DNA-Based One-Time Pad Encryption Method Using Mandelbrot Set and Chaotic Systems (Version3)

1. Efe Ali Mert
Istek Bilge Kagan Anatolian High School
İstanbul, Turkey
ali.mert.bk.07@istek.k12.tr

Abstract — Today, computer-aided encryption techniques have become rather complex due to increasing data security requirements and sophisticated attacking methods. Even though each newly developed encryption algorithm promises high security at the beginning, vulnerabilities that emerge over time and technological advancements may threaten the security of these systems. Particularly, with increased computing power and more developed quantum computing, many encryption methods thought to be secure today may be breakable in the future. Therefore, the fact that each encryption algorithm has theoretically a limited security life and can be broken over time calls for the continuous updating of security measures. These future threats require the development of more innovative and sophisticated encryption approaches. In this project, chaotic systems such as the Lorenz system, logistic map and Hénon map were used and combined with the One-Time Pad (OTP) method to develop a strong DNA-based encryption algorithm. The initial values of the Lorenz system were selected using the logistic map and The initial values of the Logistic map were determined using the Mandelbrot set and the 1st cipher was created with plaintext by converting these numbers to ASCII codes. Likewise, a new cipher was obtained by creating the 2nd cipher using the Hénon map and converting it into ASCII codes and applying the OTP between the letters. Then, the plaintext was encrypted using the One-Time Pad (OTP) key. The encrypted data was first converted to binary codes and then the 0s and 1s in the binary underwent the XOR operation. The binary set obtained following the XOR operation was converted to DNA bases (A, T, C, G). Finally, encryption security is increased by adding complementary DNA sequences. The proposed method provides a powerful solution for data security by utilizing the high information density of DNA and the randomness properties of chaotic systems. On the other hand, this encryption was translated into the computer language and published on a web page.

Keywords —Algorithm, Chaos, OTP, DNA

I. INTRODUCTION

With the rapid development of technology today, information can be instantly transmitted and shared across the world in electronic environments. Although these developments enable us to access and share information easily, the problem of accessing correct information from secure channels and information security arises. Cryptology, as an essential element of information security, plays a crucial role in solving this problem. In this context, the present study will focus on the subjects of information, information security and cryptology (Avaroğlu, E. (2022). THE BUILDING BLOCK OF INFORMATION SECURITY: CRYPTOLOGY. Düşünce Dünyasında Türkiz, 8(43), 53-65). Chaos theory has aroused a great interest in many fields of science, such as mathematics, engineering, biology and cryptology, in recent years. Chaotic systems have become an effective tool for encryption algorithms with their sensitivity to initial conditions, complex dynamic structures and random behaviours. These characteristics of chaotic systems enable them to provide high protection for data security and enhance encryption methods. Conventional encryption methods can be breakable over time, with especially advancements in computing power. Although commonly used encryption methods such as AES, DES and RSA are still deemed secure today, their computing costs and processing speed are increasingly questionable. On the other hand, chaotic encryption methods can better meet the need for low cost and high speed, providing speedier, flexible computing and low-cost solutions. Along with this, DNA-based encryption has emerged as an innovative approach in the field of cryptology. DNA molecules with high data density and biological computing capabilities have opened up a promising field for encryption techniques. While DNA's information storage capacity provides solutions to existing data storage problems, sequences formed over DNA bases (A, T, C, G) can be used in cryptographic processes. In this context, DNA encryption can be effectively used in especially One-Time Pad encryption methods (Alavı Milani, M. M. R., Pehlivan, H., & Hosein Pour, S. (2012). A OTP (One Time Pad)Based DNA Encryption Method. The Black Sea Journal of Sciences, 5(2), 108-116.). The biological structures of DNA can be used as a new source in OTP's key generation, which can increase the security level.

II. METHODS

A. Mandelbrot Set

The Mandelbrot set is one of the sets that attract attention in the field of mathematics. Named after the French mathematician Benoit Mandelbrot, this set has proven that a simple iteration formula $(Z_{n+1} = Z_n^2 + c)$ can produce infinitely complex patterns. This set, which has inspired many fields of art, is also known by some different names, such as "God's Fingerprint" and "Mona Lisa of Mathematics".

The result in this system is used to determine the initial value of the Logistics map.

The Mandelbrot set is defined by the following equation:

$$z_{n+1} = z_n^2 + \mathrm{c}$$

In this equation:

z_0: Initial value (typically set to 0)

c: Constant complex parameter (e.g., 0.5 + 0.3*i*)

If $|z| \leq 2$: The point belongs to the Mandelbrot set (remains bounded).

If $|z| > 2$: The point escapes to infinity (excluded from the set).

If $|z| \approx 2$: It starts to show chaotic behavior. Even a small change determines whether the result will be inside or outside. Fractal and chaotic behaviors are observed in these regions. The most visually interesting structures emerge in these border regions (e.g. spirals, branches, etc.). In this system, iterations are taken until $|z| \approx 2$, and when it reaches this level, the resulting z value is divided by 10 and substituted in the x_0 parameter of the Logistic map. We have normalized z to x_0 by dividing it by 10.

B. *Logistic Map*

Logistic map is a simple but powerful random number generation method among chaotic systems. Hence, it is used for generating secure keys in cryptology. Logistic map provides high randomness thanks to its high sensitivity to initial conditions and complex dynamic structure. In this section, we will show in detail how an encryption process is performed on letters using a logistic map.

B.1 Generating Random Numbers Using Logistic Map

The equation below represents the logistic map:

$$x_{n+1} = r \cdot x_n \cdot (1 - x_n)$$

In the equation:

x_0: Initial value (usually selected between 0 and 1)

r: Control parameter (usually takes a value between 3.57 and 4)

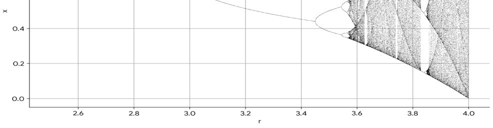


TABLE 1

Example: When x_0= 0.7 and r = 3.9 are selected as the initial value, the values obtained with the first few iterations are:

x_1 = 3.9 × 0.7 × (1−0.7) = 0.819

x_2 = 3.9 × 0.819 × (1−0.819) = 0.5786

x_3 = 3.9 × 0.5786 × (1−0.5786) = 0.949

x_4

x_5

…

These values exhibit a chaotic characteristic and provide randomness.

C. *Lorenz System*

The Lorenz system is one of the most popular chaotic systems. The Lorenz system was first proposed by the meteorologist and mathematician Edward N. Lorenz. The Lorenz system consists of an ordinary 3-dimensional differential equation and exhibits deterministic chaos for given parameter values and initial conditions. The Lorenz attractor represents a set of chaotic solutions, and these solutions suggest that small changes in initial values may create big differences over time.

The term butterfly effect borrows its name from the shape resembling a butterfly in the Lorenz attractor. In a conference, Edward N. Lorenz reinforced the meaning of the term butterfly effect, giving an ironic example and saying “The flap of a butterfly's wings might ultimately cause a tornado that can travel the halfway around the world.” This saying was only an ironic metaphor to emphasize that small changes in initial values may create big differences over time. People believed this might really happen, and it is dramatized in many movies, cinemas and books.

C.1 Lorenz Equation

The equation below represents the Lorenz system:

$$\frac{dx}{dt} = \sigma(y - x),$$
$$\frac{dy}{dt} = x(\rho - z) - y,$$
$$\frac{dz}{dt} = xy - \beta z.$$

System variables in the equation:

σ : Sigma (the value is selected as 10)

ρ : Rho (the value is selected as 28) β : Beta (the value is selected as 8/3)

State variables in the equation:

x : Represents a parameter like temperature difference or speed in the process. (the value is given from the logistic map)

y : Represents a parameter like horizontal temperature change. (the value is given from the logistic map)

z : Represents a parameter like vertical temperature change. (the value is given from the logistic map)

C.2 Valuing State Variables Using Logistic Map for Lorenz System

First, the iteration number will be selected in this system, and the iteration number for each variable will be one less than the previous iteration number starting with the first selected iteration number. The x value obtained from the selected iterations will be multiplied by 20 so it can be normalized for the Lorenz system (The reason for multiplying by 20 is to have bigger initial values and make clear the chaoticness).

Example: When the iteration number is selected as 1000, the values of state variables are as follows:

$$x = x_{1000} \times 20$$

$$y = x_{999} \times 20$$

$$z = x_{998} \times 20$$

D. Euler Method

The Euler method was discovered by the Swiss mathematician and physicist Leonhard Euler and is one of the simplest and fastest methods in the numerical calculation of differential equations. The basic logic of this method is that the next step of the function is increased depending on the derivative value and the steps proceed in this way.

The solution of the Lorenz equation using the Euler method is shown below:

$$x_1 = x_0 + \Delta t \times \sigma \times (y_0 - x_0)$$
$$y_1 = y_0 + \Delta t \times (x_0(p_0 - z_0) - y_0)$$
$$z_1 = z_0 + \Delta t \times (x_0 \times y_0 - \beta \times z_0)$$

It will be selected at the value of * $\Delta t = 0.01$.

Example: When the initial values of state variables are selected as $x_0 = 10$, $y_0 = 10$, $z_0 = 10$ ve $\Delta t = 0.01$, the first 3 steps will be as follows:

Step 1 :

$$x_1 = 10 + 0.01 \times 10 \times (10 - 10) = 10$$
$$y_1 = 10 + 0.01 \times (10 \times (28 - 10) - 10) = 11.7$$
$$z_1 = 10 + 0.01 \times (10 \times 10 - 2.6667 \times 10) = 10.73333$$

Step 2 :

$$x_2 = 10 + 0.01 \times 10 \times (11.7 - 10) = 10.17$$
$$y_2 = 11.7 + 0.01 \times (10 \times (28 - 10.7333) - 11.7) = 13.30967$$
$$z_2 = 10.7333 + 0.01 \times (10 \times 11.7 - 2.6667 \times 10.7333) = 11.617034$$

Step 3 :

$$x_3 = 10.17 + 0.01 \times 10 \times (13.30967 - 10.17) = 10.483967.$$
$$y_3 = 13.3433 + 0.01 \times (10.17 \times (28 - 11.4878) - 13.3433) = 15.047998$$
$$z_3 = 11.617034 + 0.01 \times (10.17 \times 13.30967 - 2.6667 \times 11.617034) = 12.664787$$

Since these values cover the first 3 steps, they may not exhibit chaotic features or may exhibit less chaoticness compared to higher steps. The largeness of the step number is positively related to chaoticness.

E. Normalization: Converting to Letters

The numbers obtained from the Lorenz system do not directly match the characters in the ASCII table. Since letters will be used in the encryption process, these chaotic values should be normalized for the relevant ASCII code ranges. The normalization process converts chaotic numbers to specific letters, making them usable for encryption.

E.1.Normalization Process:

Step 1 :
The maximum and minimum values that x, y and z can reach are found at this stage. Then, these values are normalized in the interval 0 -1 by performing min-max normalization.

E.2. Normalization for Upper Case Letters (A-Z):

* *Normalizing the Obtained Value from the Lorenz System in the Interval 0 - 1*

$$x = \frac{x\ (last\ obtained\ x\ value\ from\ Lorenz\ system) - min\ lorenz}{max\ lorenz - min\ lorenz}$$

(Minimum and maximum values possible for x are taken)

$$y = \frac{y\ (last\ obtained\ y\ value\ from\ Lorenz\ system) - min\ lorenz}{max\ lorenz - min\ lorenz}$$

$(Minimum\ and\ maximum\ values\ possible\ for\ y\ are\ taken)$

$$z = \frac{z\ (last\ obtained\ z\ value\ from\ Lorenz\ system) - min\ lorenz}{max\ lorenz - min\ lorenz}$$

$(Minimum\ and\ maximum\ values\ possible\ for\ z\ are\ taken)$

Step 2 :
At this stage, the new x, y and z values are normalized between numbers 65 and 90 using a different variation of min-max normalization.

* *x = Round(65+(90−65)× x)*
* *y = Round(65+(90−65)× y)*
* *z = Round(65+(90−65)× z)*

E.3. ASCII Codes and Letters:

* Upper Case Letters (A-Z): have ASCII codes in the range 65-90.
* Lower Case Letters (a-z): have ASCII codes in the range 97-122.

ASCII values outside these ranges correspond to other characters such as symbols, digits or control characters, not letters. Hence, chaotic numbers should be only normalized within these ranges to obtain letter codes during encryption.

This equation converts the x value to an ASCII code in the range 65-90, which corresponds to an upper case letter.

Step 3:
At this stage, before the numbers are converted to letters, the ASCII codes of x, y and z are added, mod 26 is applied and a letter matching is performed.

- A → 1
- B → 2
- C → 3
- ...
- Z → 26

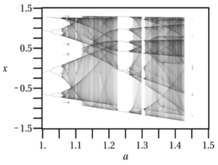
At the final stage, the obtained values were combined into a single value, and instead of getting output separately for each x, y and z, i.e. 3 outputs in total, 1 output was obtained.

F. Hénon Map

Hénon map, a chaotic system, is another system used in this study to generate keys. The Hénon map is a two-dimensional dynamic system. Although it is defined with simple equations, it may exhibit complex and unpredictable behaviours.

The equation below represents the Hénon map :

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n. \end{cases}$$



System parameters in the equation:

TABLE 2

a : the value is selected as 1.4.
b : the value is selected as 0.3.

State variables in the equation:

x : selected between -2 and 2.
y : selected between -2 and 2.

G. Normalization: Converting the Obtained Values from the Hénon map to Letters

Step 1

$$combined = (\frac{x+y}{2})$$

$$operation\ 1\ = Round\ (\frac{combined - min(combined)}{max(combined - min(combined)}\ x\ 25)$$

Step 2

$$Letter\ Output\ =\ chr(65\ +\ operation1)$$

H. One-Time Pad

One-Time Pad (OTP) is one of the simplest and most secure encryption methods, which employs a key string generated randomly. In this method, each character is paired with a random character to encrypt a message. The true randomness and one-time use of the key string ensure perfect secrecy to OTP.

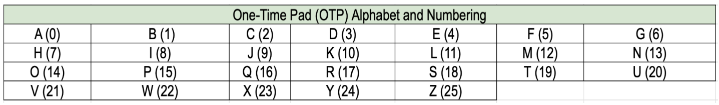
H.1. Plain Text

We choose "TUBITAK" as the plain text to be encrypted in the study. The plain text consists of only upper case letters and contains 7 characters in total.

H.2. Letter Matching

The letter-matching system used is shown below:

A = 0
B = 1
C = 2
...
Z = 25



One-Time Pad (OTP) Alphabet and Numbering						
A (0)	B (1)	C (2)	D (3)	E (4)	F (5)	G (6)
H (7)	I (8)	J (9)	K (10)	L (11)	M (12)	N (13)
O (14)	P (15)	Q (16)	R (17)	S (18)	T (19)	U (20)
V (21)	W (22)	X (23)	Y (24)	Z (25)		

TABLE 3

According to this matching, for example, the letter "T" has the value 19, the letter "U" has the value 20, the letter "B" has the value 1, the letter "I" has the value 8, the letter "A" has the value 0, and the letter "K" has the value 10.

H.3. Random String

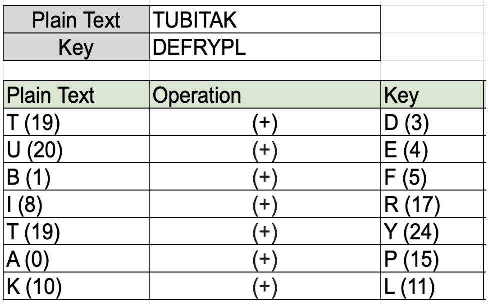
When OTP is applied to the random key string for encryption, i.e. the outputs obtained from the Lorenz system and Hénon map, we get "DEFRYPL". This key string is converted using the same letter matching as well:

D = 3
E = 4
F = 5
R = 17
Y = 24
P = 15
L = 11

H.4. Encryption Process

Each letter in the plain text is encrypted by adding it to the corresponding random letter. For example, the letter "T" (19) and the letter "D" (3) add up to 22, which corresponds to the letter "W". Similarly, the letter "U" (20) and the letter "E" (4) add up to 24, which corresponds to the letter "Y". This process is repeated for all the letters in the plain text to create the cipher text.

$$OTP\ Key\ =\ (Hénon\ Output\ +\ Lorenz\ Output)\ mod\ 26$$
$$Cipher\ text\ =\ (Plain\ Text\ +\ OTP\ Key)\ mod\ 26$$



Plain Text	TUBITAK
Key	DEFRYPL

Plain Text	Operation	Key
T (19)	(+)	D (3)
U (20)	(+)	E (4)
B (1)	(+)	F (5)
I (8)	(+)	R (17)
T (19)	(+)	Y (24)
A (0)	(+)	P (15)
K (10)	(+)	L (11)

TABLE 4

Some extraordinary situations may happen:

If the Addition Result is 26 or Greater: If the sum of the plain text and random key is 26 or greater, the “loop” process is applied. For example, if the sum of “T” (19) and “H” (7) is 26, then the result is considered 0 (A). In other words, as 25 is followed by 0, we return “A”. If the sum is 27, then the result is 1 (B). For example, since the sum of “T” (19) and “I” (8) is 27, the encrypted character will be 1 (B).

If the Random Text is Shorter or Longer Than the Plain Text:

If the random text is shorter or longer than the plain text, the numerical values of the corresponding letters in the random string, instead of the sum of letters, will be used, which will ensure encryption consistency.

Eventually, we get the cipher text "WYGZRPV" as a result of this process:

I. DNA Encryption

To encode DNA bases for"WYGZRPV", we can follow these steps:

Finding ASCII Equivalents: We find the corresponding ASCII value for each character:

W: 87
Y: 89
G: 71
Z: 90
R: 82
P: 80
V: 86

Converting ASCII Codes to Binary System: Equivalents of ASCII values in the binary system:

W: 87 → 01010111
Y: 89 → 01011001
G: 71 → 01000111
Z: 90 → 01011010
R: 82 → 01010010
P: 80 → 01010000
V: 86 → 01010110

XOR Operation between 0s and 1s in the Binary System:

01010111 → 1110
01011001 → 1111
01000111 → 1010
01011010 → 1111
01010010 → 1101
01010000 → 1100
01000010 → 1111

Assigning DNA Equivalents: Every two bits in the binary system is mapped to correspond to a DNA base:

00 → A
01 → T
10 → C
11 → G

Now we encode each character with DNA bases:

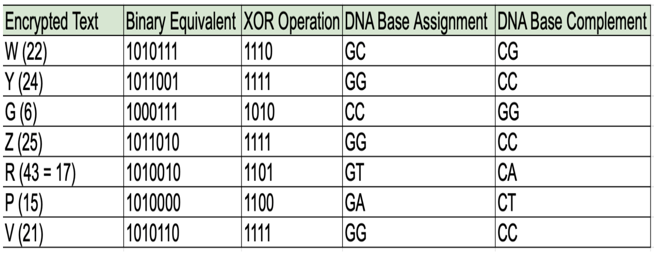
* 1110 - 1111 - 1010 - 1111 - 1101- 1100 - 1111→ GC-GG-CC-GG-GT-GA-GG

Generating Complementary DNA Sequences: We find complementary bases corresponding to each DNA base according to Watson-Crick rules:

T ↔ A
G ↔ C
A ↔ T
C ↔ G

Now we find the complementary sequence corresponding to the DNA sequence of **"WYGZRPV"** string:

W: GC → CG
Y: GG → CC
G: CC → GG
Z: GG → CC
R: GT → CA
P: GA → CT
V : GG → CC



Encrypted Text	Binary Equivalent	XOR Operation	DNA Base Assignment	DNA Base Complement
W (22)	1010111	1110	GC	CG
Y (24)	1011001	1111	GG	CC
G (6)	1000111	1010	CC	GG
Z (25)	1011010	1111	GG	CC
R (43 = 17)	1010010	1101	GT	CA
P (15)	1010000	1100	GA	CT
V (21)	1010110	1111	GG	CC

TABLE 5

Finally, we obtain "**CGCCGGCCCACTCC**" as our cipher text.

III. RESULTS

The current paper proposes a new DNA-based encryption method that combines chaotic systems such as the Mandelbrot set, Lorenz system, logistic map and Hénon map with the science of Cryptology. Using the randomness of chaotic systems and DNA structure, we put forward a more random encryption method compared to popular encryption methods in the market. This method provides an innovative solution needed by modern data security. In particular, we created a system that can endure potential threats to be caused by quantum computing. The proposed algorithm can be used in fields requiring high security, such as banking, health, e-commerce and particularly military communication. The study indicates that a significant step for data security has been taken and such innovative approaches can lay the foundation of stronger and more secure security systems in the future.

Practise Areas

1. **Banking:** Due to the high-security requirements, the DNA-based encryption method can be used in banking systems to protect data transmission. In this way, the security of sensitive financial information can be enhanced.
2. **Military Communication:** Ensuring communication security is of critical importance in military operations. DNA-based encryption methods can provide an effective solution for protecting sensitive military information.
3. **Health Services:** Since health data is extremely sensitive, DNA-based encryption systems can be used to protect the sensitive information of patients. These systems allow for the secure transmission of health data and ensure patient privacy.
4. **E-commerce:** It is highly important to protect user information and financial data in e-commerce platforms. DNA-based encryption methods provide protection against fraud and data breaches by enhancing user security.
5. **Cloud Computing:** With the widespread use of cloud computing services, data security becomes a crucial problem. DNA-based encryption can make access to user data more secure by enhancing the security of data stored in the cloud environment.

Advantages over Other Methods

High Security Level: DNA's information density and randomness provided by chaotic systems significantly increase the security provided by this encryption method. This method can be stronger against vulnerabilities experienced by conventional methods (AES, DES, RSA).
Complexity and Flexibility: DNA-based systems are capable of processing different types of data. This flexibility enables us to use this method to encrypt data with different types and sizes.
Advanced Key Management: DNA-based encryption systems can prevent intruders from accessing keys by making these keys more complex, which increases the overall security of the system.

All the above-mentioned steps are applied on the following web page. To access it, you can click https://dnaencryption.net/.

REFERENCES

[1] Alligood, K. T., Sauer, T. D., & Yorke, J. A. (1996). Chaos: An introduction to dynamical systems. Springer Science & Business Media.

[2] Alvarez, G., Montoya, F., Pastor, G., & Romera, M. (2003). Cryptanalysis of an ergodic chaotic cipher. Physics Letters A, 311(2-3), 172-179.

[3] Alavı Milani, M. M. R., Pehlivan, H., & Hosein Pour, S. (2012). A OTP (One Time Pad)Based DNA Encryption Method. The Black Sea Journal of Sciences, 5(2), 108-116.

[4] Avaroğlu, E. (2022).THE BUILDING BLOCK OF INFORMATION SECURITY: CRYPTOLOGY. Düşünce Dünyasında Türkiz, 8(43), 53-65

[5] Bechhoefer, J. (2005). The logistic map. Reviews of Modern Physics, 77(3), 633.

[6] Butcher, J. C. (2016). Numerical methods for ordinary differential equations. John Wiley & Sons.

[7] Devaney, R. L. (2018). An introduction to chaotic dynamical systems. CRC press.

[8] Enayatifar, R., Abdullah, A. H., & Isnin, I. F. (2014). DNA-based cryptography: An overview. Journal of Theoretical and Applied Information Technology, 61(3), 647.

[9] Frøyland, J. (1983). Lyapunov exponents for the Lorenz system. Physics Letters A, 97(6), 217-222.

[10] Gehani, A., LaBean, T. H., & Reif, J. H. (2004). DNA-based cryptography. In Aspects of molecular computing (pp. 167-188). Springer, Berlin, Heidelberg.

[11] Hilborn, R. C. (2000). Chaos and nonlinear dynamics: an introduction for scientists and engineers. Oxford University Press on Demand.

[12] Kumar, M., Iqbal, A., Kumar, P., & Singh, K. (2016). A new RGB image encryption algorithm based on DNA encoding and chaotic maps. Optik, 127(24), 12184-12194.

[13] Lorenz, E. N. (1963). Deterministic nonperiodic flow. Journal of the atmospheric sciences, 20(2), 130-141.

[14] May, R. M. (1976). Simple mathematical models with very complicated dynamics. Nature, 261(5560), 459-467.

[15] Mondal, M. K., & Mandal, J. K. (2016). An efficient image encryption scheme based on chaotic logistic map and DNA computing. In 2016 International Conference on Computational Intelligence and Networks (CIN) (pp. 304-308). IEEE.

[16] Rasband, S. N. (1990). Chaotic dynamics of nonlinear systems. Wiley.

[17] Schuster, H. G. (1989). Deterministic chaos: an introduction. VCH.

[18] Sparrow, C. (1982). The Lorenz equations: bifurcations, chaos, and strange attractors. Springer-Verlag.

[19] Sprott, J. C. (2003). Chaos and time-series analysis. Oxford University Press.

[20] Strogatz, S. H. (1994). Nonlinear Dynamics and Chaos. Addison-Wesley.

[21] Strogatz, S. H. (2018). Nonlinear dynamics and chaos with student solutions manual: With applications to physics, biology, chemistry, and engineering. CRC press.

[22] Süli, E., & Mayers, D. F. (2003). An introduction to numerical analysis. Cambridge University Press.

[23] Tucker, W. (1999). The Lorenz attractor exists. Comptes Rendus de l'Académie des Sciences-Series I-Mathematics, 328(12), 1197-1202.

[24] Viswanath, D. (2003). The fractal property of the Lorenz attractor. Physica D: Nonlinear Phenomena, 190(1-2), 115-128.

[25] Wang, X., & He, D. (2013). A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik, 124(13), 1222-1230.

[26] Xiao, G., Lu, M., Qin, L., & Lai, X. (2012). A new DNA-based image encryption algorithm. Multimedia Tools and Applications, 59(3), 817-832.

[27] Yang, Shyi-Kae, Chieh-Li Chen, Her-Terng Yau, Control of chaos in Lorenz system, Chaos, Solitons & Fractals, Volume 13, Issue 4, 2002.

[28] Zhang, X., Wang, S., & Liu, A. (2011). A novel image encryption scheme based on DNA sequences and chaotic systems. Journal of Software, 6(12), 2386-2393.