Nonlinear Dynamics and Systems Theory, **24** (4) (2024) 366–379

Sharing Keys Using Some Toeplitz Matrices and Logistic Maps

Benzeghli Brahim [*] and Adoui Salah

University of Batna 2, Batna, Algeria.

Received: February 12, 2024; Revised: June 21, 2024

Abstract: In symmetric cryptosystems, we use the same keys to encrypt and decrypt data, our question is how to share this common keys? Using the commutativity of the multiplication of circular matrices and sensibility to initial conditions in chaotic logistic maps through two different channels, we give some new techniques for creating and sharing two keys and use them to increase the level of security during the encryption and decryption of texts or digital images.

Keywords: *Toeplitz matrices; circular matrices; logistic maps; chaos; cryptography; BB84 protocol; Diffie-Hellman protocol.*

Mathematics Subject Classification (2010): 70K55, 37D45.

1 Introduction

The main goal of this work is the creation of two keys through two different channels. For the first key, based on the same techniques as in our previous work [1], we set a $t \in [-1, 1]$ and we create a circular matrix generated by the vector $(a(t), b(t), c(t))$ such that $a = t^2 + 1$, $b = t$ and $c = -t$. This choice is made so that the trace and the determinant of the generated circular matrix are strictly positive, which allows us to calculate the initial parameters of a logistic sequence as follows:

$$\mu = \frac{\det \mathcal{T}}{\det \mathcal{T} + 1} + 3 \quad \textit{and} \quad x_0 = \frac{tr\mathcal{T}}{tr\mathcal{T} + 1}. \tag{1}$$

This choice checks the chaotic case because $\mu \in]3, 4[$ and $x_0 \in]0, 1[$. These two parameters will be shared through a quantum channel by the exchange protocol BB84.

[*] Corresponding author: mailto:b.benzeghli@univ-batna2.dz

So, the key K created will be the circular matrix generated by the vector $V(y_1, \cdots, y_n)$, where

$$\forall i \in \mathbb{N}, \quad y_i = [10^{15} x_i] \mod (p) \in (\mathbb{Z}/p\mathbb{Z})^*;$$

p is a prime number such that $\forall i \in \mathbb{N}, \quad p > y_i$ and x_i are the terms of the logistic sequence

$$\forall n \in \mathbb{N}, \quad x_{n+1} = \mu x_n(1 - x_n).$$

Then $K = \langle y_1, y_2, \cdots, y_n \rangle$.

The creation of the second key will be done using the first key K and based on the commutativity of the multiplication of circular matrices.

These two keys K and C will be used for the encryption and decryption of digital images.

2 Toeplitz Matrices of Order 3

In 1911, *Otto Toeplitz* introduced the*Toeplitz matrices* after the study of the quadratic forms $\sum \varphi_{i,j} x_i y_j$, for which the coefficients of these forms verify the particular property $\varphi_{i,j} = \varphi_{i-j}$, and thus obtained associated matrices $\mathcal{T} = (\varphi_{i,j})_{i,j}$ on diagonal and on-diagonal and sub-diagonal constants that are now called the Toeplitz matrices [3,4]. More recently, the particular structure with diagonals and on-diagonals and/or sub-diagonals constants of the Toeplitz matrices appears in various problems as a result of the different methods of resolution used or by the methods of raising data at regular time interval or space which will make appear systems with diagonal matrices and on-constant diagonals and sub-constant diagonals.

Definition 2.1 We call the Toeplitz matrix, any matrix $\mathcal{T} \in \mathcal{M}_n(\mathbb{R})$ with diagonal and on-diagonal and sub-diagonal constants, that is to say, any matrix of the form

$$\mathcal{T} = \begin{bmatrix} t_0 & t_1 & \cdots & t_{-(n-1)} \\ t_1 & t_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & t_{-1} \\ t_{n-1} & \cdots & t_1 & t_0 \end{bmatrix}, \text{ where } t_i \in \mathbb{R} \text{ for all } i \in \{-(n-1), \cdots, n-1\}.$$

We can distinguish two particular cases in the following remark.

Remark 2.1

1. If $t_{n-j} = t_{-j}$ for $j \in \{0, \cdots, n\}$, the matrix $\mathcal{T}$ is said to be a circular matrix.
2. If $t_{n-j} = -t_{-j}$ for $j \in \{0, \cdots, n\}$, so we are talking about an anti-circular matrix.

The particular case of circular and anti-circular matrices is interesting in the context of diagonalization. Indeed, these matrices with a particular structure can be diagonalized using the *FFT* (*Fast Fourier Transform*) with a lower complexity than any matrix without a particular structure.

The shape of a circular matrix is given in the following definition.

Definition 2.2 A circular matrix is a Toeplitz matrix given by

$$\mathcal{C}_n = \mathcal{C}_n(c_1, \cdots, c_n) = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ c_n & c_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & c_2 \\ c_2 & \cdots & c_n & c_1 \end{bmatrix} \in \mathcal{M}_n(\mathbb{R}).$$

3 The Abelian Group of *Circular Matrices* of Order 3 with Some Conditions

The aim of this section is to create an abelian group of circular matrices of order 3 with matricial composition, we denote it by $\mathbf{C}_3(I)$, where $I \subset \mathbb{R}$ such that the elements of $\mathbf{C}_3$ are invertible, see [7, 9].

Definition 3.1 A square matrix C of order 3 is said to be circular if and only if it is generated by one vector $V(a, b, c)$. Such a matrix is of the form

$$C = \langle V \rangle = \langle a, b, c \rangle = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}. \tag{2}$$

We know that an abelian group must verify the commutativity, the associativity, the existence of a neutral element and the invertibility of all elements.

Theorem 3.1 (Commutativity in $\mathbf{C}_3$) *For any $A, B \in \mathbf{C}_3$, we have $AB = BA$.*

Proof. By definition, A and $B \in \mathbf{C}_3$ means that there exist $V(a, b, c)$ and $V'(a', b'c')$ such that

$$A = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \quad \textit{and} \quad B = \begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix}.$$

We have

$$\begin{aligned} AB &= \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix} \\ &= \begin{pmatrix} aa' + bc' + cb' & ab' + ba' + cc' & ac' + bb' + ca' \\ ca' + ac' + bb' & cb' + aa' + bc' & cc' + ab' + ba' \\ ba' + cc' + ab' & bb' + ca' + ac' & bc' + cb' + aa' \end{pmatrix} \\ & (\textit{ addition and multiplication are commutatives in } \mathbb{R}) \\ &= \begin{pmatrix} a'a + c'b + b'c & b'a + a'b + c'c & c'a + b'b + a'c \\ a'c + c'a + b'b & b'c + a'a + c'b & c'c + b'a + a'b \\ a'b + c'c + b'a & b'b + a'c + c'a & c'b + b'c + a'a \end{pmatrix} \\ &= \begin{pmatrix} a' & b' & c' \\ c' & a' & b' \\ b' & c' & a' \end{pmatrix} \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \\ &= BA. \end{aligned}$$

Theorem 3.2 (Associativity in $\mathbf{C}_3$) *For any A, B and $C \in \mathbf{C}_3$ we have*

$$A(BC) = (AB)C = ABC.$$

It is easy to verify the equality with a useful calculus.

Theorem 3.3 *The identity matrix I_3 is the neutral element in $\mathbf{C}_3$ for matrix multiplication.*

We know that the Toeplitz matrices are not always invertible, and to have the invertibilty, we must impose some conditions on its terms.

For a matrix to be invertible, it is necessary and sufficient that its determinant is not null.

We choose the vector $V = (a, b, -b)$, where $a = t^2+1$ and $b = t$. The matrix becomes

$$\mathcal{T} = \begin{pmatrix} a & b & -b \\ -b & a & b \\ b & -b & a \end{pmatrix} = \begin{pmatrix} t^2+1 & t & -t \\ -t & t^2+1 & t \\ t & -t & t^2+1 \end{pmatrix}. \tag{3}$$

Then, the determinant of $\mathcal{T}$ is

$$\begin{aligned} \det(\mathcal{T}) &= a^3+b^3+c^3-3abc \\ &= t^6+6t^4+6t^2+1. \end{aligned}$$

We can see that $\det(\mathcal{T})$ is a function of t.

Proposition 3.1 *The function*

$$\begin{array}{rccl} f: & \mathbb{R} & \to & \mathbb{R} \\ & t & \mapsto & f(t) = det(\mathcal{T}) = t^6+6t^4+6t^2+1 \end{array}$$

is strictly positive ($f > 0$).

Proof. By plotting the function f with *GeoGebra*, we get the following graph (Figure 1).

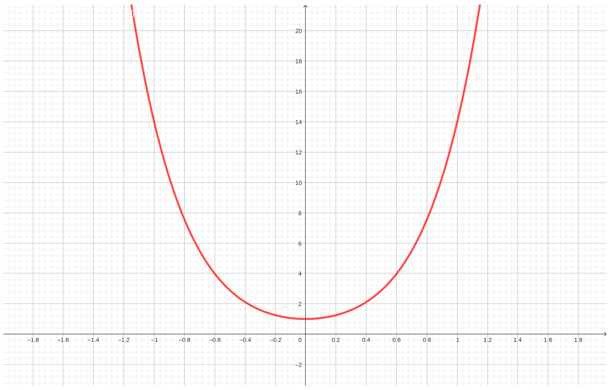


Figure 1: The graph of $f(t) = det(\mathcal{T})$ on $\mathbb{R}$.

We observe that the curve of the function f is always on the x-axis, which shows that f is strictly positive.

Theorem 3.4 *The matrix $\mathcal{T}$ in (3) is invertible and the inverse $\mathcal{T}^{-1}$ is given by*

$$\mathcal{T}^{-1} = \frac{1}{t^6 + 6t^4 + 6t^2 + 1} \begin{pmatrix} t^4 + 3t^2 + 1 & -t^3 + t^2 - t & t^3 + t^2 + t \\ t^3 + t^2 + t & t^4 + 3t^2 + 1 & -t^3 + t^2 - t \\ -t^3 + t^2 - t & t^3 + t^2 + t & t^4 + 3t^2 + 1 \end{pmatrix}. \quad (4)$$

Proof. The existence of the inverse matrix is ensured by Proposition 3.1.

To calculate it, we use the formula $\mathcal{T}^{-1} = \frac{1}{\det \mathcal{T}} Com({}^t\mathcal{T})$, the desired result is obtained.

Theorem 3.5 *The set $\mathbf{C}_3$ menu by the law of matrix composition forms an abelian group.*

Proof. The demonstration is immediate according to Theorems 3.1, 3.2, 3.3 and 3.4.

4 Logistic Maps

In mathematics, a logistic map is a real simple sequence, but its recurrence is not linear, see [2,10,11].

Definition 4.1 A logistics map $(x_n)_{n\in\mathbb{N}}$ is a non-linear real sequence defined by its first term $x_0 \in [0,1]$ and the following recurring formula:

$$\begin{array}{rccl} x_n : & \mathbb{N} & \to & \mathbb{R} \\ & n & \mapsto & x_{n+1} = \mu x_n(1 - x_n)\ , \quad \mu \in [0,4]. \end{array} \quad (5)$$

Depending on the value of the parameter $\mu \in [0,4]$, to ensure that the values of X remain in $[0,1]$, it generates either a convergent sequence, a series subjected to oscillations, or a chaotic sequence.

4.1 The chaotic case ($\mu \in [3.57, 4]$)

We are interested in the chaotic case, where $\mu \in [3.57, 4]$.

Most values above 3.57 have a chaotic character, but there are some isolated values of μ with a behaviour that is not. For example, from $1 + \sqrt{8}$ (about 3.82), a small range of μ values has an oscillation between three values and for a slightly larger μ, between six values, then twelve, etc. Other ranges offer oscillations between 5 values, etc. All periods of oscillation are present, again independently of the initial population.

The horizontal axis bears the values of the parameter μ (noted r), while the vertical axis shows the possible adhesion values.

4.2 Sensitivity to the initial conditions

The most important property of the logistic maps is sensitivity to the initial conditions. This results in a radical change in the sequence behaviour as soon as there is a very small change in the initial value x_0.

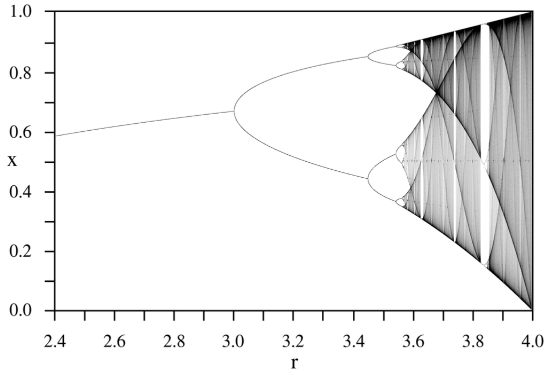


Figure 2: A bifurcation diagram of a logistic map.

5 Application in Cryptography

In general, cryptography is a writing technique where an encrypted message is written using secret codes or encryption keys. Cryptography is primarily used to protect a message considered confidential. This method is used in many areas such as the secret army, information technology, privacy, etc. There are many cryptographic algorithms that can be used to encrypt (and decrypt for the recipient) the message, see [8, 14].

Definition 5.1 [Cryptosystem] A cryptosystem is a term used in cryptography to refer to a set of cryptographic algorithms and all possible plain texts, encrypted texts and keys.

Definition 5.2 [Components of a cryptosystem] A basic cryptosystem consists of the following variants:

1. **Plain text:** This is the data (text or images) that we want to protect during transmission.

2. **Encryption Algorithm:** This is a mathematical process that produces encryption for all data in clear and key encryption. It is a cryptographic algorithm that takes the plain text and an encryption key as an input and produces an encrypted text.

3. **Encrypted text:** This is the scrambled version of the plain text produced by the encryption algorithm using a specific encryption key. The encrypted text is not protected. It circulates on a public channel. It can be intercepted or compromised by anyone with access to the communication channel.

4. **Decryption algorithm:** This is a mathematical process, which produces a single clear text for any given digit and decryption key. It is a cryptographic algorithm that takes a number and a decryption key as an entry, and produces a plain text. The decryption algorithm essentially reverses the encryption algorithm and is therefore closely related to it.

5. **Encryption key:** This is a value known to the sender. The sender enters the encryption key into the encryption algorithm with the plain text to calculate the encrypted text.

6. **Decryption key:** This is a known value of the receiver. The decryption key is linked to the encryption key, but it is not always identical. The receiver enters the decryption key into the decryption algorithm with encryption to calculate the plain text.

5.1 Asymmetric and symmetric cryptograpy

Definition 5.3 [Asymmetric cryptography] In the case of asymmetric encryption, each user has two keys:

- The private key, which must be kept secret;
- The public key, which is available to all other users.

These two keys are mathematically linked.

Definition 5.4 [Symmetric cryptography] It is about multiple people using the same key to encrypt and decrypt messages.

The main problem of this system is the exchange of a single key between different people. So we must ask the question: How can this unique key be shared, allowing each person to encrypt and decrypt safely?

5.2 Key exchange protocols

Definition 5.5 A key exchange protocol (or key negotiation, or key establishment, or key distribution) is a mechanism through which multiple participants agree on a cryptographic key.

The invention of public key cryptography in the $1970's$ produced the first key exchange protocol that can be demonstrated to be secure, even when communications are made over an unprotected channel, without the use of trusted third parties. One of the first protocols of this type, due to *Whitfield Diffie* and *Martin Hellman*, is now the most used on the *Internet*, see [5, 12].

5.3 Diffie and Hellman key exchange protocol

Diffie and Hellman proposed in 1976 a completely secure key exchange protocol. The problem was as follows.

Two persons want to exchange an encrypted message using an algorithm requiring a key K. They want to exchange this key, but they do not have a secure channel for it. Diffie and Hellman's key exchange protocol addresses this problem when K is an integer. The idea of Diffie and Hellman is based on modular arithmetic, and on the following postulate

Being given integers p, a and x with p prime and $0 < a < p$, in $(\mathbb{Z}/p\mathbb{Z})^*$, it is easy to calculate the integer $y = a^x \mod (p)$. But, if we know $y = a^x \mod (p)$, a and p, it is very difficult to find x since p is big enough. This problem is called the discrete logarithm problem on $(\mathbb{Z}/p\mathbb{Z})^*$.

5.4 Steps of the key exchange protocol

We resume five steps of the key exchange protocol in the following table.

	Salah	**Brahim**
Step 1	Salah and Brahim choose together a sufficiently large prime number p and an integer $1 \leq a \leq p-1$. This exchange does not need to be secured.	
Step 2	Salah secretly chooses x_1	Brahim secretly chooses x_2
Step 3	Salah calculates $y_1 = a^{x_1} \mod (p)$	Brahim calculates $y_2 = a^{x_2} \mod (p)$
Step 4	Salah and Brahim exchange the values of y_1 and y_2 . This exchange does not need to be secured.	
Step 5	Salah calculates $y_2^{x_1} = (a^{x_2})^{x_1} \mod (p) = a^{x_1 x_2} \mod (p)$ and calls this number K, the secret key to shared with Brahim.	Brahim calculates $y_1^{x_2} = (a^{x_1})^{x_2} \mod (p) = a^{x_1 x_2} \mod (p)$ and calls this number K, the secret key to shared with Salah.

Figure 3: Steps of the key exchange protocol

5.5 Our contribution

In Subsection 5.3, we saw that in the *Diffie-Hellman key exchange protocol*, the integer a was public and our variables were integers that belong to the commutative group $(\mathbb{Z}/p\mathbb{Z})^*$.

According to the same techniques as in our last paper [1], we propose to work in the set of the circular matrices and more. The integer a will be replaced by a secrete matrix built with a safe exchange of parameters using a quantum protocol $BB84$ and also using logistic maps.

Our new technique will be given through the following steps.

Two persons Salah and Brahim want to create a common secrete key.
Step 1: Creating the first common secrete key

- Using the famous exchange quantum protocol $BB84$ through the quantum channel, Salah and Brahim share two parameters: $t \in [-1, 1]$ and $p \in \mathbb{N}$ (p prime), see [6,13].

  1. Each one calculates
  $$a = t^2 + 1, \quad b = t \quad and \quad c = -t. \tag{6}$$
  2. Creates the circulate matrix $\mathcal{T}$ of order 3 generated by the vector $V = (a, b, c)$. So,
  $$\mathcal{T} = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}, \quad with \quad \forall t \in [-1, 1], \quad \det(\mathcal{T}) > 0. \tag{7}$$

- Using the famous logistic maps
$$x_{n+1} = \mu x_n(1 - x_n), \quad 3 < \mu < 4 \quad and \quad 0 < x_0 < 1. \tag{8}$$

Proposition 5.1 *We can choose*

$$\mu = \frac{\det(\mathcal{T})}{\det(\mathcal{T})+1} + 3 \quad and \quad x_0 = \frac{tr(\mathcal{T})}{tr(\mathcal{T})+1}.$$

Proof.

- From Section 3, we have $\det(\mathcal{T}) > 0$, so, $\det(\mathcal{T}) < \det(\mathcal{T}) + 1$, then

  $$0 < \frac{\det(\mathcal{T})}{\det(\mathcal{T})+1} < 1.$$

  by adding 3 to all terms of the inequality, we get

  $$3 < \frac{\det(\mathcal{T})}{\det(\mathcal{T})+1} + 3 < 4,$$

  so, the choice of μ is good.
- We have

  $$tr(\mathcal{T}) = 3a = 3t^2 + 3 > 0,$$

  then

  $$0 < \frac{tr(\mathcal{T})}{tr(\mathcal{T})+1} < 1,$$

  so, the choice of x_0 is good too.

The first key K created will be the circular matrix generated by the vector $V(y_1, \cdots, y_n)$, where

$$\forall i \in \mathbb{N}, \quad y_i = [10^{15} x_i] \mod (p) \in (\mathbb{Z}/p\mathbb{Z})^*;$$

p is a prime number such that $\forall i \in \mathbb{N}, \quad p > y_i$ and x_i are the terms of the logistic sequence

$$\forall n \in \mathbb{N}, \quad x_{n+1} = \mu x_n (1 - x_n).$$

Now Salah and Brahim can build the following circular matrix of order n using the terms of the previous logistic map.

We denote by K the first shared key

$$K = \langle y_1, y_2, \cdots, y_n \rangle = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_n & y_1 & \cdots & y_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ y_2 & y_3 & \cdots & y_1 \end{pmatrix}.$$

Step 2: Creating the second common secrete key

We take the first shared key K created in the first step, then

- Salah chooses twice private circular matrices (M_1, M_2), calculates and sends to Brahim the cipher

  $$K_A = M_1 K M_2.$$

- Likewise, Brahim chooses twice private circular matrices (M_3, M_4), calculates and sends to Salah the cipher
$$K_B = M_3 K M_4.$$

- Salah receives K_B and calculates
$$C_A = M_1 K_B M_2.$$

- Also, Brahim receives K_A and calculates
$$C_B = M_3 K_A M_4.$$

Proposition 5.2 *We have*
$$C_A = C_B := C \qquad \textit{Same key shared.}$$

Proof. By construction, we have
$$\begin{array}{rcll} C_A & = & M_1 K_B M_2 & \\ & = & M_1 M_3 K M_4 M_2 & , \textit{ because} \quad K_B = M_3 K M_4 \\ & = & M_3 M_1 K M_2 M_4 & , \textit{by commutativity} \\ & = & M_3 K_A M_4 & , \textit{ because} \quad K_A = M_1 K M_2 \\ & = & C_B. & \end{array}$$

So, we have managed to build a matrix C which will be the secret common key between two interlocutors. It will also be used to encrypt and decrypt a text or image.

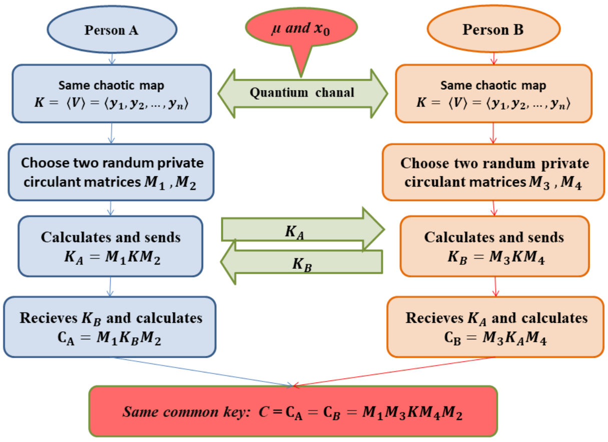

Person A
μ and x_0
Person B
Same chaotic map $K = \langle V \rangle = \langle y_1, y_2, \ldots, y_n \rangle$
Quantium chanal
Same chaotic map $K = \langle V \rangle = \langle y_1, y_2, \ldots, y_n \rangle$
Choose two randum private circulant matrices M_1, M_2
Choose two randum private circulant matrices M_3, M_4
Calculates and sends $K_A = M_1 K M_2$
K_A
K_B
Calculates and sends $K_B = M_3 K M_4$
Recieves K_B and calculates $C_A = M_1 K_B M_2$
Recieves K_A and calculates $C_B = M_3 K_A M_4$
Same common key: $C = C_A = C_B = M_1 M_3 K M_4 M_2$

Figure 4: Diagram explaining the mechanism of creating a common key C.

In the following table (see Table 1), we show the time required to run the key K, using *Matlab R 2018a (9.4.0.813654) 64-bit (Win64) on PC Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz 2.71 GHz RAM 12Go.*

For $\mu = 3.61$ and $x_0 = 0.73$, we get the following results.

Size of the key K	64×64	128×128	256×256	512×512	1024×1024
Time required (second)	0.000042	0.000147	0.000697	0.003108	0.024277

Table 1: Execution time of the proposed method to generate the key K.

In the following table (see Table 2), we show the time required to run the key C, using *Matlab R 2018a (9.4.0.813654) 64-bit (Win64) on PC Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz 2.71 GHz RAM 12Go.*

For this, we use three logistic maps with the parameters ($\mu = 3.61, x_0 = 0.73$), ($\mu' = 3.65, X'_0 = 0.77$) and ($\mu'' = 3.67, X''_0 = 0.82$), we get the following results.

Size of the key C	64×64	128×128	256×256	512×512	1024×1024
Time required (second)	0.000286	0.001477	0.005092	0.031820	0.186870

Table 2: Execution time of the proposed method to generate the key C.

6 Encryption and Decryption of Some Digital Images Using Our Method

In this paragraph, we test our method on some images of different sizes, using the key created in Section 5.1, see [1, 8, 14].

Salah wants to send Brahim an image m of size $n \times n$. To encrypt and decrypt this image, they must proceed as follows.

- Salah converts the image m to a matrix M of the same size as m.
- **Image Encryption:**
  Salah encrypts the image M to the matrix H as follows:
  $$CMK = H,$$
  where K and C are the common keys created in the previous Section 5.1 (K, C and H have the same size). Then he sends H to Brahim.
- **Image Decryption:**
  Brahim receives H and deciphers it as follows:
  $$C^{-1}HK^{-1} = M$$
  because
  $$C^{-1}HK^{-1} = C^{-1}CMKK^{-1} = M.$$
- Brahim converts the matrix M into an image, it gets the initial image.

To study the effectiveness of our image encryption, we analyse its security. The proposed method should withstand several types of attacks, as it is symmetrical, the keys that would be used during encryption and decryption must be transmitted through the secured and other unsecured channels. For the implementation of the proposed scheme, we choose $n \in \{64, 128, 256, 512, 1024\}$.

7 Performance and Safety Analysis

7.1 The key space

The secret key K is probabilistic because the transmitter and receiver use any circular matrices (C_1 and C_2) to obtain a common key K.

If we use the proposed key generation method with $(n = 256)$, $x_i \in \{0, \cdots, 255\}$, this provides 256^{256} possible keys (the elements used are not null) for the C_1 key, we have 256^{256} possible keys for the key C_2, as well as we have 15^{60} possible keys to get the key K (with fifteen decimal digits after the comma), the one-dimensional logistic map used has interesting properties such as periodicity and significant dependence on initial values, but it has low security, to overcome the inconvenience of its small key space, we must use several logistic maps to generate the K key in the first phase. The proposed schema key space size is greater than $256^{256} \times 256^{256} \times 15^{60}$ and the key space is large enough for a brute force attack or comprehensive attack is not possible.

7.2 Statistical analysis

The proposed image encryption scheme is examined using different statistical measures. These measures involve histogram, information entropy analysis and correlation analysis.

Each of these measures is described in detail in the subsections.

We use five test images: Pict6464.jpg, Pict128128.jpg, Pict256256.jpg, Pict512512.jpg and Pict10241024.jpg.

Histogram

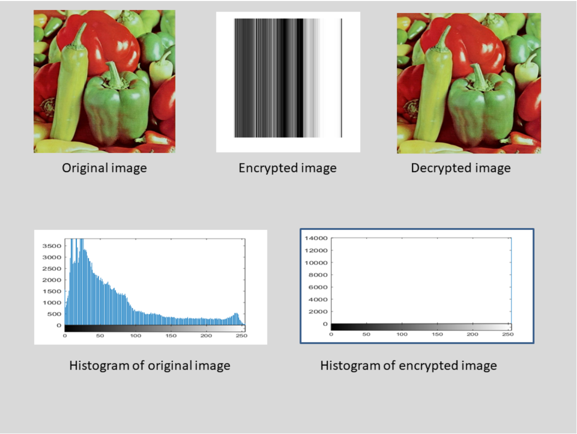


Figure 5: Encrypted and decrypted Pict256256.jpg images and their histograms.

In image processing, the histogram of an image normally represents a histogram of the pixel intensity values. This is a graph showing the pixel variety in an image at each other intensity value in that image.

For an $8 - bit$ gray-scale image, there are 256 different possible extremes, so the histogram will graphically display 256 numbers showing the distribution of pixels among these gray-scale values.

The histogram of the encryption system image must be uniform as it shows in our encryption diagram in Figure 5. The histogram of our encrypted images is almost uniform and significantly different from the histogram of simple images that makes statistical attacks difficult.

Information Entropy Analysis

Entropy is one of the best functions for calculating and measuring the random character of the encrypted image. Ideally, the information entropy should be $8-bits$ for gray-scale images. If an encryption generates an output digit image with lower entropy at $8-bits$, then there would be a possibility of predictability, which could threaten its security. The entropy of the information is calculated using the previous equation.

Simulation results for entropy analysis for the images used are presented in the table.

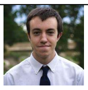
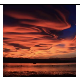
Encrypted image	Size	(μ, x_0)	(μ', x_0')	(μ'', x_0'')	Entropy
	64×64	$(3.61, 0.73)$	$(3.65, 0.77)$	$(3.67, 0.82)$	7.2955
	128×128	$(3.61, 0.73)$	$(3.65, 0.77)$	$(3.67, 0.82)$	7.7326
	200×200	$(3.61, 0.73)$	$(3.65, 0.77)$	$(3.67, 0.82)$	7.8159
	256×256	$(3.61, 0.73)$	$(3.65, 0.77)$	$(3.67, 0.82)$	7.7050
	300×300	$(3.61, 0.73)$	$(3.65, 0.77)$	$(3.67, 0.82)$	7.2768

Table 3: Entropy results for some encrypted images.

Correlation analysis of two adjacent pixels

Correlation determines the connection between two variables. In other terms, correlation is a measure that determines the level of similarity between two variables. The correlation coefficient is a useful evaluation to judge the encryption quality of any cryptosystem. Any image cryptosystem is said to be good if the encryption method hides all attributes and features of a plain text image, and the encrypted image is totally random and extremely uncorrelated.

For a regular image, each pixel is highly associated with its nearby pixels. An ideal encryption technique should generate the cipher images with no such correlation in the adjacent pixels. We have examined the correlation of two adjacent pixels in the original image and encrypted image in several images like Pict6464.jpg, Pict128128.jpg, Pict256256.jpg, Pict512512.jpg and Pict10241024.jpg. We find their correlation very close to 1, we mean there is a perfect match between the original and decrypted images.

8 Concluding Remarks

This paper deals with clear image encryption and decryption techniques. A new technique has been proposed using logistic maps.

We merged between the creation of circulant matrices of order n generated by a vector in the components being the first n elements of a logistic map taken in order from a given rank.

Two parameters in (1) of our logistic map will be generated also by a circulant matrix of order 3 whose components are parametric curves of order 3 chosen in a way that insures the invertibility, so the existence of a non-zero determinant that insures that μ and x_0 in (1) satisfy $\mu \in]3,4[$ and $x_0 \in]0,1[$ for any $t \in]-1,1[$.

These choices assure us that the chaotic case of our system mentioned earlier is very sensitive to changes in the initial value x_0 or the parameter μ that, in our work, change mutually for each $t \in]-1,1[$ without loosing stability.

References

[1] 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.

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

[3] B. Silbermann, A. Böttcher, I. Gohberg and P. Junghanns. *Toeplitz Matrices and Singular Integral Equations:* The Bernd Silbermann Anniversary Volume. Birkhäuser Basel, 2012.

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

[5] C. Boyd and A. Mathuria. *Protocols for Authentication and Key Establishment.* Allemagne: Springer, Berlin, Heidelberg, 2013.

[6] C. Kollmitzer and M. Pivk. *Applied Quantum Cryptography.* Springer, 2010.

[7] P. J. Davis. *Circulant Matrices.* Wiley, 1979.

[8] H. Delfsa and H. Knebl. *Introduction to Cryptography: Principles and Applications.* Allemagne: Springer, Berlin, Heidelberg, 2012.

[9] R. M. Gray. *Toeplitz and Circulant Matrices: A Review.* Pays-Bas: Now Publishers, 2006.

[10] K. D. R. Dewi, K. Fahim and S. Subchan. Application of Model Predictive Control (MPC) to Longitudinal Motion of the Aircraft Using Polynomial Chaos. *Nonlinear Dynamics and Systems Theory* **23** (5) (2023) 487–498.

[11] K. M. Hosny. *Multimedia Security Using Chaotic Maps: Principles and Methodologies.* Studies in Computational Intelligence, **884**. Springer International Publishing, 2020.

[12] A. Mahalanobis. *Diffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups.* (n.p.): Florida Atlantic University, 2005.

[13] D. F. Urrego González. *Implemetation of the protocol BB84 for encryption of a message.* Colombie: Uniandes, 2014.

[14] M. Veni. *Encryption and Watermarking for Digital Images.* Japon: Mohd Abdul Sattar, 2023.

[15] W. S. Mada Sanjaya, A. Roziqin, A. W. Temiesela, M. Fauzi Badru Zaman, A. D. Wibiksana and D. Anggraeni. *Moore-Spiegel Chaotic Encryption for Digital Images and Voices. Nonlinear Dynamics and Systems Theory.* **23** (5) (2023) 445–460.