ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 12, December 2022

Encryption of Medical Images Using Chaotic Maps and DNARuleswith Genetic Algorithm

[1] K.Sudha Kumari, [2] C.Nagaraju

[1] Assistant Professor, MallaReddy Engineering College, Hyderabad, Telangana.
[2] Professor, YSR Engineering College of Yogivemana University, Proddatur.
Corresponding Author Email: [1] Sudhakumari.kanchegara@gmail.com, [2] nagaraju.c@yogivemanauniversity.ac.in

Abstract— Sensitive information of medical images related to the patients is important to secure from intruder. DNA cryptography is very importantmethodology to provide Security. In this paper three level Genetic based DNA cryptographic technique is proposed. In the first level the logistic Chaotic mapsareapplied to shuffle positions of Pixels in Medical Image. In second level a mutation and crossover operations of GA are used for exchanging position of binary values within the gray values.In the third level Encoding rules of DNA are applied to selected part of inImage to generate diffused unique DNA structure which is difficult to understand by the intruders. The proposed system provides high-level security and resistant to the varies attacks.

Keywords: DNA Decoding rules, Logistic Chaotic Map, Permutation, Diffusion, Genetic algorithm.

I. INTRODUCTION

In this digital world providing security for digital medical images will play a crucial role. These digital medical images contain sensitive and confidential information related to the patients. For providing security to digital medical images, cryptography will provide the best and efficient encryption techniques [1]. As we are unable to encrypt the digital medical images directly, we have to convert these digital medical images into grayscale images which will be in the form of a matrix that contains picture element values of the medical image in range of 0-256. This matrix is divided into two matrices A1 and A2 by using the pixel selection algorithm [2]. If the pixels satisfy the pixel selection algorithm, then those pixels will be cached in A1 and the remaining pixels will be cached in A2. The randomized key which will be used while decrypting the medical image willbe generated by applying thelogistic chaotic map equation on the matrix A1 [4] .Then, apply dual hyperchaotic maps on this logistic chaotic encrypted image for generating the initial values [5,6] So, encrypting the medical images using chaotic maps will provide high complexity which is hard to predict by the intruder. Chaotic encrypted matrix and the matrix m2 will be encrypted to get DNA-encoded Imageswith specified encoding rules of DNA which will use four nucleotides like A, T, G, C for encrypting the medical images, and creates a unique DNA structure [7,8] that is difficult to understand. Now apply permutation and diffusion techniques [9] which are used for shuffling the pixels and changing their values respectively. Then combine both DNA encoded matrices using the DNA XOR operation. This generated encoded image with DNA is converted to binary image. So, here we are encrypting this binary image by using the genetic algorithm [10] which performs the operations of GA. The selection operation is used for selecting the chromosomes and calculating the proficiency value to find the best population. If the proficiency value is less than “0.2” then no operation will be performed. If the proficiency value is greater than 0.2 and is less than 0.8 then the crossover operation will be performed [11]. If the proficiency value is greater than 0.8 then the mutation operation will be performed. The crossover operation will be performed for generating the new off-springs by swapping the chromosomes between the selected parent chromosomes. After this crossover operation, apply mutation operation for flipping the bits [12]. These operations will be performed iteratively until there will be no new off-springs will be generated compared to the existing ones and then we will get the genetic encrypted medical image. This encrypted medical image along with the randomized keys sent to the receiver, over internet for diagnosis. receiver has to decrypt Image to read the image [13]. So, he will decrypt the medical image which is the reversal of the encryption process. So, first genetic decryption will be performed on the encrypted medical image. Then decrypt the medical image using the DNA-decoding rules. Now, apply chaotic decryption on this DNA-decoded medical image. Then we will get the grayscale medical image which will be converted into the original image by using RGB. So, by using the above techniques we will encrypt the medical images by providing high security and able to reduce the computational time for processing the digital images.

II. ENCRYPTIONTECHNIQUE

Encryption of digital medical images uses the techniques like Logistic chaotic maps, Dual hyper chaos maps, DNA Encoding rules, Permutation, Diffusion, and Genetic Algorithm. By using the logistic chaotic map equation, a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 12, December 2022

randomized key will be going to generate and that will be used for decrypting the image. Dual hyper chaos maps are used for generating the initial values. DNA encoding rules are used for generating a unique Deoxyribonucleic acid structure that will be hard to understand by intruders. Permutation and diffusion processes are used for shuffling and scrambling the pixels. The medical image is encrypted using genetic algorithm by performing the operations like selection, crossover, and mutation. The logistic chaotic map equationa randomized key will be going to generate and that will be used for decrypting the image. Dual hyperchaos maps are used for generating the initial values. DNA encoding rules are used for generating a unique Deoxyribonucleic acid structure that will be hard to understand by intruders. Permutation and diffusion processes are used for shuffling and scrambling the pixels. The medical image is encrypted using genetic algorithm by performing the operations like selection, crossover, and mutation.

2.1. Logistic-Chaotic Map (LCM)

The LCM is one of the popular 1-D chaotic-maps. This LCM varies with initial conditions with high sensitivity. Depending upon the bifurcation parameter it produces unpredictable nonperiodic pseudo-random sequence. So, by using this function while encrypting the medical images this will play a key role in shuffling pixels and Values of pixels by applying Permutation and diffusion of GA. This Logistic chaotic Map function is simple 1-D dynamical equation with complex randomized behavior. The mathematical equation of this LCM can be expressed by using the following equation:

$$xn_{+1} = \lambda xn\,(1 - x_n) \quad (1)$$

Where λ is a control variable with a limit of (0, 4] and $_n$ is the output chaotic sequence.

By getting x_n value we cannot predict x_n +1value, hence the map is irreversible. We can observe completely different behavior by following the ambit of this map over time. These behaviors depend on control parameter λ and initial conditions x_n. So, by using this logistic chaotic equation, pixel shuffling and scrambling can be done easily by using permutation and diffusion processes will help to improve the security to medical Images to protect sensitive and confidential information related to the patients.

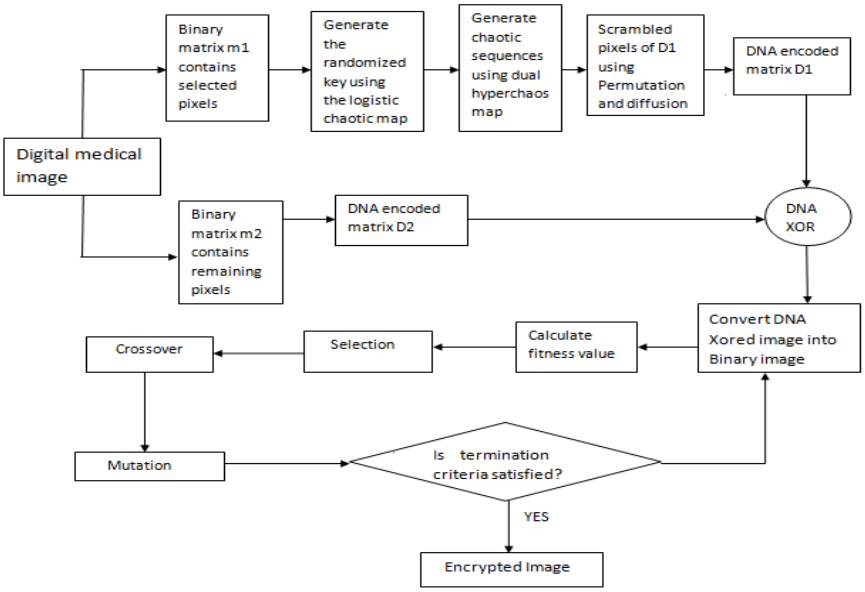


Fig:1 Architecture of encrypting the digital Medical Image.

2.2. Dual-hyper chaos map

A hybrid Mapsare generated by combining the Taylor-Chirikov and Chen's equation and the initial values and chaotic values are generated by using the hybrid map. The chaotic values generated by this hybrid map are composite and difficult to understand by the intruder. In this dual hyper chaos map, starting value of parameter with ChenHyperChaotic mapsare generated by Taylor ChirikovMap. This dual hyper chaotic map provides confusion assets and is vastlydelicate to the initial state that helps for providing security to digital Images. This dual hyper chaos map is used along with DNA sequences and genetic algorithms (GA)for improving the security of Image.

2.3. DNA Sequences

Sequencing of DNA is the process used to link the nucleotide sequences by framing components of DNA. DNA Sequences are used for generating the unique structure of DNA for every medical Image which will be difficult to understand. The DNA structure contains 4nucleotides (Adenine, Guanine, Cytosine, and Thymine). The nucleotides T and A are always complimentary with each other, and the nucleotides C and G are always complimentary with each

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 12, December 2022

one. Pixels of the digital medical image will be expressed by using the eight-bit binary numbers. Since the binary digits 0 and 1 are complimentary, 01 is complimentary to10.00 and 11 is complimentary. So, the nucleotides [A, T, G, C] will be encoded as00, 11, 10and 01respectively. Based on these rules, it generates 24 types of different encoding patterns. According to deoxyribonucleic acid-pairing rule, eight patterns are considered as encoding and decoding rules among 24 patterns. Those DNA encoding rules are:

Rule	Binary value	DNA Structure
One	“00110110”	[ATGC]
Two	“00111001”	[ATGC]
Three	“01100011”	[ATGC]
Four	“01101100”	[ATGC]
Five	“10010011”	[ATGC]
Six	“10011100”	[ATGC]
Seven	“11000110”	[ATGC]
Eight	“11001001”	[ATGC]

2.4. SelectiveImage Encryption

To provide security to medical Images DNA sequence &hybrid map operations are used. By using the Pixel-selection technique select the pixels from medical image.

2.4.1. Pixel Selection

I/P: Original digital medical image IMGwith row size R and column sizeC.

O/P: Selected pixels are cached in A1,A2 matrices

for p = 0 to R do
for q = 0 to C do
G=IMG (p, q) % 3;
N = floor (G);
W = N-G;
if (W< 0) then
A1[p, q] = IMG[p, q];
else
A2[p, q] = IMG[p, q];
end
end
end

2.4.2. Encryption of Selective Medical Image

I/P: Medical image IMG (R, C)

O/P: Encrypted image IMG1(R, C)

Start

Convert the original medical image into the grayscale image which is in the matrix form that contains the pixels in the decimal form.

Divide the grayscale image into two matrices

A1(R, c) = This matrix contains the selected pixels of the grayscale image IMG (R, C) using the Pixel-Selection Algorithm.

A2(R, C) = This matrix contains the pixels of the grayscale image IMG (R, C) which do not satisfy the Pixel-Selection algorithm.

Convert the grayscale images into the Binary Image (BI)

B1(R× 8, C × 8) =Dec2Bin (A1(R, C));

B2(R × 8, C × 8)=Dec2Bin (A2(R, C));

Use the DNA encoding rules which will convert the binary images into the DNA-encoded matrix (DEM)

D1(R × 4, C × 4) = DEM (B1(R × 8, C × 8))

D2(R× 4, C× 4) = DEM (B2(R × 8, C × 8))

Dual hyper chaos maps are used for generating the chaotic sequences p, q.

S = [p0, p1, p2, p3…,pN];

R = [q0, q1, q2, q3,…., qN];

S= SORT (S);

R= SORT (R);

Jumble pixels of D1(R × 4, C× 4) by using the chaotic sequences of S and R which are sorted based on their index values.

Merge the two DNA-encoded matrices by using the XOR operation:

D12 (R × 4, C × 4) = D1(R× 4, C × 4) DNA XORD2(R × 4, C× 4)

Based on DNA decoding rules change the DEM into an eight-bit binary image.

B12(R× 8, C × 8) = D12 (R × 4, C × 4)

Convert the 8-bit binary image into the encrypted image

IMG (R, C) = Bin2Dec (B12(R × 8, C × 8))

Stop

2.4.3.Pixel Scrambling

The method which alters the relevant image pixels to tangled image for providing security to digital medical images is known as pixel scrambling. For this, we apply the Diffusion and Permutation processes on picture element of the Medical Images.

2.4.4. Permutation

The process of rearrangement of pixels position of the image is known as permutation. Pixels of the DEM D1 are rearranged by using the hybrid map which will generate the randomized sequences. Depending on the index values chaotic sequences are sorted. Then the permutation process will be applied to those sorted chaotic sequences for shuffling the pixels by using their index values.Forexample:If the chaotic sequence C = {0.2, 1.4, 2.6, 3.5} with index C [0, 1, 2, 3] then the sorted chaotic sequence will be C = {0.2, 2.6, 1.4, 3.5} with the index C [0, 2, 1, 3]. So, by using those index values, pixels of the DNA- Encoded matrix D1 will be shuffled.

2.4.5 Diffusion

The diffusion process is completely different from the permutation process. This diffusion process is possible by

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 12, December 2022

using the transportation algorithm, in which altering of single pixel-value of the plain image may affect several or whole pixels values for the encrypted Image Sothat, it increases the expandability of the plain image by expanding it across the rows and columns. In this diffusion process pixel values of the DNA-encoded matrix will change sequentially by using DNA XOR operation. Hence a n unit transpose in the pixel value may expand to as many pixels in the cipher-image as possible.

III. GENETIC ALGORITHM (GA) FOR IMAGE ENCRYPTION

GA (Genetic Algorithm) is an optimization search Techniques. This algorithm will be applied after combining the two DNA encoded matrices by performing the DNA XOR operation. This genetic algorithm performs the operations on the pixels of the digital Medical Image which is combined with DNA XOR operation. By performing those operations iteratively genetic algorithm will generate a new generation of chromosomes called "off-springs". Chromosomes with higher proficiency will be selected after calculating the proficiency function. For generating the new chromosomes apply the crossover and mutation operations on the selected chromosomes. It passes through several generations iteratively, until no new chromosomes will be generated. So, like this, it will encrypt all the pixels of the medical image and will provide high security. As it is the best optimization search algorithm, it will also reduce the computation time for processing the digital medical image.

3.1. Selection

Selection operation is used for selecting the chromosomes based on calculated proficiency values. Proficiency value can be calculated by using the formula

$F = N + (\Sigma 0 + \Sigma 1) / \Phi$

WhereF = proficiency,

N = no. of Bits in a sample,

$\Sigma 0$ = percentage of "O" bits,

$\Sigma 1$ = percentage of "I" bits,

Φ = most occurred bit percentage (0 or 1).

3.2.Cross over operation

Crossover is one of the operators used in genetic algorithms for generating new chromosomes values by combining two or more parent chromosomes values to create new and efficient chromosomes. Crossover occurs if the random number (rn) lies in the range of 0.2 and 0.8 excluding 0.2 and 0.8. It occurs after selecting the pair of parent chromosomes for creating new offspring by exchanging the information between the parent chromosomes. These offspring will be the next generation parent chromosomes. There are different types of crossover operations. Here we use the One-Point crossover.

3.3 One-Point Crossover

It is one of the simplest crossover operators. In this, a crossover cut point is selected randomly in both selected parent chromosomes. At this point, swapping can be done between the two parent chromosomes to either left or right for producing new off-springs. For example,

Before Swapping

Parent1	0	0	0	0	0	0	0
Parent2	1	1	1	1	1	1	1

After Swapping

Offspring1

1	1	1	0	0	0	0

Offspring2

0	0	0	1	1	1	1

Here the line indicates the crossover cut point which is used for swapping between the 2 parent chromosomes which will generate new off-springs effectively.

3.4.Mutation

The mutation operation will be performed after the crossover operation. This mutation operator will apply the changes randomly to one or more "genes" that will produce a new offspring. Mutation occurs if the generated random number (rn) is greater than 0.8. Applying mutation along with crossover will give the best results. There are different types of mutations, here we use bit flip mutation.

3.5.Bit Flip Mutation

The process of selecting more than zero random bits and flip them is known as Bitflip mutation. This is used for binary encoded genetic algorithms.

Before Mutation

0	0	1	0	1	0	1

After Mutation

1	0	1	0	1	0	0

encryption withGA

3.6. Pixel Scrambling and Substitution:

Read the combined DNA encoded matrices with help of DNA XOR operation.

Compute the proficiency(F) of every block of data with the proficiency function.

i.e.$F = N + (\Sigma 0 + \Sigma 1) / \Phi$

Arrange the blocks based on the decreasing value of their proficiency values.

Random numbers ofeach block of data are produced based onfunctionwhich is generatedRandom number

if (Rn<0.2) then

write ("No-operation will be performed")

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 12, December 2022

else if (0.2 <Rn< 0.8) then
write ("Apply Crossover-operation")
else if (Rn> 0.8) then
write ("Apply Mutation-operation")
After that, an intermediate image is generated.
Replicate step 2 to step8 for the rest of the blocks of data.

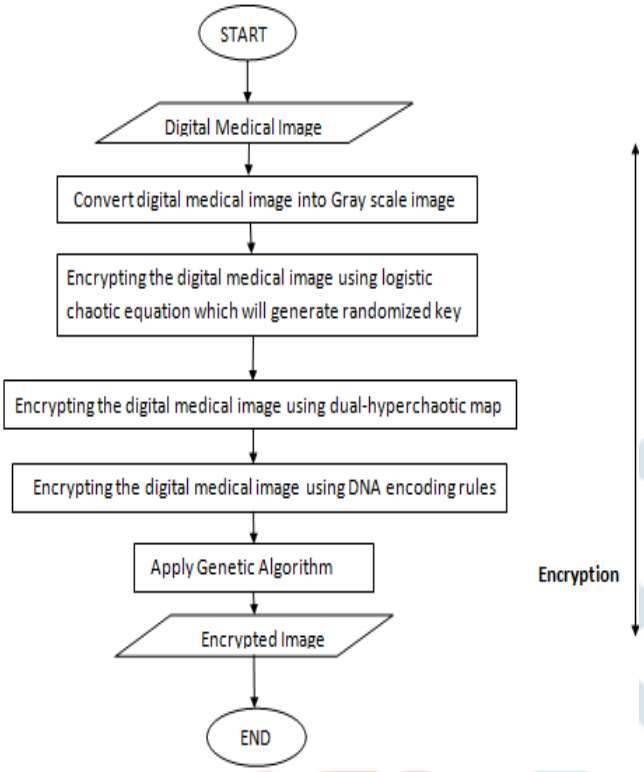


Fig.2. Encryption process

IV. DECRYPTION OF MEDICAL IMAGE

The reverse process of encryption is decryption. So, decrypt the image by using the genetic algorithm first and then apply chaotic-based decryption by using the randomized key and finally decrypt the medical image by using DNA Decoding rules.

4.1 Reverse Pixel-Substitution

Input the encrypted Medical Image and translate it into a 256 by 256 matrix in contains Pixels of the medical Image.

Divide the converted 256 X 256 matrices into 32X32 matrix by taking each 8X8 matrix as single block.

Apply XOR operation for the 8 substrings and in between each block with same 8 substrings of DNA in the encryption stage.

Finally repeat the left over 31 matrices with unique 8 DNA substrings and generates intermediate image as output.

4.2 Reverse Pixel-Scrambling

Bisect the intermediate image which is in the form of a 256X 256 matrix into a 32 X 32 matrix of each 8X 8 matrix as one block.

Next, we are going to study the first four blocks i.e., the first & second blocks of the first & second row.

The random number (Rn) which was initiated by the sender is used to perform the underneath operations:

if (Rn< 0.2) then
write ("NoOperation will be performed")
else if (0.2 <Rn< 0.8) then
write ("Apply Crossover operation")
else if (Rn> 0.8) then
write ("Apply Mutation operation")
end
end
end

Replicate steps 2 & 3 for all blocks of the matrix. The original Image which will be in the form of a 256X 256 matrix will be going to generate at the end.

Transmogrify the above matrix into binary Image and again change it to the DNA encoded matrix.

4.3 Decodedrulesof DNA

The decoding rules of DNA are used for converting the matrix of DNA-encoded to (Binary Image) BM after performingDiffusionandPermutation. The selection of decodedRulesarein terms of the 7th and 8th bits of each Pixel inmatrix ofDNA-encoded.

Rules selection	Rules	Binary value	DNA Structure
AA|GA	One	"00110110"	[ATGC]
AT|GT	Two	"00111001"	[ATGC]
AG|GG	Three	"01100011"	[ATGC]
AC|GC	Four	"01101100"	[ATGC]
TA|CA	Five	"10010011"	[ATGC]
TG|CG	Six	"10011100"	[ATGC]
TC|CC	Seven	"11000110"	[ATGC]
TT|CT	Eight	"11001001"	[ATGC]

For example, if ACGT is the pixel value, then by using the last 2 bits GT, we are going to use the Rule_2 is used for converting the DEM into the binary Image.

obtained binary Image (BI) is again transmogrified to the grayscale Image that will give the cipher image. After that, apply Decryption technique with the inverse process of the Selective part of Image encryption algorithm. With this algorithm, the security level will be enhanced for the medical images with all the DNA encodedand decoded rules. So, that we will get the original digital medical image by applying the DNA decoding rules.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 12, December 2022

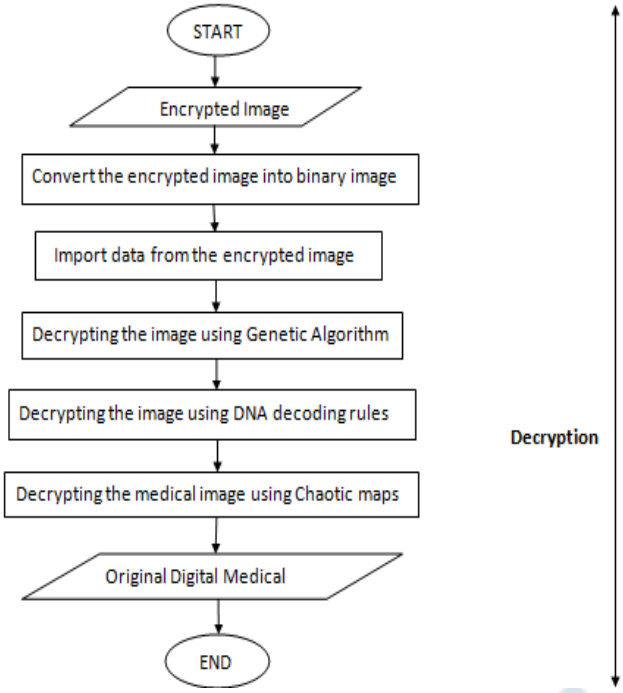


Fig.3. Decryption process.

V. DIFFERENTIAL ATTACK

Attackers will try to study the cipher image for extracting the information related to the plain image in this differential attack. The methods which we used to verify of (DA)differential attacks.

5.1 NPCR&UACI

NPCR&UACI are the main factors that will be used for determining the resistance against pixel change rate in the differential attacks. Attackers try to access the cipher images to get keys and plain medical images while transmitting the digital medical images. In proposed technique, entire Pixel of the Image is altered and obtained encrypted Image is completely different. NPCR is used for calculating the pixel change rate. It is defined as

$$\text{NPCR} = \frac{\sum_{x,y} D_1(x,yn)}{W_1 X H_1} X\ 100\ \%$$

The UACI is defined as

$$\text{UACI} = \frac{1}{w_1 + H_1}\left[\sum_{x,y}\frac{|I_{ee}(x,y) - I_e(x,y)|}{255}\right]$$

where Ieefirst encrypted image

Iesecond encrypted image

5.2 PSNR &MSE

Digital medical images quality will be checked with metrics similar toPSNR andMSE metrics and similarity is measured between original Image and the encrypted Image will be measured by using the MSE. If the value is higher, then it shows less similarity and if it is close to zero then it shows more similarity. The Mean Squared Error technique calculates the average of MSE between original medical Image and encrypted Image 'Ie'.

$$\text{MSE} = \frac{\Sigma_S |I_0(x,y) - I_e(x,y)|^2}{S}$$

where S denotes the size (x×y) of the digital Image.

The PSNR values are used to check whether adding of noise distraction reputation of t Image while transmission. If PSNR value is low indicates well encryption technique. This is shown as

$$\text{PSNR} = 10 \log_{10} \frac{(256-1)}{\text{MSE}}$$

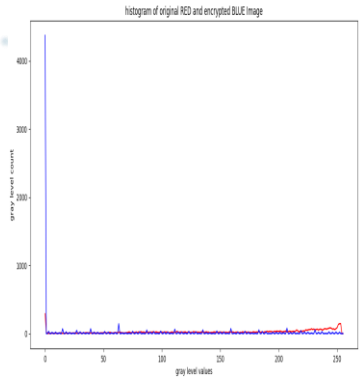
5.3 Entropy

Entropy value is used for measuring the worth of the encryption procedure based on probability spreading of Gray- levels. If the entropy valuesare high representingauniform distribution of Gray _levels and possess respectable confusion value. The entropy is represented as

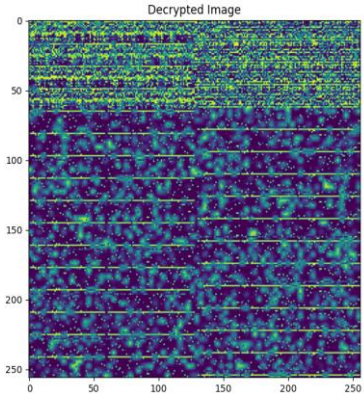
$$H(U) = p(u_i) \log_2 p(u_i)$$

5.4. HistogramAnalysis

Analysis of histogram is graphical spreading of Pixels. By observing histogram, we can say that the pixels distribution in the original medical image is similar to the encrypted medical image. This shows that there is lossless information even after encrypting Images.



(a)



(b)

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 12, December 2022

VI. RESULTS

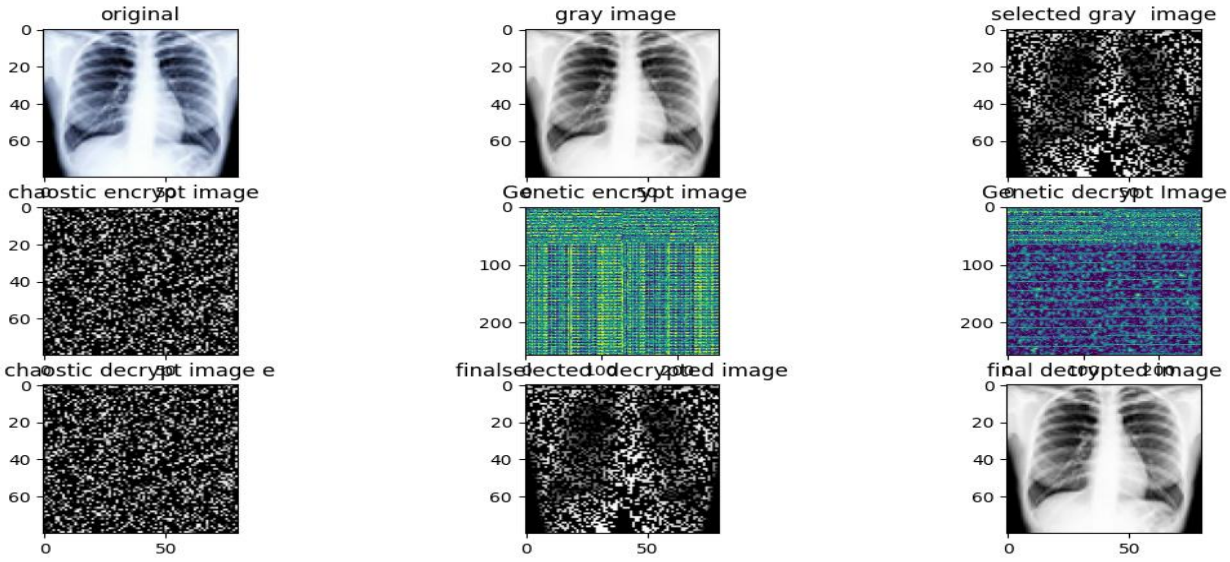


Fig 4.

VII. CONCLUSIONS

This paper describes three level Genetic DNA cryptographic technique. This method encrypts only the selected part of the medical image. so that it reduces the computational time for processing medical images and acquired high security. However fixed length codes are using for four letters of DNA so that it leads to brute force attacks. If variable length and dynamic codes are assigned then more security will be provided against brute force attacks.

REFERENCES

[1]. Prema T. Akkasaligar& Sumangala Biradar (2020) "Selective Medical Image Encryption Using DNA Cryptography", Information Security Journal: A Global Rerspective,29:2,91-101.

[2]. Walid El-Shafai, Fatma Khallaf, El-Sayed M. El-Rabaie, Fathi E. Abd El-Samie. (2021)"Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications". Journal of Ambient Intelligence and Humanized Computing 350.

[3]. K Sudha Kumari, C Nagaraju(2021) " DNA Encrypting rules with Chaotic Maps for Medical Image Encryption " published in 5th International Conference on Intelligent Computing and Control Systems (ICICCS) IEEE pp. 832-837.

[4]. S. Ma, Y. Zhang, Z. Yang, J. Hu, and X. Lei,(2019) ''A new plaintext-related image encryption scheme based on chaotic sequence'', IEEE Access, vol. 7, pp. 30344–30360.

[5]. Jian Wang, (2016)"Digital Image Encryption Algorithm Design Based on Genetic Algorithm", International Journal of Optics, vol. 2016, Article ID 2053724, 14 pages.

[6]. K Sudha Kumari, C Naga Raju(2021)"Medical Image Encryption Technique using DNA Cryptography " published in I-Manager's Journal on Information Technology val.no9 issueno:2.

[7]. X. Wang and H. Zhang(2016). "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," Nonlinear Dyn., vol. 83, no. 1/2, pp. 333–346.

[8]. Vallathan, G, G. Gayathri Devi, and A. Vinoth Kannan (2016) "Enhanced data concealing technique to secure medical image in telemedicine applications," International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE, pp.186- 190.

[9]. C.NagarajuU.Sesadri(2016/9)" Image Segmentation based on Fuzzy Genetic Algorithm" published in International Journal of Engineering and Technology (IJET) volno: 8 issue no:4 pp: 1642-1649.

[10]. L. Liu, Z. Zhang, and R. Chen, (2019) ''Cryptanalysis and improvement in aplaintext-related image encryption scheme based on hyper chaos'' IEEE Access, vol. 7, pp. 126450–126463.

[11]. C. Hun, C. Ruan, and Z. Niu,(2019) ''Image encryption algorithm based on improved logistic mapping,'' Comput. Syst. Appl., vol. 28, no. 6, pp. 125–129.

[12]. C NagaRaju, S NagaMani, G Rakesh Prasad, S Sunitha(2011)"Morphological edge detection algorithm based on multi-structure elements of different directions "published in International Journal of Information and Communication Technology Research valno.1 issueno:1.

[13]. E Suresh Babu, C Naga Raju, Munaga HM Krishna Prasad (2016)"Inspired Pseudo Biotic DNA Based Cryptographic Mechanism Against Adaptive Cryptographic Attacks" published in International Journal of Network Security, Vol.18, No.2, PP.291-303.