An Enhanced Security in Medical Image Encryption Based on Multi-level Chaotic DNA Diffusion

Mousumi Gupta[1,*], Snehashish Bhattacharjee[2], and Biswajoy Chatterjee[2]

[1] Department of Computer Applications, Sikkim Manipal Institute of Technology, Sikkim, India
[2] Department of Computer Science and Engineering, University of Engineering & Management, Kolkata, India;
Email: snehashishbhattacharjee@gmail.com (S.B.); biswajoy.chatterjee@iemcal.com (B.C.)
*Correspondence: mousumi.g@smit.smu.edu.in (M.G.)

***Abstract*—A novel medical image encryption technique has been proposed based on the features of DNA encoding-decoding in combination with Logistic map approach. The approach is proven for encryption of highly sensitive medical images with 100 percent integrity or negligible data loss. Testing is done on both high and low-resolution images. Proposed encryption technique consists of two levels of diffusion using the actual structure of the DNA. In the first level of diffusion process, we have used DNA encoding and decoding operations to generate DNA sequence of each pixel. The originality of the work is to use a long DNA structure stored in a text file stored on both sender and receiver's end to improve the performance of the proposed method. In this initial level of diffusion, DNA sequences are generated for each pixe-land in each of the DNA sequence. Index values are obtained by employing a search operation on the DNA structure. This index values are further modified and ready to be used for next diffusion process. In the second level diffusion, a highly chaotic logistic map is iterated to generate sequences and is employed to extract the chaotic values to form the cipher images. The correlation coefficient analysis, Histogram analysis, Entropy analysis, NPCR, and UACI exhibit significant results. Therefore; the proposed technique can play an important role in the security of low-resolution medical images as well as other visible highly sensitive images.**

***Keywords*—Encryption, DNA, ChaoticMap**

I. Introduction

Smart storage and Transformation of medical images become essential for health care system. From accurate diagnosis of disease to insurance claim, medical images play an important role for each segment. These medical images include X ray, ultrasound, MRI, CT scan etc. and also contain the patient's data. Security and integrity both are required for further use and only the authorized people can have the access. Due to the increasing access of digital devices like smart phones, Tablets etc., accessing of medical data become very easy for the people, but at the same time, any unsecured network or individual devices or server can lead to data breaches. Tempering of any sensitive health care data can be a huge loss for health care organization. Personal health information can be considered as more powerful than credit card information and is valuable for black market. From 2005 to 2009, health care data breach affected around 249.09 million people [1–8].

Many encryption algorithms have already been proposed in literatures for securing medical images. Among these, AES (Advanced Encryption slandered), RSA and DES (Data Encryption standard) are traditional encryption algorithms and is very useful for text but not convenient for Image due to the high correlation among adjacent pixels and large size nature. Among other schemes, chaos theory has been extensively famous in image encryption due to its non-linear nature, high sensitiveness to its initial parameter, optimized time complexity and pseudo randomness. Generally, encryption using chaotic map involves confusion and diffusion technique where confusion refers to Pixels scrambling and diffusion refers to pixels manipulation [9–16].

DNA based encryption technique has attracted many researchers due to its capability in achieving strong encryption effect. The advantage of DNA based encryption technique is its vast storage, high parallelism, minimal power utilization and high information density. Another advantage of DNA encryption is its ability to operate the pixel position and pixel value at the same time. So, as many literatures have already been proposed, combination of DNA based encryption technique with the chaotic map provides a stronger encryption scheme than that of if used individually.

The rest of paper are organized as following. Section II is the literature reviews of the current literatures based on the various methods of the DNA encryption followed by research gaps. In Section III, Level 1 and Level 2 diffusion techniques have been highlighted followed by proposed

Manuscript received December 12, 2022; revised March 24, 2023; accepted April 9, 2023.

doi: 10.18178/joig.11.2.153-160

algorithm. Section IV discusses the results and discussions obtained with statistical analysis and comparison analysis with existing literatures. Finally, performance analysis has been provided in Section V followed by conclusion.

II. Related Work

A. DNA Encryption

Over the years, DNA encryption in combination of chaotic maps becomes a promising technique in image encryption in terms of security and performance. In existing literatures, chaotic maps are used in position scrambling and DNA sequences are used to diffuse the pixel values.

B. Dynamic DNA Coding

Cun and Tong *et al.* [17] have surveyed the different security indicators and encryption and decryption rates of dynamic DNA coding in the field of picture encryption, a selective image encryption approach based on chaotic map and dynamic DNA coding is proposed. The author uses a one-dimensional chaos map with a high Lyapunov exponent and excellent dynamic behavior, improves the local graph structure algorithm to improve image region selection, and uses a constructed chaos map to create a pseudo-random sequence. Generates and dynamically encodes and manipulates selected DNA regions to finally produce a fully encrypted image.

Similarly, Walid *et al.* [18] provide an efficient medical image security cryptosystem based on the advantages of deoxyribonucleic acid (DNA) rules and chaotic maps. A logistic chaos map, a Piecewise Linear Chaotic Map (PWLCM), and DNA encoding are used in the design of the proposed medical image cryptosystem. A secret key image is generated using PWLCM and by employing DNA rules, both the secret image and the input plain image are encoded. Finally, the proposed logistic map is used to obtain the ciphered image.

C. DNA with SHA-2

In 2021, Ramzi *et al.* [19] have proposed a novel medical image encryption algorithm on a hybrid model of deoxyribonucleic acid (DNA) masking, a Secure Hash Algorithm SHA-2 and a new hybrid chaotic map. The research includes the manipulations of DNA sequences to reinforce the cryptosystem. Chaotic hybrid map along with DNA computing is used causing extensive benefits like improved information entropy, randomness and resistance to various typical attacks like plain text and cyber text attacks.

D. DNA with LDCML

In 2021, Xingyuan *et al.* [20] have proposed Logistic-Dynamics Coupled Map Lattices (LDCML) which is combined with DNA coding to form the cryptosystem. LDCML forms the chaotic sequence to carry out initial scrambling on the original image. The resulting image is converted to DNA matrix using specified rule and further diffusion is carried out to create the cipher image.

E. DNA with hyper-Chaotic System

In 2020, Yu-Guang *et al.* [21] address the limitations of the existing compressive sensing algorithms and propose a new algorithm based on fractional hyper-chaotic system and DNA approach. The proposed scheme is a multi-order image compression providing good confusion performances for the encrypted images. In another study, Rania *et al.* [22] reported the issues while utilizing low dimensional map in cryptosystem. The design includes DNA and binaries chaotic cores and has the ability to withstand known attacks. Similarly, Yuanyuan *et al.* [23], proposed a framework to provide solution over poor performance exhibiting by the single chaotic system. The authors have proposed a new 4-D hyperchaotic system with better unpredictability and larger key space and have the ability in resisting plaintext attacks and statistical attacks. Studies in 2021, Pooja and Chiranjeev *et al.* [24] propose a novel technique to remove the algorithmic imperfections of the existing literatures. The authors have proposed a unique encryption technique of masking the images before encryption. The technique is used in both natural and medical images and is experimented against differential, occlusion, and noise attacks. In 2021, in the literature, Abhishek *et al.* [25] have proposed DNA based Encryption with searchable indexing strategy along with fuzzy based cryptosystem to improve security in cloud storage server. Another study, Prabir *et al.* [26] presented a secured encryption strategy to address the security risks retained in low dimensional chaotic maps. The authors have formulated a cryptosystem using permutation and diffusion strategy using 2-D sine logistic map with different initial parameters. The study in Mousomi *et al.* [27] addressed the issues of computational overhead of the existing algorithms and proposed a cryptosystem based on DNA and chaos theory. Shubha *et al.* [28] used the technique of dynamic generation of key streams and use two level scrambling based medical image encryption techniques to overcome issues of plain text attack. In the literature, Jun et *al.* [29] addressed the issues of the resistance of the chosen plain text attack and adopted the techniques of random number embedding and DNA level self-adaptive permutation and diffusion.

F. Research Gaps

Although lots of researches have been carried out in DNA computing, there lies lot of scopes to remove the imperfections of the existing techniques. We mainly categorize the below issues faced by the recent researches. Single chaotic system is easy to implement but security issues are still there and most of the time not ready for real-time uses. Traditional scrambling technique is used for most of the algorithms. Original image can be restored by performing certain number of iterations which can be a potential risk for the algorithms. These risks can be reduced by utilizing more properties of the DNA structure. In most of the literatures, different type of images has not been presented such that Images with high correlation need to be considered for security analysis along with the detailed statistical analysis for testing the performance of the cryptosystem.

Based on the above discussion, we develop a novel image encryption technique, a different from the traditional encryption strategy based on the features of DNA encoding and decoding strategy in combination with Logistic map approach. In this technique, we have used the actual structure of the DNA and hence utilizing DNA properties. We can encrypt highly sensitive Image while taking into account with 100 percent integrity or negligible data loss. The main focus of our work is to implement a cryptosystem exhibiting high security which can resists both plaintext and cipher text attacks. Our encryption technique consists of two levels diffusion result a completely different cipher text image. In level one diffusion process, we have used DNA encoding and decoding operations to generate DNA sequence of each pixel. The originality of the work is to use a long DNA structure stored in a text file to improve performance of the proposed method. The indexing values obtained by employing a search operation on the DNA structure for each of the DNA sequences. The indexing values are further modified and ready to be used for the further diffusion process. In Level 2 diffusion, a logistic map is iterated to generate sequences. These sequences of values are mapped with the values generated in the Level 1 diffusion process. The experimental results show the performance of the proposed technique.

III. Porposed Modelling

The architecture of the flow diagram has been proposed in the Fig. 1. The proposed scheme is divided into mainly three parts. Firstly, each pixel is converted to DNA sequences. At the second stage, the DNA sequences are further diffused to gain more complexity and at this stage of encryption a DNA structure is used to search the index of the input DNA sequences in the DNA structure. Finally, a chaotic map is used to generate the chaotic sequences which are further used for Level-2 diffusion.

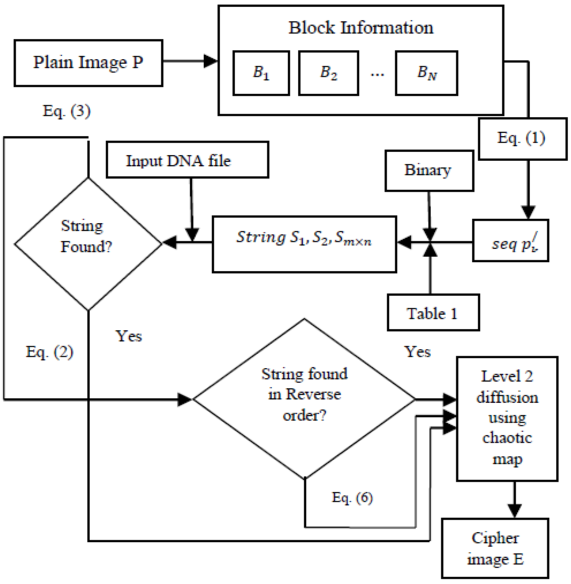


Figure 1. Detail flowchart of the DNA operations.

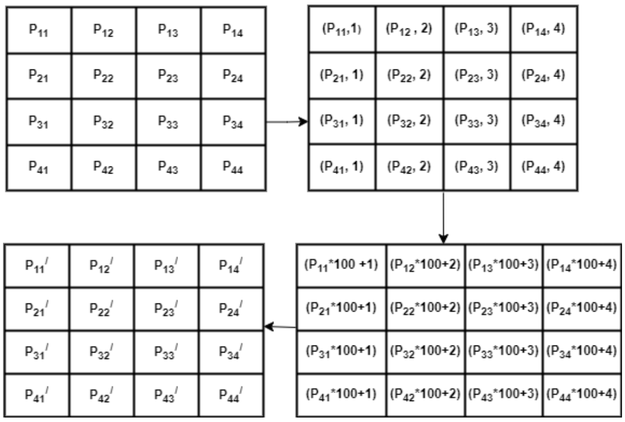
A. Operations on DNA Sequences

All In this paper, we encode the image pixels by using DNA sequence. DNA sequence contains four nucleic acid A (Adenine), T (Thymine), G (Guanine) and C (Cytosine). In our proposed model, based on the DNA rule, for each pixel, a corresponding DNA string is obtained by using the proposed model. The whole image is divided into n 8 × 8 sub matrix.

For each pixel in the sub matrix, our system returns corresponding sequence in the form

$$P_k^{/} = P_k \times 100 + Pos_k \quad (1)$$

For example, if the channel intensity of the pixel is 120_{10} which is in the first position of the matrix, then the corresponding modified pixel value is $P_k^{/}$ = 120 × 100 +1 = 12001= 10111011100001_2. Thus, the corresponding DNA sequence using Rule 4 described in Table I is GAGAGTC. So, for each sub matrix, a modified set of values for the corresponding pixels are generated which hold uniqueness for each sub-matrix. The advantage of position mapping with each pixel value is to retrieve the original pixel value at the receiver end during the process of decryption. Keeping the importance of the integrity of information of the medical images, each step of the encryption procedure should lead to zero data loss during decryption. The initial set of operations on the input pixels are captured in Fig. 2. It can be seen that for each input pixel, we can get a modified pixel value which is quite different from the original pixel value.



P_{11}	P_{12}	P_{13}	P_{14}
P_{21}	P_{22}	P_{23}	P_{24}
P_{31}	P_{32}	P_{33}	P_{34}
P_{41}	P_{42}	P_{43}	P_{44}

$(P_{11},1)$	$(P_{12}, 2)$	$(P_{13}, 3)$	$(P_{14}, 4)$
$(P_{21}, 1)$	$(P_{22}, 2)$	$(P_{23}, 3)$	$(P_{24}, 4)$
$(P_{31}, 1)$	$(P_{32}, 2)$	$(P_{33}, 3)$	$(P_{34}, 4)$
$(P_{41}, 1)$	$(P_{42}, 2)$	$(P_{43}, 3)$	$(P_{44}, 4)$

$(P_{11}*100 +1)$	$(P_{12}*100+2)$	$(P_{13}*100+3)$	$(P_{14}*100+4)$
$(P_{21}*100+1)$	$(P_{22}*100+2)$	$(P_{23}*100+3)$	$(P_{24}*100+4)$
$(P_{31}*100+1)$	$(P_{32}*100+2)$	$(P_{33}*100+3)$	$(P_{34}*100+4)$
$(P_{41}*100+1)$	$(P_{42}*100+2)$	$(P_{43}*100+3)$	$(P_{44}*100+4)$

$P_{11}^{/}$	$P_{12}^{/}$	$P_{13}^{/}$	$P_{14}^{/}$
$P_{21}^{/}$	$P_{22}^{/}$	$P_{23}^{/}$	$P_{24}^{/}$
$P_{31}^{/}$	$P_{32}^{/}$	$P_{33}^{/}$	$P_{34}^{/}$
$P_{41}^{/}$	$P_{42}^{/}$	$P_{43}^{/}$	$P_{44}^{/}$

Figure 2. Operations of DNA sequence.

TABLE I: DNA Coding Rules for Encoding and Decoding

Rule No	A	T	G	C
Rule 1	00	11	10	01
Rule 2	00	11	01	10
Rule 3	11	00	01	10
Rule 4	11	00	10	01
Rule 5	10	01	01	10
Rule 6	10	01	10	01
Rule 7	01	10	11	00
Rule 8	01	10	01	11

B. String search Operations

Once the DNA sequence is generated, the corresponding sequence is searched in the DNA file. Let the strings ($S_1, S_2, S_3, \ldots, S_{m\times n}$) obtained for each pixels $P_1, P_2, P_3, \ldots P_{m\times n}$. These strings are further searched in DNA file to obtain the string position.

E.g., for the pixel P_i , the corresponding string is S_i searched from the DNA structure and the position obtained is (Pos_j, Pos_i).

So for each pixel P_i, the new value Val_i obtained from the below Eq. (2):

$$Val_i^{/} = Pos_j \times 10 + Pos_j - Pos_i \qquad (2)$$

Here Pos_j is the start position and Pos_i is the end position of the string $S_i$over the DNA structure. This step will generate unique value for each input value to compute. Suppose the input string is 'ATGGCA' and it is searched over the DNA structure and it is found to be in the position 1200 in the DNA structure. So, the changed value will be in this case 1200×10+(1206−1200) = 12006.

If the corresponding string is not found in the DNA file, the string is searched in the DNA file again in the reverse order

$$Val_i^{/} = Pos_j \times 10 + Pos_j - Pos_i + \text{Length (DNA)} \qquad (3)$$

where 'Length (DNA)' refers the length of the DNA structure which is used in the DNA computation. This step provides more complexity on the algorithm and also very difficult to guess, e.g., suppose the input string is 'ATGGCAG' which is not found when the search operation has been accomplished in forward order over the DNA structure of length (1,500,000). Then the same string will be searched in the reverse order and found in the position 1200.So the changed value will be in this case 1200 × 10 + (1206−1200) + 1,500,000 = 1,512,006. So during the decryption at receiver end any value greater than 1,500,000, the search operation of the DNA structure needs to be carried out in the reverse order to get our desired string.

If still the corresponding string is not found in both of the above cases, the value is replaced by

$$Pos_{k-1} = P_k \qquad (4)$$

$$Pos_k = 2 \times \text{Length (DNA)} + k \qquad (5)$$

$$Val_k = Pos_{k-1} \times 10 + (Pos_k - Pos_{k-1}) \qquad (6)$$

In this case suppose the initial position of the string of the kth pixel is Pos_{k-1} which is replaced by the actual position of the pixel. The final position Pos_k is replaced by 2 × Length (DNA) + *k*. So, if the position of the input string 'GTAGTTA' is 1200, the initial position becomes as 1200 and the final position will be 2 × 1,500,000+7=1,500,007. During the decryption any value greater than 2 × Length (DNA) will be considered as the string which is not found in the DNA structure.

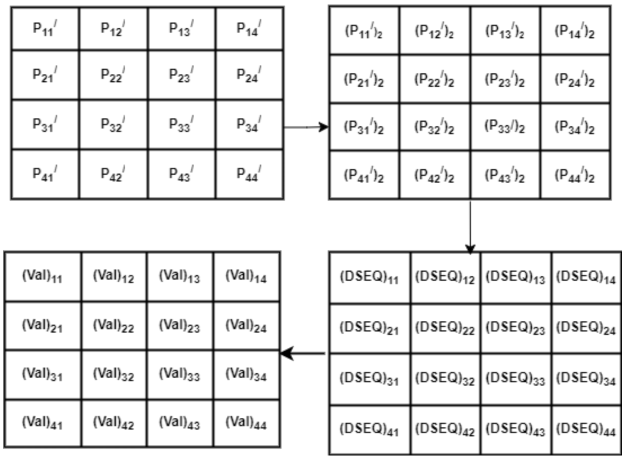

$P_{11}^{/}$ $P_{12}^{/}$ $P_{13}^{/}$ $P_{14}^{/}$
$P_{21}^{/}$ $P_{22}^{/}$ $P_{23}^{/}$ $P_{24}^{/}$
$P_{31}^{/}$ $P_{32}^{/}$ $P_{33}^{/}$ $P_{34}^{/}$
$P_{41}^{/}$ $P_{42}^{/}$ $P_{43}^{/}$ $P_{44}^{/}$
$(P_{11}^{/})_2$ $(P_{12}^{/})_2$ $(P_{13}^{/})_2$ $(P_{14}^{/})_2$
$(P_{21}^{/})_2$ $(P_{22}^{/})_2$ $(P_{23}^{/})_2$ $(P_{24}^{/})_2$
$(P_{31}^{/})_2$ $(P_{32}^{/})_2$ $(P_{33}^{/})_2$ $(P_{34}^{/})_2$
$(P_{41}^{/})_2$ $(P_{42}^{/})_2$ $(P_{43}^{/})_2$ $(P_{44}^{/})_2$
$(DSEQ)_{11}$ $(DSEQ)_{12}$ $(DSEQ)_{13}$ $(DSEQ)_{14}$
$(DSEQ)_{21}$ $(DSEQ)_{22}$ $(DSEQ)_{23}$ $(DSEQ)_{24}$
$(DSEQ)_{31}$ $(DSEQ)_{32}$ $(DSEQ)_{33}$ $(DSEQ)_{34}$
$(DSEQ)_{41}$ $(DSEQ)_{42}$ $(DSEQ)_{43}$ $(DSEQ)_{44}$
$(Val)_{11}$ $(Val)_{12}$ $(Val)_{13}$ $(Val)_{14}$
$(Val)_{21}$ $(Val)_{22}$ $(Val)_{23}$ $(Val)_{24}$
$(Val)_{31}$ $(Val)_{32}$ $(Val)_{33}$ $(Val)_{34}$
$(Val)_{41}$ $(Val)_{42}$ $(Val)_{43}$ $(Val)_{44}$

Figure 3. String search operations.

So, the level 1 diffusion value is obtained from any of the Eqs. (2), (3) or (6). The set of operations are depicted in Fig. 3. The steps in the Level 1 diffusion consist of simple mathematical calculations but will provide more security in the technique. The value generated by the above equations is completely different from the initial pixel values. So, it is very difficult for the hackers to extract the original information and hence the information will be secured from the ciphertext attack.

C. Diffusion Using Chaotic Map

The diffusion is performed by modifying or changing each pixel value for the specified image. In this Level 2 diffusion, we have generated the sequences of the chaotic model defined in Eq. (7). The values generated in the Level 1 diffusion are modified using the chaotic sequence generated by the logistic map.

$$x_{j+1} = 3.999 \times x_j \times (1 - x_j), j = 0, 1, 2\ldots \qquad (7)$$

The initial value x_0 can be calculated by the steps defined in Initial Parameter generation section.

The set of operations performed in this step is shown in the Fig. 4.

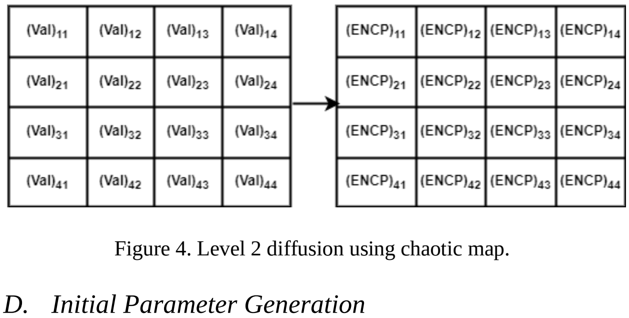

$(Val)_{11}$ $(Val)_{12}$ $(Val)_{13}$ $(Val)_{14}$
$(Val)_{21}$ $(Val)_{22}$ $(Val)_{23}$ $(Val)_{24}$
$(Val)_{31}$ $(Val)_{32}$ $(Val)_{33}$ $(Val)_{34}$
$(Val)_{41}$ $(Val)_{42}$ $(Val)_{43}$ $(Val)_{44}$
$(ENCP)_{11}$ $(ENCP)_{12}$ $(ENCP)_{13}$ $(ENCP)_{14}$
$(ENCP)_{21}$ $(ENCP)_{22}$ $(ENCP)_{23}$ $(ENCP)_{24}$
$(ENCP)_{31}$ $(ENCP)_{32}$ $(ENCP)_{33}$ $(ENCP)_{34}$
$(ENCP)_{41}$ $(ENCP)_{42}$ $(ENCP)_{43}$ $(ENCP)_{44}$

Figure 4. Level 2 diffusion using chaotic map.

D. Initial Parameter Generation

The sender sends a 256-bit random binary key which is of the form ($K_1, K_2, \ldots, K_{256}$). The key is subdivided in to 32 groups each containing 8 bits.

Let $G = G_1, G_2, \ldots, G_{32}$ where $G_1 = K_1, K_2, K_3, \ldots, K_8$, $G_2 = K_9, K_{10}, K_{11}, \ldots, K_{16}$, $G_{32} = K_{248}, K_{249}, K_{250}, \ldots, K_{256}$ be the groups. Now forming $G_1^{'}, G_2^{'}, G_3^{'}, \ldots, G_8^{'}$ be the eight groups in the following way.

$$G_1^{'} = (G_1 \oplus G_2) \oplus (G_3 \oplus G_4)$$

$$G_2^{'} = (G_5 \oplus G_6) \oplus (G_7 \oplus G_8)$$

$$G_3^{'} = (G_9 \oplus G_{10}) \oplus (G_{11} \oplus G_{12})$$

$$G_4^{'} = (G_{13} \oplus G_{14}) \oplus (G_{15} \oplus G_{16})$$

$$G_5^{'} = (G_{17} \oplus G_{18}) \oplus (G_{19} \oplus G_{20})$$

$$G_6^{'} = (G_{21} \oplus G_{22}) \oplus (G_{23} \oplus G_{24})$$

$$G_7^{'} = (G_{25} \oplus G_{26}) \oplus (G_{27} \oplus G_{28})$$

$$G_8^{'} = (G_{29} \oplus G_{30}) \oplus (G_{31} \oplus G_{32})$$

Each $G_i^{'}$ is an 8-bit binary code. The initial parameter x_0 is calculated by the below equation

$$x_0 = \frac{\sum_{i=1}^{8} G_i^{'}}{2^{32}} \tag{8}$$

E. Algorithm

Step 1: The original medical image P having size $M \times N$ is firstly subdivided into n parts. So $(M \times N)/n$ numbers of sub blocks have been created, where n < 100.

Step 2: For each sub matrix, using Eq. (1), each pixel value P_i is encoded and a sequence is generated $(P_1, P_2, \dots, P_{M\times N})$. From Eq. (1), we must find a modified pixel value for each sub-matrix.

Step 3: This step includes generation of binary number. The decimal number of each pixel is changed to binary numbers (0s and 1s) $(B_1, B_2, \dots, B_{M\times N})$ where B_i = Binary (P_i).

Step 4: The binary numbers of each sequence is broken into pairs like 00, 01, 10, 11. Each pair is substituted by the nucleotide by choosing any rule as mentioned in Table I. Let the sequence generated be $(S_1, S_2, S_3, \dots, \mathrm{S}_{\mathrm{M\times N}})$

Step 5: For each string ($S_1, S_2, S_3, \dots, S_{M\times N}$) the corresponding value obtained after diffusion by Eqs. (3), (4) and (6) is $(V_1, V_2, V_3, \dots, V_{M\times N})$

Step 6: The Level 1 diffusion values $(V_1, V_2, V_3, \dots, V_{M\times N})$ obtained in step 5 are further defused by Iterating the logistic map. The values generated in the Level 1 diffusion are modified using the chaotic sequence generated by the logistic map.

IV. Results And Discussions

In this section, we have experimented with more than 100 images easily available in the public database [30]. We have considered both standard images and the medical images for experiment. The testing images include medical images with high correlation and standard images having high resolution.

A. Correlation Coefficient

The degree of correlation among the pixels is measured using the metric Correlation coefficient analysis. Mathematically, correlation coefficient is given by

$$\boldsymbol{C_r} = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{(N\sum_{j=1}^{N} x_j^2 - (\sum_{j=1}^{N} x_j)^2 \times (N\sum_{j=1}^{N} y_j^2 - (\sum_{j=1}^{N} y_j)^2}} \tag{9}$$

where *N* is the total number of pixels whereas, x and y are pixel intensity values of two adjacent pixels intensities.

Table II lists the correlation among the medical images in horizontal, vertical and in diagonal pixels for medical Image. From the values listed in the table, it is noticed that the proposed technique exhibits low correlation values which implies high security and robustness from the various type of attacks. In Table II, we have calculated the correlation coefficients for the natural images in all the directions. We note that the correlation coefficients for the source images are close to 1; this indicates that the pixels are highly correlated. However, encrypted images correlation coefficients are close to 0. These results indicate that there is no correlation between the source and encrypted images. So, we have no similarity between the source and encrypted images.

TABLE II. Correlation Coefficients, NPCR, UACI of Medical Images

Name	Directions	Image 1	Image 2	Image 3	Image 4	Image 5
Correlation	Horizontal	0.00025	0.00032	0.00021	0.00053	0.00026
	Vertical	0.00014	0.00056	0.00012	0.00064	0.00027
	Diagonal	0.00087	0.00058	0.00047	0.00041	0.00018
NPCR	NA	99.5643	99.5223	99.3344	99.1232	99.5333
UACI	NA	0.3322	0.3316	0.3324	0.3334	0.3333

We concluded that in all directions (horizontal, diagonal and vertical), the correlation coefficients between two adjacent pixels, and in all presented schemes are close to 0.

B. Gray Histogram Analysis

The gray histogram depicts the frequency of each grey level in a digital image, as well as the grey value distribution. It can indicate the number of pixels that belong to each grey level as well as the frequency with which each gray level occurs. It is worth mentioning that most of the plain images exhibits non uniform histogram [27]. The proposed algorithm when applied to the meaningful images provides an equally distributed gray level intensity. Fig. 5 shows the histograms for the original images (b1–b5) and the corresponding cipher images (e1–e5). It is evident that the histograms of the cipher images are uniformly distributed over all the intensity levels and exhibits complete difference from the histograms of the original images. Consequently, it is highly challenging to decipher the information in the cipher text image. Thus, we can secure the patient's medical data from any Plaintext and ciphertext attack.

C. Entropy Analysis

Information Entropy provides the randomness. For a good ciphering technique, a higher entropy is desired. So, when the histogram is well distributed, larger entropy can be found [15]. Mathematically, Entropy can be written as

$$H(S) = \sum_{i=1}^{N} P(x_i) log_2(1/P(x_i)) \quad (10)$$

where $P\ (x_i)$ is the probability of occurrences on N symbols of the source. The limit of entropy is given by Shanon [24] where the value of $H(S)$ should lie in the interval $[0, \log N_2]$. The entropy value obtained for the medical image is shown in the Table IV. It can be seen that the entropy for the plain image is around 7.1 and that for the cipher image is around 7.9. The ideal value of the entropy of the gray scale image is 8 [31]. Table V presents the entropy for the natural images and it is evident from the result that the entropy is very close to the ideal value.

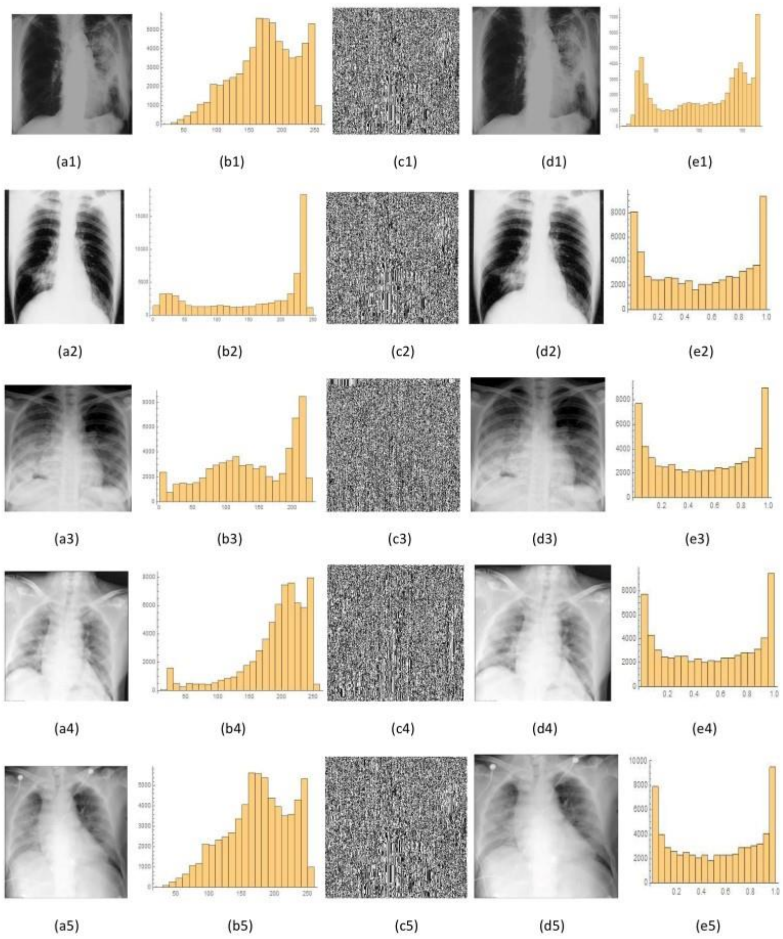


Figure 5. (a1)–(a5) input X-ray images; (b1)–(b5) image histogram of the input images; (c1)–(c5) cipher images, (d1)–(d5) decrypted images; (e1)–(e5) image histogram of the cipher images.

TABLE III. CORRELATION COEFFICIENTS, NPCR, UACI OF NATURAL IMAGES

Name	Directions	Leena	Peppers	Baboon	Lake	Barbara
Correlation	Horizontal	0.00001	0.00053	0.00043	0.00032	0.00034
	Vertical	0.00002	0.00058	0.00087	0.00089	0.00054
	Diagonal	0.00005	0.00005	0.00009	0.00028	0.00058
NPCR	NA	99.6565	99.6765	99.6685	99.6465	99.6468
UACI	NA	0.3374	0.3348	0.3378	0.3371	0.3364

TABLE IV. ENTROPY ANALYSIS FOR THE MEDICAL IMAGES

Images	a1	a2	a3	a4	a5
Plain Image	6.2134	6.7251	7.1023	7.2056	6.6543
Cipher Image	7.9921	7.9956	7.9943	7.9954	7.9987

TABLE V. ENTROPY ANALYSIS FOR THE NATURAL IMAGES

Name	Leena	Peppers	Baboon	Lake	Barbara
Plain Image	6.5127	6.2777	6.7657	6.3452	7.1023
Cipher Image	7.9966	7.9875	7.9952	7.9975	7.9935

TABLE VI. ENTROPY ANALYSIS OF THE PROPOSED SCHEME AND WITH THE OTHER SCHEMES

Proposed scheme	Yuanyuan *et al.* [23]	Prabir *et al.* [26]	Yang *et al.* [21]	Chiranjeev *et al.* [24]	Ramzi *et al.* [19]
7.9985	7.9976	7.9875	7.9976	7.9980	7.9972

Table VI presents the entropy value of the proposed algorithm for the Leena image and other schemes. It can be evident from the result that entropy value obtained by our proposed scheme is 7.9985 which is better than the references.

D. NPCR and UACI

The Number of Pixel Change Rates (NPCR) and Uniform average intensity change are one of the two measures to judge the anti-differential attack [32]. These two measures can detect the efficiency of the encryption technique. Mathematically NPCR and UACI can be expressed as

$$\mathrm{NPCR} = \frac{\sum_{i,j} \mathrm{D}[i,j]}{\mathrm{W} \times \mathrm{H}} \times 100$$

$$\mathrm{UACI} = \sum \frac{\mathrm{CP}_1(i,j) - \mathrm{CP}_2(i,j)}{\mathrm{W} \times \mathrm{H} \times 255}$$

where $CP_1(i,j)$ is the cyphertext image and $CP_2(i,j)$ is the cyphertext image after changing one pixel.

E. Performance Analysis

The speed is an important factor of any encryption algorithm. An algorithm provides high security but also has high execution time has no practical use. In ideal case, an algorithm should provide high security, low time complexity and also should be light weighted so that that it can be executed in low precision devices. Our proposed algorithm is computed in the machine with following software and hardware specifications: Windows 10 (64 bit) operating system is chosen with Wolfram Mathematica 11 kernel. Intel (R) Pentium (R) CPU @3.80 GHz with RAM of 8 GB Memory. We have computed the encryption time which is illustrated in the Table 7 for various input images. The time complexity is also plotted in a line graph for better visualization and captured in the figure 6. It can be seen that the average speed of the images having dimension 56×56 is approximately 0.5 minutes. For the images having sizes 112×112, 256×256 and 512×512 are approximately 1.02, 2. Three minutes respectively.

TABLE VII. Time Analysis for the Medical Images

Image Name	Image Size	Time Taken (in minutes)
a1	56 × 56 112 × 112 256 × 256 512 × 512	0.56 1.05 1.98 3.05
a2	56 × 56 112 × 112 256 × 256 512 × 512	0.61 1.09 1.97 3.36
a3	56 × 56 112 × 112 256 × 256 512 × 512	0.62 1.26 1.95 3.25
a4	56 × 56 112 × 112 256 × 256 512 × 512	0.71 1.05 1.98 3.1
a5	56 × 56 112 × 112 256 × 256 512 × 512	0.81 1.26 1.98 3.26

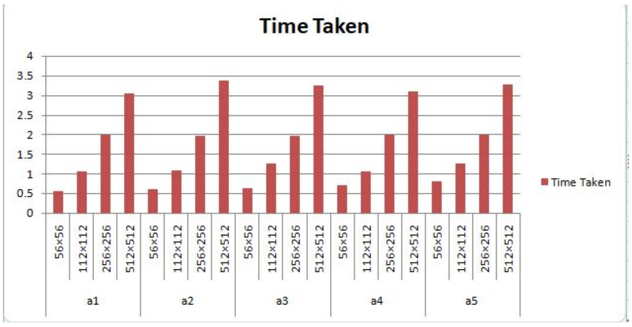


Figure 6. Performance analysis of the encryption technique based on sizes of the images.

V. Conclusion

A novel encryption algorithm based on the DNA properties and the logistic map is proposed. Our encryption technique consists of two levels diffusion results a complete different ciphertext image. In level one diffusion process, we have used DNA encoding and decoding operations to generate DNA sequence of each pixel. The originality of the work is to use a long DNA structure stored in a text file to provide more complexity of the proposed method. The different test like correlation coefficient analysis, NPCR, UACI, histogram analysis and Entropy analysis are performed and the result show that the algorithm is very powerful against plain-text and the cyphertext attack.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

SB wrote the manuscript. MG, SB and BC involve in study design and performed the experiment. All authors have gone through the manuscript and approved the submitted version.

References

[1] K. Fares, K. Amine, and E. Salah, "A robust blind color image watermarking based on Fourier transform domain." *Optik*, vol. 208, 164562, 2020.

[2] A. J. Paul, "Recent advances in selective image encryption and its indispensability due to Covid-19," in *Proc. 2020 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, 2020, pp. 201–206.

[3] R. Gupta, "Elliptic curve cryptography based secure image transmission in clustered wireless sensor networks," *International Journal of Computer Networks and Applications*, vol. 8, no. 1, pp. 67–78, 2021.

[4] S. S. Tyagi, "Enhancing security of cloud data through encryption with AES and fernet algorithm through Convolutional-Neural-Networks (CNN)," *International Journal of Computer Networks and Applications*, vol. 8, no. 4, 288–299, 2021.

[5] R. Denis and P. Madhubala, "Evolutionary computing assisted visually-imperceptible hybrid cryptography and steganography model for secure data communication over cloud environment," *International Journal of Computer Networks and Applications (IJCNA)*, vol. 7, no. 6, pp. 208–230, 2020.

[6] O. Reyad and M. E. Karar, "Secure CT-image encryption for COVID-19 infections using HBBS-based multiple key-streams," *Arabian Journal for Science and Engineering*, vol. 46, no. 4, pp. 3581–3593, 2021.

[7] G. D. Zhang, W. K. Ding, and L. Li, "Image encryption algorithm based on tent delay-sine cascade with logistic map," *Symmetry*, vol. 12, no. 3, p. 355, 2020.

[8] J. Thiyagarajan, B. Murugan, and N. G. A. Gounden, "A chaotic image encryption scheme with complex diffusion matrix for plain image sensitivity," *Serbian Journal of Electrical Engineering*, vol. 16, no. 2, pp. 247–265, 2019.

[9] H. Y. Xiang and L. F. Liu, "An improved digital logistic map and its application in image encryption," *Multimedia Tools and Applications*, vol. 79, no. 41, pp. 30329–30355, 2020.

[10] Z. J. Liu, L. Xu, T. Liu, H. Chen, P. F. Li, C. Lin, and S. T. Liu, "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," *Optics Communications*, vol. 284, no. 1, pp. 123–128, 2011.

[11] R. Z. Li, Q. Liu, and L. F. Liu, "Novel image encryption algorithm based on improved logistic map," *IET Image Processing*, vol. 13, no. 1, pp. 125–134, 2019.

[12] C. H. Li, G. C. Luo, K. Qin, and C. B. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[13] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, F. Masood, F. Khan, and W. J. Buchanan, "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8 pp. 140876–140895, 2020.

[14] L. Teng, X. Y. Wang, and J. Meng, "A chaotic color image encryption using integrated bit-level permutation," *Multimedia Tools and Applications*, vol. 77, no. 6, pp. 6883–6896, 2018.

[15] A. Jolfaei and A. Mirghadri, "Image encryption using chaos and block cipher," *Computer and Information Science*, vol. 4, no. 1, p. 172, 2011.

[16] Y. Zhang, C. Q. Li, Q. Li, D. Zhang, and S. Shu, "Breaking a chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 69, no. 3, pp. 1091–1096, 2012.

[17] Q. Q. Cun, X. J. Tong, Z. Wang, and M. Zhang, "Selective image encryption method based on dynamic DNA coding and new chaotic map," *Optik*, vol. 243, 167286, 2021.

[18] W. El-Shafai, F. Khallaf, E.-S. M. El-Rabaie, and F. E. A. El-Samie. "Robust medical image encryption based on DNA—Chaos cryptosystem for secure telemedicine and healthcare applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 10, pp. 9007–9035, 2021.

[19] Guesmi, Ramzi, and M. A. Farah. "A new efficient medical image cipher based on hybrid chaotic map and DNA code," *Multimedia Tools and Applications*, vol. 80, no. 2, pp. 1925–1944, 2021.

[20] X. Y. Wang, W. H. Xue, and J. B. An, "Image encryption algorithm based on LDCML and DNA coding sequence," *Multimedia Tools and Applications*, vol. 80, no. 1, pp. 591–614, 2021.

[21] Y.-G. Yang, B.-W. Guan, Y.-H. Zhou, and W.-M. Shi, "Double image compression-encryption algorithm based on fractional order hyper chaotic system and DNA approach," *Multimedia Tools and Applications*, vol. 80, no. 1, pp. 691–710, 2021.

[22] R. A. Elmanfaloty, A. M. Alnajim, and EhabAbou-Bakr, "A finite precision implementation of an image encryption scheme based on DNA encoding and binarized chaotic cores," *IEEE Access*, vol. 9, pp. 136905-136916, 2021.

[23] Y.-Y. Hui, H. Liu, and P.-F. Fang, "A DNA image encryption based on a new hyperchaotic system," *Multimedia Tools and Applications*, pp. 1–25, 2021.

[24] P. Mishra, C. Bhaya, A. K. Pal, and A. K. Singh, "A medical image cryptosystem using bit-level diffusion with DNA coding," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–22, 2021.

[25] A. Majumdar, A. Biswas, A. Majumder, S. K. Sood, and K. L. Baishnab, "A novel DNA-inspired encryption strategy for concealing cloud storage," *Frontiers of Computer Science*, vol. 15, no. 3, pp. 1–18, 2021.

[26] P. K. Naskar, S. Bhattacharyya, K. C. Mahatab, K. G. Dhal, and A. Chaudhuri, "An efficient block-level image encryption scheme based on multi-chaotic maps with DNA encoding," *Nonlinear Dynamics*, vol. 105, no. 4, pp. 3673–3698, 2021.

[27] M. Roy, S. Chakraborty, K. Mali, D. Roy, and S. Chatterjee, "A robust image encryption framework based on DNA computing and chaotic environment," *Microsystem Technologies*, vol. 27, no. 10, pp. 3617–3627, 2021.

[28] S. Pankaj and M. Dua, "A novel ToCC map and two-level scrambling-based medical image encryption technique," *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 10, no. 1, pp. 1–19, 2021.

[29] J. Wang, X.-C. Zhi, X.-L. Chai, and Y. Lu, "Chaos-based image encryption strategy based on random number embedding and DNA-level self-adaptive permutation and diffusion," *Multimedia Tools and Applications*, vol. 80, no. 10, pp. 16087–16122, 2021.

[30] J. P. Cohen, P. Morrison, L. Dao, K. Roth, T. Q. Duong, and M. Ghassemi, "Covid-19 image data collection: Prospective predictions are the future," arXiv preprint arXiv:2006.11988, 2020.

[31] N. Iqbal, R. A. Naqvi, M. Atif, M. A. Khan, M. Hanif, S. Abbas, and D. Hussain, "On the image encryption algorithm based on the chaotic system, DNA encoding, and castle," *IEEE Access*, vol. 9, pp. 118253–118270, 2021.

[32] X. P. Yan, X. Y. Wang, and Y. J. Xian, "Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10949–10983, 2021.