ISSN: 2229-6956 (ONLINE)
DOI: 10.21917/ijsc.2023.0418
SPECIAL ISSUE ON INNOVATIONS AND INTELLIGENCE FOR COMPUTING AND TECHNOLOGIES (IICT-2023)

DESIGN AND ANALYSIS OF DNA BASED CIPHER FOR IMAGE USING DUAL CHAOTIC MAP

Ajit Singh and Bijendra Singh
Department of Computer Science Engineering, Baba Mastnath University, India

Abstract

Design and analysis of an image encryption technique using DNA computation and chaos function has been emphasized in the present paper. The plain image was scrambled using Henon map followed by the implementation of a DNA sequence addition operation over the scrambled image with the DNA sequence-based key generated by the Logistic map. Thereafter, the generated sequence was subjected to exclusive-or operation with partial key and modulo of sum of all the pixel values. The experimental and safety analysis highlighted that the proposed encryption technique was not only invertible and computationally efficient, but also had a large key space, was extremely sensitive to secret key credentials, had a high NPCR value and a low correlation coefficient, rendering the system efficient and secure against brute-force, statistical and differential attack.

Keywords:

Chaos Function, DNA Coding, DNA Computation, DNA Sequences, Image Encryption

1. INTRODUCTION

During the last two decades, the globe has witnessed a revolutionary advancement in the field of wireless communication technology. The communication has become so easy and reachable; one can’t restrict himself from sending a text message only. Rampant rise in mobile communication technology enabled devices allows the user to exchange the multimedia data such as images, audio and video files etc. Therefore, data is the most precious asset of the world in recent times. The days are not so far off, when the economy of the developed countries will rely on the authenticity and integrity of data. Among different forms of data, digital image is the most widely used over the internet. Fred R. Barnard rightly quoted that “A picture is worth than thousand words”. So, image security is the utmost requirement for transferring over unsecured network. Undoubtedly, various traditional encryption techniques based on number theory and large computation power exists such as RSA, AES, DES, ECC etc., but the aforesaid techniques are not appropriate for digital images due to the inherent characteristics, such as their capacity for large amounts of data, data redundancy, and higher pixel correlation [1]-[5].

Henceforth in view of the security concern, the chaos-based systems are highly applicable for the image encryption owing to the intrinsic property like high sensitivity to the initial values, pseudo randomness and ergodicity. Chaos based cryptosystem mainly employs two types of chaotic maps. One dimensional chaotic map considerably simple, easy to implement however it has low key space, so it is difficult to resist brute force attack. Multidimensional chaotic maps possess large key space, but it is difficult to implement. While additionally the later adds to extra complexity overheads in terms of high computation time [6]-[11]. In view of the redundancy, of each map individually this paper exploits the features of both; 1-D Logistic map and 2-D Henon map in a balanced mode to add the dynamicity and randomness by chaotic sequence generation.

The high parallelism, enormous storage capacity, and energy-efficient operation promised by DNA computation technology have drawn a lot of attention from researchers in recent years. DNA based image encryption is mainly carried out in two steps. First, encode the pixel values of the image into DNA nucleotides base sequences and secondly, to perform DNA sequence operation over DNA nucleotides base sequences of an image with key [12]-[24].

Zhang et al. [25] suggested that a bio-molecular computation-based image fusion encryption technique. This technique enhances the image security by generating a random DNA based key matrix which is ultimately utilized to operate exclusive-or operation with scrambled matrix. Rehman et al. [26] proposed DNA based image encryption for grey images which offers great advantage for encryption even for larger size. Subsequently, Jangid et al. [27] proposed a hybrid hill cipher for digital images using DNA technology. The outcomes demonstrated better quality and security than existing variation of Hill cipher. Hu et al. [28] done a marvellous work by designing DNA insertion and DNA deletion-based cryptosystem with superior performance and resilience against statistical and differential attack. Kar et al. [29] gave a novel idea for image cryptosystem by using hyper chaotic function for pixel confusion, diffusion, DNA encoding and decoding to achieve a secure and reliable cryptosystem. Subsequently, Zhang et al. [30] designed a secured, efficient and robust unique approach of image scrambling by employing fiestal network and dynamic DNA coding rules. Bendaud et al. [31] presented a novel approach of an ECC based image encryption using DNA computing which provide two fold security and is highly sensitive to the secret key along with large key space. Subsequently, Alireza [32] proposed an encryption algorithm for images by blending chaotic function with modified AES. Arnold map is used to add the diffusion ability by generating key which makes it strong against attacks. Real time image encryption by combining the flavour of chaos and DNA theory was proposed by Balazi [33]. According to him, image undergoes two rounds with six operations in each round and SHA-256 hash is used to generate key during encryption process. Results proved that robust security and linear computation time make it best suited for real time environment.

Wang and Chen [34] jointly designed a dynamic spiral scrambling algorithm which dynamically combined the chaotic sequence with plain image. Gang et al. [35] proposed a novel scheme by using block scrambling operation with finite state machine. It was performed by using zigzag scanning curve. Combined effect of scrambling, chaos with DNA generates the ciphered output. Further, Malik et al. [36] proposed an algorithm for colourful images using hyper chaotic dynamical system with

DNA computation which is robust and efficient in time computation. Iqbal et al. [37] in 2021 found that combination of DNA with chaos is not sufficient, so author injects castle movement in image encryption using chaotic sequence to obtain promising results. Further, Uddin et al. [38] presented DNA based key scrambling technique which provides extra dynamicity and randomness in ciphered image. Subsequently, Akhiwati et al. [39] designed a technique which can withstand against linear cryptanalysis, differential, and noise resistance attack by combining dynamicity of DNA coding with chaos system.

Accordingly, an image encryption technique by combining the flavour of DNA computation with chaotic map has been proposed in the current research work. A blend of two-dimensional Henon map with one dimensional Logistic map is utilized to add the randomness, dynamicity and also to produce a wider chaotic range. First, the plain image is scrambled, then DNA based diffusion process is carried out over an image by operating different DNA computation function. Finally, exclusive-or operation is performed over an image with partial generated key and modulo of sum of all values of the pixels of an image for further diffusion. The experimental and safety analysis proved that proposed encryption method was more efficient and secure against the unauthorized attacks.

The subsequent sections of the paper are structured as follows: The fundamentals of chaos theory are covered in section 2. Section 3 mainly covered DNA coding rules and operations, while generation procedure of indices and key mentioned in section 4. The proposed encryption technique is fully explained in section 5. Section 6 discusses the experimental and safety analysis of the proposed technique to prove its efficiency and security. Finally, the conclusion is drawn in section 7.

2. CHAOS THEORY

The concept of Chaos Theory was first introduced by Edward Lorenz in 1972. The principle of chaos theory stated that, a nonlinear system apparently shows random behavior for some specific small range value. One of the most remarkable features of chaos system is that it is extremely sensitive to the initial parameters of the nonlinear system. Small variation in initial seeds leads to divergent outcome, exhibiting highly dynamic and unpredictable behavior [40], [41]. This section presents brief overview of some chaotic systems, namely one dimensional Logistic map and two dimensional Henon map respectively.

2.1 1-DLOGISTIC MAP

The logistic map, a dynamic chaotic system that is one dimensional and exhibits complicated chaotic behavior was proposed by Robert May in 1976. Mathematically, the logistic map can be expressed by an Eq.(1):

$$Z_{n+1} = r.Z_n(1\text{-}Z_n) \tag{1}$$

where Z is the input parameter which is confined to an interval (0, 1), and the control parameter, r, is located between the values of (0, 4]. It was interestingly to see that for $r > 3.567$, there is a periodic window, and the darker region shows the unpredictable chaotic behavior [42].

2.2 2-D HENON MAP

A Henon map is a two dimensional dynamic chaotic system, which can be represented by an Eq.(2):

$$\alpha_{n+1} = 1\text{-}a\alpha_n^2 + \beta_n \tag{2}$$

$$\beta_{n+1} = b\alpha_n$$

where α, β are the initial parameters, which are real values and close to zero, whereas a, b are the control parameters of the Henon map. It was observed that when control parameters b=0.3 and a lie in an interval [1.06, 1.22] U [1.27, 1.29] U [1.31, 1.42], Henon map show chaotic behavior with more random outputs [43].

3. DNA CODING RULES AND OPERATIONS

DNA is a genetic material present in all organisms responsible for passing genes from parents to their offspring's. In 1994, Leonard Adleman gave a revolutionary idea of DNA computation field by solving the NP-complete problem. DNA consists of four bases: A (Adenine), T (Thymine), G (Guanine) and C (Cytosine). These bases are employed to represent the binary codes since the development of DNA computing. In terms of binary number system, there are only two base digits 0 and 1, which are also complementary to each other. So here, 00 and 11 are complementary in the same manner as 01 and 10. Therefore, four DNA nucleotides bases are used to encode in binary system as A (00), T (01), C (01) and G (10). So, there is in total 24 encoding permutations. According to the Watson - Crick Model [44], [45], only 8 encoding schemes are valid, due to the above-mentioned complementary rule of binary number system, which is given in Table.1.

Table.1. DNA encoding and decoding rules

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

During DNA encoding process, the decimal value of gray image pixel is converted into 8-bit binary number, which can be further represented by a sequence of four nucleotide bases. In the same fashion, DNA decoding process is just the reverse operation of DNA encoding process. For example, DNA_Encoding(27, 4) means first encode a decimal value 27 by using rule 4, so binary equivalent of 27 is 00011011 which can be further represented as TCGA. In the similar manner, DNA_Decoding(AGCT, 6) means first decode AGCT in binary number system by using rule 6, so AGCT is equivalent to 10001101, which can be further represented as 141 in decimal value. In addition, these DNA nucleotide bases also undergo addition and subtraction operation in various applications of DNA computing in cryptographic techniques [45], [46]. Table 2 and 3 respectively show possible outcomes of addition and subtraction between these DNA bases.

Table.2. DNA Addition operation over nucleotide bases

+	A-00	G-01	C-10	T-11
A-00	A-00	G-01	C-10	T-11
G-01	G-01	C-10	T-11	A-00
C-10	C-10	T-11	A-00	G-01
T-11	T-11	A-00	G-01	C-10

Table.3. DNA Subtraction operation over nucleotide bases

-	A-00	G-01	C-10	T-11
A-00	A-00	T-11	C-10	G-01
G-01	G-01	A-00	T-11	C-10
C-10	C-10	G-01	A-00	T-11
T-11	T-11	C-10	G-01	A-00

4. GENERATION OF CHAOTIC SEQUENCES BASED INDICES, KEYS, CODING RULE AND MODULO OF SUM

4.1 GENERATION OF CODING RULE

The coding rule r mainly defines selection of one of the encoding and decoding rules out of total eight, as mentioned in the Table.1. Mathematically, coding rule r can be evaluated as in Eq.(3):

$$r = Mod\left(\sum_{i=1}^{M}\sum_{j=1}^{N}P(i,j),8\right) \quad (3)$$

where, $P(i,j)$ represents the pixel value at i^{th} row and j^{th} column of an image.

4.2 MODULO OF SUM OF ALL PIXEL VALUES OF AN IMAGE

The modulo of sum of all pixel values of an image can be evaluated by using an Eq.(4):

$$Sum = Mod\left(\sum_{i=1}^{M}\sum_{j=1}^{N}P(i,j),256\right) \quad (4)$$

where, *Sum* is the modulo of sum of all pixel values of an image.

4.3 CHAOTIC KEYS

1-D logistic map is employed to construct two different chaotic sequence pairs of the size M×N by using two different initial conditions parameters, where M and N denote the image's width and height. These Chaotic sequences will serve as Key_1 and Key_2, generated by using Eq.(1):

$$Key_1 = f(r_0, Z_0)$$

$$Key_2 = f(r_1, Z_1)$$

Following that, the resultant Key sequence K of same size will be generated by using modulus operator. After obtaining this, encode the Key sequence K into DNA base pair by using the DNA encoding function. Finally, obtain the DNA based key sequence KEY_{DNA} by using Eq.(5) and Eq.(6):

$$K = Mod((Key_1+Key_2),256) \quad (5)$$

$$KEY_{DNA} = f(DNA_{Encoding}(K,p)) \quad (6)$$

where p is the encoding rule, which is equivalent to r-1.

4.4 CHAOTIC SEQUENCE BASED INDICES

A 2-D Henon map is employed to produce two different random chaotic nature-based sequences X and Y having the dimension of M and N, where M and N denote the image's width and height. The chaotic nature based sequences X and Y are generated by using Eq.(2):

$$X,Y = f(a,b,X_0, Y_0)$$

where $X = \{X_1,X_2,X_3,X_4\ldots X_m\}$, and $Y=\{Y_1,Y_2,Y_3,Y_4\ldots Y_m\}$.

After generating X and Y random sequences, sort these sequences in ascending order and consequently generate the Indices *X-index* and *Y-index* using the sort function. Sort is a function for sorting a chaotic sequence either in ascending or in descending order. After the sorting, obtain the indexes of the sorted values. These unordered indexed values are used to scramble the image by row-wise and column-wise subsequently. Fig.1 shows the steps for generating unordered indexed values of an image using unsorted chaotic sequence.

$$X\text{-}index=\mathrm{Sort}(X,X\text{-}index)$$

$$Y\text{-}index=\mathrm{Sort}(Y,Y\text{-}index)$$

Unsorted chaotic sequence	11	32	9	21	7
Ordered indexed values of an image	1	2	3	4	5

(a)

Sorted chaotic sequence	7	9	11	21	32
Unordered indexed values of an image	5	3	1	4	2

(b)

Fig.1(a). Matrix of unsorted chaotic sequence and ordered indexed value of an image before scrambling (b). Matrix of sorted chaotic sequence and unordered indexed value of an image after scrambling

5. IMAGE ENCRYPTION TECHNIQUE

The proposed encryption technique mainly includes a blend mode of permutation and diffusion phases. Permutation phase mainly includes scrambling of an image by using generated chaotic sequence, while diffusion phase mainly operate DNA based Encoding, Decoding, Addition and Ex-OR operation over an image. The dual chaotic functions are employed to control the permutation and the diffusion process. The Fig.2 depicts the process flow of image encryption procedure. The thorough explanation of the image encryption technique is covered in the following steps:

Step 1: Select the secret credentials keys $\{Z_0, r_0, Z_1, r_1, X_0, Y_0, a, b\}$ which are considered as the initial parameters of dual chaotic map.

Step 2: Generate the chaotic sequence based unordered indices X-index, Y-index, and chaotic keys Key_1, Key_2, K, KEY_{DNA}.

Step 3: Input a plain gray image P. Convert the plain image P into a two dimensional matrix $P[M,N]$ with pixel values ranging from 0-255, where M and N parameter represents the width and the height of an image.

Step 4: The pixel values of the image matrix P are shuffled randomly in row-wise manner using the chaotic sequence based unordered X-index to obtain a row wise scrambled image P_1.

Step 5: Following the row-wise shuffling, the pixels of the image P_1 is also shuffled randomly in column wise manner using the chaotic sequence based unordered Y-index to obtain a column wise scrambled image P_2.

Step 6: Next, convert a two dimensional image matrix P_2 $[M,N]$ into a one dimensional image sequence P_3 as $\{p_0, p_1, p_2, p_3, \ldots p_{mxn-1}\}$. Convert the decimal values of P_3 into 8-bit binary number system. After this, encode the pixels of P_3 image sequence matrix into a quadruples of DNA base pair by using DNA Encoding function to obtain a one dimensional DNA based image sequence P_4, as in Eq.(7):

$$P_4 = DNA\_Encoding(P_3,r+1) \tag{7}$$

Step 7: By using Eq.(8), perform DNA addition operation between the DNA based image sequence P_4 and the DNA based key sequence KEY_{DNA} using DNA addition table 2 to obtain DNA based image sequence P_5.

$$P_5 = DNA\_Addition(P_4 + KEY_{DNA}) \tag{8}$$

Step 8: Then by using Eq.(9), decode the P_5 into 8 bit binary number system by using DNA decoding function, and now convert into decimal values to obtain P_6.

$$P_6 = DNA\_Decoding(P_5,r) \tag{9}$$

Step 9: After that by applying Eq.(10) and Eq.(11), perform an Ex-or operation in two steps as first applying between P_6 and Key$_1$, then applying between resultant image sequence P_7 with modulo of sum of all the pixel values of the image to obtain an image sequence P_8.

$$P_7 = P_6 \oplus Key_1 \tag{10}$$

$$P_8 = P_7 \oplus Sum \tag{11}$$

Step 10: After this, convert the image sequence P_8 into a two dimensional cipher code matrix P_9 [M,N].

Step 11: Finally convert a cipher code matrix into a cipher image.

The above-mentioned technique is mainly applicable for 8-bit gray image. For a 24-bit RGB colored image, the proposed technique will be implemented as: First split the RGB color image into 8-bit R, G and B components, and then apply the above said technique to encrypt each component separately. And after that, integrate the entire encrypted component into a single unit in the form of 24-bit cipher image.

6. IMAGE DECRYPTION TECHNIQUE

As the proposed DNA based image encryption technique is symmetric in nature, so the process of decryption is exactly the reverse of the encryption procedure phases. Before operating decryption technique, a receiver must receive all the secret credentials through a secured channel and generate the required indices and keys. After that, apply the already defined permutation and diffusion phases in the same operating way but in reverse manner with some minute alterations as use of DNA Subtraction operation instead of DNA Addition operation. Ultimately, the proposed technique effectively retrieves a 2-D plain image.

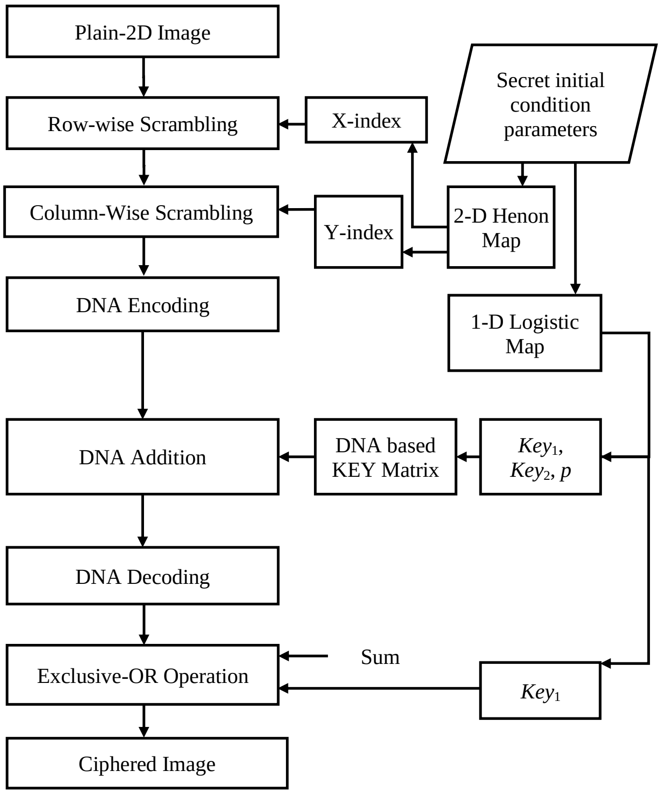


Fig.2. Process flow of image encryption technique

7. EXPERIMENTAL AND SAFETY ANALYSIS

The proposed DNA based image encryption technique is realized on windows 10 environment using a HP machine with Intel core i5, 2.30GHz processor with 4GB RAM.

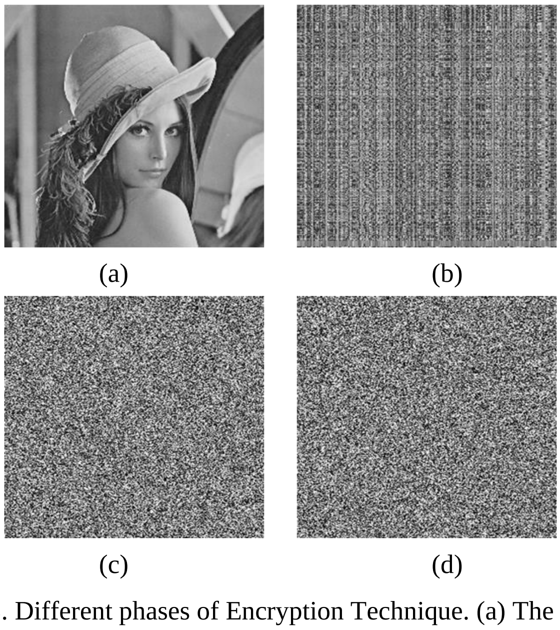
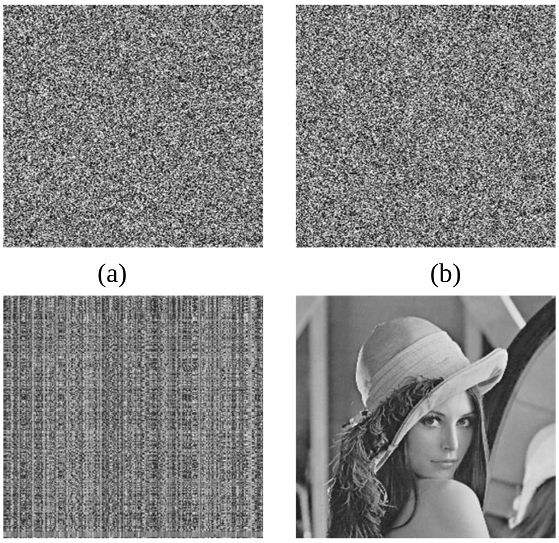


Fig.3. Different phases of Encryption Technique. (a) The Plain image “Lenna”. (b) Intermediate image after image scrambling phase. (c) Intermediate image after DNA Addition phase. (d) Final Ciphered image after Ex-or operation phase

The proposed image encryption technique is implemented in Python language using a cloud computing based Online IDE Google Colab. The proposed technique has been applied on multiple images with varying sizes. The Fig.3 and Fig.4 show the different resultant images during different phases of image encryption and decryption. It is clearly seen that the proposed technique is invertible in nature, and the ciphered image doesn't bear any resemblance with the plain image. Moreover, the efficiency and safety of the proposed technique in terms of computation and robustness against different kinds of attacks is analysed experimentally in this section.



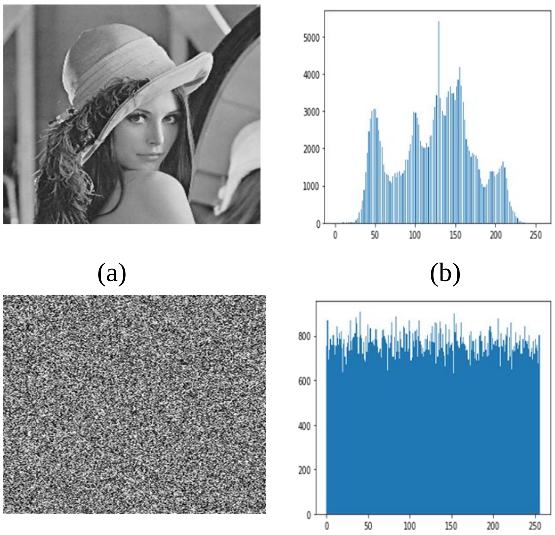
(a) (b)

(c) (d)

Fig.4. Different phases of Decryption Technique. (a) The ciphered image (b) Intermediate image after Ex-or operation phase (c) Intermediate image after DNA subtraction phase (d) Final decrypted image after image scrambling phase

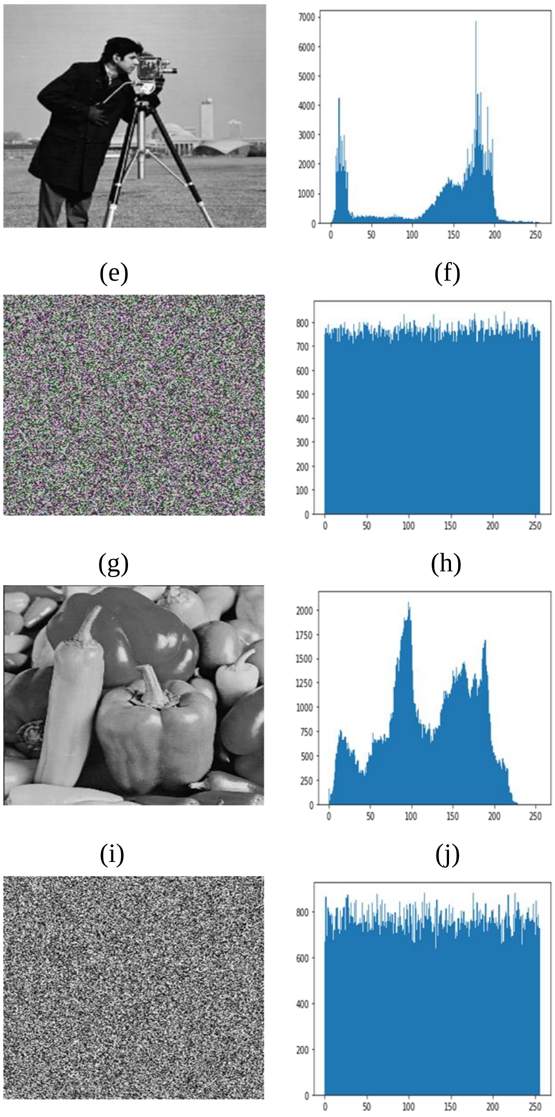
7.1 HISTOGRAM ANALYSIS

An image histogram is a statistical parameter which determines the quality of an encrypted image. Graphically, it reflects the distribution of information in terms of pixel values over a range of 0-255.



(a) (b)

(c) (d)



(e) (f)

(g) (h)

(i) (j)

(k) (l)

Fig.5. Histograms of plain image and corresponding cipher image (a) Plain image "Lena" (b) Histogram of "Lena" image (c) Cipher image "Lena" (d) Histogram of Cipher "Lena" image (e) Plain image "Cameraman" (f) Histogram of "Cameraman" image (g) Cipher image "Cameraman" (h) Histogram of cipher "Cameraman" image (i) Plain image "Peppers" (j) Histogram of "Peppers" image (k) Cipher image "Peppers" (l) Histogram of cipher "Peppers" image

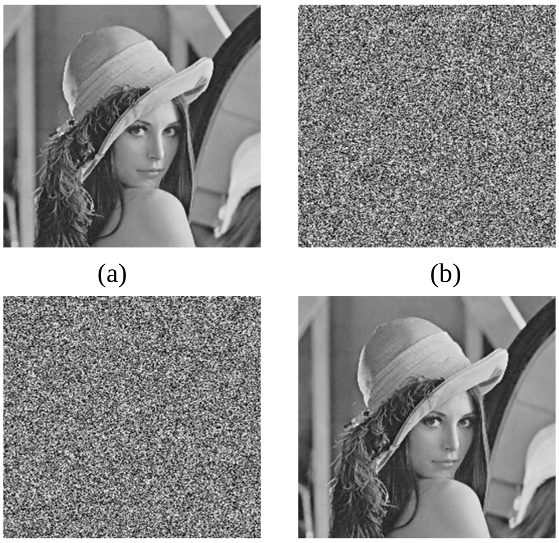
A good encryption technique should have a uniform distribution of pixels so that no statistical clues to the original image are left for an attacker. The Fig.5 shows that the histograms of cipher images are very much uniform and flat, which make it significantly distinct from the histograms of the plain images which are much centralized.

7.2 KEY SPACE

The key space plays a significant role to determine the strength of an encryption technique against exhaustive attack. The larger the key space, the more resistant it is against exhaustive kind of attack likes brute-force and dictionary attack. In the proposed technique, the secret key credentials in terms of initial values to the chaotic function are (Z_0, r_0, Z_1, r_1, X_0, Y_0, a, b), if each of the credential has a precision of 10^{14}, then the key space would be $(10^{14})^8 = 10^{112} > 2^{100}$ which is large enough to resist the exhaustive attack [33] [35].

7.3 KEY SENSITIVITY

Key sensitivity parameter determines the sensitivity of an encryption technique, i.e., a minute alteration in secret key credential would cause a significant change in cipher output. A good cryptosystem possesses an extreme key sensitivity. Key sensitivity can be tested during the decryption phase; a minute alteration in secret key will not be able to decrypt the image successfully. From Fig.6, it can be clearly seen that a minute alteration in secret key credentials would not be able to decrypt the ciphered image correctly. So, proposed encryption technique is highly sensitive to the secret key credentials.


(a) (b)

(c) (d)

Fig.6. (a) The Plain Image Lena, (b) The Decrypted Image by minute altering r1'=3.95000000000001 instead of r1=3.95000000000000 (c) The Decrypted Image by minute altering z1'=0.01000000000002 instead of z1=0.01000000000001 (d) The Decrypted Image with correct secret credentials

7.4 TIMING ANALYSIS

An encryption technique's efficiency is determined not only by its robustness, but also by its computing speed. Lower the encryption and decryption time, reflect the faster performance of the cryptosystem. The encryption and decryption time of the proposed technique are linearly increased with the increasing size of the image. Hence, the linear complexity of the proposed technique ensures that the optimal utilization of resources either in terms of CPU time cycle or memory. The Fig.1 and Fig.2 clearly show that the proposed technique's encryption and decryption times rise linearly with the size of the Lena image.

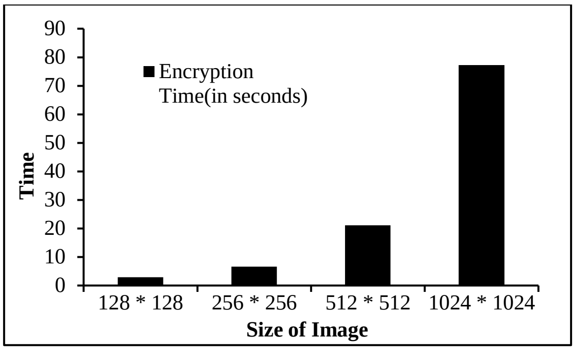


Fig.7. Encryption time analysis by varying size of Plain "Lena image"

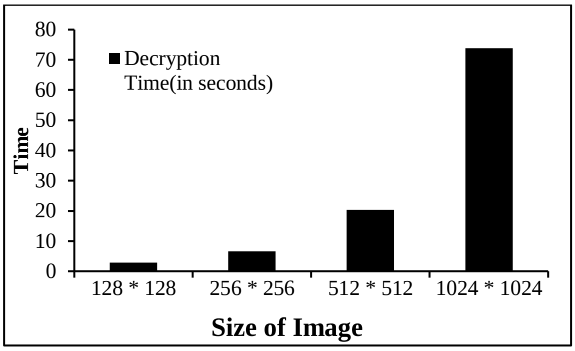


Fig.8. Decryption time analysis by varying size of Cipher "Lena image"

7.5 CORRELATION COEFFICIENT ANALYSIS

It is a statistical parameter which determines the relationship between the adjacent pixels of an image. Smaller the value of correlation coefficient, higher is the image resistance against statistical attack. Table 4 shows the correlation coefficient between the adjacent pixels of three different images before and after encryption in horizontal and vertical directions. Here, it can be observed that plain images possess a strong correlation between adjacent pixels, while cipher images have significantly low value of correlation coefficient, which helps them resist against statistical attack.

Table.4. Correlation Coefficient Values

Image	Before Encryption		After Encryption	
(256×256)	Vertical	Horizontal	Vertical	Horizontal
Lena	0.9912	0.9993	-0.0005	0.0015
Cameraman	0.9993	0.9991	0.0025	-0.0031
Peppers	0.9921	0.9965	-0.0015	0.0067

7.6 NPCR ANALYSIS

The number of pixels change rate is a performance metrics that shows the strength and robustness of any cryptosystem. The NPCR determine the effect over the image by changing the value of a single pixel. Evaluation of NPCR by using the given Eq.(12):

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \quad (12)$$

where, $D(i,j)=0$, if $C_1 = C_2$; else set to 1 and M and N represents the width and height of an image, C_1 and C_2 represent the cipher images corresponding to the same plain image just by changing the value of a single pixel.

The cryptosystem having NPCR values nearly or greater than 99% make the cryptosystem strong and resistive against differential attack. The Table.5 shows that NPCR values of all three different images are greater than 99%, which in turn reflects the robustness of the cryptosystem against the differential attack.

Table.5. NPCR values

Metric	Lena Image	Peppers Image	Cameraman Image
NPCR	99.99	99.44	99.8

8. CONCLUSION

A DNA-based image encryption technique based on a dual chaotic function was proposed in the current research. A blend of two-dimensional Henon map with one dimensional Logistic chaotic map was employed to add the randomness and dynamicity in the cryptosystem, and to produce a wider chaotic range for generation of keys and indices. Primarily, the plain image was scrambled in row-wise and column-wise manner utilizing different indices generated by the Henon map. Thereafter, DNA based diffusion was carried out over an image by performing encoding, decoding and addition operations with the help of generating chaotic keys using Logistic function. Subsequently, partially generated chaotic key via usage of logistic function assisted to operate exclusive-or operation over an image with modulo of sum of all values of the pixels for further diffusion. Experimental and safety analysis showed that proposed encryption technique possessed a large key space, extreme sensitivity to the secret key credentials, a uniform flat distribution curve of histogram, a very high value of NPCR greater than ideal value and correlation coefficient close to zero. The findings of the study ensued that the proposed technique was robust and secure against the exhaustive, statistical and differential attack. Additionally, linear time complexity makes it efficient and suitable for real time applications.

Undoubtedly, proposed technique was strong enough, efficient, and resilient against different kinds of attacks, however there is no denying the fact that there is scope of extending to the same for 24-bit color images and to encrypt the selective portion of medical images. There's an additional possibility, to employ the compression techniques along with encryption for multimedia form of data to make it more efficient in terms of bandwidth consumption during transmission.

REFERENCES

[1] P. Isasi and J.A. Hern, "Introduction to the Applications of Evolutionary Computation in Computer Security and Cryptography", *Computational Intelligence*, Vol. 20, No. 3, pp. 445-449, 2004.

[2] A. Kahate, "*Cryptography and Network Security*", Tata McGraw Hill, 2012.

[3] N. Sharma, Prabhjot and H. Kaur, "A Review of Information Security using Cryptography Technique", *International Journal of Advanced Research in Computer Science*, Vol. 8, pp. 323-326, 2017.

[4] X. Lin, J.H. Li, S.L. Wang, F. Cheng and X.S. Huang, "Recent Advances in Passive Digital Image Security Forensics: A Brief Review", *Engineering*, Vol. 4, No. 1, pp. 29-39, 2018.

[5] M. Kaur and V. Kumar, "A Comprehensive Review on Image Encryption Techniques", *Computational Methods in Engineering*, Vol. 27, pp. 15-43, 2020.

[6] X. Chai, K. Yang and Z. Gan, "A New Chaos-Based Image Encryption Algorithm with Dynamic Key Selection Mechanisms", *Multimedia Tools and Applications*, Vol. 76, No. 7, pp. 9907-9927, 2017.

[7] X. Su, W. Li and H. Hu, "Cryptanalysis of a Chaos-Based Image Encryption Scheme Combining DNA Coding and Entropy", *Multimedia Tools and Applications*, Vol. 76, No. 12, pp. 14021-14033, 2017.

[8] A. Belazi, A.A.A. El-Latif and S. Belghith, "A Novel Image Encryption Scheme based on Substitution-Permutation Network and Chaos", *Signal Processing*, Vol. 128, pp. 155-170, 2016.

[9] X. Chai, Y. Chen and L. Broyde, "A Novel Chaos-Based Image Encryption Algorithm using DNA Sequence Operations", *Optical Lasers Engineering*, Vol. 88, pp. 197-213, 2017.

[10] X. Chai, Z. Gan, K. Yang, Y. Chen and X. Liu, "An Image Encryption Algorithm based on the Memristive Hyperchaotic System, Cellular Automata and DNA Sequence Operations", *Signal Process Image Communication*, Vol. 52, pp. 6-19, 2017.

[11] Y. Liu, X. Tong and J. Ma, "Image Encryption Algorithm based on Hyper-Chaotic System and Dynamic S-Box", *Multimedia Tools and Applications*, Vol. 75, No. 13, pp. 7739-7759, 2016.

[12] S. Jain and V. Bhatnagar, "A Novel DNA Sequence Dictionary Method for Securing Data using Spiral Approach and Framework for DNA Cryptography", *Proceedings of IEEE International Conference on Advances in Engineering and Technology Research*, pp. 1-7, 2014.

[13] U.S. National Library of Medicine, "Genetic Home Reference", Available at: http://ghr.nlm.nih.gov/handbook/basics/dna, Accessed at 2017.

[14] IRMAMY, USA, "DNA Structure, IRMAMY In the world of Environmental Biology", Available at: https://ijarovic.wordpress.com/2012/02, Accessed at 2017.

[15] G. Condon, and E. Rozenberg, "DNA Computing", *Proceedings of International Workshop on DNA-Based Computers*, pp. 1-13, 2000.

[16] M. Amos, S. Wilson, D.A. Hodgson, G. Owenson and A. Gibbons, "Practical Implementation of DNA Computations", *Proceedings of International Conference on Unconventional Models of Computation, Springer*, pp. 1-18, 1998.

[17] S. Jeevidha, M.S.S. Basha and P. Dhavachelvan, "Analysis on DNA based Cryptography to Secure Data Transmission",

International Journal of Computer Applications, Vol. 29, No. 8, pp. 16-20, 2011.

[18] A. Leier, C. Richter, W. Banzhaf and H. Rauhe, "Cryptography with DNA Binary Strands", *Elsevier Biosystems*, Vol. 57, No. 1, pp. 13-22, 2000.

[19] A. Gehani, T. LaBean and J. Reif, "*DNA-Based Cryptography*", Springer, 2004.

[20] N.N. Rao, "A Cryptosystem Based on Recombinant DNA Technique", *Acta Electronica Sinica*, Vol. 32, No. 7, pp. 1216-1218, 2004.

[21] S.B. Sadkhan, "Information Security based on DNA Importance and Future Trends", *Proceedings of International Conference on Communication and Information Technology*, pp. 310-314, 2021.

[22] R.J. Lipton, "Using DNA to solve NP-Complete Problems", *Science*, Vol. 268, No. 5, pp. 542-545, 1995.

[23] D. Boneh, C. Dunworth and R. Lipton, "Breaking DES Using a Molecular Computer", CS Tech-Report CS-TR Princeton, pp. 489-95, 1996.

[24] C.T. Clelland, V. Risca and C. Bancroft, " Hiding Messages in DNA Microdots", *Nature*, Vol. 399, No. 3, pp. 533–534, 1999.

[25] Q. Zhang, L. Guo and X. Wei, "A Novel Image Fusion Encryption Algorithm based on DNA Sequence Operation and Hyper-Chaotic System", *Optik*, Vol. 124, No. 6, pp. 3596-3600, 2013.

[26] A.U. Rehman, X. Liao, A. Kulsoom and S.A. Abbas, "Selective Encryption for Gray Images based on Chaos and DNA Complementary Rules", *Multimedia Tools and Applications*, Vol. 74, No. 6, pp. 4655-4677, 2015.

[27] R. K. Jangid, N. Mohmmad, A. Didel and S. Taterh, "Hybrid Approach of Image Encryption using DNA Cryptography and TF Hill Cipher Algorithm", *Proceedings of IEEE International Conference on Communication and Signal Processing*, pp. 934-938, 2014.

[28] T. Hu, Y. Liu, L.H. Gong and H.M. Yuan, "Chaotic Image Cryptosystem using DNA Deletion and DNA Insertion", *Signal Processing*, Vol. 134, pp. 234-243, 2016.

[29] M. Kar, A. Kumar, D. Nandi and M.K. Mandal, "Image Encryption using DNA Coding and Hyper Chaotic System", *IETE Technical Review*, Vol. 37, No. 1, pp. 12-23, 2018.

[30] X. Zhang, Z. Zhou and Y. Niu, "An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding", *IEEE Photonics Journal*, Vol. 10, No. 4, pp. 1-14, 2018.

[31] S. Bendaoud, F. Amounas, E. Hassan and E. Kinani, "A New Image Encryption Scheme based on Enhanced Elliptic Cryptosystem using DNA computing", *Proceedings of International Conference on Networking, Information Systems and Security*, pp. 234-242, 2019.

[32] A. Arab, M.J. Rostami and B. Ghavami, "An Image Encryption Method based on Chaos System and AES Algorithm", *The Journal of Supercomputing*, Vol. 75, No. 2, pp. 6663-6682, 2019.

[33] A. Belazi, M. Talha, S. Kharbech and W. Xiang, "Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding", *IEEE Access*, Vol. 7, pp. 36667-36681, 2019.

[34] X. Wang and S. Chen, "Chaotic Image Encryption Algorithm Based on Dynamic Spiral Scrambling Transform and Deoxyribonucleic Acid Encoding Operation", *IEEE Access*, Vol. 8, pp. 160897-160914, 2020.

[35] S. Geng, T. Wu, S. Wang, X. Zhang and Y. Wang, "Image Encryption Algorithm Based on Block Scrambling and Finite State Machine", *IEEE Access*, Vol. 8, pp. 225831-225844, 2020.

[36] M.G.A. Malik, Z. Bashir, N. Iqbal and M.A. Imtiaz, "Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing", *IEEE Access*, Vol. 8, pp. 88093-88107, 2020.

[37] N. Iqbal, R. A. Naqvi, M. Ati, M.A. Khan, M. Hanif, S. Abbas and A.D. Hussain, "On the Image Encryption Algorithm Based on the Chaotic System, DNA Encoding and Castle", *IEEE Access*, Vol. 9, pp. 118253-118270, 2021.

[38] M. Uddin, F. Jahn, M.K. Islam and M.R. Hassan, "A Novel DNA-based Key Scrambling Technique or Image Encryption", *Complex and Intelligent Systems*, Vol. 7, No. 6, pp. 3241-3258, 2021.

[39] B. Akhiwati and L. Parthiban, "Secure and Efficient Cryptography Technique using Chaos and DNA Encoding Methodology", *Turkish Journal of Computer and Mathematics Education*, Vol. 12, No. 2, pp. 2754-2764, 2021.

[40] L. Liu, Q. Zhang and X. Wei, "A RGB Image Encryption Algorithm based on DNA Encoding and Chaos Map", *Journal of Computers and Electrical Engineering*, Vol. 38, No. 5, pp. 1240-1248, 2012.

[41] A. Kulsoom, D. Xiao, A.U. Rehman and S.A. Abbas, "An Efficient and Noise Resistive Selective Image Encryption Scheme for Gray Images based on Chaotic Maps and DNA Complementary Rules", *Multimedia Tools and Applications*, Vol. 75, No. 1, pp. 1-23, 2016.

[42] M.K. Khairullah, A.A. Alkahtani, M.Z.B. Baharuddin and A.M. Al-Jubari, "Designing 1D Chaotic Maps for Fast Chaotic Image Encryption", *Electronics, Vol.* 10, No. 17, pp. 2116-2123, 2021.

[43] W. Jiahui, L. Xiaofeng and B. Yang, "Image Encryption using 2D Henon-Sine Map and DNA Approach", *Signal Processing*, Vol. 153, pp. 11-23, 2018.

[44] X. Chai, Y. Chen and L. Broyde, "A Novel Chaos-Based Image Encryption Algorithm using DNA Sequence Operations", *Optics and Laser in Engineering*, Vol. 88, pp. 197-213, 2017.

[45] J.D. Watson and F.H.C. Crick, "A structure for Deoxyribose Nucleic Acid", *Nature*, Vol. 421, No. 6921, pp. 141-143, 2003.

[46] R. Enayatfifar, A.H. Abdullah and I.F. Isnin, "Chaos-Based Image Encryption using A Hybrid Genetic Algorithm and a DNA Sequence", *Optik*, Vol. 124, pp. 3596-3600, 2013.