ISSN 2347 - 3983
Volume 8. No. 8, August 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter98882020.pdf
https://doi.org/10.30534/ijeter/2020/98882020

Text Encryption Approach using DNA Computation and Chaotic Indexing

Siham Oleiwi Tuam , Sahar Adill Kadum, Fayiz Ali Rashad.
Collage of Science for Women, University of Babylon, Babylon, Iraq, alzhranwr97@gmail.com.
Collage of Science for Women, University of Babylon, Babylon, Iraq, dr.sahar.adill@gmail.com.
Collage of Science for Women, University of Babylon, Babylon, Iraq, faez@itnet.uobabylon.edu.iq.

ABSTRACT

The key to every security system is the important part as it defines if the system is security strength or weakness. Security has become a key issue in digital data transmission over insecure communication network, which can be accomplished using robust ciphering algorithms. At the other side, the chaotic systems have excellent features, such as Mixing data, ergodicity, sensitivity to initial conditions, control parameters, etc., all of which are useful for designing cryptographic algorithms with large key size and efficient permutation . The addition of using DNA in cryptography creates a novel domain for three reasons:: storage space, computing power and huge parallelism. This paper presents a hybrid approach of the chaotic map as well as DNA computation to Text encryption. Two logistic maps are employed for key generation to be used in permutation process, and 1D logistic map is used for generating index permutation. DNA computation coding rules and addition operation are used to frame the final result of the encryption process to produce encrypted text. The proposal results show that the proposal algorithm is highly secure, resistant to brute force attack. and has a bigger key space.

Key words : text encryption, chaotic Logistic Map, confusion, Diffusion, DNA coding.

1. INTRODUCTION

. There are numerous ways of securing sensitive information. One method is through encryption or the transformation of data into unintelligible format. Data is secured based on the cryptographic and cipher algorithm [1]. In recent years, the DNA features in encryption have emerged to exploit DNA characteristics. These characteristics are represented by high capacity storage, and parallelism. Although, the four DNA bases and their coding rules are used to encode the data and used as the secret key [2][3]. On the other side , the chaotic algorithm is characterized by very distinct characteristics such as mixing data the sensitivity of both initial condition and control parameters are all useful in designing cryptographic algorithms for text, images, audios [4].

2. RELATED WORK

In [5], this research presents a new way to generate the key stream depending on the combination of the chaotic maps, where each of them is used 3DHenoun map and 3D cat map. The basic principle of this method consists of generating random numbers, and those numbers are converted into a binary sequence that 3DHenoun map These sequence positions is permuted and Xor by 3D Cat map

In [6]," proposed The algorithm first uses Keccak to calculate the hash value for a given DNA sequence as the initial value of a chaotic map second, it uses a chaotic sequence to scramble the image pixel locations and the butterfly network is used to implement ion the bit permutation then the image is coded into a DNA matrix dynamic and an algebraic operation is performed with the DNA sequence to realize the substitution of the pixels ,which further improves the security of the encryption. Finally The confusion and diffusion properties of the algorithm are further enhanced by the operation of the DNA sequence and the ciphertext feedback

In [7], proposed a text-encoding algorithm. This algorithm uses the chaotic nature of the map by using MS map. MS map is a key stream generator. The difficult of recognizing the encrypted text by a brute force attack resulted from the decoding process that tested by three different secret keys.

In [8], in this research two types of chaotic map are used: Sine Map and Henoun Map. The coding capabilities of the algorithm for a text data are verified in different sizes.

In [9], "this paper proposed a new low weight cryptographic scheme for secure image Communication. In this scheme the plain image is permitted first with a pseudo random sequence Number (PRN) and computation encrypted with DeoxyriboNucleic Acid (DNA) Four PRN Sequences are generated by a Pseudo Random, Cross-Coupled Number Generator (PRNG). The Chaotic logistics map use two key-sets. The first sequence of PRNs is used to permute the plain Image while the second PRN sequence is used for random DNA sequence generation.

3. DNA CRYPTOGRAPHY

Cryptography of deoxyribose nucleic acid is the promising and rapid development filed in data protection. The Traditional binary data uses two digits '0' and '1.' But data is encoded by four bases for DNA molecules, which is the natural transporter of information. 'A' and 'T' and 'G' and 'C'. Few grams of DNA molecules are capable of curtailing all data contained in the world. Some of the benefits of computing DNA is that DNA molecules are massively parallel. About 1018 processors operating in parallel can be easily managed in an in vitro assay Besides the immense parallelism, DNA molecules do have tremendous capacity for storage. A gram of DNA molecules is made up of 1021 DNA bases that are almost 108 tera-byte. This benefits of DNA computing justify the concept of DNA cryptography [10].

3.1 Deoxyribonucleic Acid (DNA)

The human body contains trillions of cells, each of them Serves numerous duties. much of the DNA material is in a nucleus known as Nuclear DNA. DNA controls every cell 's function. all Chromosome of DNA consists of a molecule of DNA that is hold genes. The gene is a whole genetic makeup that contains all a chromosomal information [12].

DNA strands contain 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) [11] . figure 1 shows the general structure of DNA.

Figure 1: Simple DNA structure [13]

4. CHAOS THEORY

This is one of the big systems, because of two essential systems The complex nonlinear behavior results in irreversibility and unpredictability [14] .

4.1 Logistic map

Logistic map was used as a sequence generator pseudorandom .One of the most common and useful chaotic functions is the logistic map .

$$x_{n+1} = \mu x_n (1 - x_n) \quad \ldots\ldots\ldots\ldots \quad (1)$$

Obviously, $x_n \in [0,1]$ under the conditions that the initial $x_0 \in [0,1]$, where n is the iteration number and $\mu = 4$ [13] .

5. PROPOSED METHOD

The proposed method consists of two processes : Permutation and substitution , with two stage. In the first stage: the text is shuffled using the secret key generated by a logistic map. The second stage: the series of permutated code is converted to DNA using DNA encoding rules as shown in table (1) and DNA addition operation as shown in table (2) . Table (3) gives the final encrypted text. figure 2 shows The general structure of the proposed method .

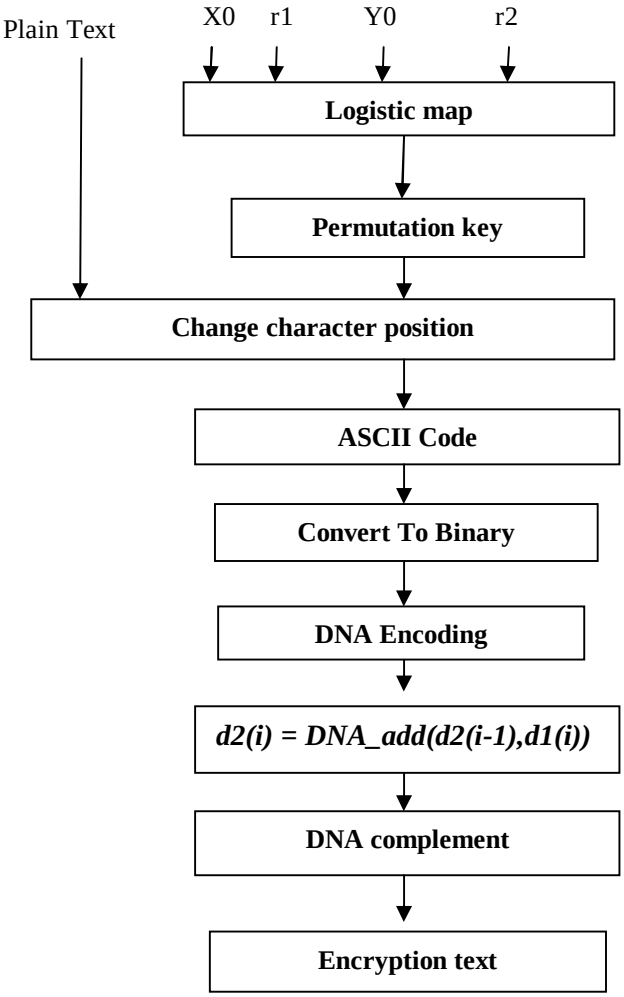

Figure 2: Block Diagram of the Proposed system

Table 1: DNA digital coding

DNA nucleotide	Decimal	Binary
A	0	00
G	1	01
C	2	10
T	3	11

Table 2: addition operation of DNA sequence

+	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: Complementary tables

Base	Complement
A	T
C	G
G	C
T	A

5.1 generating chaotic key

Chaotic sequence is a real value sequence. This real value sequence can be transformed into the integer sequence. In this method, an index based chaotic sequence is created. First, the chaotic sequence is created using two logistic map, Input the initial value (x0,yo) and control parameter(r1,r2), combined two logistic maps after which the index values that are stored in a vector, are created according to ascending order of the chaotic sequence. Index values represent the location of chaotic sequence. The resultant row array contains the integer sequence which can be used for key permutation figure 3 shows key permutation Generation.

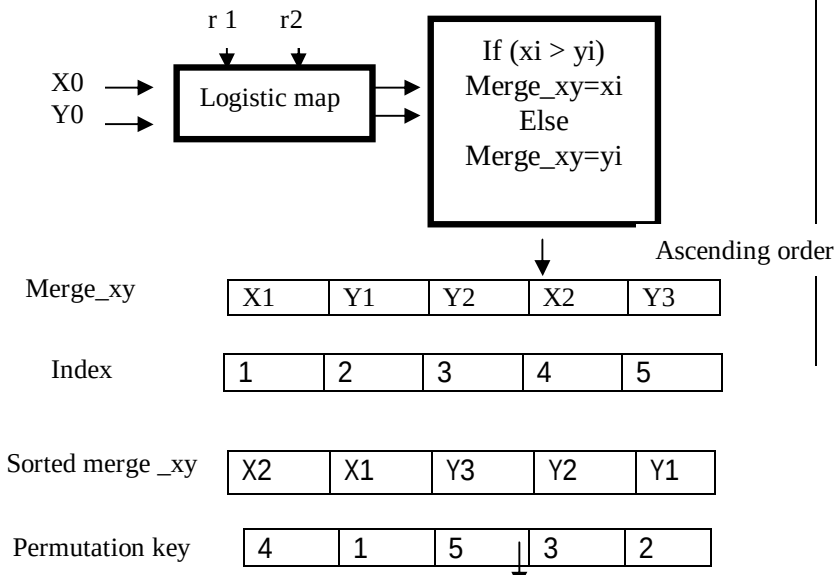

Figure 3: key permutation Generation

5.2 Permutation

The rearrangement of the text location is achieved by creating a series of integers. Chaotic based on index is used in permutation.

Algorithm 1. Permutation process

Input: initial condition (x0,yo,r1,r2)

Output: permutation key .

Begin

Step1: Input the initial value(X0,y0)and the values of the control parameters(r1,r2) in the logistic map. The initial values (x0,y0) are number of floating points with a range of $\mathbf{10^{-15}}$

Step2: the logistic map is iterated n times using equation.

$$x \leftarrow r1 * x * (1- x)$$
$$y \leftarrow r2 * y * (1 - y)$$

step3: the index values that are stored in a row matrix .

Step4: Compare the chaos values, whichever is the smallest value, and the values are arranged in ascending order with change value of index.

```
if(x(i)>y(i))
    mergexy(i,1)=x(i)
else
    mergexy(i,1)=y(i)
end
```

step5: swap between Index values and the position of chaos sequence.

```
for i=1tol
    for j =i+1to l
        if (mergexy(i)>mergexy(j))
            tem=mergexy(i)
            mergexy(i)=mergexy(j)
            mergexy(j)=tem
            tem=index(i)
            index(i)=index(j)
            index(j)=tem
        end if
    end for
end for
```

step6: The resultant the array contains an integer sequence which can be used for permutation .

Step7: original Text are scrambling using the permutation key .

Step8: the scrambling ASCII codes are converted to the corresponding binary code.

End

5.3 Substitution

Is the process where actual text value is changed To make this encoding method extra secure and hard to analyze by attack . Steps include the following.

step 1: Each bit of Binary (Text), can be encoded into a single DNA strand.
step2: DNA addition is applied on step 1.
step 3:DNA complement is applied on step 2.

Algorithm2. shuffling the Text

Input : text
Key: permutation key
Out put: scrambling the text .
Begin
Step1: read the plaintext (message).
Step2: compute the number of the message character.
Step3: generate permutation key equal to length of message by two 1D logistic map using algorithm (1) .
Step4:
For m from 1to length of text
h=result(m)
shuff(m)= text(h)
End for

End

Algorithm 3.encryption stage

Input :scrambling the text
Out put :encryption text

Begin
step1: Take the result of the scrambling message from the algorithm(2).
step2: read the message (M).
step3: convert Ascll code to BinMsg .
step 4:convert the Bin Msg to DNA encoding using rule 1 in table (1).
step5:each bases of DNA is addition as show in Table (2) with previous bases .
Step6:the result of step 5 is applied the DNA complement as show in Table (3).
Step 7 :in this step the encryption text is obtain .
End

6. PERFORMANCE ANALYSIS

The output sequences must have a high degree of security, randomness and be absolutely decorrelated from each other. Some cryptographic tests must be performed to gauge the degree of security. The key space and key sensitivity are included.

6.1 key space

The total number of different sub-keys that can be used in the encryption represents Key space size. For a $\mathbf{10^{-15}}$ floating point precision, all keys parameters **(2)** introductory status **(2)** control parameter to produce permutation key can take $\mathbf{10^{-15}}$ possible values. Therefore, the key space comes out as $\mathbf{2^{198}(10^{-15})^4}$, which is big as much as necessary to defend against the brute force attack .

6.2 key sensitivity analysis

The key sensitivity of the proposed algorithm is tested based on two experiments:

1. Experiment one uses the same secret key for encryption and decryption with the following details. as shown in Table 4.

Table 4:key sensitivity with same secret key in permutation

For permutation
X0=0.546981427419036
yo=0.918273475610374
r1=3.999999999999996
r2=3.999999999999995

"**Hello this is a key Sensitivity test**". The result will recover the same text.

2. Experiment two uses a different secret key for Logistic map in permutation process and as follow. as shown in Table 5.

Table 5 :key sensitivity with two different secret key in permutation

Permutation	Inverse Permutation
x0=0.546981427419036	x0=0.446981427419036
y0=0.918273475610374	y0=0.918273475610374
r1=3.999999999999996	r1=3.999999999999996
r2=3.999999999999995	r2=3.999999999999995

The recovered text " **h syt ehnsivsltke ay telo itise**" is meaningless .

7. CONCLUSION

The purpose of this study is to build an efficient text encryption algorithm that combines DNA and chaotic map to achieve a robust security. The chaos systems' powerful properties such as sensitivity dependency on initial

conditions and system parameters . The feature of chaotic keys used in permutation stage difficult enough to any cryptanalyst in determining the actual parameters. any intruder could not figure out the key. thus, parameters confidentiality also enforces the security of the text messages. in diffusion stage, using DNA cryptography model to enhance the strength of security of the overall proposed system. using operations of DNA computing and coding rules gives a flexibility in structuring and scrambling the ciphered message. Although, using the DNA molecular to exploit the characteristics of high-density of storage and parallelism to deal with huge data and decrease the time of data processing.

REFERENCES

[1] Jan Carlo T. Arroyo , Allemar Jhone P. Delima "**A Keystream-Based Affine Cipher for Dynamic Encryption"** International Journal of Emerging Trends in Engineering Research Volume 8. No. 7, July 2020

[2] L. M. Adleman, "**Molecular computation of solution to combinatorial problems**", Science, Vol. 266, pp. 1021-2024, 1994.

[3] L. XueJia, L. MingXin, Q. Lei, H. JunSong and F. XiWen, "**Asymmetric encryption and signature method with DNA technology",** Sci China Inf Sci, 53: 506ñ514, doi: 10.1007/s11432-010-0063-3, 2010..

[4] M. Mishra and V.H. Mankar, **"Message embedded cipher using 2-D chaotic map",** International Journal of Chaos, Control, Modelling and Simulation (IJCCMS) Vol.1, No.1, 2012.

[5] Albhrany, Dr EA, and TayseerKaram Alshekly. "**A New Key Stream Generator Based on 3D Henon map and 3D Cat map."** International Journal of Scientific & Engineering Research 8.1 (2017)

[6] Zhang, Xuncai, Feng Han, and Ying Niu. **"Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding."** Computational intelligence and neuroscience. 2017

[7] Irsan, M. Y. T., and S. C. Antoro. **"Text Encryption Algorithm based on Chaotic Map."** Journal of Physics: Conference Series. Vol. 1341. No. 6. IOP Publishing, 2019.

[8] Sheela, S. J., K. V. Suresh, and Deepaknath Tandur. **"Secured text communication using chaotic maps."** 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET). IEEE, 2017.

[9] Mondal, Bhaskar, and Tarni Mandal. "**A light weight secure image encryption scheme based on chaos & DNA computing."** Journal of King Saud University-Computer and Information Sciences 29.4 (2017): 499-504. https://doi.org/10.1016/j.jksuci.2016.02.003

[10] Mondal, Mandrita, and Kumar S. Ray. **"Review on DNA Cryptography."** arXiv preprint arXiv:1904.05528 (2019)..

[11] Rathi, Mansi, et al. "**Data security using DNA cryptography."** *International Journal of Computer Science and Mobile Computing, IJCSMC* 5.10 (2016): 123-129.

[12] M. Borda and O. Tornea, "**DNA secret writing techniques,"** 2010 8th Int. Conf. Commun. COMM 2010, no. May, pp. 451–456, 2010.

[13] Mohamed Fathi El-Santawy**."** **A Novel Chaotic Multi-Objective Brain Storm Optimization Approach for Multi-Plate Disk Brake Design Problem.**" International Journal of Emerging Trends in Engineering Research Volume 8. No. 7, July 2020

[14] A. M. Raheema ; S. B. Sadkhan; and S. M. Abdul Sattar, "**Performance Comparison of Hybrid Chaotic Maps Based on Speech Scrambling for OFDM Techniques** ", 2018 Third Scientific Conference of Electrical Engineering (SCEE).