Advances on Societal Digital Transformation
DIGITAL 2021
November 14, 2021 to November 18, 2021 - Athens, Greece

# Chaos-based Protection Data for Digital Communication

**BOUTEGHRINE Belqassim**, C. Tanougast and S. Sadoudi

***Mail***: *belqassim.bouteghrine@univ-lorraine.fr*

*Laboratoire de Conception, Optimisation et Modélisation des Systèmes*

UNIVERSITÉ DE LORRAINE

13/11/2021

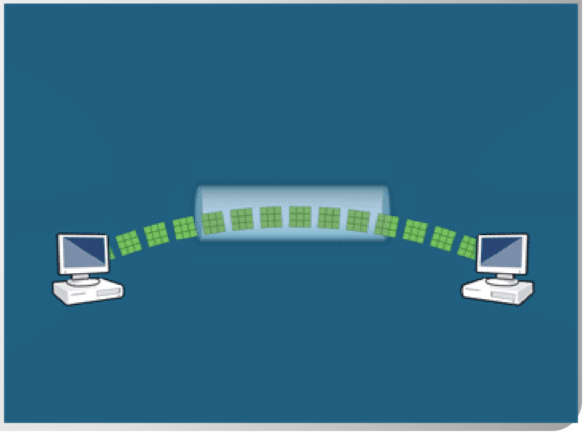
# Plan

- Introduction
- The proposed Chaotic Discrete Time Systems
- Chaotic Behavior of the Proposed System
- The Proposed Solution & Simulation Results
- Conclusion

# Introduction

❖ Data **safety**, **security** and **integrity** are the targets for the different network service providers.

❖Lacks of these features = communication vulnerable.



- Chaotic cryptosystems have been widely investigated to provide fast and highly secure data encryption.

- The unpredictable behavior of the chaotic maps is used to generate **random numbers** (**Key Cipher**).

# Introduction

## Problem Statement :

- ❖ Reduce the complexity
- ❖ Satisfy requirements (for encryption applications)

# The Proposed Chaotic Systems

We introduce three (03) chaotic discrete time systems, as follows:

$$\begin{cases} X(n+1) = 1 - a * X(n)^2 + Y(n) \\ Y(n+1) = d * X(n) \end{cases} \quad (1)$$

$$\begin{cases} X(n+1) = 1 - a * X(n)^2 + (Y(n) * Z(n)) \\ Y(n+1) = 1 - b * Y(n)^2 + (X(n) * Z(n)) \\ Z(n+1) = d * X(n) * Y(n) \end{cases} \quad (2)$$

$$\begin{cases} X(n+1) = 1 - a * X(n)^2 + (Y(n) * Z(n) * P(n)) \\ Y(n+1) = 1 - b * Y(n)^2 + (X(n) * Z(n) * P(n)) \\ Z(n+1) = 1 - c * Z(n)^2 + (X(n) * Y(n) * P(n)) \\ P(n+1) = d * X(n) * Y(n) * Z(n) \end{cases} \quad (3)$$

# System’s Behavior

## Signals

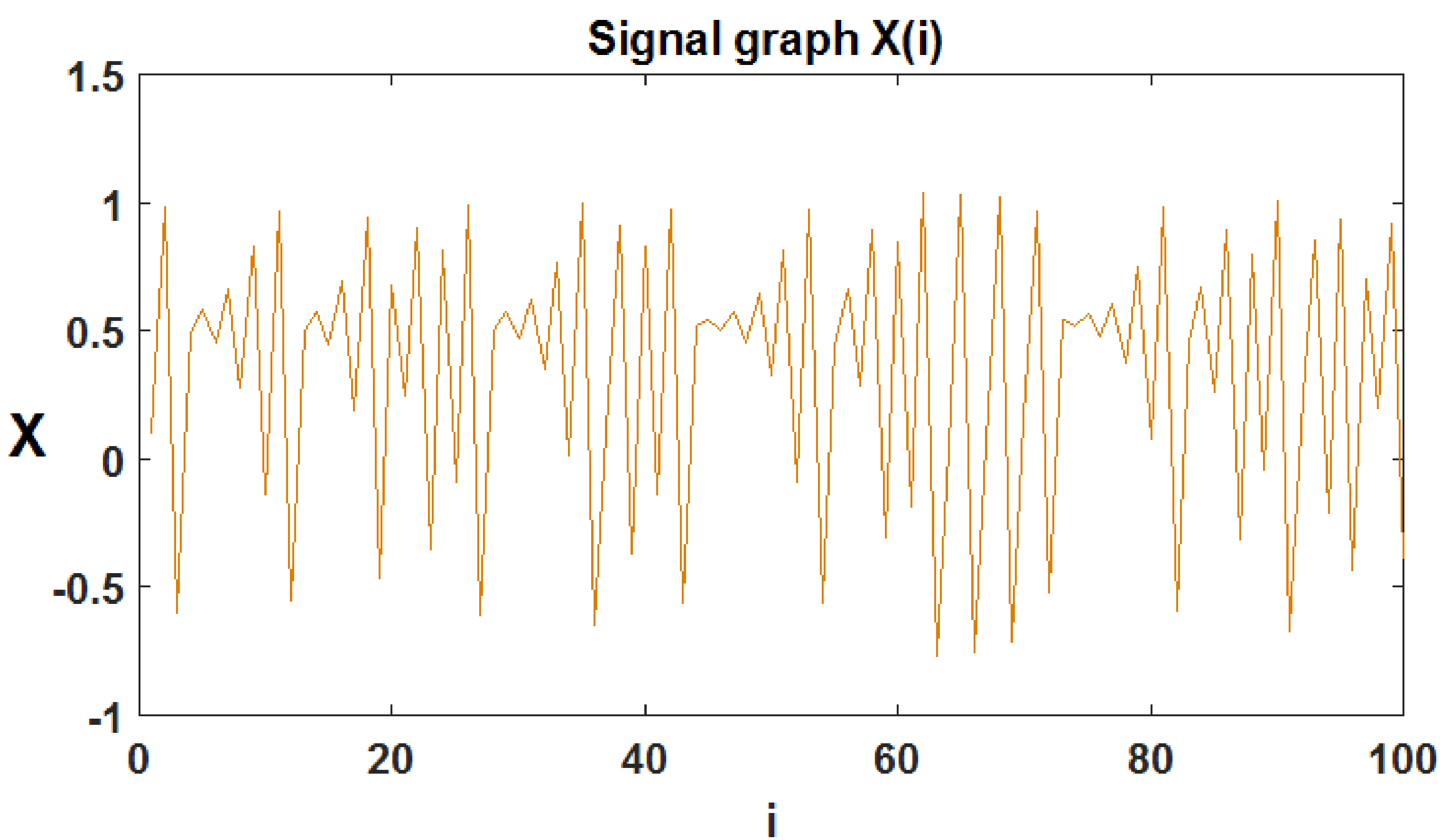
➢ We follow the guidelines proposed in our work(*), based on the bifurcation and Lyapunov exponents 'theories .

✓ As a result, we define : $a$=1.65; $b$=1.45; $c$=1.7 and $d$=0.35; all with initial state of $X(0)=Y(0)=Z(0)=P(0) = 0.1$.

**(*) B.Bouteghrine,, C.Tanougast, and Said Sadoudi. "*Design and FPGA Implementation of New Multidimensional Chaotic Map for Secure Communication.*" *Journal of Circuits, Systems and Computers* (2021): 2150280.**

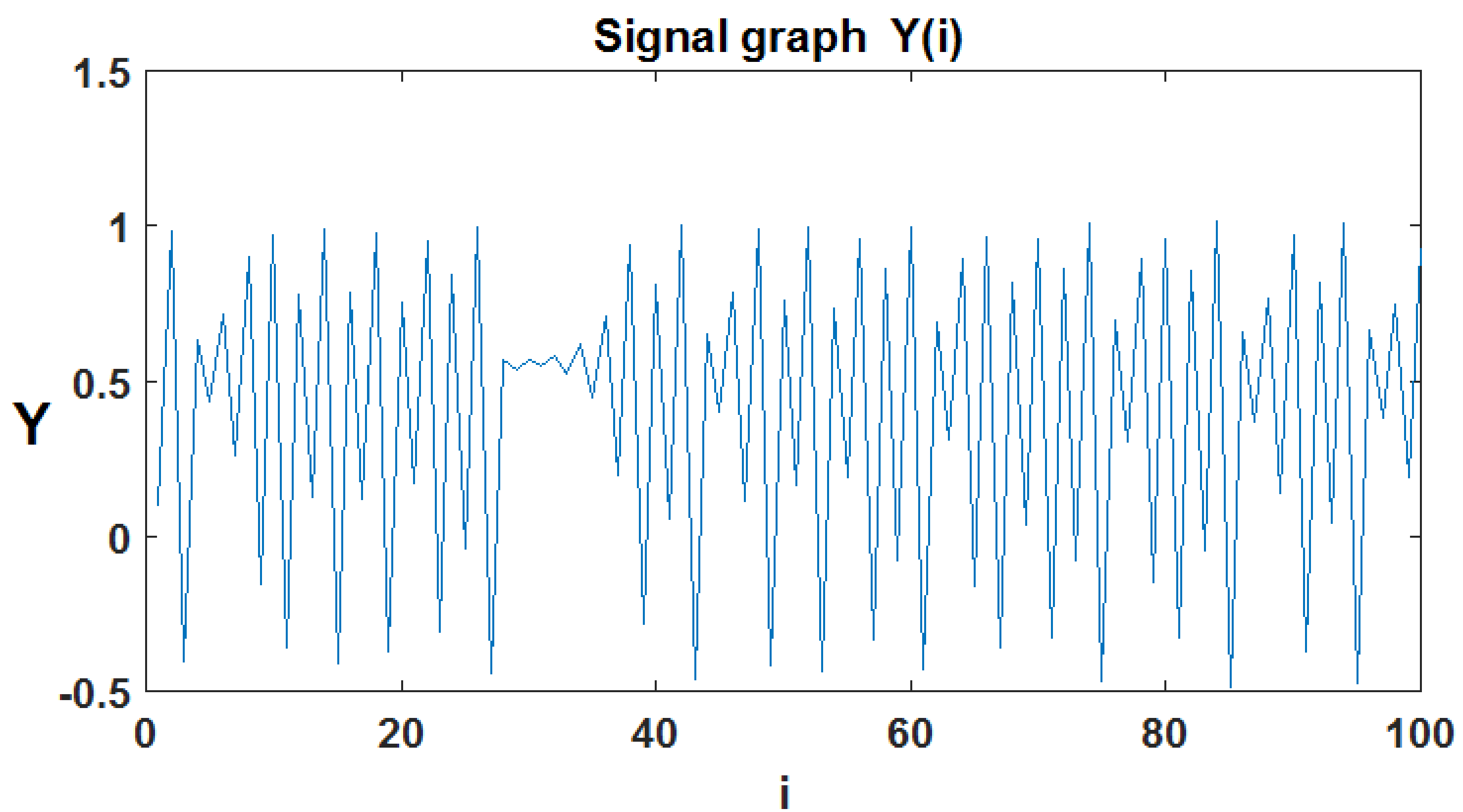
# System's Behavior

## Signals



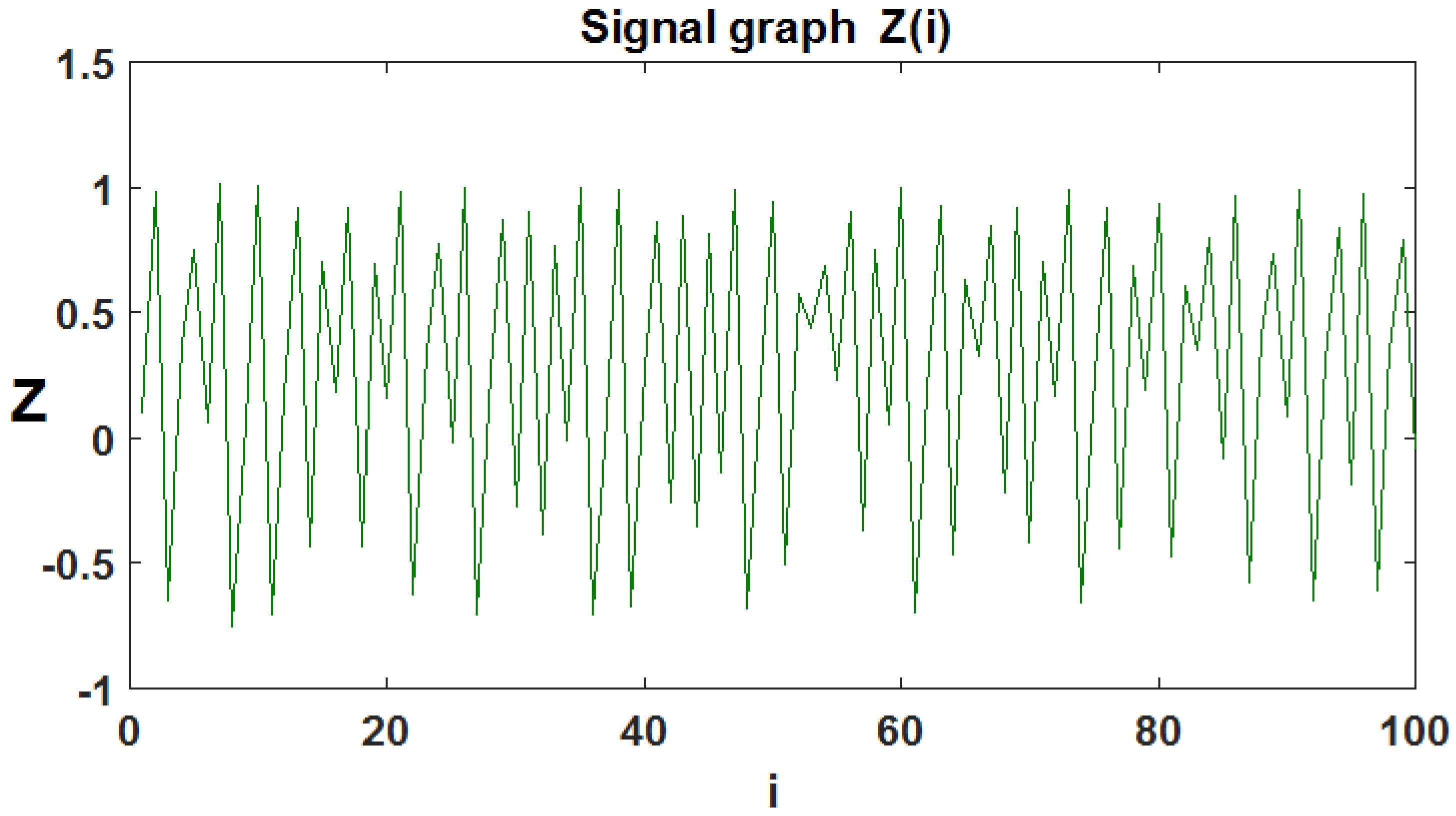
# System's Behavior

## Signals



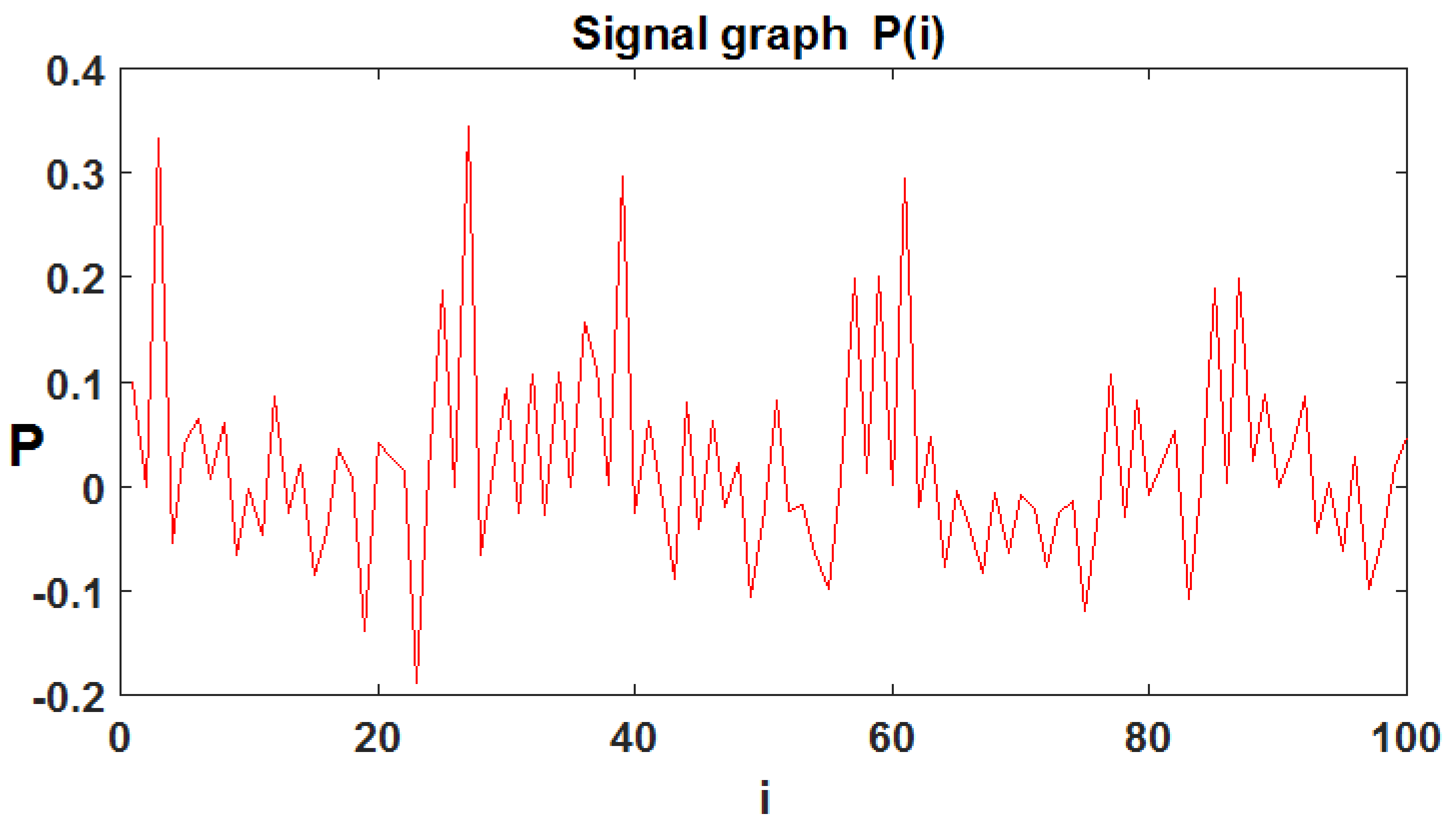
# System's Behavior

## Signals



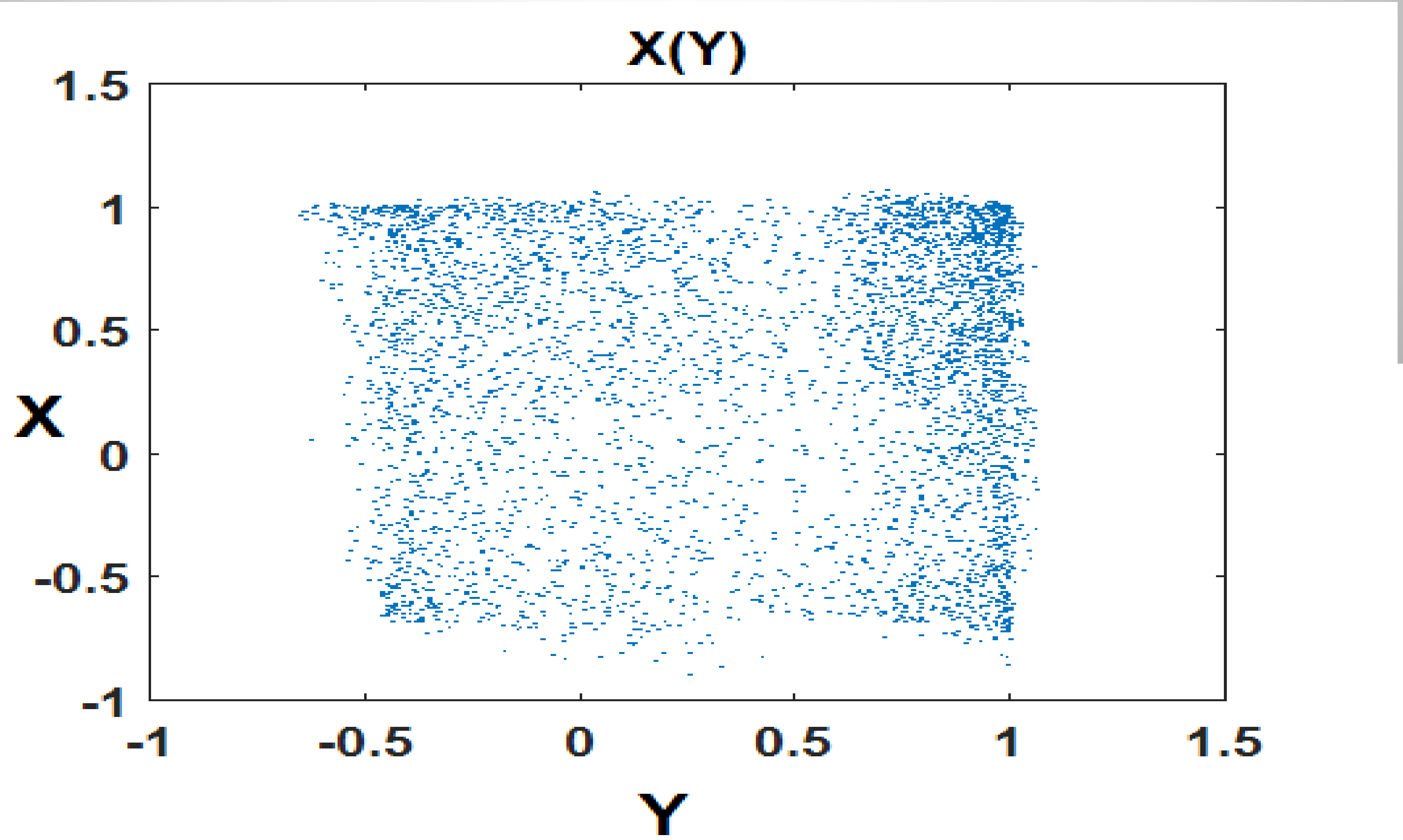
# System's Behavior

## Signals



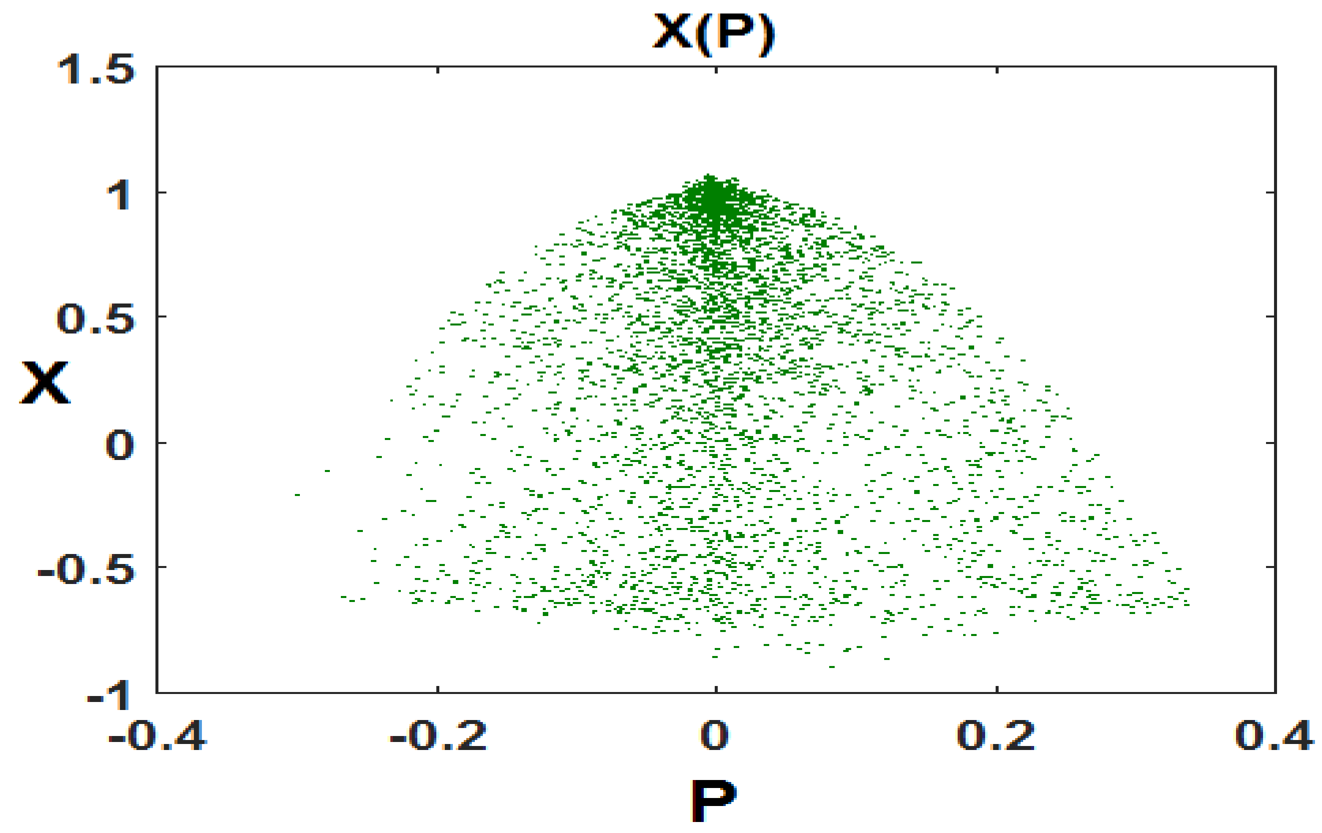
# System’s Behavior

## Trajectory



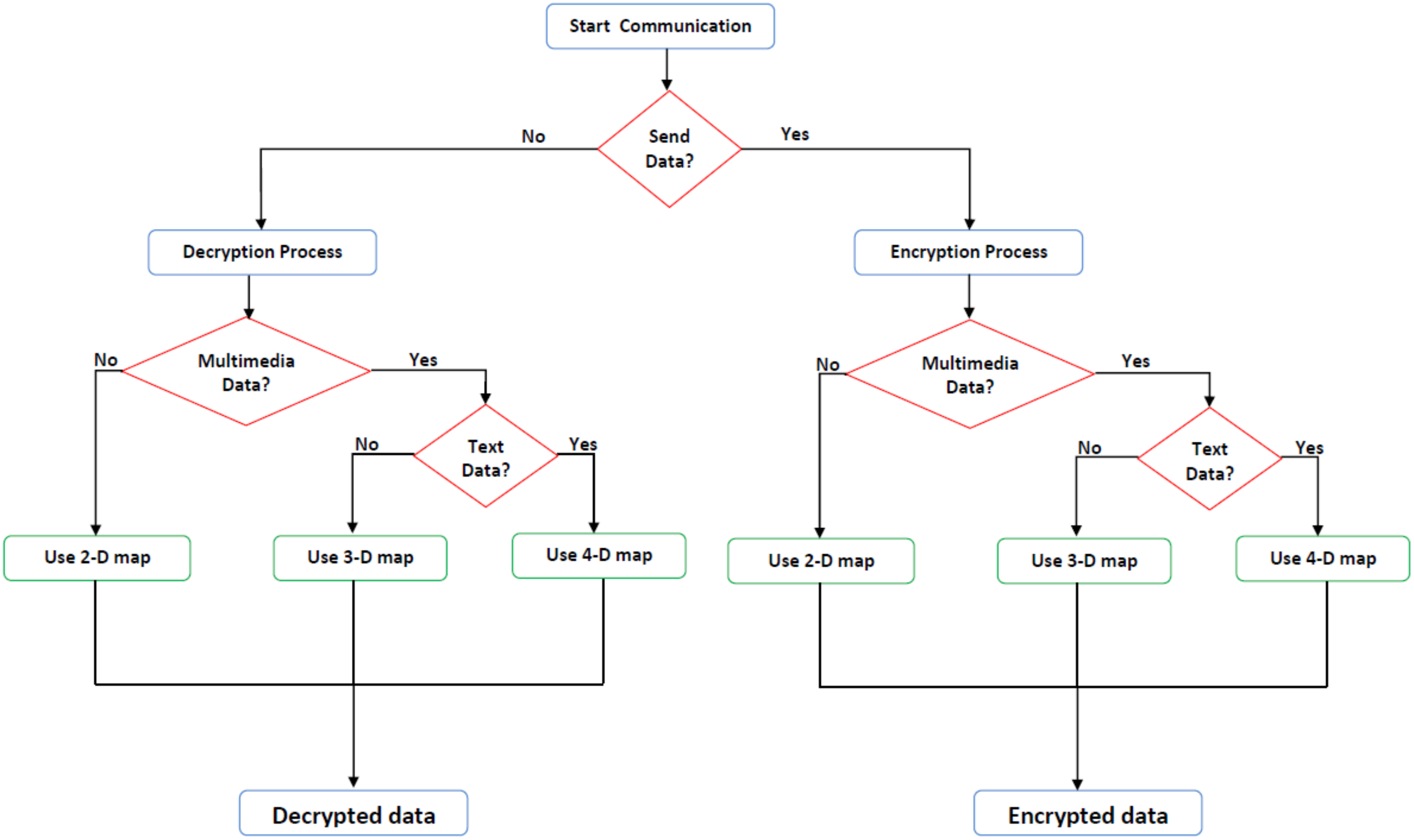
# System's Behavior

## Trajectory



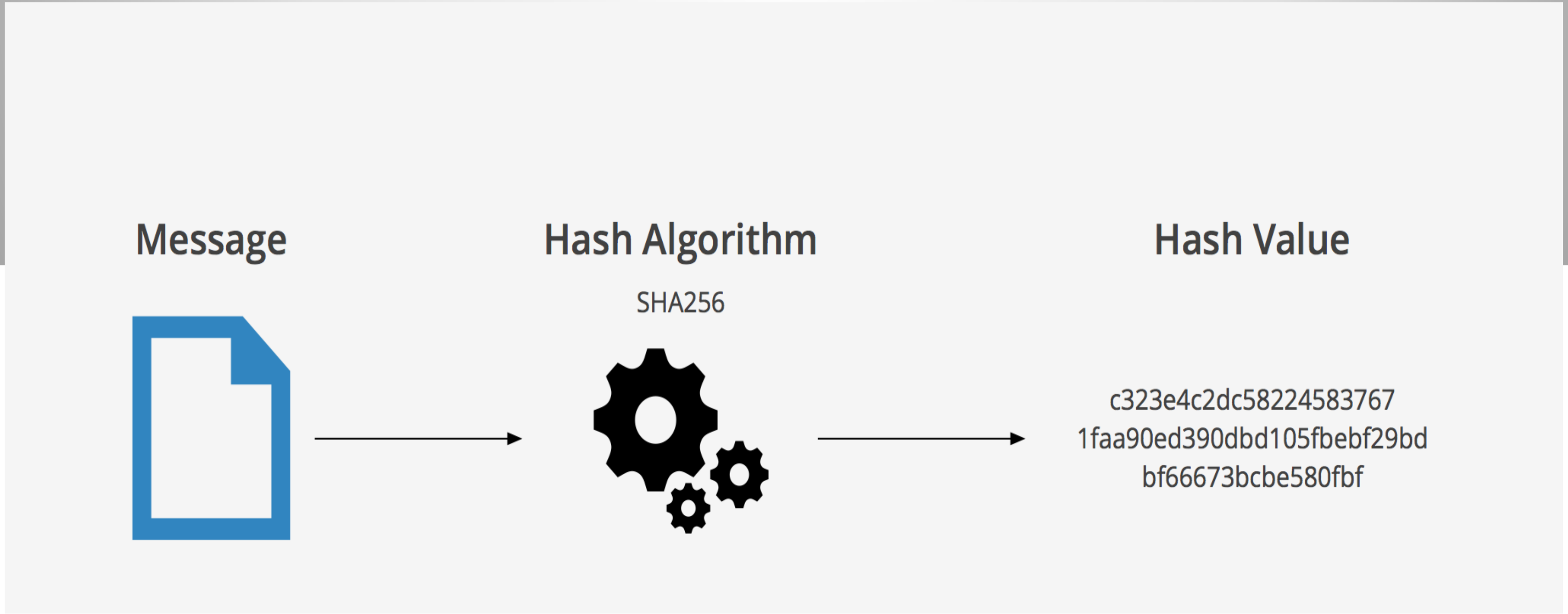
# The Proposed Solution & Results

## The Proposed Algorithm



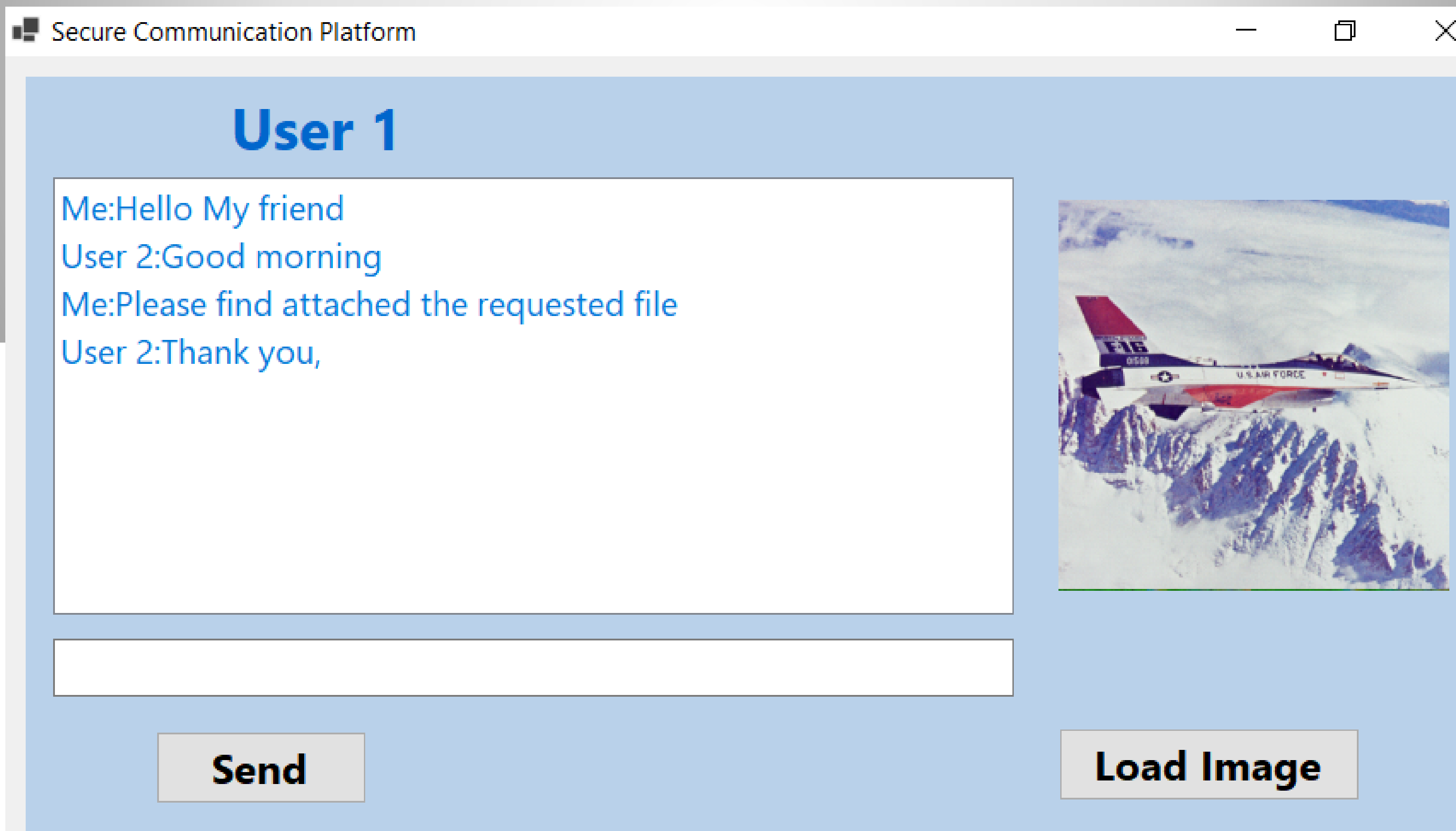
# The Proposed Solution & Results

## The Proposed Algorithm



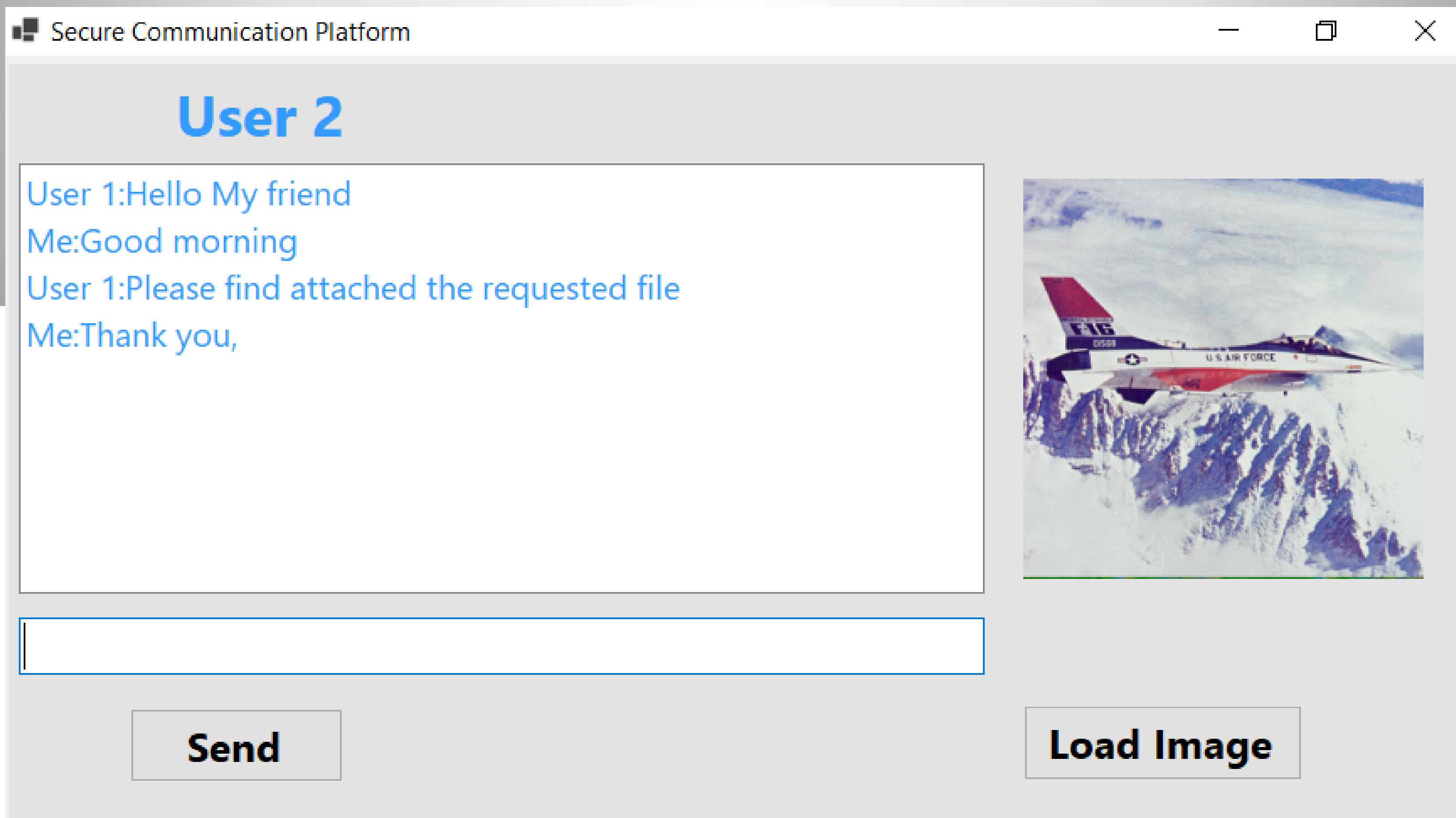
# The Proposed Solution & Results

## Results



# The Proposed Solution & Results

## Results

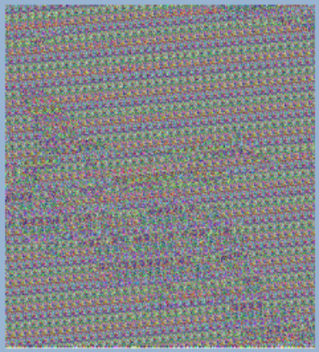


# The Proposed Solution & Results

## Results

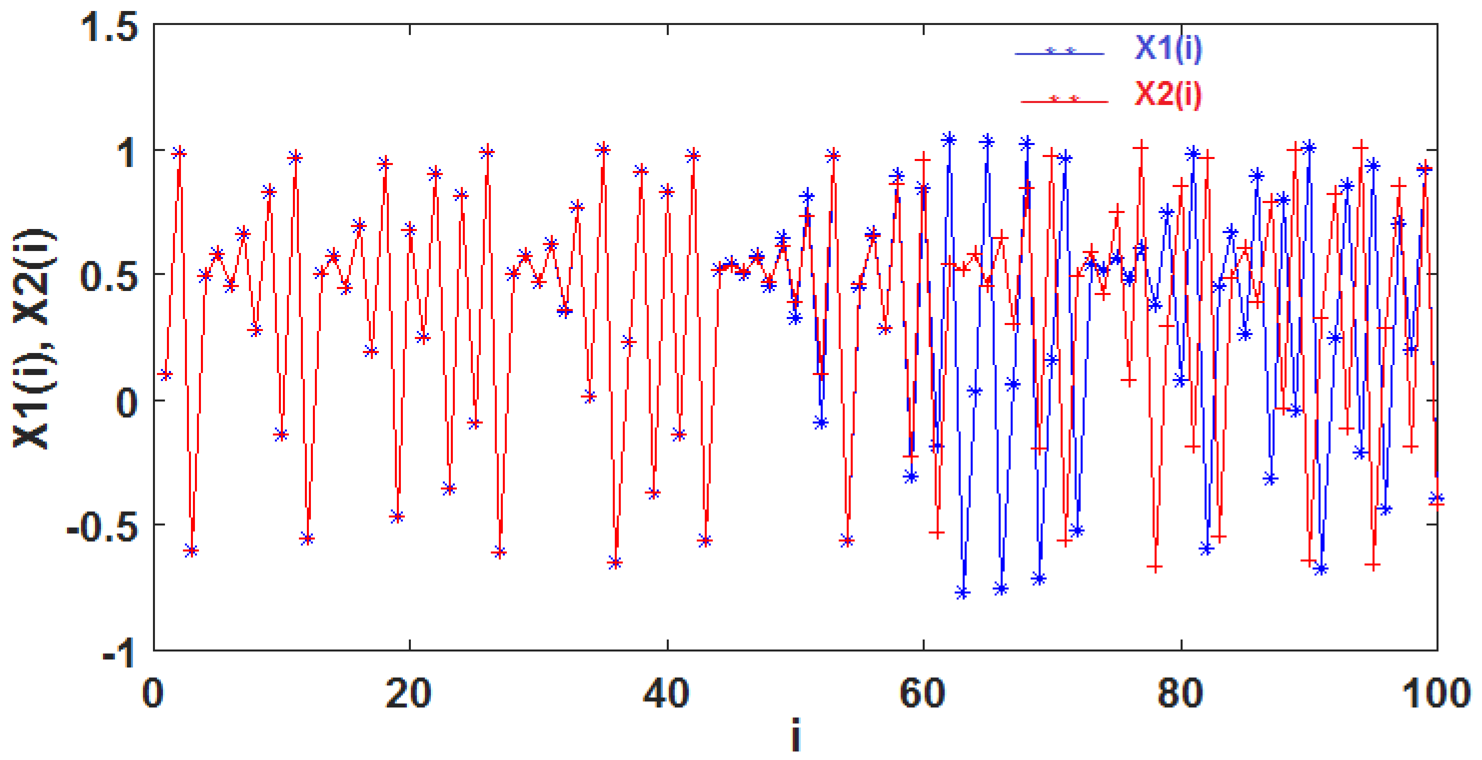
### Encrypted Data

User 1:5DF30059C0C05820BA01BE95195F4D958E52B06EE17178E0162F68FD06BD3D9B
User 2:16B9108413E9C4C590F2CCBF7CE6A47B71BA7158B649FFFBD057B004CBDB28BD
User 1:0C9783256B53B50D579104663EEF4EE04A13658A91491717B403E98198D80355
User 2:F33D48855BF1353E743F112D17A230C0253B66FF14146DD954EF555425E0AF00



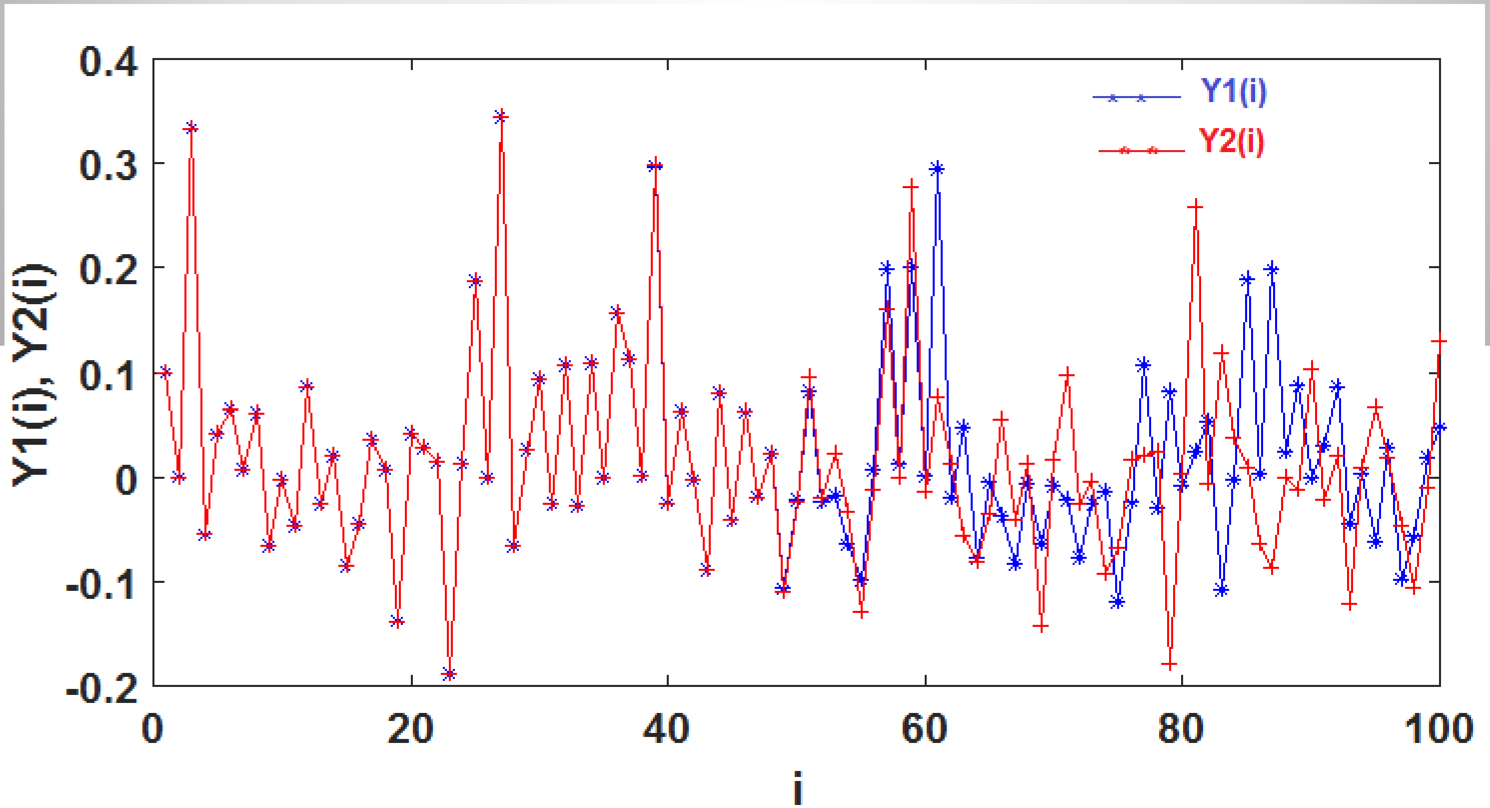
# The Proposed Solution & Results

## Discussion



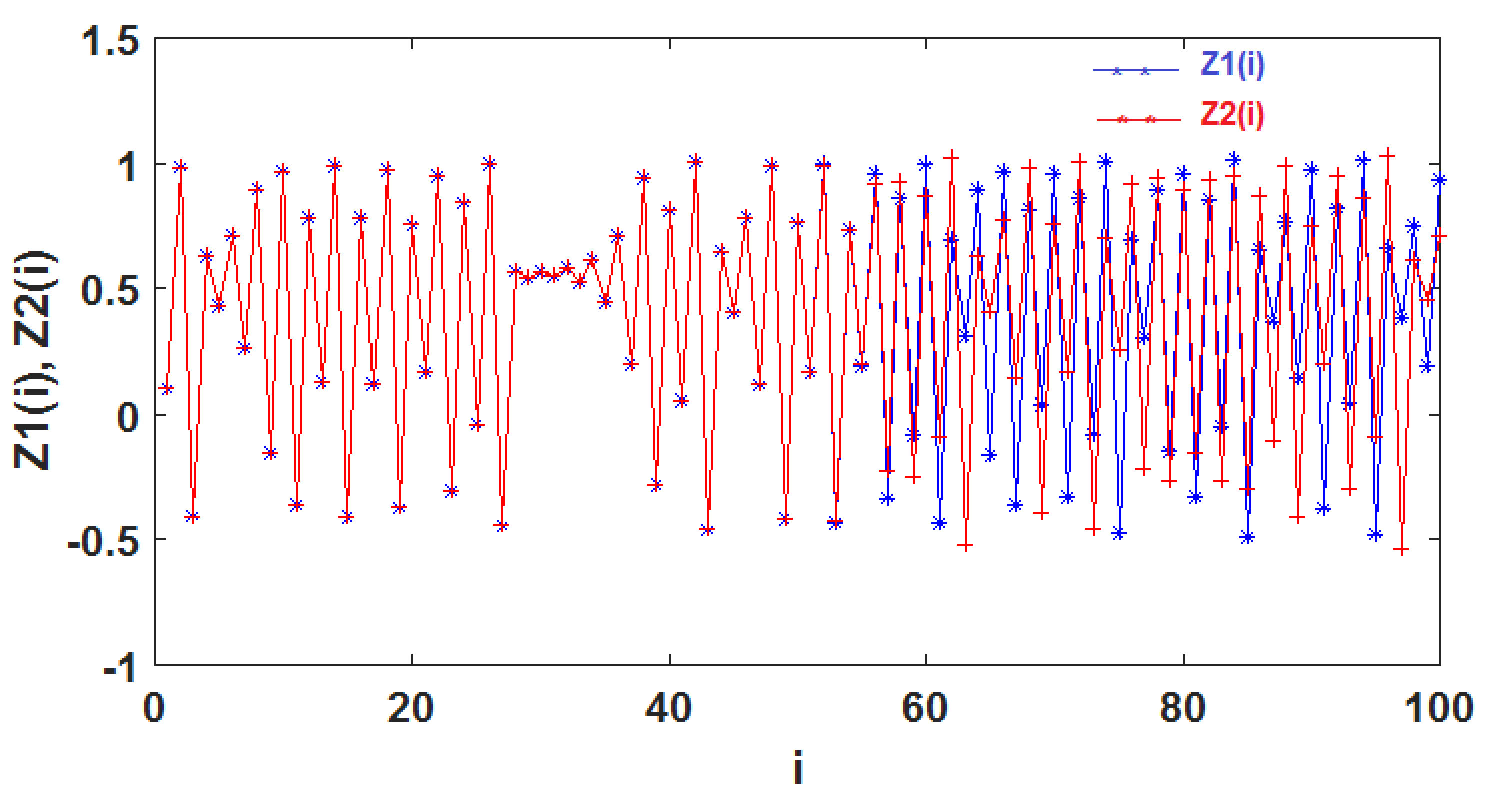
# The Proposed Solution & Results

## Discussion



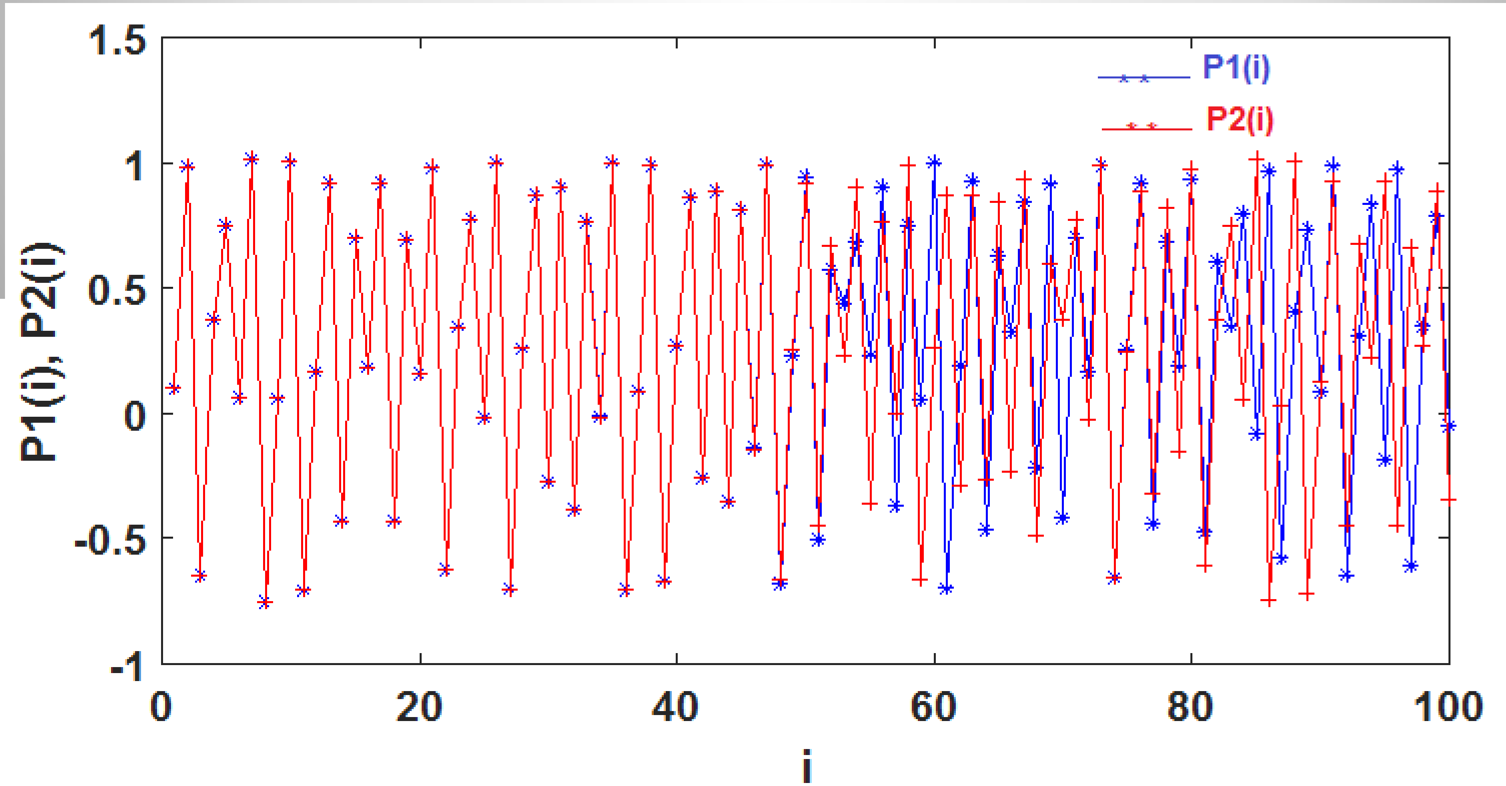
# The Proposed Solution & Results

## Discussion



# The Proposed Solution & Results

## Discussion



# The Proposed Solution & Results

## Discussion

TABLE I
KEY SPACE COMPARISON

| Cryptosystems | Key space value |
|---|---|
| The proposed (2-D) | $2^{128}$ |
| The proposed (3-D) | $2^{192}$ |
| The proposed (4-D) | $2^{256}$ |
| AES | $2^{128}$ |
| DES | $2^{56}$ |
| 3-DES | $2^{168}$ |

# The Proposed Solution & Results

## Discussion

Hash Function analysis:

- ❖ The first method is based on finding the collision by introducing different characters which would help to get the same hash values when the collision occurs. Therefore, the attacker could crack the SHA256 by obtaining the same hash value with the one using during the encryption process.

However, in our case with 256 bits of SHA256 and 32 bits of the generated chaotic sequence, the task of cracking our algorithm becomes impossible.

# The Proposed Solution & Results

## Discussion

- ❖ The second method found in the literature for attacking the hash encryption algorithm is called exhaustive method. For some short and simple combination, this method is very efficient.

Nevertheless, due to the adopted process of this method based on single character scan, and the combination of the words in the dictionary, the exhaustive method is difficult to work regarding the number of the characters included in the output of the SHA256 hash encryption algorithm.

# Conclusion & future work

- ✓ Described and analyzed the different dimensional chaotic systems (2-D, 3-D and 4-D).
- ✓ Applied the proposed chaotic systems inside a C# chat application for secure exchanged data .

❑As future work, the integration on digital FPGA technology for data encryption in an IP-communication of the proposed solution will be investigated as well as the security analysis.


# Thank you for your attention

***Mail***: *belqassim.bouteghrine@univ-lorraine.fr*