

AN IMAGE ENCRYPTION SCHEME BASED DNA SEQUENCES RULES

M. Purnachandra Rao^{1*}, Dr. Ramesh Makala²

¹*Department of CSE, KKR & KSR Institute of Technology & Sciences, Guntur, AP, India,
purnamailroom@gmail.com.*

²*Department of Information Technology, RVR & JC College of Engineering, Guntur, AP, India,
mrameshmailbox@gmail.com.*

ABSTRACT

Transmission of digital image over the internet has become more and more popular. However, the openness and sharing of networks exposes the security of digital image to serious threats in the process of transmission. Cryptography in images is used in our real world very often. The social communication apps like Whatsapp uses end-to-end encryption to transmit text messages and images. The power of encryption is based on the time of encryption and decryption, strength of the key used. The traditional algorithms like AES, DES cannot resist all kinds of attacks. This paper proposes a new dynamic cryptographic technique based on the eight DNA encoding and decoding rules. The chaotic sequence in this system is generated using DNA addition and DNA subtraction rules. Since no XOR operations are used in this proposed system, it enhances the security.

Keywords: *DNA, Image Encryption, Decryption*

I. INTRODUCTION

Chaos based optical encoding and image encryptions have attracted considerable attention due to their superiority. Spatiotemporal chaotic systems are gradually regarded with better properties suitable for optical image encryptions than one dimension chaotic system such as larger parameter range, better randomness and more chaotic sequences.

DNA computing is applied in cryptography for massive parallelism, huge storage and ultra-low power consumption. Therefore, the DNA-based schemes have been well studied and achieved good results in recent years. In these DNA based the schemes, the ideas are focused on two main approaches. The first consists of applying different DNA operations, like DNA addition and DNA subtraction, on DNA coefficients after transforming the decimal matrixes

values. The second consist of adopting a dynamic DNA encoding rule depending on a secret key. However, some of the schemes in the both approaches are not satisfied in the security performance. The scheme in employs XOR operations and the DNA encoding rules to calculate the ciphered image, which leads equivalent keys in its key space. The scheme in applied a fixed DNA encoding rule and the ciphered pixel values only depend on the key of the algorithm, which can be cracked in chosen plaintext attacks. The proposed scheme in this paper avoids using XOR operations, which breaks the reduction of key space. To prevent such loop-holes of the fixed DNA encoding rule, the proposed scheme employs the DNA encoding/decoding rule as a part of secret key and one-time pad encryption policy to enhance the sensitivity of the plaintext. Besides, the superior approach to the former DNA based schemes is that the DNA matrix is calculated and determined by the index lattice of the MLNCML system which depends on the plaintext image. Since the spatiotemporal chaos has $L=100$ lattices, each lattice can be selected as the potential one for generating the corresponding DNA matrices in the specific encryption procedure by the plaintext image.

In addition, the former DNA based encryption schemes are based on low dimension chaotic maps. The drawback of periodic degrading with finite precision in digital computers still remains. In order to overcome the above drawbacks, high dimensions spatiotemporal chaotic system is employed in the proposed scheme, which can alleviate the dynamical degradation and provide multiple chaotic sequences for encryptions in the proposed scheme. The motivation of the work is to avoid such vulnerabilities and obtain a high level security encryption scheme.

1.1 DNA :

DNA stands for deoxyribonucleic acid. DNA shapes living organisms. It stores all the information about the body features of any organism. It is unique for each individual. DNA is the polymer made of monomers called deoxyribo-nucleotides. Each nucleotide is made of deoxyribose sugar, phosphate group and nitrogenous base. Nitrogenous bases are of two types purines (adenine and guanine) and pyrimidines (cytosine and thymine). These bases are represented as A (adenine), G (guanine), C (cytosine) and T (thymine). A bonds with T and G bonds with C. These bases and bonding play an important role in DNA processes like DNA computing and DNA cryptography.

Bioinformatics play very important role in DNA computing and DNA cryptography.

The definition of Bioinformatics is: “The mathematical, statistical and computing



methods that aim to solve biological problems using DNA and amino acid sequences and related information DNA stands for deoxyribonucleic acid. DNA shapes living organisms. It stores all the information about the body features of any organism. It is unique for each individual. DNA is the polymer made of monomers called deoxyribo-nucleotides. Each nucleotide is made of deoxyribose sugar, phosphate group and nitrogenous base. Nitrogenous bases are of two types purines (adenine and guanine) and pyrimidines (cytosine and thymine). These bases are represented as A (adenine), G (guanine), C (cytosine) and T (thymine). A bonds with T and G bonds with C. These bases and bonding play an important role in DNA processes like DNA computing and DNA cryptography. Bioinformatics play very important role in DNA computing and DNA cryptography. The definition of Bioinformatics is: “The mathematical, statistical and computing methods that aim to solve biological problems using DNA and amino acid sequences and related information DNA stands for deoxyribonucleic acid. DNA shapes living organisms. It stores all the information about the body features of any organism. It is unique for each individual. DNA is the polymer made of monomers called deoxyribo-nucleotides. Each nucleotide is made of deoxyribose sugar, phosphate group and nitrogenous base. Nitrogenous bases are of two types purines (adenine and guanine) and pyrimidines (cytosine and thymine). These bases are represented as A (adenine), G (guanine), C (cytosine) and T (thymine). A bonds with T and G bonds with C. These bases and bonding play an important role in DNA processes like DNA computing and DNA cryptography. Bioinformatics play very important role in DNA computing and DNA cryptography. The definition of Bioinformatics is: “The mathematical, statistical and computing methods that aim to solve biological problems using DNA and amino acid sequences and related information

DNA stands for deoxyribonucleic acid. DNA shapes living organisms. It stores all the information about the body features of any organism. It is unique for each individual. DNA is the polymer made of monomers called deoxyribo-nucleotides. Each nucleotide is made of deoxyribose sugar, phosphate group and nitrogenous base. Nitrogenous bases are of two types purines (adenine and guanine) and pyrimidines (cytosine and thymine). These bases are represented as A (adenine), G (guanine), C (cytosine) and T (thymine). A bonds with T and G bonds with C. These bases and bonding play an

important role in DNA processes like DNA computing and DNA cryptography. Bioinformatics play very the body features of any organism. It is unique for each individual. DNA is the polymer made of monomers called deoxyribo-nucleotides. Each nucleotide is made of deoxyribose sugar, phosphate group and nitrogenous base. Nitrogenous bases are of two types purines (adenine and guanine) and pyrimidines (cytosine and thymine). These bases are represented as A (adenine), G (guanine), C (cytosine) and T (thymine). A bonds with T and G bonds with C. These bases and bonding play an important role in DNA processes like DNA computing and DNA cryptography. Bioinformatics play very important role in DNA computing and DNA cryptography. The definition of Bioinformatics is: “The mathematical, statistical and computing methods that aim to solve biological problems using DNA and amino acid sequences and related information DNA stands for deoxyribonucleic acid. DNA shapes living organisms. It stores all the information about the body features of any organism. It is unique for each individual. DNA is the polymer made of monomers called deoxyribo-nucleotides.

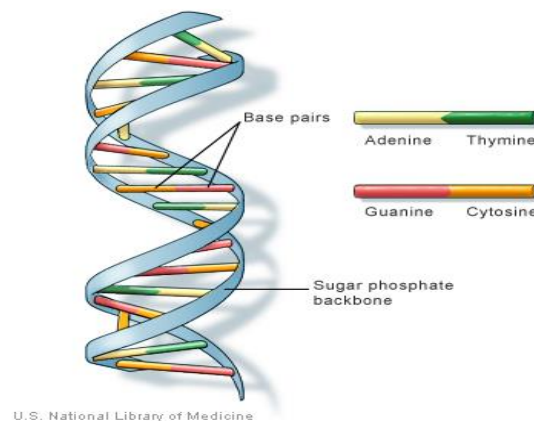


Fig.1 DNA Structure

Each nucleotide is made of deoxyribose sugar, phosphate group and nitrogenous base. Nitrogenous bases are of two types purines (adenine and guanine) and pyrimidines (cytosine and thymine). These bases are represented as A (adenine), G (guanine), C (cytosine) and T (thymine). A bonds with T and G bonds with C. These bases and bonding play an important role in DNA processes like DNA computing and DNA cryptography. Bioinformatics play very important role in DNA computing and DNA cryptography. The definition of Bioinformatics is: “The mathematical, statistical and computing methods that aim to solve biological problems using DNA and amino acid sequences and related information

1.2 DNA Cryptography:

DNA cryptography is one of the rapid emerging technology which works on concepts of DNA computing. A new technique for securing data was introduced using the biological structure of DNA called DNA Computing (aka molecular computing or biological computing). It was invented by Leonard Max Adleman in the year 1994, for solving the complex problems such as directed Hamilton path problem, NP-complete problem similar to The Travelling Salesman problem. Adleman is also known as the ‘A’ in the RSA algorithm – an algorithm that in some circles has become the de facto standard for industrial-strength encryption of data sent over the Web. The technique later on extended by various researchers for encrypting and reducing the storage size of data that made the data transmission over the network faster and secured.

DNA can be used to store and transmit data. The concept of using DNA computing in the fields of cryptography and steganography has been identified as a possible technology that may bring forward a new hope for unbreakable algorithms. Strands of DNA are long polymers of millions of linked nucleotides. These nucleotides consist of one of four nitrogen bases, a five carbon sugar and a phosphate group. The nucleotides that make up these polymers are named after the nitrogen base that it consists of; Adenine (A), Cytosine (C), Guanine (G) and Thymine (T).

1.3 DNA RULES

a) DNA Encoding rules:

A DNA sequence is composed of four nucleic acid bases (hereinafter abbreviated to base): A (adenine), C (cytosine), G (guanine), T (thymine), where A and T are complementary, G and C are complementary. Because 0 and 1 are complementary in the binary, so 00 and 11 are complementary, 01 and 10 are also complementary. By using four bases A, C, G and T to encode 00, 01, 10 and 11, there are 24 kinds of encoding rules. But there are only 8 kinds of encoding rules satisfying the Watson–Crick complement rule, as listed in Table 1.

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



01	G	C	G	C	A	T	A	T
10	C	G	C	G	T	A	T	A
11	T	T	A	A	C	C	G	G

Table.1 DNA Encoding

b) DNA Decoding rules:

The DNA decoding rules are the reverse of DNA encoding rules. By using four sequences 00, 01, 10 and 11 to decode A, G, C, T there are 24 kinds of decoding rules. But there are only 8 kinds of decoding rules satisfying the Watson–Crick complement rule, as listed in 2.

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

Table.2 DNA Decoding

c) DNA Addition Rules:

Addition and subtraction operations for DNA sequences are performed according to traditional binary addition and subtraction. Corresponding to 8 kinds of DNA encoding rules, there also exists 8 kinds of DNA addition rules. For example, according to DNA encoding Rule 1, the DNA addition Rule 1 is shown in Table 3 .

+	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 Addition

d) DNA Subtraction Rules:

Subtraction operation for DNA sequences is performed according to traditional binary subtraction. Corresponding to 8 kinds of DNA encoding rules, there also exists 8 kinds of DNA subtraction rules. For example, according to DNA encoding Rule 1, the DNA subtraction Rule 1 is shown in Table 4.

-	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 Subtraction

II. PROPOSED APPROACH

2.1 Algorithm for Encryption:

Without loss of generality, the gray images are employed to present the encryption scheme for simplicity. In this approach we take gray image as input source image. The corresponding encryption algorithm can be presented as follows:

Input:

$L=100$ and the source image sp . Secret keys: $\mu, \eta, \varepsilon, x_0(1)$, the index of the used DNA encoding rule, the index of the used DNA decoding rule. Generate 128 bits random number R .

Output:

Returns ciphered image c .

Method:

Step 1:

Combine η, ε and $x_0(1)$ with the random number R , and calculate the new sub key $\eta', \varepsilon', x'_0(1)$ and random number R' in the SHA-3 hash algorithm by the equation

$$(\eta', \varepsilon', x'_0(1), R') = \text{hash}(\eta, \varepsilon, x_0(1), R) \quad \text{Eq. (1)}$$

Step 2:

Calculate the initial values in Eq. (2) by using logistic map for as follows:

$$x'_0(i) = \mu x'_0(i-1)(1-x'_0(i-1)) \quad \text{Eq. (2)}$$

where $i \in [2, L]$. Iterate the MLNCML system $M \times N$ times to obtain sequences in Eq(3). Suppose sp is an one-dimensional pixel sequence and the k th pixel of sp is $sp(k)$. For each pixel, implement the following operation to obtain an $M \times N$ confused image G :

$$G(k) = \text{mod}\{\text{mod}(x'_k k \text{ mod}(G(k-1), L) \times 10^{16}], 256) + sp(k)G(k1)], 256\} \quad \text{Eq. (3)}$$

where the initial value $G(0) = 1$.

Encode G by a kind of DNA encoding rule (the index of this DNA encoding rule serves as secret keys) and transform it into an $M \times (N \times 4)$ DNA matrix D, i.e., encode every pixel of G as a 4-base DNA sequence:

$$D_k = D^1_k D^2_k D^3_k D^4_k, (k \in [1, M \times N]). \quad \text{Eq. (4)}$$

Step 4:

Compute z_k from the MLNCML system from

$$x_q = \{x_1(q), x_2(q), \dots, x_{M \times N}(q)\}$$

Where $q = (1 / (M \times N) (\sum sp(i))) \bmod L$ and each element denoted as

$$x_k(q) (k \in [1, M \times N]), \text{implement the following operation: } z_k = \text{mod}([x_k(q) \times 110^{16}], 256).$$

Encode z_k by a kind of DNA encoding rule (the index of this DNA encoding rule serves as secret keys) and transform it into an $M \times (N \times 4)$ DNA matrix D' .

Step 5:

Calculate the D'' as follows:

$$\begin{aligned} D_k + D'_k, \text{ mod}(R' \gg (k \bmod 128), 2) &= 1 \\ D_k - D'_k, \text{ mod}(R' \gg (k \bmod 128), 2) &= 0 \end{aligned}$$

Eq. (5)

where “ + ” and “ - ” are respectively the DNA addition operation and DNA subtraction operation in the proposed algorithm, “ >> ” is the binary left shift operation. The indexes of the used DNA addition rule and DNA subtraction rule serve as secret keys.

Step 6:

Decode D'' by a kind of DNA decoding rule (the index of this DNA decoding rule serves as secret keys), and we obtain the ciphered image, denoted by C.

Step 7:

If the one round encryption or the complete multi-rounds encryptions are accomplished, the value of (M, N)-pixel in the ciphered image is assigned with the value of q. The encryption process finishes.

2.2 Algorithm for image decryption :

The decryption algorithm, is the reverse process of encryption algorithm as follows:

Input:

$L = 100$ and the ciphered image C . Secret keys: $\mu, \eta, \varepsilon, x_0(1)$, the index of the used DNA encoding rule, the index of the used DNA decoding rule. Receive 128 bits random number R .

Output:

Returns the plaintext image sp .

Method:**Step 1:**

Combine η, ε and $x_0(1)$ with the random number R , and calculate the new sub key $\eta', \varepsilon', x_0'(1)$ and random number R' in the SHA-3 hash algorithm by the equation

$$(\eta', \varepsilon', x_0'(1), R') = \text{hash}(\eta, \varepsilon, x_0(1), R)$$

Step 2:

Calculate the initial values in Eq. (2) by using logistic map for as follows:

$$x_0'(i) = \mu x_0'(i-1)(1-x_0'(i-1))$$

where $i \in [2, L]$. Iterate the MLNCML system $M \times N$ times to obtain sequences in Eq. (2).

Step 3:

Extract the value q from the (M, N) -pixel in the ciphered image and compute z_k values by Eq. (4) from

$$x_q = \{x_1(q), x_2(q), \dots, x_{M \times N}(q)\}$$

Encode z_k by a kind of DNA encoding rule (the index of this DNA encoding rule serves as secret keys) and transform it into an $M \times (N \times 4)$ DNA matrix D' .

Step 4:

Compute DNA matrix D'' by encoding the ciphered image C in a kind of DNA decoding rule (the index of this DNA decoding rule serves as secret keys).

Step 5:

Compute DNA matrix D by the equation as follows:

$$D_k + D'_k, \text{ mod}(R' \gg (k \text{ mod } 128), 2) = 1$$

$$D_k - D'_k, \text{ mod}(R' \gg (k \text{ mod } 128), 2) = 0$$

Step 6:

Obtain the matrix G by decoding DNA matrix D by the kind of DNA decoding rule.

Step 7:

Compute the plaintext image sp by the following equation:

$$sp(k)=\text{mod}\{[\text{mod}(G(k) - G(k - 1))[\text{mod}([x_k(\text{mod}(G(k - 1),L) \times 10^{16}),256)],256)\}$$

III. RESULTS AND ANALYSIS

In this proposed algorithm, the gray image is given as input source image and a secret key will be generated. The decryption takes the secret key and the encrypted image. It outputs the original image. The above algorithm can provide cryptography features to the images of types, jpg,png....,with all possible sizes. However, this scheme is highly recommended to gray scale images. We can also apply this algorithm for color images by converting them to gray scale images. The decrypted image can't be represented back in color image.

From the above encryption and decryption scheme, it is clear that the key space is large enough to make brute-force attacks infeasible. The 128 bit random number generated will serve as one time pad thereby enhancing the security of the proposed scheme. The attackers will find difficulty in breaking the index rules of DNA rules used.


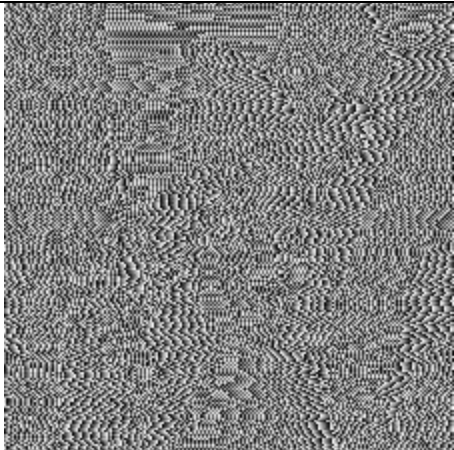
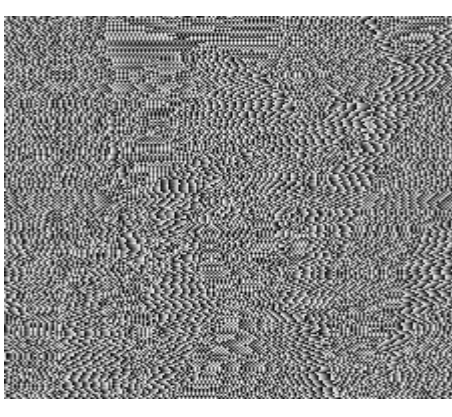

	Input image	Output image
Encryption		
Decryption		

Fig. 2 lena.png

Even though, if the attacker get the encrypted image, he can't get the original image which should be decrypted with the secret key. It is highly impossible to get the secret key for an attacker or man in the middle with this proposed algorithm.

Secret key:

$\mu=0.81, \eta= 0.09, \epsilon=0.11, x_0(1)=0.7986677779625615$, index of DNA encoding rule=5, index of DNA decoding rule=5, R= 8970879561344528630202215993876242528


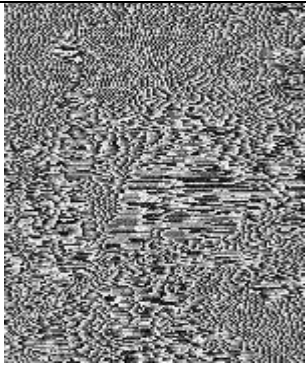
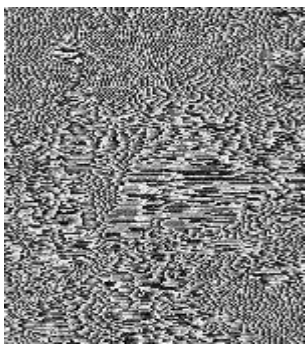

	Input image	Output image
Encryption		
Decryption		

Fig.3 parrot.png

Secret key:

$\mu=2.41, \eta= 0.06, \epsilon=0.55, x_0(1)=0.6033876937569501$, index of DNA encoding rule=8, index of DNA decoding rule=8, R= 8404454930013216980326650163520073148

	Input image	Output image
--	-------------	--------------

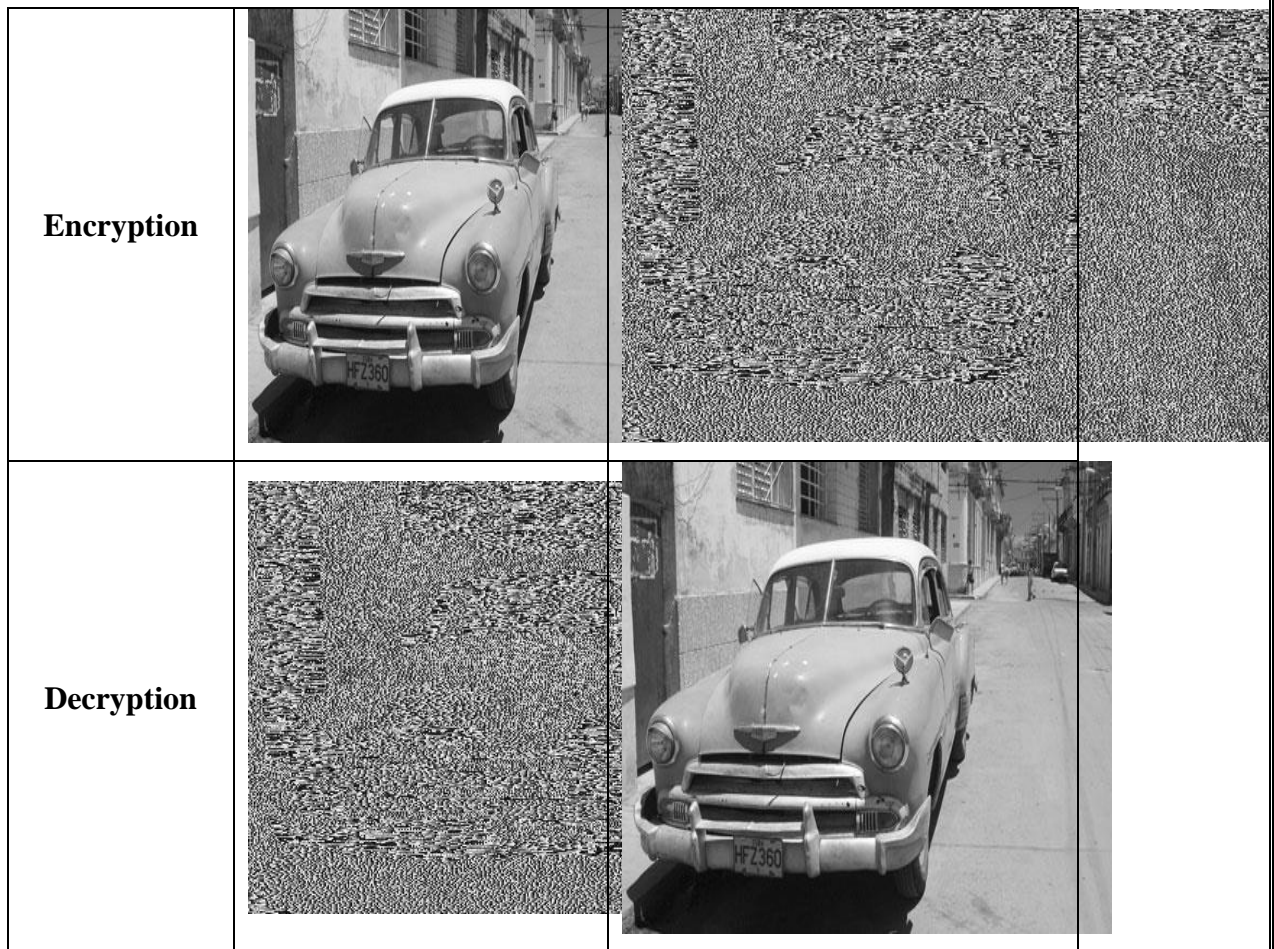

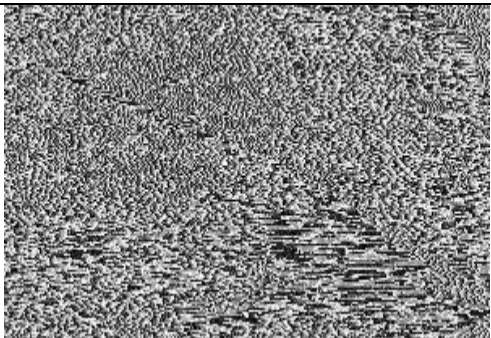


Fig.4 car.png

Secret key:

$\mu=3.4, \eta= 0.14, \varepsilon=0.12, x_0(1)= 0.3210534203474621$, index of DNA encoding rule=8, Index of DNA decoding rule=8, R= 852918341143717606803799350734504821

	Input image	Output image
<p>Encryption</p>		

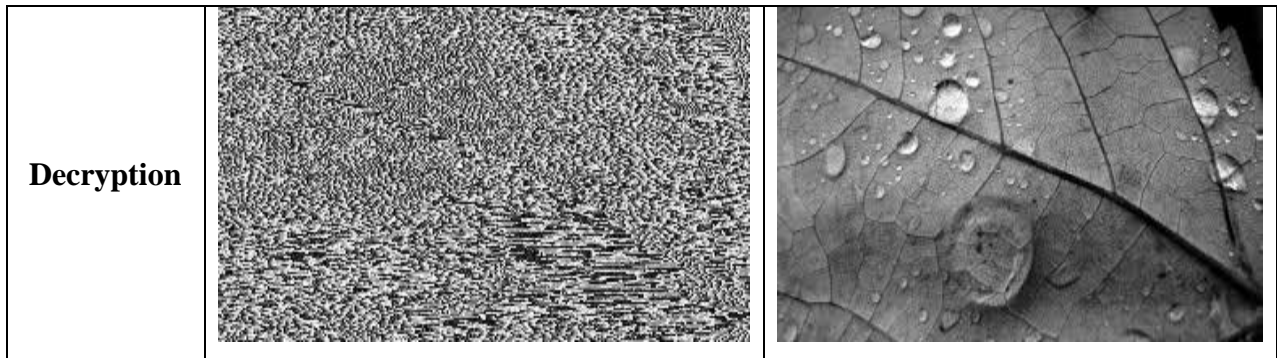


Fig.5 leaf.jpg

Secret key:

$\mu=1.76$, $\eta= 0.79$, $\varepsilon=0.39$, $x_0(1)=0.507037170858568$, index of DNAencodingrule=1, index of DNA decoding rule=1, R= 27343962730959355641428909503466716430


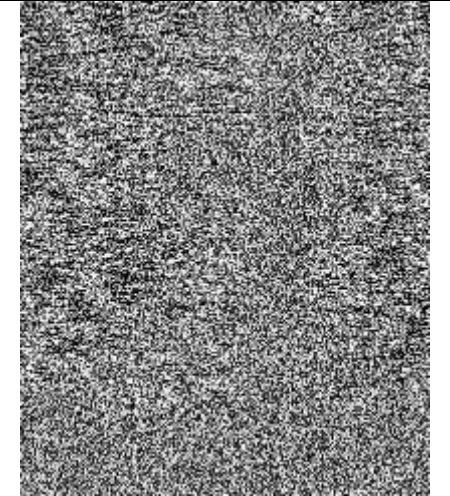
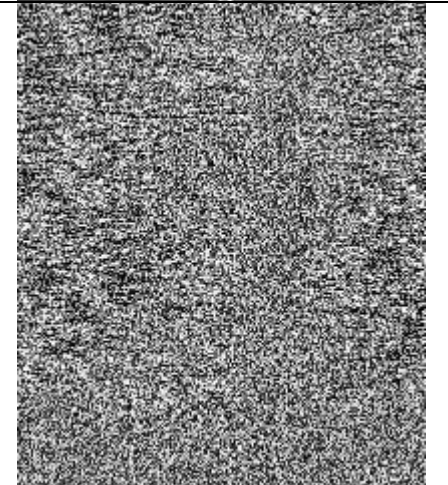

	Input image	Output image
Encryption		
Decryption		

Fig.5 charlie.png



Secret key:

$\mu=1.78$, $\eta= 0.49$, $\varepsilon=0.42$, $x_0(1)=0.6303310337840997$, index of DNA encoding rule=2, index of DNA decoding rule=2, R= 51976571822428959455026115835641084163

IV. CONCLUSION

DNA Cryptography is a new born cryptography that overcomes the difficulties of traditional cryptography due to its extraordinary information density inherent in DNA molecules, exceptional energy efficiency and vast parallelism. A lot of work have been done in this area based on different techniques like –DNA synthesis, PCR, Electrophoresis etc.

The proposed encryption scheme uses DNA Rules, In addition, the DNA computing is suitable in cryptography for massive parallelism, huge storage. Therefore, the proposed scheme has a good significance in chaotic cryptography. The security analyses are given to prove that the key space and sensitivity is better enough to make brute-force attacks infeasible. The secret keys include μ , η , ε , $x_0(1)$, the index of the used DNA encoding rule, the index of the used DNA decoding rule.

It is time consuming to examine the sensitivity of secret keys by enumerating all the possible combinations of secret key parts. Simulations results indicate that the proposed scheme leads to a higher security level.

V. FUTURE ENHANCEMENT:

Due to the rapid development in the field of artificial intelligence (AI) with the introduction of the artificial neural networks (ANN), The ANN can be considered for data encryption which to a great extent resembles the working of the human brain. Implement it in parallel and design it into a multi-level encryption and decryption to provide more security for cloud computing and storage.

REFERENCES

- [1] Ying-Qian Zhang , Xing-Yuan Wang , Jia Liu , Ze-Lin Ch (2016). “An image encryption scheme based on MLNCML system using DNA sequences”. Opt Lasers Eng;95-103

- [2] Wang XY, Liu LT, Zhang YQ.(2015).” A novel chaotic block image encryption algorithm based on dynamic random growth technique” . Opt Lasers Eng;66:10–8.
- [3] Chen JX, Zhu ZL, Fu C, Yu H, Zhang LB(2015). “An efficient image encryption scheme using gray code based permutation approach”. Opt Lasers Eng;67:191–204.
- [4] Xu L, Li Z, Li J, Hua W(2016). “A novel bit-level image encryption algorithm based on chaotic maps”. Opt Lasers Eng;78:17–25.
- [5] Arroyo D, Rhouma R, Alvarez G, Li SJ, Fernandez V(2008). “On the security of a new image encryption scheme based on chaotic map lattices”.
- [6] Ercan S, Cahit C(2011). “Algebraic break of image ciphers based on discretized chaotic map lattices”. Inform Sci;181:227–33.
- [7] Ge X, Liu FL, Lu B, Wang W(2011). “Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem and its improved version”. Phys Lett A;375:908–13.
- [8] Liu HJ, Wang XY(2011). “Color image encryption using spatial bit-level permutation and high-dimension chaotic system”. Opt Commun;284:3895–903.
- [9] Tang Y, Wang ZD, Fang JA(2010). “Image encryption using chaotic coupled map lattices with time-varying delays”. Commun Nonlinear Sci;15:2456–68.
- [10] Xiang T, Wong KW, Liao XF(2007). “Selective image encryption using a spatiotemporal chaotic system”. Chaos;17:023115.
- [11] Kaneko K.(1989) Pattern dynamics in spatiotemporal chaos. Physica D;34:1–41.
- [12] Wei XP, Guo L, Zhang Q, Zhang JX, Lian SG(2012). “A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system”. J Syst Softw;85(2):290–9.
- [13] Liu HJ, Wang XY, kadir A(2012). “Image encryption using DNA complementary rule and chaotic maps”. Appl Soft Compute;12(5):1457
- [14] Zhang Q, Wei XP(2013). “RGB Color Image Encryption Method Based on Lorenz Chaotic System and DNA Computation”. IETE Tech Rev;30(5):404–9.
- [15] Zhang Q, Guo L, Wei X(2010). “Image encryption using DNA addition combining with chaotic maps”. Math Compute Model;11–12(52):2028–35.
- [16] Belazi A, Hermassi H, Rhouma R, Belghith S.(2014) “Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map”. Nonlinear Dyn ;76:1989–2004.

- [17] Liu L, Zhang Q, Wei X.(2012) “A RGB image encryption algorithm based on DNA encoding and chaos map”. *Comput Electr Eng*;38(5):1240–8.
- [18] Wang XY, Zhang YQ, Bao XM.(2015) “A novel chaotic image encryption scheme using DNA sequence operations”. *Opt Lasers Eng*;73:53–61.
- [19] Zhang YQ, Wang XY(2014). “Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation”. *Nonlinear Dyn* ;77(3):687–98.
- [20] Zhang YQ, Wang XY(2014). “A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice”. *Inform Sci*;273:329–5.
- [20] Zhu ZL, Zhang W, Wong KW, Yu H (2011). “A chaos-based symmetric image encryption scheme using a bit-level permutation”. *Inform Sci*;181:1171–86.