Nonlinear Dynamics and Systems Theory, **24** (6) (2024) 537–548

Using a 2-D Discrete Chaotic Map to Create a Safe Data in Symmetric Systems

Salah Adoui * and Brahim Benzeghli

Department of Mathematics, University of Batna 2, Batna, Algeria

Received: May 5, 2024; Revised: November 24, 2024

Abstract: In this work, we focus on the utility of chaotic systems of dimension 2 to generate symmetric keys which will be used to encrypt and decrypt data. Non-linear dynamical 2-D systems with chaotic logistic maps have properties that give us the means to hide data to be shared [10]. The two most important properties that are very useful in this work are: the non-linearity that gives a significant complexity to our keys, and the sensibility to the initial conditions that radically transforms our systems as soon as there is a minimal change [1].

Keywords: *matrices; Zeraoulia-Sprott maps; logistic maps; chaos; cryptography; xor operation.*

Mathematics Subject Classification (2010): 70K55, 70K75, 93-00.

1 Introduction

The use of chaotic maps of dimension 2 can be an interesting approach for the encryption of text. 2-D chaotic maps such as the Henon map or the standard map have 2-dimensional dynamic chaos properties [3]. Zeraoulia and Sprott [6] have proposed a new chaotic map of dimension 2,

$$\forall n \in \mathbb{N}; \quad \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} \dfrac{-ax_n}{1+y_n^2} \\ x_n + by_n \end{pmatrix},$$

where $\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ are given initial terms, that has the same properties, moreover, these maps can be used to generate complex pseudo-random sequences serving as encryption keys.

* Corresponding author: mailto:s.adoui@univ-batna2.dz

The chaotic transformations of these maps allow to introduce a strong confusion and diffusion in the encryption process. This blurs the links between the clear and encrypted texts and makes statistical analysis more difficult.

Zeraoulia and Sprott map parameters (such as the initial x_0 and y_0 terms, control parameters a and b) [6], [7] can be used to generate unique and unpredictable encryption keys. The sensitivity to the initial conditions ensures a strong uniqueness of the keys. The unpredictability and complexity of these maps make encryption more resistant to brute force attacks etc.

The implementation of 2-D chaotic maps in encryption algorithms requires additional calculations, but increases computing power and facilitates their integration. The use of 2-D chaotic maps for text encryption can provide enhanced security due to the complexity and unpredictability introduced by 2-dimensional chaos. However, it is important to design and optimize the implementation to achieve a balance between security and performance.

In this work, we used the chaotic maps for the creation of a key in matrix form, whose components are the successive terms of a logistic map. This key will be used in symmetric encryption [8], [9] and decryption of our data (text, digital image [11], etc.) using the logical operation xor.

2 The 2-D Rational Discrete Chaotic Map

In [6], [7], a 2-D discrete rationale map is given by

$$\forall n \in \mathbb{N};\quad \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} \dfrac{1}{0.1 + x_n^2} - a y_n \\ \dfrac{1}{0.1 + y_n^2} + b x_n \end{pmatrix} \text{ , where } \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \text{ are given initial terms,} \quad (1)$$

a and b are parameters, the 2-D chaotic map (1) is more complicated than the 1-D one. In their papers [6, 7], Zeraoulia and Sprot have proposed a new 2-D chaotic map given by

$$\forall n \in \mathbb{N};\quad \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} \dfrac{-a x_n}{1 + y_n^2} \\ x_n + b y_n \end{pmatrix} \text{ , where } \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \text{ are given initial terms,} \quad (2)$$

and a and b are bifurcation parameters. This map is algebraically simple but with more complications, it produces several new chaotic attractors. It leads, according to the values of a and b, to a convergent sequence, a continuation subject to oscillations or a chaotic sequel [6], [7]. The following four cases are considered, with the associated properties proved:

- $|a| < 1$, $|b| < 1$: Global asymptotic stability;
- $|a| < 1$, $|b| > 1$: Existence of unbounded solutions;
- $|a| > 1$, $|b| < 1$: Localization of non-trivial global attractor;
- $|a| > 1$, $|b| > 1$: Existence of unbounded solutions.

And there are some regular and chaotic regions when

$$\begin{cases} (a,b) \in [2,4] \times [0,1] \\ (a,b) \in [3,4] \times [-1,0]. \end{cases} \quad \text{or}$$

3 Construction of a Matrix $\mathfrak{M}$ Using Terms of 2-D Rational Discrete Chaotic Map

Consider the square matrix $\mathfrak{M} = (\mathfrak{m}_{ij})$ generated by the Zeraoulia-Sprott terms. And we obtain the following similar *Toeplidz* matrix $\mathfrak{M}$ [5]:

$$\mathfrak{M}_n = \begin{pmatrix} \frac{x_1+y_1}{2} & x_2 & x_3 & x_4 & \cdots & \cdots & \cdots & x_n \\ y_2 & \frac{x_2+y_2}{2} & x_{n+1} & x_{n+2} & \cdots & \cdots & \cdots & x_{2n-3} \\ y_3 & y_{n+1} & \frac{x_3+y_3}{2} & x_{2n-2} & \cdots & \cdots & \cdots & x_{3n-6} \\ y_4 & y_{n+2} & y_{2n-2} & \frac{x_4+y_4}{2} & \cdots & \cdots & \cdots & x_{4n-9} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & y_{\frac{n^2-n}{2}} \\ y_n & y_{2n-3} & y_{3n-6} & y_{4n-9} & \cdots & \cdots & y_{\frac{n^2-n}{2}} & \frac{x_n+y_n}{2} \end{pmatrix}. \tag{3}$$

We can also write

$$\mathfrak{M} = (m_{ij}) = \begin{cases} m_{ii} = \frac{x_i+y_i}{2} & if \quad i = j, \quad \forall i \in \{1, 2, \cdots, n\}, \\ m_{ij} = x_i & if \quad 1 < i < j, \\ m_{ij} = y_i & if \quad i > j > 1. \end{cases}$$

Encryption data using the matrix $\mathfrak{M}$

We recall that the BB84 protocol (proposed by Charles Bennett and Gilles Brassard in 1984) is a quantum key distribution protocol (QKD) that guarantees the security of the key generation process against attacks. The protocol uses the principles of quantum mechanics to establish a secure key between two interlocutors while detecting the presence of an attempted espionage [2].

4 Application

In our work, the matrix operation we will use is the logical *xor* between two matrices applied component by component. We recall that the *xor* operation is often used in cryptography, especially in flood encryption. This is how it works [4]:

1. **Plain text:** It is the original text that is being protected.
2. **Encryption flow:** It is a sequence of random bits generated using a secure cryptographic algorithm. This bit stream is used as the encryption key.
3. *xor* **operation:** It is a logical operation to compare each bit of the plain text with the corresponding bit of the encryption stream, bit by bit. The result of this *xor* operation gives the encrypted text.

The principle of the *xor* operation is as given in Table 1.

A	1	1	0	0
B	1	0	1	0
$A \oplus B$	0	1	1	0

Table 1: The *xor* operation.

Thus, by applying the *xor* operation between the plain text and the encryption flow, the encrypted text is obtained. Decryption works similarly: the *xor* operation is applied again between the encrypted text and the same encryption stream used for encryption. This makes it possible to find the original plain text. The advantage of the *xor* operation is that it is reversible and very fast to calculate. This is why it is often used in flood encryption algorithms such as One-Time Pad encryption.

Encryption and decryption of a text

In this section we give an application for encrypting and decrypting of a text using some cryptographic techniques.

Let $\mathcal{T}$ be a text to be encrypted, we start by converting it to binary and putting it in a square matrix $\mathcal{T}_c$ of order n.

Let L be the number of characters of the text (letters, symbols, numbers, etc,). We fix the size of the matrix by

$$n = \begin{cases} \sqrt{L} & if \quad \sqrt{L} \in \mathbb{N}, \\ E(\sqrt{L}+1) & if \quad \sqrt{L} \notin \mathbb{N}. \end{cases} \tag{4}$$

Then, we propose the encoding dictionary, see Table 2.

Character	A	B	C	D	E	F	G	H	I	J	K	L	M
Encoded character	01	02	03	04	05	06	07	08	09	10	11	12	13
Character	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Encoded character	14	15	16	17	18	19	20	21	22	23	24	25	26

Character	?	Space	,	.	!	;	:	’
Encoded character	27	28	29	30	31	32	33	34

Table 2: The proposed encoding dictionary.

4.1 Examples

Case 1: (when $n = \sqrt{L} \in \mathbb{N}$).

Let us have the text $\mathcal{T}$= ”HELLO BRAHIM, I AM SALAH.” We encode it using the previous dictionary, we obtain

$$\begin{aligned} \mathcal{T} &= \text{HELLO BRAHIM, I AM SALAH.} \\ &= 08051212142802170108091229280928011228180112010830. \end{aligned}$$

In this case, we have 25 characters, so $L = 25$ and the matrix size will be $n = 5$.

We set the order $n = 5$ and create a matrix using the code obtained, we get

$$\mathcal{T}_d = \begin{pmatrix} 08 & 05 & 12 & 12 & 14 \\ 28 & 02 & 17 & 01 & 08 \\ 09 & 12 & 29 & 28 & 09 \\ 28 & 01 & 12 & 28 & 18 \\ 01 & 12 & 01 & 08 & 30 \end{pmatrix}.$$

The matrix $\mathcal{T}_d$ has a matrix $\mathcal{T}_b$ whose elements are the binary conversions of each component of the matrix $\mathcal{T}_d$. So

$$\mathcal{T}_b = \begin{pmatrix} 01000 & 00101 & 01100 & 01100 & 01110 \\ 11100 & 00010 & 10001 & 00001 & 01000 \\ 01001 & 01100 & 11101 & 11100 & 01001 \\ 11100 & 00001 & 01100 & 11100 & 10010 \\ 00001 & 01100 & 00001 & 01000 & 11110 \end{pmatrix}.$$

The encryption key

Using the *Zeraoulia-Sprott* map:

- Let x_0, y_0, $2 < a < 4$ and $0 < b < 1$ be the four parameters exchanged between the interlocutors through the quantum channel using the $BB84$ protocol.
- After we have exchanged the four previous parameters, we introduce the Zeraoulia-Sprott map defined in (1) to calculate the $l = \frac{n^2-n}{2}$ first terms of the sequences $\{x_1, \cdots, x_l\}$ and $\{y_1, \cdots, y_l\}$.

In this case, we fix the parameters $x_0 = 2$, $y_0 = -3$, $a = 3$ and $b = 0.5$, we get the terms shown in Table 3.

i	1	2	3	4	5	6	7	8
x_i	-0,6000	1,4400	-3,8485	4,4402	-1,1743	0,3905	-1,1068	2,6322
y_i	0,5000	-0,3500	1,2650	-3,2160	2,8322	0,2417	0,5113	-0,8511
$\frac{x_i+y_i}{2}$	-0,0500	0,5450	-1,2917	0,6121	0,8289	X	X	X

i	9	10	11
x_i	-4,5791	2,3405	-0,5368
y_i	2,2066	-3,4757	0,6027

Table 3: 11 first terms of the Zeraoulia-Sprott sequence and 5 first means.

Using these terms, we construct a matrix of order $n = 5$:

$$\mathfrak{M}_5 = \begin{pmatrix} \frac{x_1+y_1}{2} & x_2 & x_3 & x_4 & x_5 \\ y_2 & \frac{x_2+y_2}{2} & x_6 & x_7 & x_8 \\ y_3 & y_6 & \frac{x_3+y_3}{2} & x_9 & x_{10} \\ y_4 & y_7 & y_9 & \frac{x_4+y_4}{2} & x_{11} \\ y_5 & y_8 & y_{10} & y_{11} & \frac{x_5+y_5}{2} \end{pmatrix}$$

$$= \begin{pmatrix} -0,0500 & 1,4400 & -3,8485 & 4,4402 & -1,1743 \\ -0,3500 & 0,5450 & 0,3905 & -1,1068 & 2,6322 \\ 1,2650 & 0,2417 & -1,2917 & -4,5791 & 2,3405 \\ -3,2160 & 0,5113 & 2,2066 & 0,6121 & -0,5368 \\ 2,8322 & -0,8511 & -3,4757 & 0,6027 & 0,8289 \end{pmatrix}.$$

As the basis of the binaries is $\{0,1\}$, then the class of a negative real number converted to binary is the same as that of the same number taken without sign (positive). For this, we can take all the components of the matrix in absolute values. So we get a new matrix with same results,

$$\mathfrak{M}_5^+ = \begin{pmatrix} 0,0500 & 1,4400 & 3,8485 & 4,4402 & 1,1743 \\ 0,3500 & 0,5450 & 0,3905 & 1,1068 & 2,6322 \\ 1,2650 & 0,2417 & 1,2917 & 4,5791 & 2,3405 \\ 3,2160 & 0,5113 & 2,2066 & 0,6121 & 0,5368 \\ 2,8322 & 0,8511 & 3,4757 & 0,6027 & 0,8289 \end{pmatrix}.$$

To be able to work with natural integer components, we must get rid of commas, for this, we propose to multiply the components of the matrix $\mathfrak{M}_5^+$ by a power k of 10 chosen according to our needs, then we take only the integer part of each component after multiplication. In our example, we can take $k = 3$, therefore, all components of $\mathfrak{M}_5^+$ must be multiplied by 10^3. We get a new matrix

$$E(\mathfrak{M}_5^+) = \begin{pmatrix} 50 & 1440 & 3848 & 4440 & 1174 \\ 350 & 545 & 390 & 1106 & 2632 \\ 1265 & 241 & 1291 & 4579 & 2340 \\ 3216 & 511 & 2206 & 612 & 536 \\ 2832 & 851 & 3475 & 602 & 828 \end{pmatrix}.$$

We convert the components of the matrix $E(\mathfrak{M}_5^+)$ into binary and we obtain a matrix K which will be the common key for encryption and decryption,

$$K = \begin{pmatrix} 110010 & 10110100000 & 111100001000 & 1000101011000 & 10010010110 \\ 101011110 & 1000100001 & 110000110 & 10001010010 & 101001001000 \\ 10011110001 & 11110001 & 10100001011 & 1000111100011 & 100100100100 \\ 110010010000 & 111111111 & 100010011110 & 1001100100 & 1000011000 \\ 101100010000 & 1101010011 & 110110010011 & 1001011010 & 1100111100 \end{pmatrix}.$$

Encryption

To encrypt the text $\mathcal{T}$, we use the formula $\mathcal{T}_c = \mathcal{T}_b \oplus K$. So

$$\mathcal{T}_c = \begin{pmatrix} 111010 & 10110100101 & 111100010100 & 1000101100100 & 10010100100 \\ 101111010 & 1000100011 & 110010111 & 10001001101 & 101001010000 \\ 10011111010 & 11111101 & 10100101000 & 1000111111111 & 100100101101 \\ 110010101100 & 1000000000 & 100010101010 & 1010000000 & 1000101010 \\ 101100010001 & 1101011111 & 110110010100 & 1001100010 & 1101011010 \end{pmatrix}.$$

$\mathcal{T}_c$ will be sent to the receiver.

Decryption

The recipient receives $\mathcal{T}_c$ and decrypts it to obtain the initial matrix using the formula

$$\mathcal{T}_c \oplus K = \mathcal{T}_b.$$

Proof.

$$\begin{aligned} \mathcal{T}_c \oplus K &= \mathcal{T}_b \oplus K \oplus K \\ &= \mathcal{T}_b \oplus O_5 \quad (O_5 \text{ is the null matrix of order 5}) \\ &= \mathcal{T}_b. \end{aligned}$$

After this, the receiver converts the binary matrix $\mathcal{T}_b$ to the decimal matrix $\mathcal{T}_d$, then he uses the dictionary, see Table 2, to obtain the initial text " $\mathcal{T}$ = HELLO BRAHIM, I AM SALAH."

Case 2: $(\sqrt{L} \notin \mathbb{N})$.

In the case when $\sqrt{L}$ is not a perfect square, we put all the obtained codes in order from left to right and down, and we put zeros in the remaining places.

Let us take the text $\mathcal{T}$= "HELLO BRAHIM, I AM SALAH'S FRIEND." We encode it using the previous dictionary, we obtain

$$\begin{aligned} \mathcal{T} &= \text{HELLO BRAHIM, I AM SALAH'S FRIEND.} \\ &= 08051212142802170108091229280928011228180112010834192806180905140430. \end{aligned}$$

In this case, we have 34 characters, so $L = 34$ and the matrix size will be $n = E(\sqrt{34}+1) = 6$.

We set the order $n = 6$ and create a matrix using the code obtained, we get

$$\mathcal{T}_d = \begin{pmatrix} 08 & 05 & 12 & 12 & 14 & 28 \\ 02 & 17 & 01 & 08 & 09 & 12 \\ 29 & 28 & 09 & 28 & 01 & 12 \\ 28 & 18 & 01 & 12 & 01 & 08 \\ 34 & 19 & 28 & 06 & 18 & 09 \\ 05 & 14 & 04 & 30 & 00 & 00 \end{pmatrix}.$$

The matrix $\mathcal{T}_d$ has a matrix $\mathcal{T}_b$ whose elements are the binary conversions of each component of the matrix $\mathcal{T}_d$. So

$$\mathcal{T}_b = \begin{pmatrix} 01000 & 00101 & 01100 & 01100 & 01110 & 11100 \\ 00010 & 10001 & 00001 & 01000 & 01001 & 01100 \\ 11101 & 11100 & 01001 & 11100 & 00001 & 01100 \\ 11100 & 10010 & 00001 & 01100 & 00001 & 01000 \\ 100010 & 10011 & 11100 & 110 & 10010 & 1001 \\ 101 & 1110 & 100 & 11110 & 0000 & 0000 \end{pmatrix}.$$

The encryption key

Using the *Zeraoulia-Sprott* map:

- Let x_0, y_0, $2 < a < 4$ and $0 < b < 1$ be the four parameters exchanged between the interlocutors through the quantum channel using the $BB84$ protocol.
- After we have exchanged the four previous parameters, we introduce the Zeraoulia-Sprott map defined in (1) to calculate the $l = \frac{n^2-n}{2}$ first terms of the sequences $\{x_1, \cdots, x_l\}$ and $\{y_1, \cdots, y_l\}$.

The matrix size will be 6, so we calculate the first 16 terms of each of the two sequences whose first 11 terms will be the same as those calculated in the first case, see Table 3. We get

i	$\cdots$	6	$\cdots$	11	12	13	14	15	16
x_i	$\cdots$	0,3905	$\cdots$	-0,5368	1,1813	-3,3577	4,7266	-1,5780	0,3952
y_i	$\cdots$	0,2417	$\cdots$	0,6027	-0,2354	1,0636	-2,8259	3,3136	0,0788
$\frac{x_i+y_i}{2}$	$\cdots$	0,3161	$\cdots$	X	X	X	X	X	X

Using these terms, we construct a matrix of order $n = 6$:

$$\mathfrak{M}_6 = \begin{pmatrix} \frac{x_1+y_1}{2} & x_2 & x_3 & x_4 & x_5 & x_6 \\ y_2 & \frac{x_2+y_2}{2} & x_7 & x_8 & x_9 & x_{10} \\ y_3 & y_7 & \frac{x_3+y_3}{2} & x_{11} & x_{12} & x_{13} \\ y_4 & y_8 & y_{11} & \frac{x_4+y_4}{2} & x_{14} & x_{15} \\ y_5 & y_9 & y_{12} & y_{14} & \frac{x_5+y_5}{2} & x_{16} \\ y_6 & y_{10} & y_{13} & y_{15} & y_{16} & \frac{x_6+y_6}{2} \end{pmatrix}$$

$$= \begin{pmatrix} -0,0500 & 1,4400 & -3,8485 & 4,4402 & -1,1743 & 0,3905 \\ -0,3500 & 0,5450 & -1,1068 & 2,6322 & -4,5791 & 2,3405 \\ 1,2650 & 0,5113 & -1,2917 & -0,5368 & 1,1813 & -3,3577 \\ -3,2160 & -0,8511 & 0,6027 & 0,6121 & 4,7266 & -1,5780 \\ 2,8322 & 2,2066 & -0,2354 & -2,8259 & 0,8289 & 0,3952 \\ 0,2417 & -3,4757 & 1,0636 & 3,3136 & 0,0788 & 0,3161 \end{pmatrix}.$$

Then we get a new positive matrix with same results

$$\mathfrak{M}_6^+ = \begin{pmatrix} 0,0500 & 1,4400 & 3,8485 & 4,4402 & 1,1743 & 0,3905 \\ 0,3500 & 0,5450 & 1,1068 & 2,6322 & 4,5791 & 2,3405 \\ 1,2650 & 0,5113 & 1,2917 & 0,5368 & 1,1813 & 3,3577 \\ 3,2160 & 0,8511 & 0,6027 & 0,6121 & 4,7266 & 1,5780 \\ 2,8322 & 2,2066 & 0,2354 & 2,8259 & 0,8289 & 0,3952 \\ 0,2417 & 3,4757 & 1,0636 & 3,3136 & 0,0788 & 0,3161 \end{pmatrix}.$$

We follow the same steps we did in the first case, we get the integer matrix

$$E(\mathfrak{M}_6^+) = \begin{pmatrix} 50 & 1440 & 3848 & 4440 & 1174 & 390 \\ 350 & 545 & 1106 & 2632 & 4579 & 2340 \\ 1265 & 511 & 1291 & 536 & 1181 & 3357 \\ 3216 & 851 & 602 & 612 & 4726 & 1578 \\ 2832 & 2206 & 235 & 2825 & 828 & 395 \\ 241 & 3475 & 1063 & 3313 & 78 & 316 \end{pmatrix}.$$

We convert the components of the matrix $E(\mathfrak{M}_5^+)$ into binary and we obtain a matrix

$K = [K^{'}|K^{''}]$, where

$$K^{'} = \begin{pmatrix} 110010 & 10110100000 & 111100001000 \\ 101011110 & 1000100001 & 10001010010 \\ 10011110001 & 111111111 & 10100001011 \\ 110010010000 & 1101010011 & 1001011010 \\ 101100010000 & 100010011110 & 11101011 \\ 11110001 & 110110010011 & 10000100111 \end{pmatrix}$$

$$K^{''} = \begin{pmatrix} 1000101011000 & 10010010110 & 110000110 \\ 101001001000 & 1000111100011 & 100100100100 \\ 1000011000 & 10010011101 & 110100011101 \\ 1001100100 & 1001001110110 & 11000101010 \\ 101100001001 & 1100111100 & 110001011 \\ 110011110001 & 1001110 & 100111100 \end{pmatrix}.$$

This matrix K will be the common key for encryption and decryption.

Encryption

To encrypt the text $\mathcal{T}$, we use the formula $\mathcal{T}_c = \mathcal{T}_b \oplus K = [\mathcal{T}_c^{'}|\mathcal{T}_c^{''}]$, where

$$\mathcal{T}_c^{'} = \begin{pmatrix} 111010 & 10110100101 & 111100010100 \\ 101100000 & 1000110010 & 10001010011 \\ 10100001110 & 1000011011 & 101000010100 \\ 110010101100 & 1101100101 & 1001011011 \\ 101100110010 & 100010110001 & 100000111 \\ 11110110 & 110110100001 & 10000101011 \end{pmatrix},$$

$$\mathcal{T}_c^{''} = \begin{pmatrix} 1000101100100 & 10010100100 & 110100010 \\ 101001010000 & 10000111101100 & 100100110000 \\ 1000110100 & 10010011110 & 110100101001 \\ 1001110000 & 1001001110111 & 11000110010 \\ 101100001111 & 1101001110 & 110010100 \\ 110100001111 & 1001110 & 100111100 \end{pmatrix}.$$

$\mathcal{T}_c$ will be sent to the receiver.

Decryption

The recipient receives $\mathcal{T}_c$ and decrypts it to obtain the initial matrix using the formula

$$\mathcal{T}_c \oplus K = \mathcal{T}_b.$$

Proof.

$$\begin{aligned} \mathcal{T}_c \oplus K &= \mathcal{T}_b \oplus K \oplus K \\ &= \mathcal{T}_b \oplus O_6 \quad (O_6 \ \textit{is the null matrix of order 6}) \\ &= \mathcal{T}_b. \end{aligned}$$

After this, the receiver converts the binary matrix $\mathcal{T}_b$ to the decimal matrix $\mathcal{T}_d$, then he uses the dictionary, see Table 2, to obtain the initial text

$$\mathcal{T} = \text{" HELLO BRAHIM, I AM SALAH'S FRIEND."}$$

Generalisation

In general, to encrypt a text of length L, we follow the same steps as in the previous example.

Step 1: The text

(a) We choose a dictionary to code the text $\mathcal{T}$ (In our example, we have used the dictionary given in Table 2).

(b) Let $\mathcal{T}_d$ be the matrix of order n. The order n is calculated according to the formula (4). And the components of $\mathcal{T}_d$ are the obtained codes put in order from left to right and down, and we put zeros in the remaining places.

(c) We convert the components of the matrix $\mathcal{T}_d$ into binaries, and we obtain a matrix $\mathcal{T}_b$.

Step 2: The encryption key

(a) Let us choose the chaotic sequence of *Zeraoulia* of dimension 2 (see formula (2)). Then we fix the first terms (x_0, y_0) and two parameters a and b such that the chaos is assured [6], [7], the calculus of the first $\dfrac{n^2-n}{2}$ terms of the vector sequence $(x_i, y_i)_{i\in\{1,\cdots,\frac{n^2-n}{2}\}}$ gives us the components of $\mathfrak{M}_n$, the matrix of order n in the form given in the expression (3).

(b) We take all the components of the matrix $\mathfrak{M}_n$ in absolute values to get the matrix $\mathfrak{M}_n^+$.

(c) We multiply the components of the matrix $\mathfrak{M}_n^+$ by a power k of 10 chosen according to our needs, then we take only the integer part of each component after multiplication, then we create a new matrix denoted $E(\mathfrak{M}_n^+)$ whose components are the integer parts of the components of $\mathfrak{M}_n^+$.

(d) We convert the components of the matrix $E(\mathfrak{M}_n^+)$ into binary and we obtain a matrix K which will be the common key for encryption and decryption.

Step 3: Encryption and Decryption

(a) To encrypt the encoded text $\mathcal{T}_b$, we use the formula

$$\mathcal{T}_c = \mathcal{T}_b \oplus K.$$

(b) To decrypt $\mathcal{T}_c$ for obtaining the initial matrix, we use the formula

$$\mathcal{T}_c \oplus K = \mathcal{T}_b.$$

(c) The binary matrix $\mathcal{T}_b$ will be converted to a decimal matrix which will decoded to a text using the initial dictionary, see Table 2, to obtain the initial text " $\mathcal{T}$ ".

5 Performance and Security Analysis

To study the efficacy of our text encryption, we test its security. The proposed method should resist several types of attacks because its symmetric keys used during the encryption and decryption must be transmitted through an unsecured channel.

Cryptanalysis

To determine the key, it is necessary to use techniques more secured and compliant against attacks, these techniques are called the key exchange protocols. In our system, we detail how we can obtain a secret key using the properties of matrices for encrypting and decrypting text and sensibility of chaotic maps to initial conditions. The question is: Can we ensure the security of this encryption? For this, to raise the security levels of our system, we have introduced chaotic logistic maps in cryptography.

For the implementation of the proposed scheme, we choose the size of text $127^2 < L \leq 128^2$. The proposed scheme key $\mathcal{K}$ is none-deterministic because the interlocutors use an arbitrary matrix $(\mathcal{K})$ for getting a common secret key $\mathcal{K}$.

We use the proposed key generation method with $x_i, y_i; \quad i \in \{0, \cdots, 8128\}$; $(x_i, y_i$ are the components of the key $\mathcal{K})$. This provides 10^{k+1} possible cases to obtain one component of the key $\mathcal{K}$. So it provides $(10^{k+1})^{n^2} = 10^{(k+1)n^2}$ possible cases to obtain the key K.

For $n = 128$ and $k = 14$, we get $(10^{15})^{128^2} = 10^{(15)16384} = 10^{245760} > (2^3)^{245760} = 2^{737280}$.

We have also 10^{20} possible cases for getting the term x_0 (with 20 decimal digits after the comma in the set of 10 numbers $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$) if we use the 2-D rational discrete chaotic map that contains 2 parameters a, b and the initial terms (x_0, y_0), so this provides

$$(10^{20})^4 = 10^{80} > 2^{260}.$$

The key space is wide enough for a brute force attack or exhaustive attack is not possible.

6 Concluding Remarks

We know that chaos can be exploited in encryption algorithms to improve the security and robustness of encryption systems. That is why we have included a chaotic system of dimension 2 with the following advantages:

- Chaotic encryption systems use non-linear dynamic systems to generate complex pseudo-random sequences that serve as encryption keys.
- Sensitivity to initial conditions of chaotic systems makes encryption very difficult to break and ensures a strong uniqueness of the generated keys.
- Chaotic properties can be used to generate complex and unpredictable encryption keys from initial parameters.
- Chaotic transformations can be incorporated into the dissemination and confusion stages of encryption algorithms to further blur the links between the plain and encrypted texts.
- This makes encryption more resistant to statistical analysis attacks.
- Unpredictability and sensitivity to chaotic system parameters can be used to enhance the security of encrypted communication protocols.

- This makes them more resistant to brute force attacks and model analysis attacks.

The judicious use of chaos in encryption algorithms leads to safer and more robust encryption systems against various cryptographic attacks.

In our work, we used a chaotic system of dimension two, which already has the venture to keep the two most important options: the non-linearity of the system and its sencibility to the initial conditions, in addition to that, it has increased the security level of the shared key to 2^{260}, which far exceeds the known threshold.

References

[1] A. Sambas, S. Vaidyanathan, S. F. Al-Azzawi, M. K. M. Nawawi, M. A. Mohamed, Z. A. Zakaria, S. S. Abas and M. Mamat. Modelling and MultiSim Simulation of a New Hyperchaos System with No Equilibrium Point. *Nonlinear Dynamics and Systems Theory* **23** (4) (2023) 422–433.

[2] S. Adoui, B. Benzeghli and L. Noui. Sharing Keys Using Circular Matrices and Logistic Maps Through Quantum Channel. *Advances in Mathematics: Scientific Journal* CCS **12** (2022) 1361–1378.

[3] M. Ausloos. *The Logistic Map and the Route to Chaos: From the Beginnings to Modern Applications*. Springer, 2006.

[4] G. Boole. *The Mathematical Analysis of Logic, Being an Essay Towards a Calculus of Deductive Reasoning*. Cambridge (London: Macmillan, Barclay and Macmillan George Bell), 2006.

[5] A. Böttcher and B. Silbermann. *Introduction to Large Truncated Toeplitz Matrices*. Springer, New York, 2012.

[6] Z. Elhadj and J. C. Sprott. On the Dynamics of a New Simple 2-d Rational Discrete Mapping. *Int. J. Bifurc. Chaos* **21** (2011) 155–160.

[7] G. Chen, E.V. Kudryashova, N. V. Kuznetsov and G. A. Leonov. Dynamics of the Zeraoulia-Sprott map revisited. *International Journal of Bifurcation and Chaos* **26** (07) (2016) 1650126.

[8] J. Lu, X. Wu, J. Lû and K. Kang. A new discrete chaotic system with rational fraction and its dynamical behaviors. *Chaos Solit. Fract.* **22** (2004) 311–319.

[9] Marzieh Azadi and Hossein Jafari. Lie Symmetry Reductions of a Coupled Kdv System of Fractional Order. *Nonlinear Dynamics and Systems Theory* **18** (1) (2018) 22–28.

[10] N. Djafri, T. Hamaizia and F. Derouiche. Boundedness and Dynamics of a Modified Discrete Chaotic System with Rational Fraction. *Nonlinear Dynamics and Systems Theory* **21** (1) (2021) 68–75.

[11] W. S. Mada Sanjaya, Akhmad Roziqin, Agung Wijaya Temiesela, M. Fauzi Badru Zaman, Aria Dewa Wibiksana and Dyah Anggraeni. Moore-Spiegel Chaotic Encryption for Digital Images and Voices. *Nonlinear Dynamics and Systems Theory* **23** (5) (2023) 445–460.