Karbala International Journal of Modern Science

Volume 5 | Issue 2 Article 7

2019

Enhancement AES based on 3D Chaos Theory and DNA Operations Addition

Alaa Kadhim
University of Technology, Iraq, dralaa_cs@yahoo.com

Rasha Subhi Ali
Al-Nisour University, Iraq, rasha.s@nuc.edu.iq

Recommended Citation

Kadhim, Alaa and Ali, Rasha Subhi (2019) "Enhancement AES based on 3D Chaos Theory and DNA Operations Addition," *Karbala International Journal of Modern Science*: Vol. 5 : Iss. 2 , Article 7.

DOI: 10.33640/2405-609X.1137

Enhancement AES based on 3D Chaos Theory and DNA Operations Addition

Abstract

The techniques modern used to encrypt text data play an important role in preventing unauthorized access. The AES algorithm is widely used in various cryptographic applications, but coz the algorithm has been subjected to several successive attacks, the need is necessary to improve the algorithm and make it more powerful the algorithm.In dis search will be inserted plaintext 1024 will be divided into four blocks each Block consists of 256 bits and each Block will pass the four stages represent(substitution,shift,Mix column and round key).A new step will be added to the four stages of permutation. Where chaos theory is adopted in the permutation stage and the shift phase.DNA will be adopted at the phase of the Mix and add round key stage due to it's high storage capacity. The time taken in the coding and decoding in the proposal enhancement algorithm will take a few milliseconds. The output will be measured using a five statistical test and a 16NIST Test. The results showed excellent efficiency in terms of randomness used in the proposal, thus preventing the tractor of sensitive data in an unsafe environment.

Keywords

AES, chaos theory 1D logistic map, DNA

1. Introduction

Today, technology has evolved dramatically we need to in the era of much sensitive information there is a need to protect personal and sensitive data from unauthorized persons. Encryption is one of the main ways to protect data. Recently, chaos theory in modern coding has been adopted due to the similarity between encryption and chaos theory. The two are the principle of their random work in addition to the use of DNA in the fields of encryption because most computers based on the DNA have a lower consumption of energy, which equals one of the billions of energy used in the traditional computer (see Figs. 1−5).

One of the most important scientific contributions that have been added is the increasing of random and break the link between the plaintext and encrypted texts by increasing the confusion and diffusion through the use of the stages of this system.

2. Aes rijndael

The AES algorithm is one of the block cipher algorithm, one of the most robust algorithms against many attacks. The input text 128-10 round, 192-12 round, and 256-14 round Depend on four stages represent (substitution, shift row, Mix column and Add round key) [1].

3. Description of the algorithm

Key Expansion: Round keys are derived from the cipher key using Rijndael key schedule. AES requires a separate 128-bit round key block for each round plus one more [1].

4. Initial round key

1. Add round key—Each byte of the state is combined with a block of the round key using bitwise xor.

4.1. 9, 11 or 13 rounds

2. Sub bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

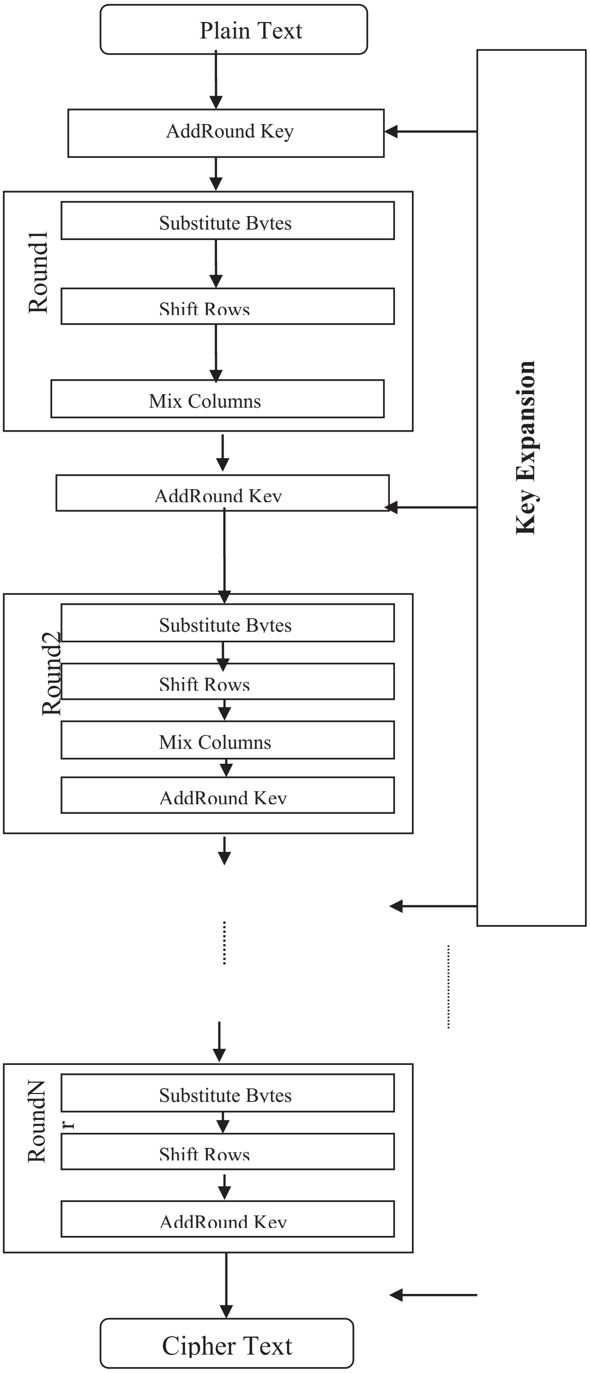


Fig. 1. Encryption and decryption AES algorithm.

3. Shift rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

https://doi.org/10.33640/2405-609X.1137

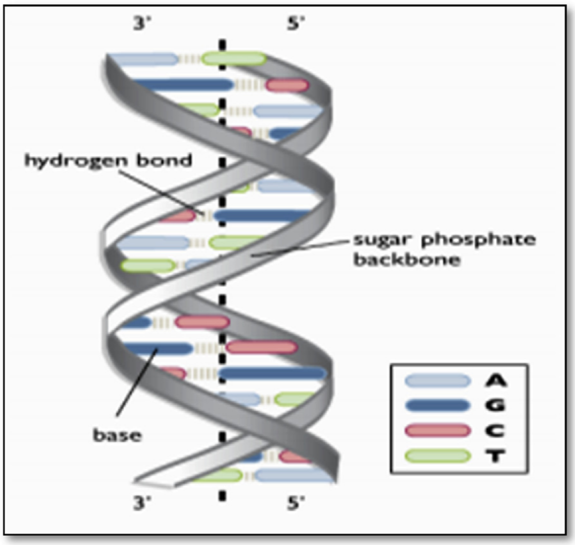


Fig. 2. Double-helical DNA structure.

4. Mix columns—a linear mixing operation which operates on the columns of the state, combining the four bytes in each column. [2]
5. Add round key

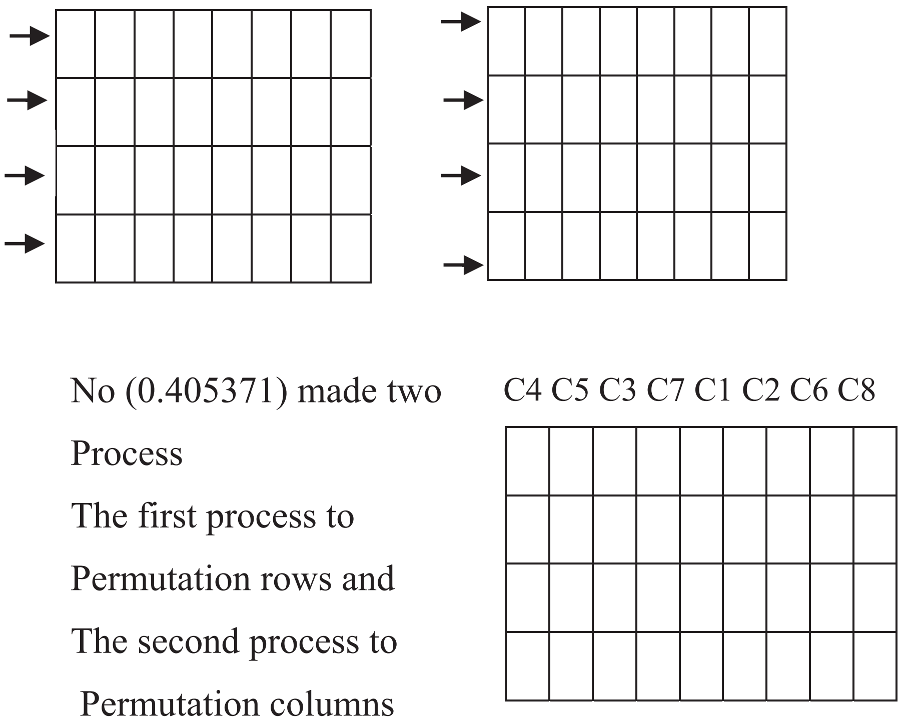
4.2. *Final round making 10/12 or 14 round in total*

1. Sub bytes
2 Shift rows
3 Add round key

5. Chaos theory

It is one of the most recent theories of physical physics - sometimes translated into chaotic theory - that deals with the subject of nonlinear (dynamic) moving sentences that exhibit a kind of random behavior known as schisms. This random behavior is either caused by an inability to determine initial conditions (butterfly effect) through the potential physical nature of quantum mechanics [3,4]. Chaos theory attempts to explore the latent hidden system in this apparent randomization trying to establish rules for the study of such systems as fluid, weather forecasts, the solar system, market economy, financial movement, and population growth [5,6].

It became necessary to generate numbers, keys and maps of permutations by using random generators and we have benefited from the theories of chaos in the production of random random real important for the random increase of the important clipping keys.


No (0.405371) made two

Process

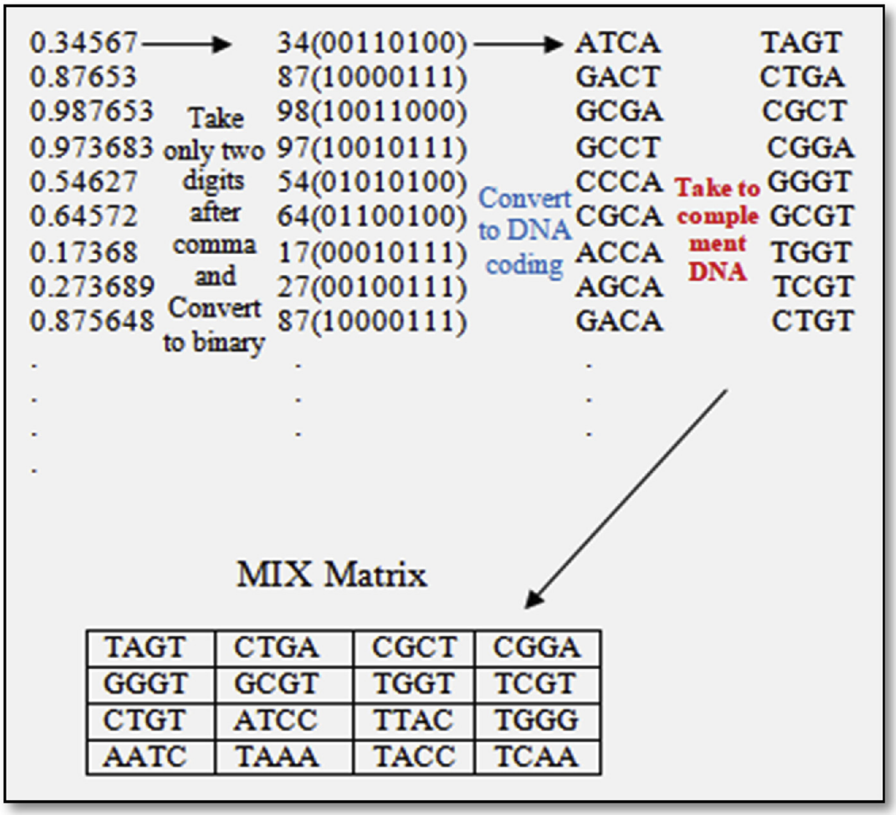
The first process to

Permutation rows and

The second process to

Permutation columns

Fig. 3. Clarification of the stage of the shift.



TAGT	CTGA	CGCT	CGGA
GGGT	GCGT	TGGT	TCGT
CTGT	ATCC	TTAC	TGGG
AATC	TAAA	TACC	TCAA

Fig. 4. MIX matrix.

6. Attack in AES

Encryption attacks are designed to sabotage the encryption security of algorithms and are used to try to decrypt data without prior access to the key. The analysis is part of decryption of encrypted data and one of the strongest attacks against BLOCK CIPHER algorithms is the differential attacks invented in 1990 by the world ELI ADI SHAMIR A normal attack against a DES algorithm that was more efficient than the brute force attack is chosen. It searches for characteristics with different patterns between two selected plain text messages that lead to specific differences in the corresponding high or low probability encrypted text messages.

The second type of attack is the interpolation attack. This attack depends on the number of s-boxes and the number of rounds of encryption. This is evidence of the success of the multiplex equations with the attacks against the block cipher algorithms. It depends on the relationship between the plain text and the encrypted text of the static key either as a single or as a multilevel vector. If these multiple limits are sufficiently low, many transactional transitions can be made from a number of encoded texts.

7. DNA

Today, the field of computer science is increasingly used in many applications as a result of many discoveries that are characterized by many developmental features. Modern science is looking for biologic information that combines biological information with information technology. These vital forms include DNA, genetic codes, etc. The living organisms are defined by cell and cell one is controlled by the protein. These proteins are made up of amino acid molecules. These amino acids and enzymes are useful for building DNA. DNA is the code that determines the genetic instructions through four nitrogen bases, and the study of DNA is useful for altering structural or altering the behavior of a given organism or to determine the similarity between two living things in terms of characteristics, function or behavior [7].

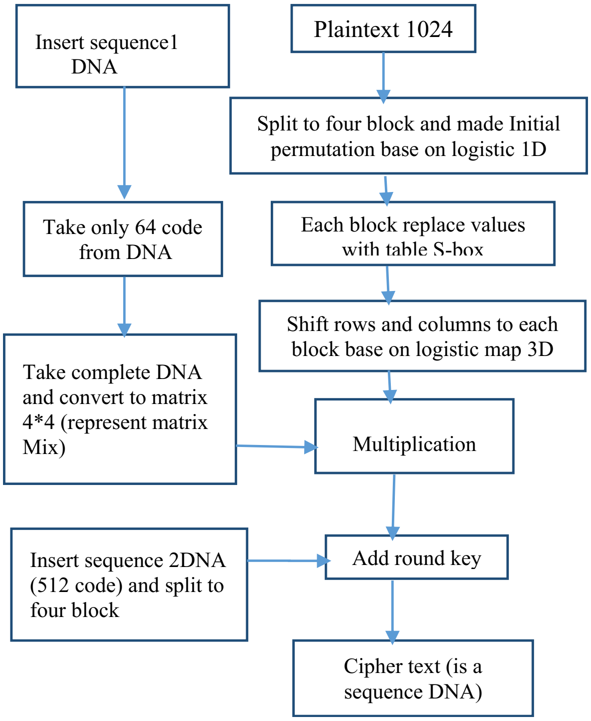

Insert sequence1 DNA
Plaintext 1024
Split to four block and made Initial permutation base on logistic 1D
Take only 64 code from DNA
Each block replace values with table S-box
Shift rows and columns to each block base on logistic map 3D
Take complete DNA and convert to matrix 4*4 (represent matrix Mix)
Multiplication
Insert sequence 2DNA (512 code) and split to four block
Add round key
Cipher text (is a sequence DNA)

Fig. 5. Structure proposal AES base on logistic map and DNA.

8. DNA encryption

Is the process of storage of genetic information through a calculation method to improve embryonic privacy in DNA sequence processes. The human genome is complex and long, but important information can be interpreted and identified human genome is a series of nucleotides associated with 3, 2 billion bases.

DNA It consists of four nitrogen bases(cytosine [C], guanine [G], adenine [A] or thymine [T])

The DNA sequence {A, C, G, T} is presented into binary code using a simplest coding pattern of four digits 0, 1, 2, and 3, respectively. Each digit is presented into the 2-bit pattern as follows: 0 as A→00, 1 as C→01, 2 as G→10, and 3 as T→11 [8].

9. Proposed algorithm to dynamic shift transformation, mix column and key

Due to the exposure of the AES algorithm to multiple attacks. It is necessary to enhance the strength and increase diffusion based on the development AES algorithm.

Step 1: The plaintext input will be 1024 bits and the output is 1024 bits. At first, the input will be split into four blocks of each block representing 256 bits. Each block has own key $k_{i=(1-4),j=(1-14)}$(i = number of block, j = number of round)

Step 2: A secret map is generated from the 1D logistic map. These numbers are adopted to make a permutation between the four blocks for each round. Eq. (1d) used to generate the random numbers is the following [9]:

$$x(i+1) = \mu * x(i) * (1 - x(i)) \tag{1}$$

The parameters values initial x (i) ∈ (0, 1) and μ ∈ (0, 4).

The first number from logistic equation is No1 = 0.34763, this No must content four digits as 4321, and the No from logistic is 0.34763 are converted to integer as 34,763 and choose then from 1 to 4 as 4,3, but we need four digits, added the numbers such as 1,2, the number becomes(3,4,1,2), the secret map to permutation the blocks in first round and such as to all round but different secret map.

No1 = 0.347643→using permutation the first four block.

Step 3: in each round, the shift layer will be developed using the secret map generated from the 3D logistic map (using only vector x).

The model is a system of three ordinary differential equations now known as the Lorenz equations:[10]

$$\begin{aligned} X &= \alpha(y - x) \\ y &= x(\rho - z) \\ z &= (xy - \beta z) \end{aligned} \tag{2}$$

X is proportional to the rate of convection, y to the horizontal temperature variation, and z to the vertical temperature variation, the constants ρ, and β are system parameters proportional to the(x, y, and z). There will be a permutation between the rows and columns of each block to increase diffusion and convert shift matrix binary to code DNA. Can explain in the following example.

$x = 0.405371$→using shift row and column (search the numbers from 1 to 4) the result process number (4312) represent shift row and the same secret using permutation columns but the search number between (1–8) the permutation becomes (45371268)

Step 4: Two series of DNA are supported and generated from the same logistic map used in shift layer, using only (vector$y$) secret map represent first sequence DNA using generate a MIX matrix and vector$z$ using second sequence DNA is depend as a key in add round key.

The first sequence DNA generated by taking 32 secret maps, made, process on all number secret map by taking only two digits after a comma and convert to coding DNA.

Generating MIX matrix:

- Input 32 secret maps from the 3D logistic map after process convert to 63 coding of DNA
- Take complement DNA sequence
- Convert complement DNA sequence to the matrix (4*4)

10. Generating key

- Take 256 secret maps from vector z (logistic map Lorenz) after process the number by taking only two digits after the comma and convert to binary and last convert to coding DNA
- Split code DNA to four blocks each block contains (128 code DNA)

```
**AlgorithmEncryptionProposal AES**
**Input:**plaintext,x=0.1,??=0.4, x1=0.3,y=0.1,z=0.9,$\alpha$ =0.4, $\beta$ =0.3
  , QUOTE =0.2
**Output:** ciphertext
***Begin***
  Step1: insert plaintext 1024 bits
  Step2: split plaintext to four blocks, each block (256 bits)
  Step3: initial permutation to four block base on the 1D logistic map
  Step4: substitution layer(Each value in step 3 is replaced by another
  value from S-box )
  Step 5: shift layer (shifting the rows and columns base on the
  logistic map 3D(vector x))
  Step 6: Mix column(The matrix is generated using a vector y in
  logistic map 3D and convert to coding DNA and this matrix
  multiplication with result step 5
  Step 7: Addround key (The second sequence of DNA get from
  logistic map 3D (vector z ) and considered as a key which is split
  into four blocks of each Block 128 code DNA)
  ***End***
```

```
**Algorithm Decryption Proposal AES**
**Input:**cipher text, x=0.1,??=0.4, x1=0.3,y=0.1,z=0.9,$\alpha$ =0.4, $\beta$
  =0.3 , QUOTE =0.2
**Output:**plaintext
***Begin***
  Step1: generated (512 code DNA) from 3D logistic map (vector
  z),split to four block each block(128 code)
  Step2: Add round key with ciphertext(after the split the ciphertext
  four blocks)
  Step3: generating inverse mix matrix from logistic map 3D(vector
  y) and multiplication with step 2
  Step4: shift layer(the inverse secret map upon agreed between
  sender and receiver to permutation rows and columns)
  Step 5: substitution (replace each value with the table S-box)
  Step 6: permutation the inverse secret map to each four block
  Step 7: merge four blocks to get ciphertext
  ***End***
```

Table 1
Types of chaotic map.

Map	Domain	Dimension
Logistic map	Discrete	1
Gaussian map	Discrete	1
Tent map	Discrete	1
Piecewise linear chaotic	Discrete	1
Baker map	Discrete	2
Cat map	Discrete	2
Standard map	Discrete	2
Lorenz map	Continuous	3
Roster map	Continuous	3
Chen map	Continuous	3
Jerk equation	Continuous	3

11. Experimental results and discussion

1-Time: The time to encrypt and decrypt was calculated and it took only a few milliseconds to select the different files

2- Basic Five Statistical Tests

The output ciphertext 1024bits: - The ciphertext was tested by the Basic Five Statistical Tests, The results are displayed in the following Table 2 (See Tables 1, 3 and 4).

Table 2
Double-helical DNA structure.

time (Millisecond)		
Size file	encryption	decryption
100 KB	40	40
200 KB	45	45
300 KB	58	58
400 KB	66	66

Table 3
Double-helical DNA structure.

Five Statistical Test		
Test	Freedom degree	Proposal AES
Frequency Test	Must be $\le$ 3.84	Pass = 0.020
Run Test	Must be $\le$ 10.788	Pass = 5.5
Poker Test	Must be $\le$ 11.1	Pass = 4.34
Serial Test	Must be $\le$ 7.81	Pass = 3.300
Auto Correlation Test	Shift No.1	Pass = 0.245
Must be $\le$ 3.84	Shift No.2	Pass = 2.234
	Shift No.3	Pass = 1.987
	Shift No.4	Pass = 0.456
	Shift No.5	Pass = 0.888
	Shift No.6	Pass = 0.132
	Shift No.7	Pass = 0.189
	Shift No.8	Pass = 0.987
	Shift No.9	Pass = 0.923
	Shift No.10	Pass = 2.023

Table 4
NIST test of the proposal.

NIST Test of proposal AES	
Frequency	success
Block Frequency	success
Cumulative Sums	success
Runs	
Longest run	success
rank	success
DFT	success
Non-periodic templates	success
Overlapping	success
Universal	success
Approximately entropy	success
Random excursion	Test not application
Random excursion variant	Test not application
Serial	success
Lempel-Ziv compression	Discrete
Linear complexity	success

3- (NIST)National Institute of Standards and Technology: -

The NIST Test is a Consists of a total of tests where the algorithm's cryptographic output running on a binary sequence is tested and these tests are represented (random excursion, universal, periodic templates, etc.).

12. Conclusion

In this paper, the AES algorithm will be developed where an initial step of permutation of the algorithm phases will be added. The rate of confusion will be increased based on the chaotic theory, which is mainly dependent on the confusion in the initial step of permutation and the shift phase. Two DNA-sequences generating from logistic map 3D will also the first sequence used to generate the mixing matrix, while the second sequence will be considered as a key in the add round key. Thus, the decryption output is a DNA sequence sent to the receiver. The output of the encryption was tested by the five tests statistical and NIST, where we found that all the tests were successful, either the time spent in encryption and decoding took only a few seconds showed in Table 2.

The task of the future is how to make the structure of the algorithm moving, not static, adding any stages, deleting the stages, p basis of basic conditions, and making them correct, breaking them, predicting them, or adding random objects, which depend on the important keys in encryption.

Data availability

The [Data type] data used to support the findings of this study are available from the corresponding author upon request.

The [Data type] data used to support the findings of this study is not static and not found on any repository it was free.

This study can be used for any [Data type] not limited from the specific resource. It can be used for numerical, flout number, double, real numbers, symbols, Arabic numbers, Arabic characters, English numbers, English characters, and any alphabetic datatype.

Conflicts of interest

This research interested in providing more protection for transmitted data by increasing confusion and diffusion.

Also, the time was reduced by taking 1024 bits instead of 256 bits; so that effort was reduced for both sides (sender and receiver).

Funding statement

This research is not funded by a particular institution because it is a personal search.

Supplementary materials

The 16 NIST tests were used to supplement the results of this study.

The 5 statistical tests were applied to support the results of this study.

The data used in this research free not limited as mentioned above.

References

[1] Joan Daemen, Rijmen Vincent, AES Proposal: Rijndael, September 3, 1999.

[2] Morris J. Dworkin, Elaine B. Barker, James R. Nechvatal, James Foti, Lawrence E. Bassham, E. Roback, James F. Dray Jr., “Advanced Encryption Standard (AES)”. Federal Information Processing Standards, US National Institute of Standards and Technology, 26 November 2001, https://doi.org/10.6028/NIST.FIPS.197.

[3] Jolfaei, Mirghadri, Image Encryption Using Chaos and Block Cipher, vol. 4, IHU Tehran, Iran, January 2011. No. 1.

[4] M.J. Donahue, An Introduction to Mathematical Chaos Theory and Fractal Geometry, Duke University, Newyourk, January, 2002.

[5] J.M. Amigó, L. Kocarev, J. Szczepanski, "Theory and practice of chaotic cryptography", Phys. Lett. 366 (2017).

[6] H. Kamelsh, A.K. Farhan, Proposal Dynamic Block Cipher Structure Depend on Secret Map, Department Computer Sciences, University of Technology, 2017.

[7] Shakir M. Hussain1, Hussein Al-Bahadili1, A DNA-Based Cryptographic Key Generation Algorithm, University of Petra, CSREA Press, Amman, Jordan, 2017, ISBN 1-60132-445-6.

[8] S. Hariram, R. Dhamodharan, A Survey on DNA Based Cryptography Using Differential Encryption and Decryption Algorithm, vol. 10, Sep − Oct .2015. ISSN: 2278-2834,p-ISSN: 2278-8735, Issue 5, Ver. II.

[9] Rami K. Ahmed, Imad J. Mohammed, Developing a New Hybrid Cipher Algorithm Using DNA and RC4, vol. 8, University of Baghdad Baghdad, Iraq, 2017. No. 10.

[10] Obaida M. Al-Hazaimeh, Mohammad F. Al-Jamal, Nouh Alhindawi, Abedal kareem Omari, Image Encryption Algorithm Based on Lorenz Chaotic Map with Dynamic Secret Keys, Springer, 30 December 2016. (Accessed 14 August 2017).