once the encoded arrays are converted into DNA based sequence, perform a DNA-based the image and the XOR procedure array and the private key using the rule. Finally, to generate a highly secure, encrypted medical image, perform a bitwise XOR on all of the arrays values, secret key, and S, and then reshape the array to an M x N size.

Then, as shown below, compute the sum of the pixels in the array and modulo to get an S value in Eq. (7).

$$S = sum(array)\%256 \quad (7)$$
$$C_i = (\, C_i \oplus S \oplus key)\%256$$

Table 4. Rule for DNA-based XOR operation

XOR	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

3.3. Decryption

The reverse stage of encryption is used to decrypt the original image and recover it. To get the final, original medical image, first permute the cipher image using the Hénon map, then XOR the cipher image and key, and then shuffle the image using hsm-2d.

4. Performance Analysis

This proposed approach offers unique methods for medical image decryption/encryption based on a DNA encoding, SHA-512, and chaos. To create an encryption image, the DNA encoding and Hénon map are used, and the HSM-2d and SHA-512 are used throughout the key creation process. Various security measures, including key space, statistical analysis, robustness analysis, and sensitivity analysis, are used to properly evaluate performance.

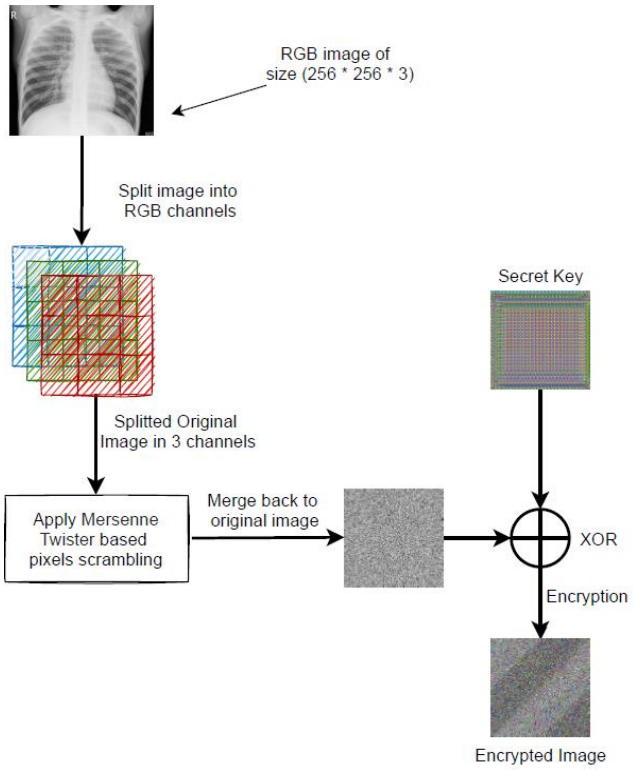

Fig. 4. Encryption process.-

4.1 Experimental Results and Dataset Details

The proposed model is implemented and evaluated on an Intel Core (TM) i5 processor running at 2.5 GHz, with 8 GB of RAM and 4 GB of Nvidia graphics memory (GPU [4]). The X-ray [28] and malaria datasets [29] are used for model evaluation. The MRI [30] and CT [31] images may also be used for encryption and decryption.

Algorithm 2: Medical mage Encryption process

Inputs: Medical image $\boldsymbol{M_{img}}$, *where img= 1,2,3,…,n.* and the Key stream with a DNA encoded pixels

Output: Cipher images C_{img}, where img = 1,2,…n

while *j in range (M* x *N)* ***do***
  shuffled_image [$sequence_1$[j] -1] = M_i[j]
  j= j+1;
end
while *i=0 to M* x *N* ***do***
  Encoded_dna[i] = DNA_{R1}
  i=i+1;
end
while *i =0 to M* x *N* ***do***
  Encoded_dna[i] = Encoded_dna[i] XOR key[i]
  i= i+1;
end
for *x in* $Encoded_{dna}$ ***do***
  Enc_{dna} = $Decode_{R2}$
end
while *j in range(M* x *N)* ***do***
  Encryption_image[$sequence_2$[j] -1] = Enc_{dna}[j]
end
while *j in range (M* x *N)* ***do***
  Encrypted_image[j] = (Encrypted_image[j] ⊕ [i] ⊕ S %256
  J=j+1;
end
Return Encrypted_image

4.2. Results and Discussion

4.2.1 Analysis of Key Space

The key space is determined by the total size of the secret key used for encryption. The key resistivity to brute force assault is shown by an analysis of the key space. For essential space, a value more than 2^{100} is ideal. The Hénon map and 2d-hsm, whose key spaces are 2^{128} and 10^{112} respectively, are utilized for permutation in the proposed key generation and encryption technique. It uses the SHA-512 algorithm, whose attack complexity may reach 2^{128}. The secret picture, which has a dimension of M x N, also has a key space of $(2^8)^{MN}$. The resulting key space of the suggested approach is $(2^{128} + 10^{112} + 2^{128}) + (2^8)^{MN} > 2^{100}$, which is suitable to avoid brute force attacks.

4.2.2. DNA sequence-based XOR operation mapping

The chest X-ray image and the malaria dataset are used to evaluate the qualitative approach of the decryption and encryption performance. The experimental findings are shown in Figs. 5 and 7, respectively. The original medical image, the encrypted image, and the decrypted image are represented in these four images by Figs. 5 and 7, respectively. Moreover, Figs. 6 and 8 show the intensity histogram of the pre- and post-encryption using the proposed GAN's private key for both grayscale and red, green, and blue (RGB) scale plots. The outcomes of performing the DNA sequence-based XOR operation mapping method on images are as follows:

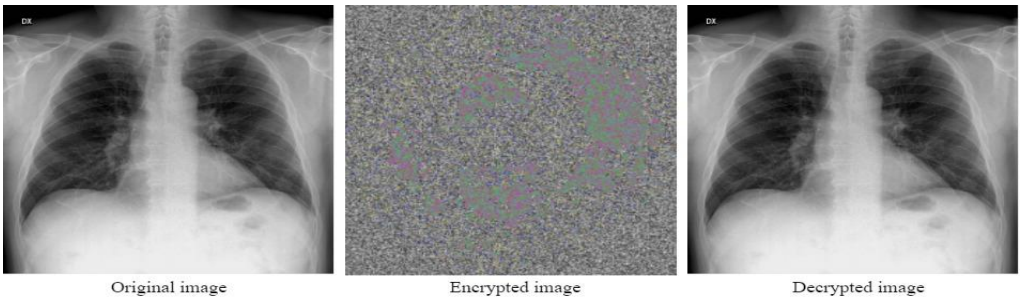

Fig. 5. X-ray image dataset encryption and decryption through proposed approach.

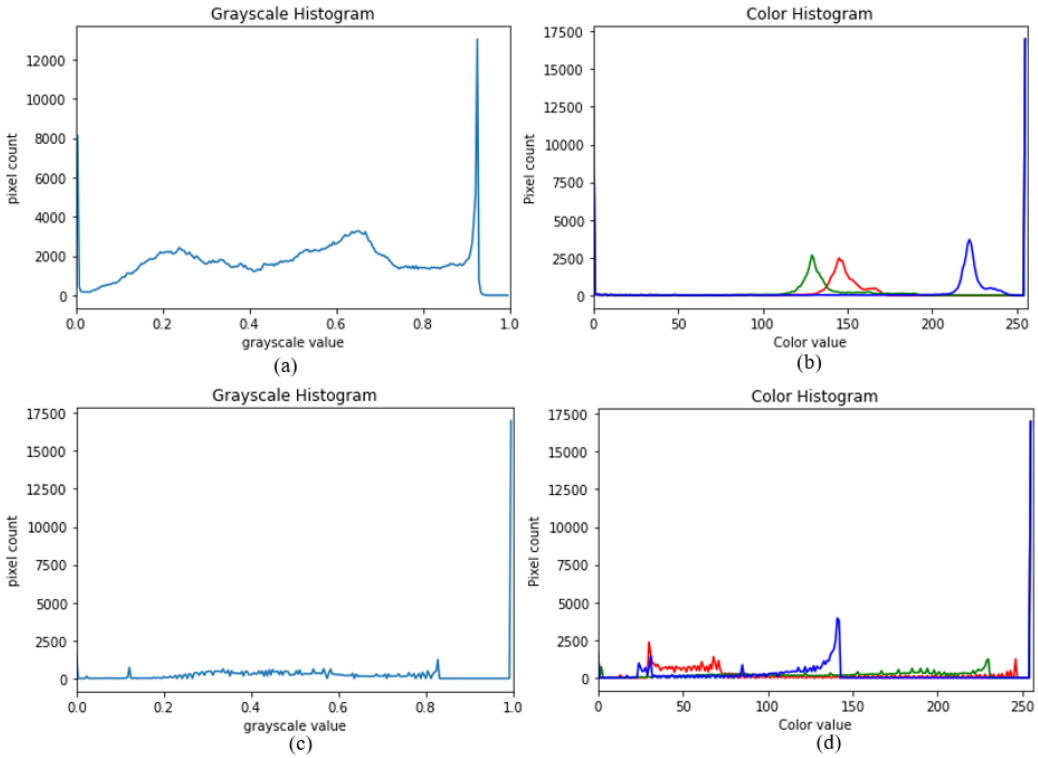

Fig. 6. Intensity histogram of X-ray image dataset (a) pre-encryption gray scale, (b) pre encryption RGB scale, (c) post encryption gray scale, and (d) post encryption RGB scale.

The encrypted medical images are used to preserve the patients' privacy in the biomedical image as it is entirely distinct from original input image. Furthermore, to complete a decryption process, the ciphertext images are changed back to the original image. The experimental findings demonstrate that the suggested system is a reliable key generation technique for securely encrypting and decrypting healthcare images, which simplifies the process of securing the sensitive data included in medical images. Moreover, it became determined that the proposed methodology is utilized to encrypt multi-modality medical imaging from various inspection techniques.

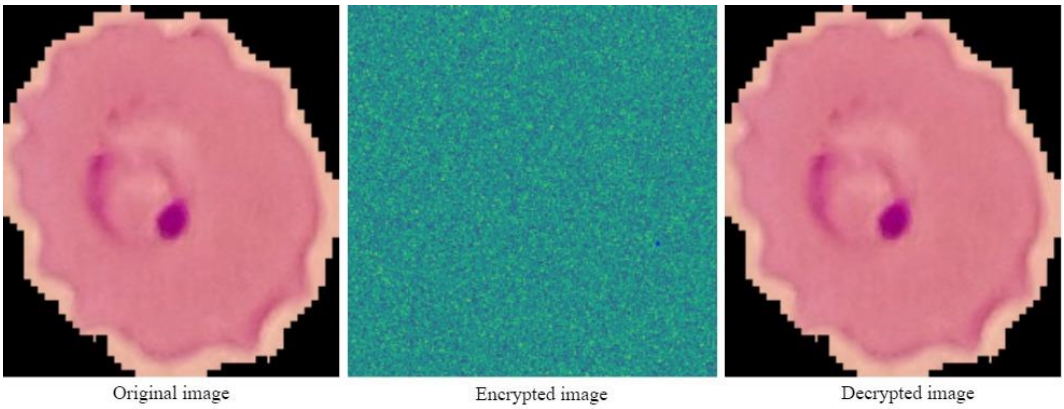

Fig. 7. Malaria dataset encryption and decryption through proposed approach.

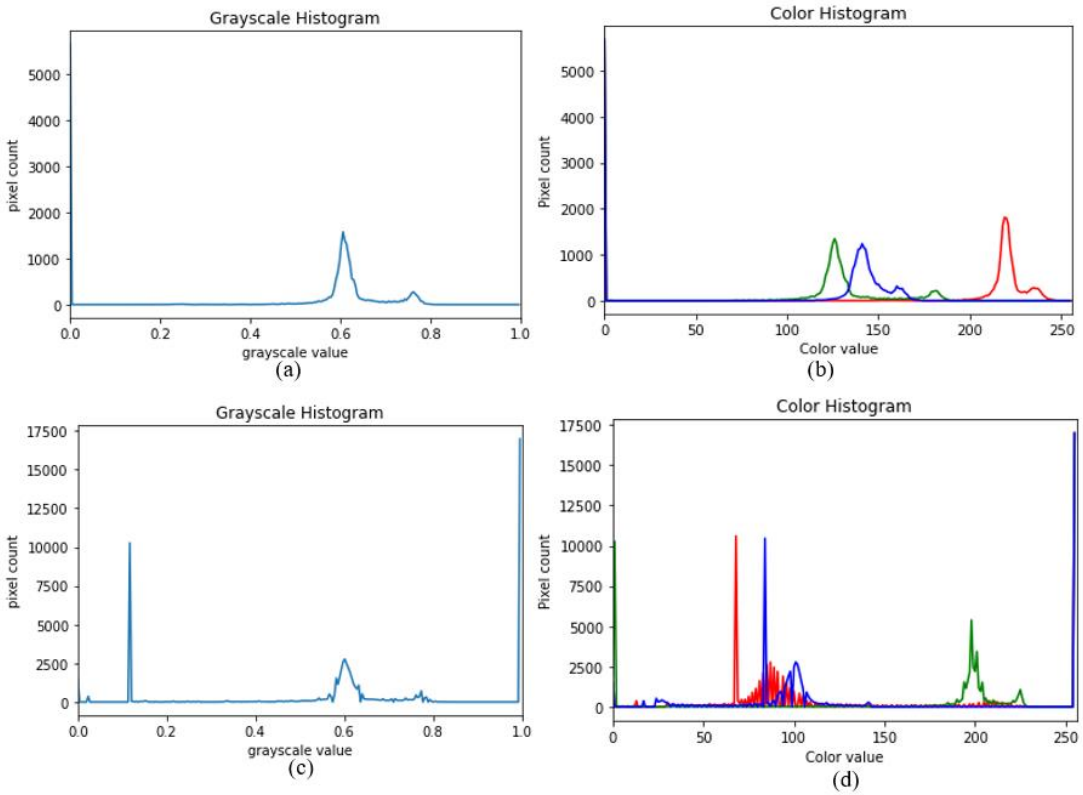

Fig. 8. Intensity histogram of malaria dataset (a) pre encryption gray scale, (b) pre encryption RGB scale, (c) post encryption gray scale, and (d) post encryption RGB scale.

The sample datasets are trained and used to improve the quality of images using the developed model. The remaining datasets are passed through testing, through the proposed system for encryption/decryption, and the results are later compared with the original image value with the entropy and PSNR values. Hence, dual encryption provided by the suggested algorithms is proven to be successful in enhancing the security of medical image data.

4.2.3. Entropy

An images entropy reveals the degree of unpredictableness in that image. Higher entropy images are more resistant to statistical attacks. When calculating it, Eq. (8) is used. The chest X-ray [28] and malaria [29] datasets information entropies are determined to be 7.999316 and 7.999316, respectively, which are almost equivalent to ideal value, which is 8. In Table 5, the comparative analysis of information entropy is shown.

$$L(x) = \sum_{i=1}^{m} q\,(y_i) log_2 q(y_i) \tag{8}$$

Table 5. Information entropy of comparative for cipher images

	Hua et al. [32]	Belazi et al. [33]	Mishra et al. [34]	Proposed
Entropy	7.999297	7.999324	7.998562	7.999316

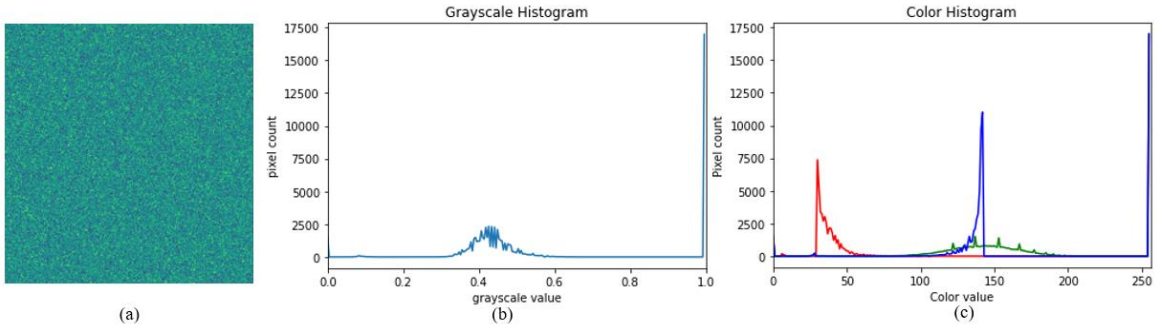

Fig. 9. Intensity histogram of (a) original encryption image, (b) gray scale, and (c) RGB scale.

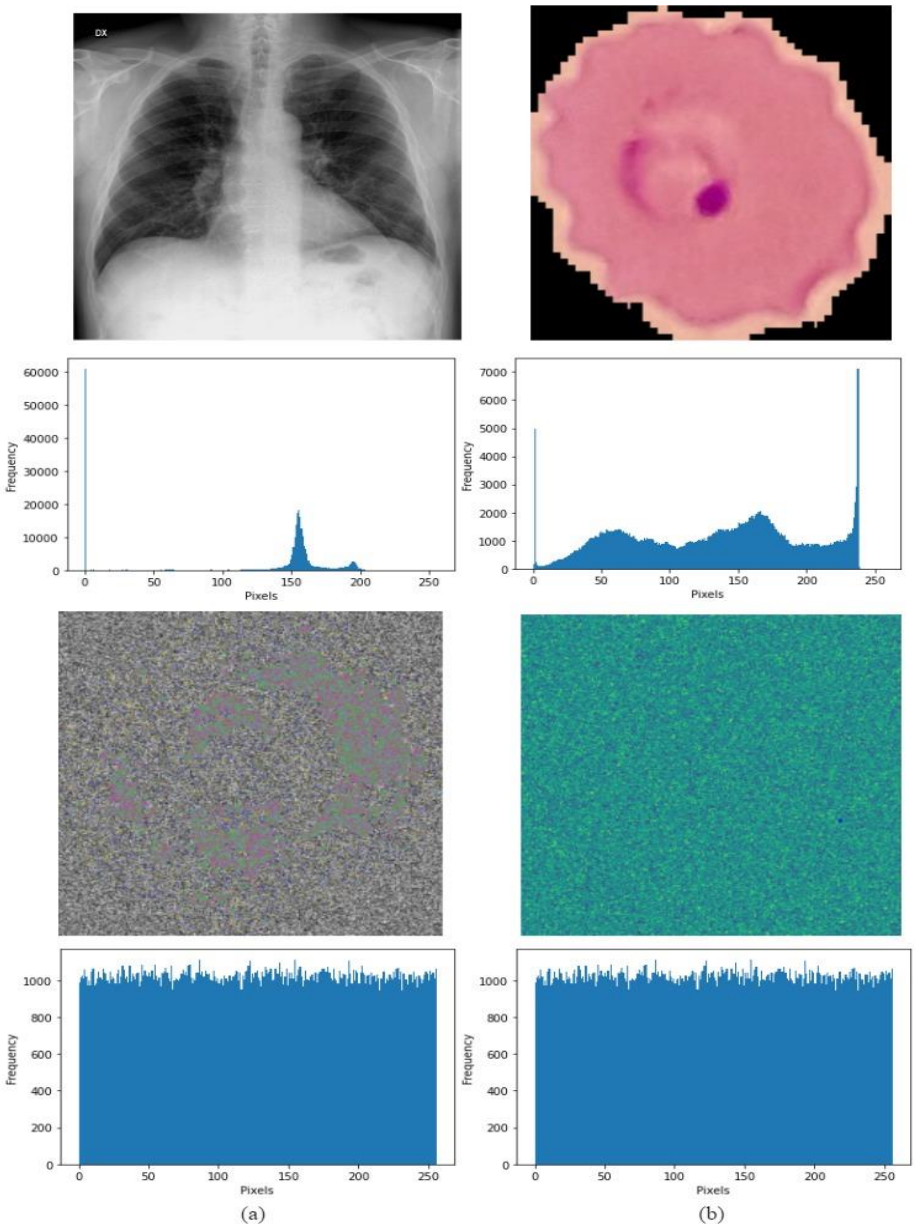

Fig. 10. Visualization of histogram of corresponding cipher and original image (a) chest X-ray image, (b) malaria dataset, respectively.

4.2.4. Histogram Analysis

The number of pixels in each image is shown in the histogram. Statistical assaults may be avoided by having uniform distribution of image pixels. The histograms of an original image and cipher images are represented in Figs 10(a)–10(b), and it is clear that they are almost similar. Moreover, the intensity histogram of encrypted key image in term of gray and RGB scale plots shown in Fig. 9. Therefore, the cipher image of the proposed approach helps guard against statistical assaults.

4.2.5. Differential Attack Analysis

The degree of change in cipher images with the lowest difference between two related original images is used to assess the resistance to different types of attacks. The difference between two cipher images are determined using the he evaluation of a proposed scheme is performed in the event of occlusion attacks using the Peak Signal to Noise Ratio (PSNR) of decrypted image. In the case of occlusion attacks, Table 6 compares the images PSNR values after decryption side by side.

Table 6. Comparative analysis of psnr(db) in case of occlusion attacks

	Hua et al. [32]	Belazi et al. [33]	Mishra et al. [34]	Proposed
PSNR(dB)	8.5675	20.6301	19.6340	22.3248

4.2.6. Differential Attack Analysis

The degree of variation in cipher images with the smallest variation among two related original images is chosen to evaluate the resistance to various sorts of attacks. The number of pixels change rate (NPCR) is used to compare two encryption images. The ideal NPCR measurement is 100% calculated by using Eq. (9). The NPCR comparative research is shown in Table 7.

$$NPCR = \Sigma i,j\, K(I,j)/wh \tag{9}$$

where $w,h \in K$ is pixel value of i^{th} and j^{th} matrix position.

$$K(i,j) = \begin{cases} 0 & if\ c_i \neq c_j \\ 1 & if\ c_i = c_j \end{cases}$$

$w,h \in$ is width and height of a medical image.

Table 7. Comparative analysis of NPCR in case of pixel changes in original images

	Hua et al. [32]	Belazi et al. [33]	Mishra et al. [34]	Proposed
NPCR (%)	99.6	99.62	99.57	99.99

4.2.7. Similarity Analysis

In similarity analysis, similarities between an original picture and its associated encrypted image are examined. This similarity study used SSIM. To ensure that there is as little difference as possible between unencrypted images and original images SSIM values should be near 0, calculated by Eq. (10), shown in Table 8.

$$SSIM(i,j) = [p(i,j)]\alpha\,.\,[q(i,j)]\beta\,.\,[(i,j)]\gamma \tag{10}$$

Table 8. Comparative analysis of SSIM in case of pixel changes in original images

	Kayalvizhi et al. [35]	El-shafai et al. [16]	Ding et al. [8]	Proposed
SSIM	0.0042	0.0051	0.0038	0.0036

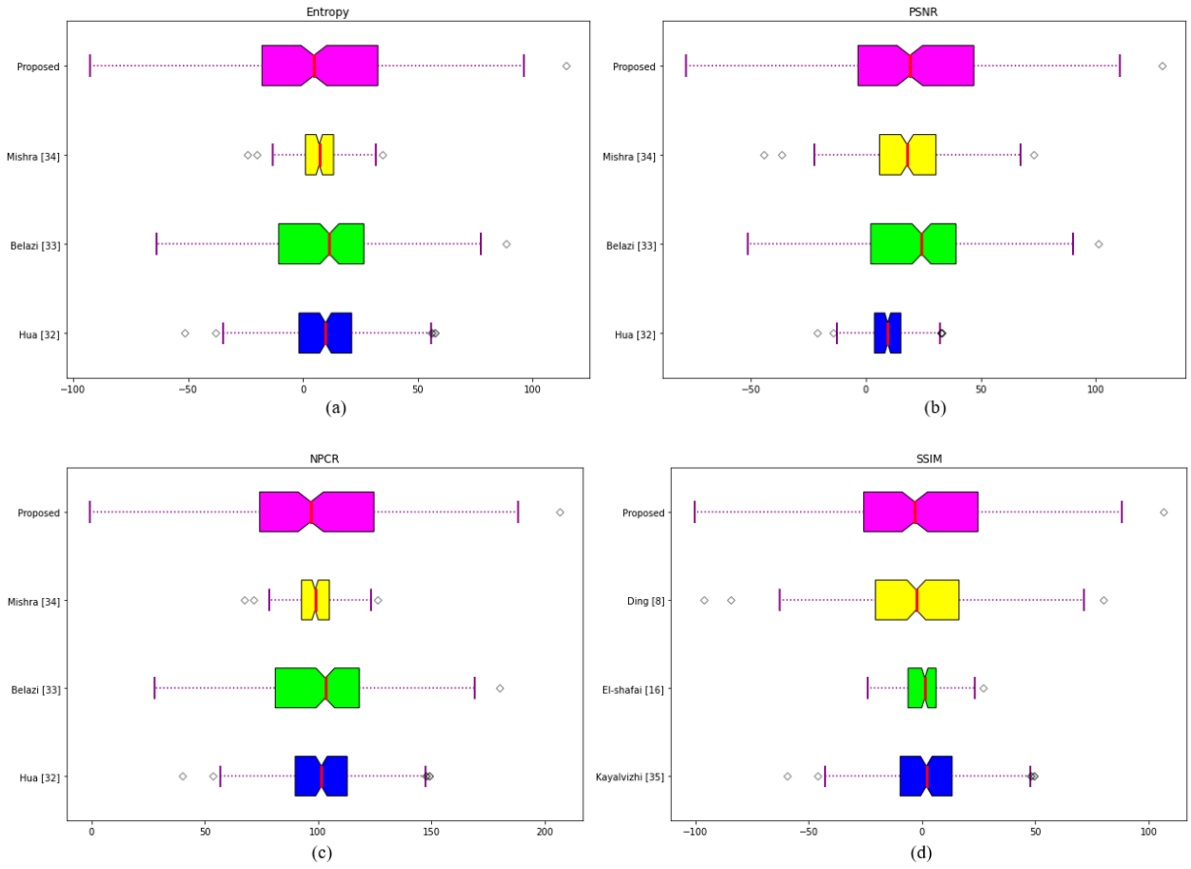

Fig. 11. Comparison of performance results with an existing state-of-the-art approach (a) Entropy, (b) PSNR, (c) NPCR, and (d) SSIM.

4.2.8. Results discussion

The outcomes from the X-ray dataset, and malaria dataset images are shown in Tables 5, and 6, respectively with state-of-the-art comparison. Hua et al. [32], Belazi et al. [33], Mishra et al. [34], Kayalvizhi et al. [35], El-shafai et al. [16], and Ding et al. [8] are three of the approaches that are compared with the proposed methodology shown in Fig. 11(a), 11(b), 11(c), and 11(d). Since all these three methods are used for medical image security. As shown, the proposed model outperforms all other models when it comes to security areas.

- The qualitative analysis for cipher image with PSNR value of 22.3248, and Entropy of 7.999316 on both two datasets, respectively are demonstrates the greatest improvement. The proposed novel deep learning-based GAN performs significantly better than Hua et al. [32], Belazi et al. [33], Mishra et al. [34], Kayalvizhi et al. [35], El-shafai et al. [16], and Ding et al. [8] on medical image security.
- The proposed technique has the potential to reduce this significant training overhead and increase performance because it uses GAN with DNA sequence and hash-based approach, which is often used to improve performance of security.

Overall, the proposed model outperforms state-of-the-art models and has comparatively minimal learning requirements.

5. Conclusion and Future Work

The secure transmission and archiving of medical images are presented using a novel method based on DL-based Generative Adversarial Network (GAN) with tent map and hash-map utilized to build a strong private key, DNA, Chaos, and SHA-512 computations. The proposed method uses SHA-512 and 2D-HSM to create keys. Data, chaos, and DNA computing are all secured using SHA-512 algorithms. The original medical images are shuffled using a Hénon map, and as part of the encryption process, the image's pixels are encoded in DNA sequences. The DNA operation based XOR operation is carried out with the help of the private key. An image that has been encoded is then produced by decoding the DNA-based sequence. The encrypted image is created by adding the original images pixel total, the secret key, and the ciphertext images. Using the basis of a number of security criteria, such as key space, entropy, occlusion attack, and histogram analysis, the proposed technique is assessed on chest X-ray and malaria datasets. The outcomes of the evaluation demonstrate that the proposed scheme performs better than the current models. In the future, we will be tested on more medical-related tasks including secured feature detection in order to increase the effectiveness of the autoencoder layers with segmentation task in medical image.

References

[1] Begum M, Uddin MS, "Digital image watermarking techniques: a review," Information, vol. 11, no.2, pp. 110, 2020.
[2] Liao X, Yin J, Guo S, Li X, Sangaiah AK, "Medical JPEG image steganography based on preserving inter-block dependencies," Computers and Electrical Engineering, vol. 67, pp. 320-329, 2018.
[3] Vengadapurvaja AM, Nisha G, Aarthy R, Sasikaladevi N, "An efficient homomorphic medical image encryption algorithm for cloud storage security," Procedia computer science, vol. 115, pp. 643-650, 2017.
[4] Kumar P, Agrawal A, "GPU-accelerated interactive visualization of 3D volumetric data using CUDA," World Scientific Journal of Image and Graphics, Vol. 13, pp. 1340003-1340018, 2015.
[5] Kumar P, Parmar A., "Versatile Approaches for Medical Image Compression: A Review," Procedia Computer Science, vol. 167, pp. 1380–1389, 2020.
[6] Ravichandran D, Banu SA, Murthy BK, Balasubramanian V, Fathima S, Amirtharajan R, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain," Medical and Biological Engineering and Computing, vol. 59, no. 3, pp. 589-605, 2021.
[7] Wu Y, Zhang L, Berretti S, Wan S, "Medical image encryption by content-aware DNA computing for secure healthcare," IEEE Transactions on Industrial Informatics, pp. 1-9, 2022.
[8] Ding Y, Tan F, Qin Z, Cao M, Choo KKR, Qin Z, "DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption," IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 9, pp. 4915-4929, 2021.
[9] Tripathi SK, Gupta B, Pandian KK, "Hybrid image sharing scheme using non-recursive hash key based stream cipher," Multimedia Tools and Applications, vol. 78, no. 8, pp. 10837-10863, 2019.
[10] Wu J, Liao X, Yang B, "Image encryption using 2d Hénon-sine map and DNA approach," Signal Processing, vol. 153, pp. 11–23, 2018.
[11] Akkasaligar PT, Biradar S, "Selective medical image encryption using DNA cryptography," Information Security Journal: A Global Perspective, vol. 29, no. 2, pp. 91–101, 2020.
[12] Hosny KM, Kamal ST, Darwish MM, "A color image encryption technique using block scrambling and Chaos," Multimedia Tools and Applications, vol. 81, no. 1, pp. 505–525, 2021.
[13] Kumar CM, Vidhya R, Brindha M, "An efficient chaos based image encryption algorithm using enhanced Thorp Shuffle and chaotic convolution function," Applied Intelligence, vol. 52, no. 3, pp. 2556–2585, 2021.

[14] Jeevitha S, Amutha Prabha N, "Novel medical image encryption using DWT block-based scrambling and edge maps", Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 3, pp. 3373–3388, 2020.
[15] Ismail R, Fattah A, Saqr HM, Nasr ME, "An efficient medical image encryption scheme for (WBAN) based on adaptive DNA and modern multi chaotic map," Multimedia Tools and Applications, pp. 1-15, 2022.
[16] El-Shafai W, Khallaf F, El-Rabaie ESM, El-Samie FEA, "Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 9007-9035, 2021.
[17] Banu SA, Amirtharajan R, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," Medical and biological engineering and computing, vol. 58, pp. 1445-1458, 2020.
[18] Guesmi R, Farah MB, "A new efficient medical image cipher based on hybrid chaotic map and DNA code," Multimedia tools and applications, vol. 80, pp. 1925-1944, 2021
[19] Zheng Y, Sui X, Jiang Y, Che T, Zhang S, Yang J, Li H, "SymReg-GAN: symmetric image registration with generative adversarial networks," IEEE transactions on pattern analysis and machine intelligence, vol. 44, no. 9, pp. 5631-5646, 2021.
[20] Chowdhuri P, Pal P, Si T, "A novel steganographic technique for medical image using SVM and IWT," Multimedia Tools and Applications, pp. 1-20, 2023.
[21] Yan X, Cui B, Xu Y, Shi P, Wang Z, "A method of information protection for collaborative deep learning under GAN model attack," IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 18, no. 3, pp. 871-881, 2019.
[22] Xiaolin wu, Zhu B, Hu Y, Ran Y, "A novel colour image encryption scheme using rectangular transform-enhanced chaotic tent maps," IEEE Access, pp. 1–1, 2017.
[23] Ding Y, Wu G, Chen D, Zhang N, Gong L, Cao M, Qin Z, "DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things," IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1504–1518, 2021.
[24] Selvi CT, Amudha J, Sudhakar R, "Medical image encryption and compression by adaptive sigma filterized SYNORR certificateless signcryptive Levenshtein entropy-coding-based deep neural learning," Multimedia Systems, vol. 27, no. 6, pp. 1059–1074, 2021.
[25] Arab A, Rostami MJ, Ghavami B, "An image encryption method based on Chaos System and AES algorithm," Springer, The Journal of Supercomputing, vol. 75, no. 10, pp. 6663–6682, 2019.
[26] Matsumoto M, Nishimura T, "Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator," ACM Transactions on Modeling and Computer Simulation (TOMACS), vol. 8, no. 1, pp. 3-30, 1998.
[27] Rahman M, Kumar P, "2D-CTM and DNA-Based Computing for Medical Image Encryption," In Intelligent Data Engineering and Analytics: Proceedings of the 10th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA), pp. 225-235, 2022.
[28] Image databases. [Online]. Available: https://www.imageprocessingplace.com/root_files_V3/image_databases.htm. [Accessed: 26-March-2023].
[29] National Library of Medicine, Lister Hill National Center for Biomedical Communications [Available online: https://ceb.nlm.nih.gov/repositories/malaria-datasets/] [Accessed: 26-March-2023].
[30] Murmu A, Kumar P, "A novel Gateaux Derivatives with Efficient DCNN-ResUNet Method for Segmenting Multi-class Brain Tumor," Medical & Biological Engineering & Computing, 2023.
[31] Murmu A, Kumar P, "Deep learning model-based segmentation of medical diseases from MRI and CT images," In IEEE Region 10 Conferenc (TENCON), pp. 608-613, New Zealand 2021.
[32] Hua Z, Zhou Y, "Design of image cipher using block-based scrambling and image filtering," Information sciences, vol. 396, pp. 97-113 2017.
[33] Belazi A, Talha M, Kharbech S, Xiang W, "Novel medical image encryption scheme based on chaos and DNA encoding," IEEE access vol. 7, pp. 36667-36681, 2019.
[34] Mishra P, Bhaya C, Pal AK, Singh AK, "A medical image cryptosystem using bit-level diffusion with DNA coding," Journal of Ambient Intelligence and Humanized Computing, pp. 1-22, 2021.
[35] Kayalvizhi S, Malarvizhi S, "A novel encrypted compressive sensing of images based on fractional order hyper chaotic Chen system and DNA operations," Multimedia Tools and Applications, vol. 79, no. 5-6, pp. 3957–3974, 2019.

Authors' Profiles

Anita Murmu is currently pursuing PhD degree in Department of CSE from National Institute of Technology Patna, India. Her research interests include medical image analysis, and deep learning.

Piyush Kumar is an Assistant Professor in CSE department at the NIT Patna, India. His major research interest includes Computer Graphics, Medical Imaging, and AI. He has more than 20 publications.

How to cite this paper: Anita Murmu, Piyush Kumar, "A Novel GAN with DNA Sequences and Hash-based Approach for Improving Medical Image Security", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.16, No.6, pp. 72-86, 2024. DOI:10.5815/ijigsp.2024.06.06