International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received**: 20 May 2023 **Revised**: 28 July 2023 **Accepted**: 16 August 2023*

An Efficient and Secure DNA based Image Encryption Technique

Ajit Singh[1], Dr. Bijendra Singh[2]
[1]Research Scholar
Department of Computer Science Engineering, Baba Mastnath University, Rohtak, India
Email : ajit713@gmail.com
[2]Assistant Professor
Department of Computer Science Engineering, Baba Mastnath University, Rohtak, India
Email : bijendra.singh046@gmail.com

Abstract — In this paper, an efficient and secure DNA based image encryption technique using hyper chaos Lorenz function is proposed. The technique employs SHA-512 hash of gray scale image and primary key to alter the initial seeds of hyper chaos Lorenz function. Initially, chaotic sequences are generated and redesigned. Then, an image is divided into blocks and randomly shuffled according to the primary key. Further perform circular shift operation over the rows of the shuffled image matrix and index based scrambling operation over the columns. After that, perform dynamic encoding and diffusion based DNA algebraic operation over the encoded DNA sequence and DNA based Key sequence using chaotic sequence. Finally, DNA decoding is employed to convert the diffused dynamic matrix into a ciphered image. The dynamicity of the chaotic sequences makes its extraordinary and contributes to the enhanced security and robustness of the technique. Implementation, security and performance analysis demonstrate that the technique has not only an outstanding encryption effect, but also posses large key space, less pixel correlation, low computation time and successfully resilient to the statistical, differential and brute-force attack. Comparative analysis with other references proves its efficiency and practicability for real time applications.

Keywords - Chaotic function, DNA computing, Image Encryption.

I. INTRODUCTION

In the 21st century, due to the rampant rise of mobile computing and internet technology, approachability and the utility of social media platforms like Facebook, WhatsApp, Snapchat, Instagram etc. have become so convenient and economical. So in a minute, millions of tons of information are disseminated over multimedia platforms. Among them, digital images are frequently transmitted over the internet because they are more communicable, mesmerizing, eye catching, visual effects and more enduring. Therefore, security concerns to the digital image have gained increasing attention nowadays. Image encryption is considered to be an efficient solution among different ways to protect the image information. The high data capacity, redundancy of pixels and strong correlation among neighboring pixels of an image make the classical techniques ineffective because these techniques cannot provide the essential security requirements to an image cryptosystems [1][2]. The chaos based system has gained a huge momentum in the field of image security due to its intrinsic properties such as extreme sensitivity to input seeds, non-periodicity, ergodicity and unpredictable behavior [3][4].

In visual encryption, two types of chaotic functions are used: low dimension [5] and high dimension [6]. Low dimensions are simple and easy to operate, however they are ineffective due to a small key space and poor security [9]. The high dimension chaos enhances the system security due to multiple input parameters and complex structure. They are, however, confronted with hefty implementation costs and complex performance assessments. Therefore, a numerous technique has been designed by researchers and achieved valuable results. Additionally, many high dimension chaos-based systems are vulnerable to cryptanalysis [7][8].

Meanwhile, the development of DNA computing and its capability of solving of complex computational problem along with the provision of energy efficient operation, high storage density and parallelism, mothered a new breed of DNA cryptography. No doubt, chaos based system provide image security by using only scrambling effect at confusion level, having no significant diffusion function and no means for the dynamicity. On the other side, DNA cryptography offers a lot of DNA based diffusion functionalities along with the provision of dynamicity of algorithm by encoding and decoding the image pixels using Watson-Crick complementary rules [10][11].

As a result, in recent years, the efficiency and defensive mechanism of the images have mostly been strengthened by integrating Biological computing with chaos functions [12]-[14]. To achieve image security criteria, DNA sequence

operations were used over image by employing logistics map in [1]. However, due to the low dynamicity of the logistic map, these methods were susceptible to known plaintext attack. To improve image security, high dimension chaotic maps were used instead of low dimensions, but it was revealed in [12]-[14] that these schemes were also suffered to serious flaws and known attacks. In view of these short period issues, a blend of spatiotemporal chaotic system was preferred along with DNA sequence operation for the design of resilient security [15][16]. For example, Wang et. al. [15][16] developed two more scheme by extending the concept of hamming distance along with logistic map based couple map lattice. Following that, Wang et al. [18] also designed the DNA-based image cipher in 2018 using a CML-based spatiotemporal chaotic function. During cryptanalysis of CML, observed that CML utilized logistic map function. Unfortunately, in the bifurcation diagram, parameter u still has a periodic window, implying that it exhibits less chaotic behavior [15]-[17].

Further, Wang and Chen [19] in 2020 summarizes the previous work about the cryptanalysis of permutation diffusion based scheme and designed a more efficient dynamic spiral scrambling scheme using high degree Lorenz chaos function. Thereafter, a unique technique was also proposed by Gang et al. [20] combining the block scrambling operation with a finite state machine. The technique also utilized zigzag scanning confusion operation along with the essence of Lorenz chaos and DNA computing to resist with statistical and differential attack. Akkasaligar and Biradar [21] in 2021 contributed a selective medical image encryption by permuting and diffusing the selected pixels of an image to reduce the computational time. Further, Bharadwaja and Ganeshan [22] jointly designed the secret image encryption scheme by using the security features of ECC before being embedded with the cover image. Moreover, the secret image is mapped with a DNA nucleotide to raise the security. As we know, cryptanalysis is ongoing process to point out the weakness of existing scheme and motivates to design more efficient work to avoid the recurrences of the same. As a result, it is critical to investigate these schemes and examine their security, applicability and feasibility. In this study, we thoroughly evaluate the Wang et. al. scheme[18] and discover that it lack the advertised efficiency and security, namely data loss attack. In addition, we also observed some issues, which addressed here as:

- Key sequence generated solely depends on the secure key credentials of the chaotic system. So, the design of multiple key sequence based image encryption techniques is the need of hour.
- The Wang et. al. [18] work employed logistic map based CML function, in which the control parameter of logistic function has a periodic window in the bifurcation diagram which makes it less chaotic in nature.
- Minute alteration in any pixel of cipher image during transmission due to noise and occlusion attack make the existing scheme non-invertible in nature. At the receiver end, the receiver will not be able to retrieve the correct pixel information of deciphered image as the decrypted technique not only depends upon the external key but also on the previous pixel information. So, the dependency of current pixel over previous one makes it non invertible and more susceptible to noise and occlusion attack.
- The existing technique carries a fixed rule for DNA encoding and decoding during encryption process which make it less dynamic in nature.
- Complex design of DNA based confusion and diffusion phase of the Wang et. al. [18] makes it computationally too slow and inappropriate for energy constrained environment. So, confusion and diffusion phase need to redesign in an efficient way without compromising the security requirements of image encryption system.

These addressed issues motivate us to design a DNA based image encryption using hyper chaos Lorenz system. The scheme employs SHA-512 hash of gray scale image and primary key to alter the initial seeds of hyper chaos Lorenz chaotic function and also even to generate different initial parameters for different images. Initially, a sequence of chaotic metrics is generated for employing a sequence of different operations such as confusion, encoding, DNA based key sequence generation, diffusion and decoding. The proposed scheme employs simple confusion techniques to minimize the correlation than the complex DNA based confusion to make it computationally efficient. Moreover, the proposed scheme diffused the DNA based image matrix by randomly selecting different kinds of DNA algebraic operations. This dynamicity of chaotic sequences makes its extraordinary and enhances the security and robustness of the proposed technique. The simulation outputs and security analysis have proved that the scheme achieve optimal values of security parameters and can also resists against different known attacks. Moreover, the comparative and performance analysis with existing standards shows its superiority, which make it more efficient, rationale and practical for real time data transmission based applications.

The remaining sections of the research article are structured as follows: The fundamentals of hyper chaos Lorenz function are covered in section 2. Section 3 mainly covers DNA computing operations; while the proposed encryption technique is thoroughly discussed in section 4. Section 5 discusses the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received**: 20 May 2023 **Revised**: 28 July 2023 **Accepted**: 16 August 2023*

implementation and cryptanalysis results of the proposed technique to prove its efficiency and security. Section 6 and 7 cover comparative study and performance analysis with the existing standards. Finally, the conclusion is drawn in section 8.

II. HYPER CHAOS LORENTZ FUNCTION

Edward Lorenz created a four-dimensional hyper chaotic Lorenz system in 1963 to characterize the flow of liquid in a bucket when the bottom of the bucket is overheated. The proposed cryptosystem makes use of a high dimensional Lorenz chaos function that consists of four ordinary differential equations, which are expressed by equation (1).

$$\begin{aligned} X_{n+1} &= a(Y_n - X_n) + W_n \\ Y_{n+1} &= X_n(c - Z_n) - Y_n \\ Z_{n+1} &= X_n Y_n - bZ_n \\ W_{n+1} &= -Y_n Z_n + rW_n \end{aligned} \quad (1)$$

Where a, b, c and r are the Lorenz system control variable, which can assume any positive real values. It was observed that when a=10, b=8/3, c=28 and -1.52 ≤ r ≤ -0.06; then the system shows dynamic unpredictable behavior called chaotic state of the system. The chaotic sequences generated here will be utilized during the confusion and diffusion process of image encryption. The bifurcation diagram and Lyapunov exponent discussed by Huang et. al. [23] proved that, the randomness, ergodicity, dynamicity and complexness of chaotic sequences make it suitable for generating chaotic sequences for image encryption.

III. DNA COMPUTING OPERATIONS

DNA is a genetically biological material present in all living beings that is liable for passing the qualities from parents to their child's. Adenine, Cytosine, Guanine, and Thymine are the four bases that make up a DNA molecule. The order of these bases is primarily responsible for a living being's growth, individuality and reproduction. The emerging DNA computing field uses these bases by representing in binary numbers. As a result, these four DNA bases are encoded in binary form as A by 00; T by 11; C by 10; and G by 01. So there are 24 encoding permutations in all. As per the Watson-Crick laws [16][18], only eight DNA coding laws are reasonable, as indicated in Table 1. To make DNA computing more applicable in the realm of cryptography, a number of algebraic and logical operations over DNA bases are depicted in Table 2, 3 and 4.

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

Table 2: DNA Addition operation over nucleotide bases

+	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

Table 3: DNA Subtraction operation over nucleotide bases

-	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

Table 4: DNA Ex-or operation over nucleotide bases

⊕	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

IV. PROPOSED ENCRYPTION TECHNIQUE

A digital grey image P (M, N) is considered as input having M and N is the width and the height of a plain image. The proposed encryption system mainly comprises of three phases which are discussed below as:

A. Generation of initial parameters to the Lorenz chaotic function

SHA-512 hash function is used to evaluate the hash digest of digital image and the primary key P_{key} separately. The use of hash digest ensure the sensitivity of techniques against the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received**: 20 May 2023 **Revised**: 28 July 2023 **Accepted**: 16 August 2023*

digital image and the primary key, means even slight change either in digital image or in primary key it will completely generate the different cipher image. The obtained hash digests of 512 bit is converted into a decimal string of length 64, which are represented as:

$$HD_I = D_I(1)D_I(2)D_I(3) \ldots\ldots\ldots\ldots\ldots HD_I(64) \quad (2)$$
$$HD_{PK} = D_{PK}(1)D_{PK}(2)D_{PK}(3) \ldots\ldots\ldots\ldots\ldots HD_{PK}(64) \quad (3)$$

Where HD_I and HD_{PK} is the hash digest of image and primary key respectively. Subsequently, $HD_I(i)$ and $HD_{PK}(i)$ is the i^{th} decimal of hash digest string of image and primary key respectively.

Now, obtained hash digest is used to evaluate the modification factor for hyper chaos Lorenz system by using the equation (4).

$$m = \frac{\sum_{i=1}^{i=64} HD_I(i)}{\sum_{i=1}^{i=64} HD_{PK}(i)} \quad (4)$$

Where, m is the modification factor.

After that, modify the randomly chosen parameters to the chaotic function by using the equation (5).

$$x_i' = \mathrm{mod}(x_i + m, 1)$$
$$y_i' = \mathrm{mod}(y_i + m, 1)$$
$$z_i' = \mathrm{mod}(z_i + m, 1)$$
$$w_i' = \mathrm{mod}(w_i + m, 1) \quad (5)$$

Where mod (a, b) represents the modulus operator for i=1 and 2 respectively. Now these pairs (x_1', y_1', z_1', w_1') and (x_2', y_2', z_2', w_2') act as initial seed to the hyper chaos Lorenz function.

B. Generation of chaotic sequences

This sub-section discusses the generation and redesign of chaotic sequences which is mainly used for operating pixel confusion, DNA based diffusion and DNA based key generation. Moreover, generation of chaotic sequence for the selection of particular DNA coding rule is also discussed here. The procedure of generation is as follows:

- Initially, by using the parameters (x_1', y_1', z_1', w_1', x_2', y_2', z_2', w_2') execute the hyper chaos function for M×N times to generate the six sequences X_1, Y_1, Z_1, X_2, Y_2 and Z_2 of size M×N.

- Redesign of each and every element of chaotic sequence. Firstly, consider the first M and N elements of sequences X_1 and Y_1. After that, update each and every elements of sequences X_1 and Y_1 by using the respective equations (6) and (7).

$$x_1'(m) = \mathrm{mod}(\mathrm{int}(x_1(m) \times 10^{16}),\ M) \quad (6)$$
$$y_1'(n) = \mathrm{mod}(\mathrm{int}(y_1(n) \times 10^{16}),\ N) \quad (7)$$

Where m = 1, 2, 3, 4……..M and n = 1, 2, 3, 4….N

- Ascend the elements of sequences X_1' and Y_1' and record their index in new sequences S_1 and S_2.

- Redesign the sequences Z_1, X_2, Y_2 and Z_2 by performing the following operations on each and every element and obtain the new sequences Z_1', X_2', Y_2' and Z_2' by using the equations (8), (9), (10) and (11).

$$z_1'(k) = \mathrm{mod}(\mathrm{int}(z_1(k) \times 10^8),\ 8) \quad (8)$$
$$x_2'(k) = \mathrm{mod}(\mathrm{int}(x_2(k) \times 10^8),\ 3) \quad (9)$$
$$y_2'(k) = \mathrm{mod}(\mathrm{int}(y_2(k) \times 10^8),\ 256) \quad (10)$$
$$z_2'(k) = \mathrm{mod}(\mathrm{int}(z_2(k) \times 10^8),\ 8) \quad (11)$$

Where k=1, 2, 3, 4……M×N.

C. Image Encryption Technique Steps

The proposed technique is mainly designed by using traditional two-step process such as confusion and diffusion process. During confusion process, circular shift and scrambling operation are to be operated over the image matrix to confuse the pixels of the original plain image, while diffusion phase mainly operate DNA based algebraic operation over an image. Figure 1 depicts the process flow of image encryption procedure. This sub-section discusses the detailed procedure of encryption technique by considering a grey scale image P(M,N), which are follows as:

Step 1: Divide the original plain image P(M,N) into equal size of 64 blocks as 8×8 size. Then, randomly shuffle them according to the primary key P_{Key} to obtain a block divided shuffled image P_1(M,N).

Step 2: After random shuffling of blocks, perform circular shift operation over the elements of the rows of P_1(M,N) according to the sequence elements of S_1. If mod(s_1(k),2)=0; then perform left circular shift operation on all the pixels of k^{th} row of P_1(M,N) image by s_1(k) positions. Else, perform right circular shift operation on all the elements of k^{th} row of P_1 (M,N) image by s_1(k) positions. After completing the above operation, P_2 (M,N) is obtained.

Step 3: Following the circular shift operation over the rows, scramble all the columns of P_2(M,N) image using the sequence elements of S_2. All the pixels of the k^{th} column of P_2(M,N) image is scrambled to $s_2(k)^{th}$ position and thus finally obtained P_3(M,N).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received**: 20 May 2023 **Revised**: 28 July 2023 **Accepted**: 16 August 2023*

Step 4: Next, convert a two dimensional image matrix $P_3(M,N)$ into a one dimensional image sequence matrix P_4. Convert each pixel's decimal value to an 8-bit binary number. Then, encode the binary number of each pixel into a quartet of DNA bases and to generate a DNA based sequence P_5. Each elements of sequence Z_1' are used to encode the 8-bit binary string of a pixel into a quadruple of DNA base by using equation (12). The equation (12) defined for all four possible values of k = 1, 2, 3and 4 for each value of i.

$$p_5(i,k) = \text{DNA Encoding}(p_4(i), z_i'(i)) \quad (12)$$

Where i = 1, 2, 3, 4……..M×N; $p_5(i, k)$ represent k_{th} DNA base of i^{th} pixel, $p_4(i)$ represent i^{th} pixel of an image sequence P_4, $z_1'(i)$ represent i^{th} element of Z_1' sequence which act as DNA Encoding rule.

Step 5: The elements of Y_2' sequence is encoded into DNA bases by using a random encoding rule r which is evaluated by using the equation (13), then the obtained DNA sequence is KEY(M×N×4).

$$r = \text{mod}(\text{Sum}, 8) \quad (13)$$

Where Sum is the sum of all the pixels value of a plain image.

Step 6: After generating the key sequence KEY of size M×N×4, operate different operations between KEY and P_5(M×N×4) to obtained a resultant one dimensional DNA sequence matrix P_6(M×N×4). The different types of diffusion operation are to be performed according to the nature of sequence X_2' which are expressed by equation (14). The equation (14) defined for all four possible values of k = 1, 2, 3and 4 for each value of i.

$$\begin{aligned} &\text{If } x_2'(i) = 0, \text{ then perform } p_6(i,k) = p_5(i,k) - \text{KEY}(i,k) \\ &\text{If } x_2'(i) = 1, \text{ then perform } p_6(i,k) = p_5(i,k) + \text{KEY}(i,k) \\ &\text{if } x_2'(i) = 2, \text{ then perform } p_6(i,k) = p_5(i,k) \oplus \text{KEY}(i,k) \end{aligned} \quad (14)$$

Where i = 1, 2, 3……..M×N, and symbols "-", "+" and "⊕" are representing DNA Subtraction, DNA Addition and DNA Ex-or operations.

After completion of the above diffusion process, a one dimensional DNA sequence P_6 ={($p_6(1,1)$, $p_6(1,2)$, $p_6(1,3)$, $p_6(1,4)$), ($p_6(2,1)$, $p_6(2,2)$, $p_6(2,3)$, $p_6(2,4)$)……(p_6(M×N, 1), p_6(M×N, 2), p_6(M×N, 3), p_6(M×N, 4))} is obtained.

Step 7: After that, each elements of sequence Z_2' are used to decode the quadruples of DNA bases of sequence P_6 into a decimal value of a pixel and finally obtained a decoded sequence of pixels P_7.

Step 8: Finally, the obtained one dimensional pixel sequence of image matrix P_7 is transformed into a two dimensional cipher image matrix P_8 (M, N).

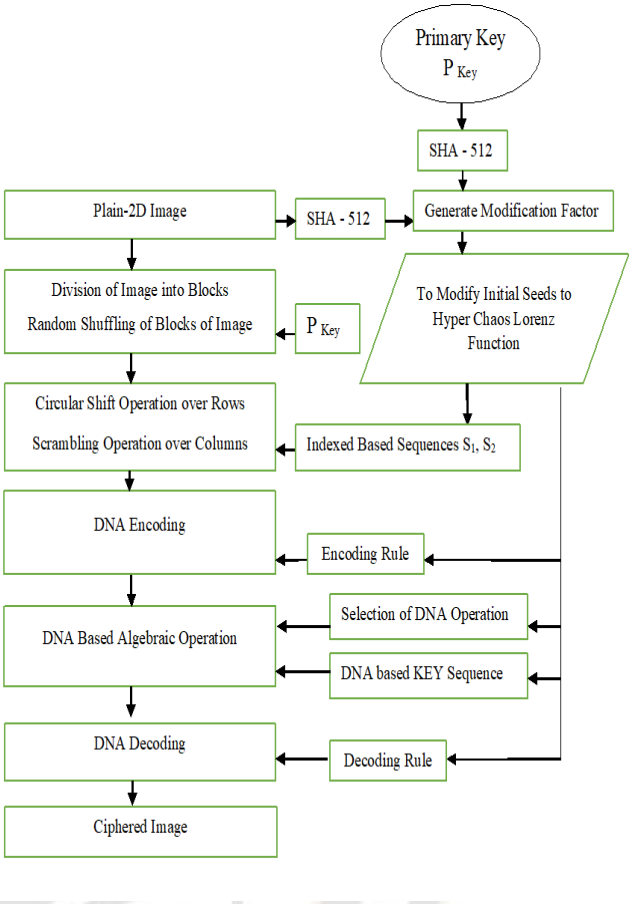


Figure 1: Process flow of image encryption technique

D. Image Decryption Technique

As the proposed image encryption technique is symmetric in nature, so the decryption process is exactly the inverse of the encryption procedure. Before using a decryption technique, a receiver must receive all of the secret credentials via a secure channel and generate the necessary indices and keys. After that, apply the previously defined permutation and diffusion phases in the same operating manner but in reverse order, with some minor changes such as use of DNA Subtraction operation instead of the DNA Addition operation and vice-versa respectively. Finally, the proposed technique successfully retrieves a 2-D plain image.

V. IMPLEMENTATION AND CRYPTANALYSIS RESULTS

The implementation of the designed technique was carried out in Python language based online IDE Google Colab. The proposed technique has been validated by considering three standard greyscale images such as Cameraman, Lena and Pepper image of dimension 256×256. . The primary key P_{key} is taken of string of minimum length of 15 characters. The secure

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received**: 20 May 2023 **Revised**: 28 July 2023 **Accepted**: 16 August 2023*

keys are considered here as primary key P_{key} = #4@7%$#!5&(%8$? and the initial input seeds to the chaotic functions are as x_1 = 0.0100080000000118, y_1 = 0.9865432123440001, z_1 = 0.3230000000100198, w_1 = 0.9125432123440001, x_2 = 0.0123080986000016, y_2 = 0.1100090000000198, z_2 = 0.1003000000010011, w_2 = 0.9235432123440001 and r = -1 respectively.

Figure 2 displays the various intermediate output images during the execution of proposed encryption technique. So, it is evident that there is no visual similarity between the plain image and the ciphered image. Furthermore, the cryptanalysis of the proposed technique against the standards attacks is observed in terms of hardness against differential, statistical and brute-force attack.

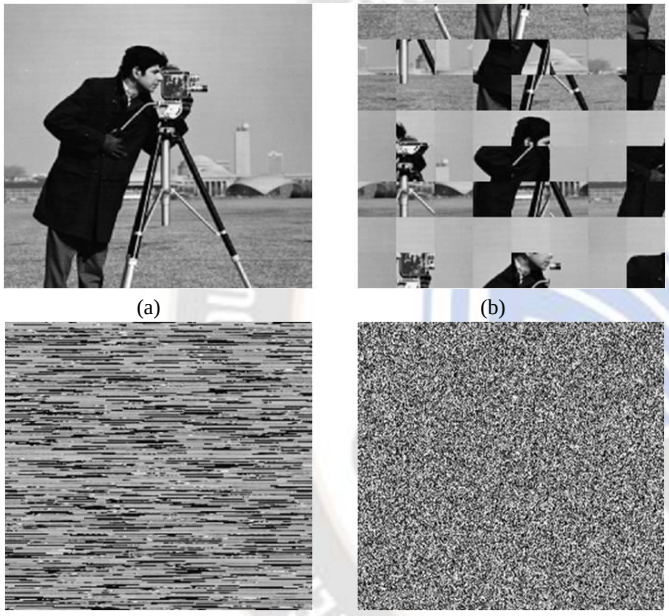
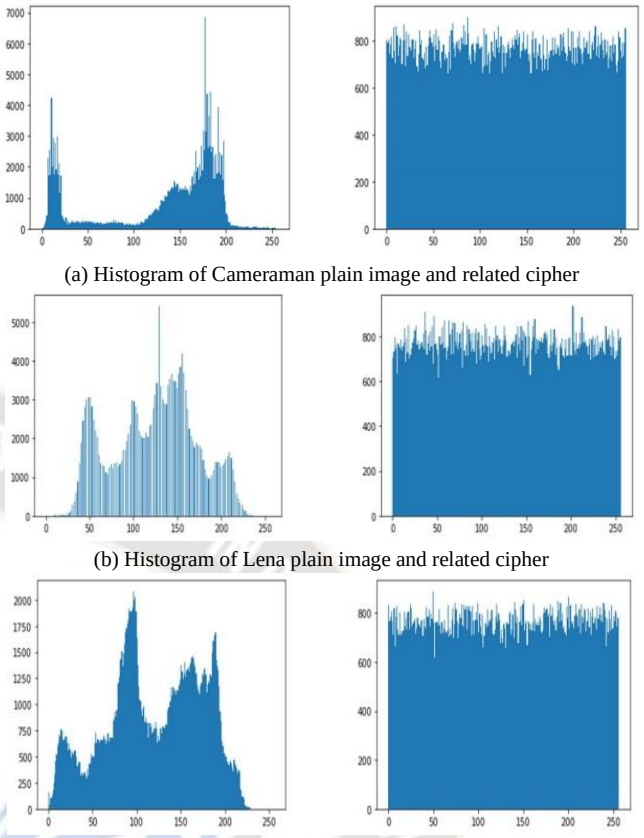


Figure 2: Exhibits the different stages of the Encryption Technique (a) The original Cameraman image (b) Interim image following random shuffling of divided blocks (c) Interim image following the pixel confusion stage (d) Final ciphered image following the DNA diffusion stage

A. Analysis of Histogram

The statistical metric that shows the graphical spectrum of an image's pixel values. A good image encryption scheme must have an even distribution of pixels in the form of a flat histogram in order to assure that the encrypted image does not provide any sort of predicted clues to an attacker. Figure 3 shows the histogram of the original images and their encrypted images. As can be seen, the plain image components' histograms are somewhat steep and focused in comparison to the cipher image histograms, which are uniform and flat. Therefore, the proposed scheme is resilient to the statistical assault due to the even distribution of pixels.



(a) Histogram of Cameraman plain image and related cipher

(b) Histogram of Lena plain image and related cipher

(c) Histogram of Pepper plain image and related cipher

Figure 3: Histograms of plain images and their related encrypted images

B. Key Space

The key space means possible numbers of keys. A reliable technique needs to be sufficiently large key space to increase the technique's resistance against the brute-force assault. Therefore, image encryption technique should possess key space greater than 2^{100} from an efficiency and hardness perspective. In the proposed scheme, the secure key is a combination of primary key and credentials of chaotic function. The primary key P_{Key} is a string having a length of at least 15 characters which provide a key space of 2^{120}. The secure parameters in terms of input seeds to the chaos function are (x_1, y_1, z_1, w_1, x_2, y_2, z_2, w_2), if each of input has a precision of 10^{-14}, then the key space would be $(10^{14})^8 = 10^{112}$ (approximately > 2^{336}). So, the total key space is $2^{456} > 2^{100}$, which is sufficiently large enough to resilience against the brute-force attack [21][22].

C. Key Sensitivity

The security parameter determines the impact of minute alteration in secret key credential over the cipher output. A robust cryptosystem should possess an extreme key sensitivity. To validate the key sensitivity, generate the cipher image by slightly changing the primary key P_{Key} from #**4**@7%$#!5&(%8$? to #**3**@7%$#!5&(%8$? ; while keeping the other secure key parameters to chaotic function remains

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received**: 20 May 2023 **Revised**: 28 July 2023 **Accepted**: 16 August 2023*

unchanged to encrypt the plain picture. As cameraman picture is illustrated in figure 4(a) and their ciphered image with P_{Key} and $P_{Key'}$ are shown in figure 4(b) and 4(c). Figure 4(d) depicts the cipher image obtained by taking difference of 4(b) and 4(c) image. Mathematically, the contrast rate between the 4(b) and 4(c) cipher image is 99.61%; which demonstrates the extreme sensitivity of technique to the secure credentials.

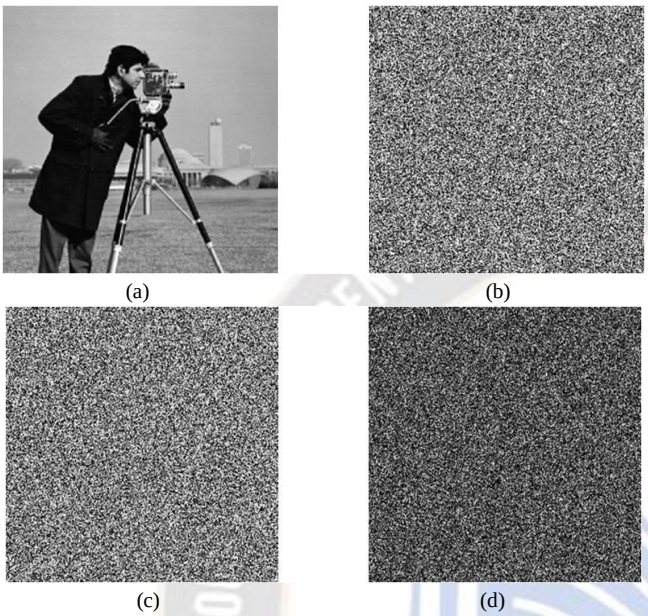


Figure 4: Validation of Key sensitivity test over Cameraman image during encryption (a) The Plain picture (b) Encrypted Image with correct key (c) Encrypted Image by minute altering P_{Key} (d) Difference Image (b - c).

D. Information Entropy

A statistical parameter introduced by Claude Shannon in 1948 to measure the randomness of the system. In image encryption, entropy measures the complexity of an encryption system. For plain image, entropy lies in a range of 0 to 8, while for encrypted image entropy near around an optimal value 7.9 is considered to be the best case. The cryptosystem having entropy closer to the optimal value ensure the brilliancy of algorithm.

Here, we considered three different test images such as Cameraman, Lena and Pepper plain image and their related cipher images. It can be observed from the Table 5 that cipher images possess entropy greater than 7.9. Therefore, proposed algorithm generates a good random cipher image.

Table 5: Entropy analysis

Images	Cameraman	Lena	Pepper
Original image	7.0254	6.4497	7.6038
Cipher Image	7.9972	7.9962	7.9976

E. MSE/PSNR Analysis

An encrypted image must vary considerably from its original state. Mean square error is defined as the average squared difference between the plain picture and the associated encrypted picture. The MSE parameter can be statistically used to identify the strength of a cryptosystem. Larger the MSE value, leads to more secure the encryption method. While, Peak signal to noise ratio parameter is an approach for determining the level of encryption quality; the higher PSNR value reflects the closeness of the ciphered image to the original image. As a result, a lower PSNR number suggests that an encryption technique is stronger. According to a scientific study of Norouziet. al. in 2013 [31], it was observed that to meet the security criterion of image encryption; the PSNR value should be less than 8.385 and the MSE value should be greater than 9,555. Table 6 depicts the output of MSE and PSNR assessments using three test images.

Table 6: MSE and PSNR Values

Images	MSE	PSNR
Cameraman	9838.24	8.2016
Lena	9786.25	8.2245
Pepper	9875.96	8.1851

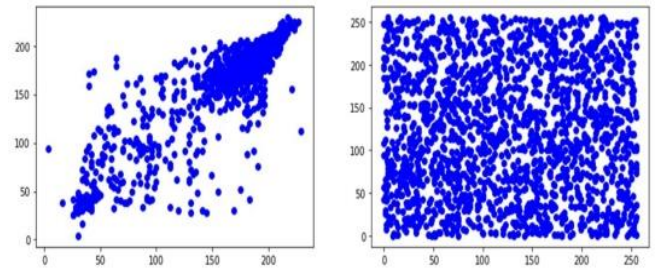
High MSE and low PSNR value obtained from the results clearly shows that the original images and the associated encrypted images differ significantly. The outcomes demonstrate that the proposed technique is effective, as proofed by high MSE and low PSNR values.

F. Correlation Coefficient Analysis

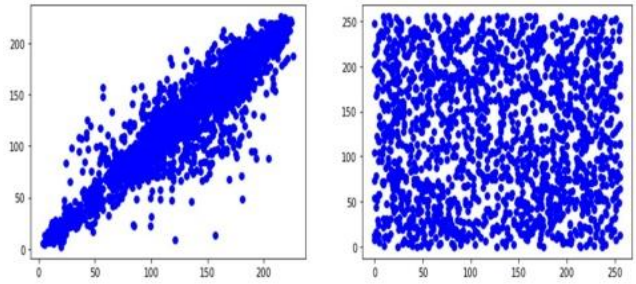
The statistical parameter which examines how neighboring pixels in an image relate to one another. Smaller the value of correlation more is the image resistant to the statistical attack. The pixels in a plain image have strong correlation with their neighboring pixels. Therefore, an attacker can so quickly take advantage of the situation obtain the crucial data. So encryption is needed to eliminate this pixel correlation.

Figure 5 shows the pixel correlation of plain images and their related encrypted images. From these figures it is visually seen that neighboring pixels in plain image is highly correlated, while in cipher images adjacent pixels are dispersed and less correlated. Additionally, Table 7 displays the results of the correlation coefficient test between the adjacent pixels in three distinct images in both the horizontal and vertical orientations, before and after encryption. Here, it can be seen that while encrypted images have substantially low values of the correlation coefficient than plain images, which helps them fend off statistical attacks.

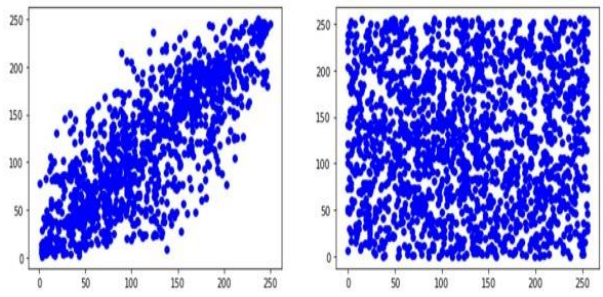
International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received**: 20 May 2023 **Revised**: 28 July 2023 **Accepted**: 16 August 2023*



(a) Pixel correlation in Horizontal direction



(b) Pixel correlation in Vertical direction



(c) Pixel correlation in Diagonal direction

Figure 5: Pixel correlation analysis of the Cameraman image and their related cipher image.

Table 7: Results of Pixel Correlation Analysis

Images	Before Encryption			After Encryption		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Cameraman	0.9393	0.9391	0.9101	-0.0017	0.0079	0.0057
Lena	0.9512	0.9493	0.9213	0.0011	0.0015	-0.0009
Peppers	0.9521	0.9365	0.9119	0.0046	0.0037	0.0029

G. Differential Attack Analysis

The differential attack analysis is validated by finding the relationship between the two encrypted images, which are generated by changing the single pixel value in a plain image. It is stated that for a robust cryptosystem, small change in plain image reflects back totally different encrypted images. The strength of any cryptosystem against differential attack can be validated by using two performance metrics NPCR and UACI. The Number of pixel change rate (NPCR) is a metrics that determine the percentage of the different pixels with respect to the same position of two ciphered images which are generated from the same image by varying a single pixel. The Unified average change in intensity (UACI) determine the average change in intensity of pixel values of two encrypted images whose plain image differ by single pixel value.

The algorithm having NPCR and UACI values nearly or greater than 99 and 33.3 percent make the cryptosystem strong and safer against the differential attack. Table 8 it is clearly seen that NPCR and UACI values of all three different cipher images are greater than 99% and 33.3%, which in turn reflects the hardness of the designed technique against the differential attack.

Table 8: Result Analysis of NPCR and UACI

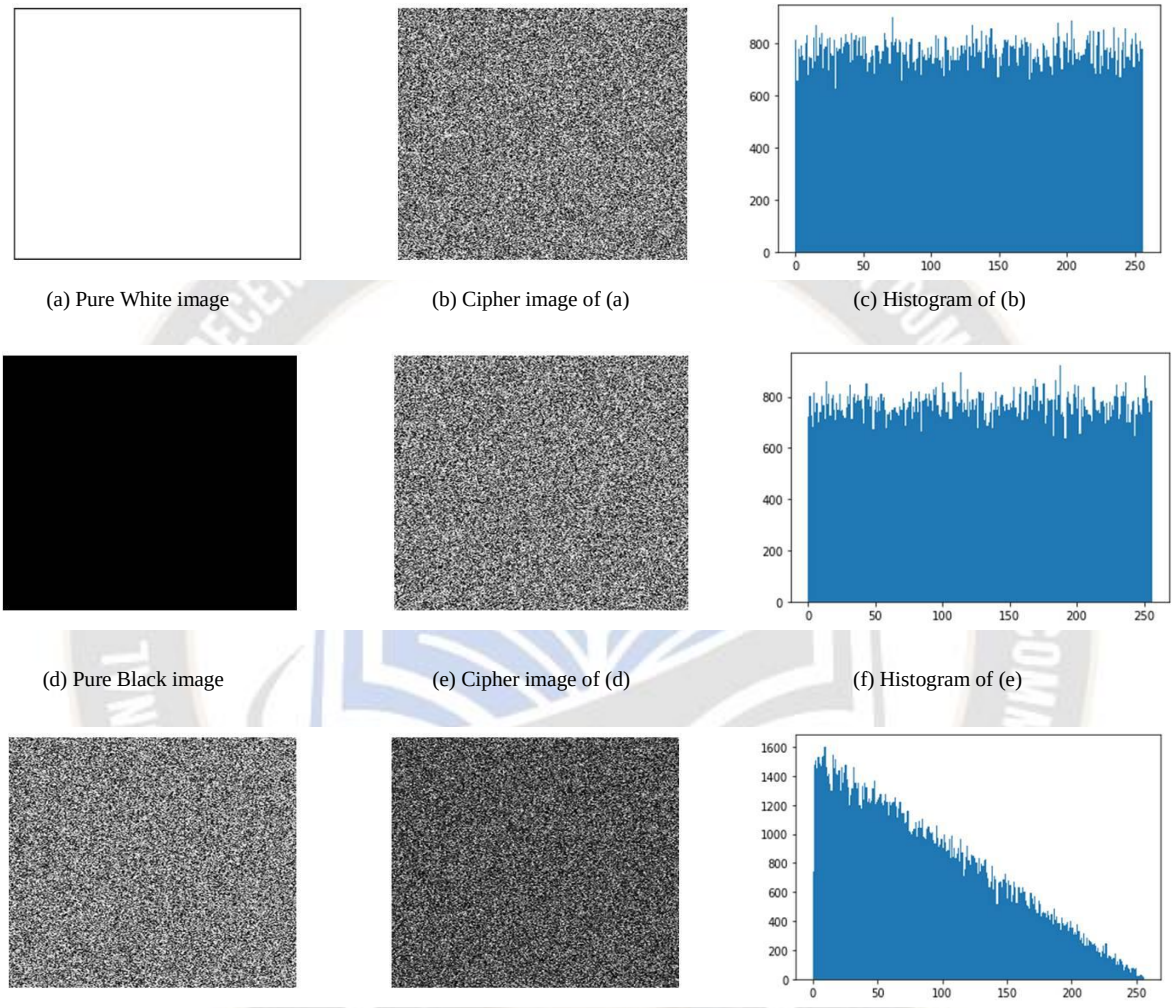
Images	Cameraman	Lena	Pepper
NPCR	99.69	99.6	99.63
UACI	33.47	33.5	33.62

H. Known and chosen plain text attack

To prove the image safety, we mainly consider four known attacks during cryptanalysis such as known plain text attack, chosen plain text attack, cipher text only attack and chosen cipher text attack. Out of these, chosen cipher text attack is most significant one. If an encryption algorithm copes soundly against this significant attack, it is strongly believed that it can also withstand against the rest three attacks comfortably. During cryptanalysis approach, an attacker try to choose particular plain text information to generate the associated cipher text information and try to deduce some kind of relationship between them, mainly secure key. To test this significant attack, we considered the encryption of three different images such as pure White, pure Black and special White image. The obtained cipher image of figure 6(a), (d) are shown in figure 6(b), (e); and cipher of special white is shown in figure 6(g) respectively. Additionally, the figure 6(c), (f) shows the histogram of ciphered image of figure 6(b), (e); while figure 6(i) show the histogram of difference image shown in figure 6(h), which was obtained by subtracting the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received**: 20 May 2023 **Revised**: 28 July 2023 **Accepted**: 16 August 2023*

pure white cipher and special white cipher. From above histograms, figure 6(c) and 6(f), it was analyzed that their shapes are flat and uniform curve which were not reflecting any substantial information. In addition, the histogram of difference image shows a decline curve which proves that ciphered image of pure white and special white are significantly different and extremely sensitive with the plain text information. Table 9, show the resultant value of different parameters such as correlation coefficient, Entropy, NPCR and UACI of pure White, pure Black and their ciphered images. From the given result, it is clear that proposed algorithm substantially outperforms in all respects. Henceforth, proposed algorithm is highly secure against the known/chosen plain text attack.



(a) Pure White image (b) Cipher image of (a) (c) Histogram of (b)

(d) Pure Black image (e) Cipher image of (d) (f) Histogram of (e)

(g) By changing one pixel of (a) (h) Difference of (b)-(g) (i) Histogram of (h)

Figure 6: Visual Result analysis of Known and Chosen cipher text attack

Table 9: Known and Chosen cipher text attack result

Images	Pixel Correlation			Entropy	NPCR	UACI
	Horizontal	Vertical	Diagonal			
Plain Pure White Image	-	-	-	0	-	-
Cipher of Pure White Image	0.0013	0.0019	-0.0010	7.9968	99.64	33.49
Plain Pure Black Image	-	-	-	0	-	-
Cipher of Pure Black Image	0.0016	-0.0031	-0.0021	7.9971	99.55	33.57

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received**: 20 May 2023 **Revised**: 28 July 2023 **Accepted**: 16 August 2023*

I. Complexity Analysis

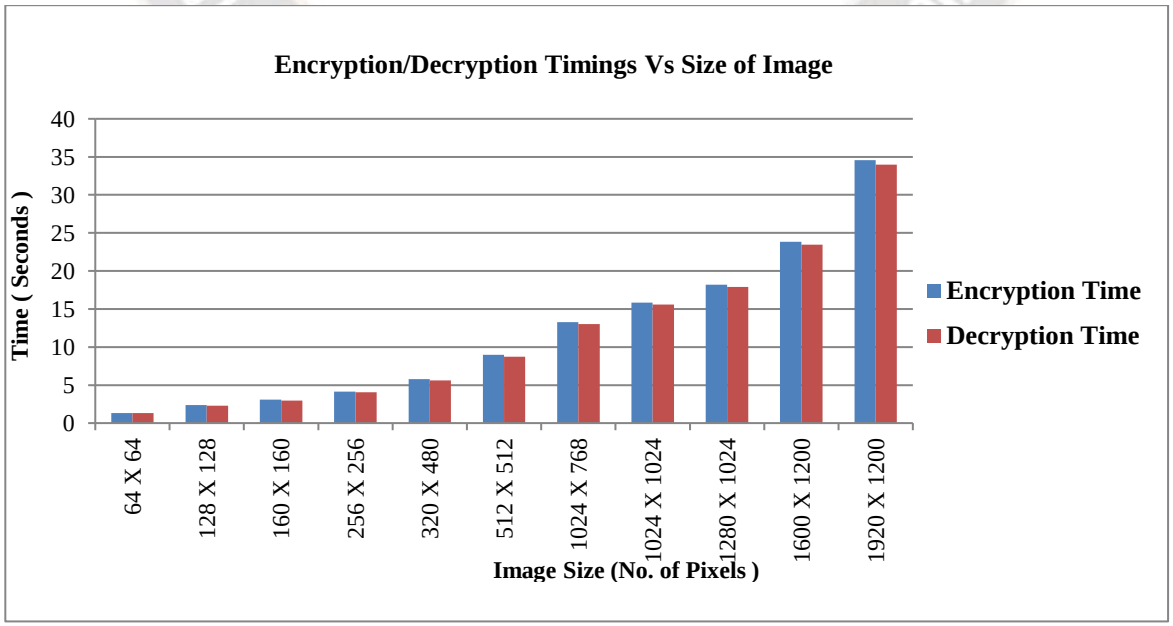
The robustness against the attacks is not only a criteria of success, even efficiency matters a lot. The efficiency is computed by the encryption time of the process, which mainly comprises of time required from generation of the keys until the cipher generation. During key generation, 6 keys are to be generated, so time required is O(6MXN). The permutation process mainly required O(M×N/64) time for random shuffling of divided blocks along with O(2M×N) for circular shit and column wise indexing operation. While DNA encoding and decoding also require O(8M×N). Beside this, time require to operate DNA diffusion operation is O(4M×N). Moreover, proposed algorithm confusion and diffusion phase's operation can easily be simulated on parallel processing environment to improve the efficiency, while in Wang et. al. [18] only scrambling operation can be parallelized. The computational complexity of the suggested scheme is order of O(20M×N), while Wang et. al. [18] scheme requires O(29M×N). Henceforth, proposed algorithm consume less computation time which make it time efficient and appealing to real time environment applications.

VI. COMPARATIVE STUDY WITH EXISTING METHODS

To validate the worthiness of an image encryption algorithm, a comparative study is made with the existing literature work [18, 24, 25, 26, 27, 28, 29, and 30]. So, here the proposed approach is compared by considering different strength analysis indicators such as pixel correlation in different directions, NPCR, UACI and entropy. The results of various parameters are presented in Table 10 by considering a standard test image "Lena image" of dimension 256×256. From the table 10, it is precisely analyzed that pixel correlation coefficient in all the directions are relatively small and close to zero compared to existing method, which suggests that the proposed approach is more resilient to statistical attack. Moreover, our technique has more entropic information and very closed to ideal value 8. The UACI and NPCR values are also in line with ideal values 99% and 33.3%, and significantly higher when compared to other techniques. This proves the effectiveness and robustness of the encryption scheme against the statistical and differential attack.

Table 10: Comparative Study

Algorithm Reference	Pixel Correlation			Entropy	NPCR	UACI
	Horizontal	Vertical	Diagonal			
Proposed	0.0011	0.0015	-0.0009	7.9972	99.69	33.35
Wang et. al. [18]	0.0013	0.0009	0.0012	7.9974	99.66	33.36
[24]	-0.0086	-0.102	0.0125	7.9976	99.41	33.26
[25]	0.0062	-0.0001	0.0018	7.5683	99.61	33.48
[26]	-0.007	0.0151	0.003	7.8963	99.6	33.63
[27]	-0.0017	0.0004	0.0028	7.9976	99.6	33.38
[28]	-0.0232	-0.0093	0.0537	7.9981	99.59	33.42
[29]	0.0039	0.0174	-0.0034	7.998	99.62	33.51
[30]	0.0048	0.0256	-0.0543	7.9981	99.6	33.43



Graph1: Encryption and Decryption timing with varying size of plain image

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received**: 20 May 2023 **Revised**: 28 July 2023 **Accepted**: 16 August 2023*

VII. PERFORMANCE ANALYSIS

The efficiency of an encryption technique is determined by its execution time. Lower the enciphering time shows the faster execution of an algorithm. In image encryption schemes, the confusion and diffusion process impact a lot on the computing speed. So, as in proposed scheme the efficient design of key generation, confusion and diffusion processes make our encryption scheme more efficient in terms of computing speed as compared to existing literature work [18, 24, 25, 27, 28, 29 and 30] given in Table 11. From table, it is observed that the proposed technique consume less time for encryption among the existing approaches; which make it faster and scalable in real time applications. Additionally, the encryption and decryption timings of different images of varying sizes of proposed techniques are shown in Graph 1. From graph, it is clearly demonstrated that the enciphering and deciphering timings of the proposed method increase linearly with the size of the plain image. Hence, the linear time complexity of both the processes enhances its time efficiency.

Table 11: Encryption Time comparative analysis

Algorithm Reference	Encryption Timings
Proposed	4.13
Wang et. al. [18]	5.98
[24]	27.6
[25]	9.6
[26]	6.42
[27]	7.14
[28]	8.03
[29]	5.1
[30]	4.68

VIII. CONCLUSION

In this work, an efficient and secure image encryption technique using DNA computing and hyper chaos function has been discussed. The proposed technique has countered the addressed issues of Wang et. al scheme [18] successfully. The scheme employs SHA-512 hash of input image and primary key to alter the initials seeds of hyper chaos Lorenz function and enhance the security features by generating one time key and make it extremely key sensitive. The dynamicity of hyper chaos Lorenz function based sequences makes it's extraordinary and help to further strengthen the security and robustness of the innovative proposed technique. Furthermore, implementation and cryptanalysis results have demonstrated that the scheme achieve optimal standard values of security parameters and can also effectively resists against statistical attack, differential attack, known plain text attack and exhaustive attack. In addition, the detailed comparative and performance analysis with the existing standards proves its worthiness and efficiency. Moreover, the algorithm has not only a better encryption effect but also cope successfully with the addressed issues, which make it more efficient, rationale and practical for real time applications.

REFERENCES

[1] A. Singh, B. Singh, "Design and analysis of DNA based cipher for image using dual chaotic map", ICTACT Journal on soft computing, Vol. 13(3), pp. 2969-2976.

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

[3] Y. Zhang, D. Xiao, K. W. Wong, J. Zhou, S. Bai, M. Su, Perturbation meets key-based interval splitting arithmetic coding: security enhancement and chaos generalization", Secure Communication Networking, vol. 9, 2016, pp. 43–53.

[4] 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, 2017, pp. 9907–9927.

[5] X. Wang, L. Teng and Q. Xue, "A novel colour image encryption algorithm based on chaos", Signal Process, vol. 92(4), 2012, 1101-1108.

[6] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki and M. R. Mosavi, "A novel image encryption based on hash function with only two-round diffusion process", Multimedia Syst., vol. 20, 2013, pp. 45–64.

[7] A. Kadir and A. Hamdulla and W. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th order CNN", Optik, Vol. 125, 2014, pp. 1671–1675.

[8] G. Ye, X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map", Neuro computing, vol. 251, 2017, pp. 45–53.

[9] A. YaghoutiNiyat, M. H. Moattar and M. NiaziTorshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata, Opt. Lasers Eng., vol. 90, 2017, pp. 225–237.

[10] M. Kar, A. Kumar, D. Nandi and M. K. Mandal, "Image encryption using DNA coding and hyper chaotic system, In IETE Technical Review, Vol. 37, no. 1, 2018, pp. 12-23.

[11] X. Zhang, Z. Zhou and Y. Niu, An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding, In IEEE Photonics Journal, vol. 10, no. 4, 2018, pp. 1-14.

[12] 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, 2013, pp. 3596–3600.

[13] Q. Zhang and X. Wei, "A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system", Optik, vol. 124, 2013, pp. 6276–6281.

[14] X. Huang and G. Ye, "An image encryption algorithm based on hyper-chaos and DNA sequence", Multimedia Tools and Applications, vol. 72, 2014, pp. 57–70.

[15] X. Wang, Y. Zhang and X. Bao, "A novel chaotic image encryption scheme using DNA sequence operations", Opt. Lasers Eng., vol. 73, 2015, pp. 53–61.

[16] X. Wang, H. Zhang and X. Bao, "Color image encryption scheme using CML and DNA sequence operations", Bio Systems, vol. 144, 2016, pp. 18–26.

[17] P. Zhen, G. Zhao, L. Min and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy", Multimedia Tools and Applications, vol. 75, 2016, pp. 6303–6319.

[18] X. Wang, Y. Hou, S. Wang and R. Li, "A New Image Encryption Algorithm Based on CML and DNA Sequence," In *IEEE Access*, vol. 6, pp. 62272-62285, 2018, doi: 10.1109/ACCESS.2018.2875676.

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

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

[21] P. T. Akkasaligiar and S. Biradar, "Selective medical image encryption using DNA cryptography", Information Security Journal: A Global Perspective, vol. 29, 2, pp 91-101.

[22] A. V. Bharadwaja and V. Ganesan, " A novel hybrid image hiding technique using Elliptic curve cryptography and DNA computing technique", International Journal of electronic security and digital forensics, vol. 14(4), 2021, pp. 460-473.

[23] X. H. Huang, Y. Dong, G. Ye, W. S. Yap, B. M. Goi, "Visually meaningful image encryption algorithm based on digital signature", Digital Communications and Networks, vol. 9, 2023, pp. 159-165.

[24] W. Liu, K. Sun and C. Zhu, "A fast image encryption algorithm based on chaotic map", Optical Lasers Engineering, vol. 84, 2016, pp. 26–36.

[25] S. Zhu, X. Deng, W. Zhang and C. Zhu, "A New One-Dimensional Compound Chaotic System and Its Application in High-Speed Image Encryption", Applied Sciences, vol. 11(23), 2021, pp. 11206.

[26] L. Huang, S. Cai, X. Xiong, and M. Xiao, ''On symmetric color image encryption system with permutation-diffusion simultaneous operation,'' Opt. Lasers Eng., vol. 115, 2019, pp. 7–20.

[27] X. Wang, N. Guan, A novel chaotic image encryption algorithm based on extended zigzag confusion and RNA operation, Opt. Laser Technol. 131 (2020) 106366.

[28] T. Hu, Y. Liu, L.H. Gong, and C.J. Ouyang, "An image encryption scheme combining chaos with cycle operation for DNA sequences," Nonlinear Dynamics, vol. 87, no. 1, 2017, pp. 51–66, 2017.

[29] W. Ran, E. Wang and Z. Tong, "A double scrambling-DNA row and column closed loop image encryption algorithm based on chaotic system", PLoS One, vol. 17(7), 2022. doi: 10.1371/journal.pone.0267094. PMID: 35819964; PMCID: PMC9275730.

[30] T. Y. Wu, X. Fan, K. H. Wang, C. F. Lai, N. Xiong and J. M. T. Wu, "A DNA Computation-Based Image Encryption Scheme for Cloud CCTV Systems", In IEEE Access, vol. 7, 2019, pp. 181434-181443.

[31] B. Norouzi, S. M. Seyedzadeh and S. Mirzakuchaki, "A novel image encryption based on hash function with only two-round diffusion process", Multimedia Systems, vol. 20, 2014, pp. 45–64.