Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Babylon
College of Education for Pure Sciences
Mathematics Department

# *Cryptosystem Based Fuzzy Chaotic Models*

A Thesis

Submitted to College of Education for Pure Sciences- University of Babylon in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Education / Mathematics

By

Bushra Hussien Aliwi Nasser

Supervised by

Asst. Prof. Dr. Ruma Kareem K. Ajeena

**2022 A.D** **1443 A.H.**

بسم الله الرحمن الرحيم

وَعَلَّمَ آدَمَ الأَسْمَاءَ كُلَّهَا ثُمَّ عَرَضَهُمْ عَلَى الْمَلاَئِكَةِ فَقَالَ أَنبِئُونِي
بِأَسْمَاءِ هَؤُلاَءِ إِن كُنتُمْ صَادِقِينَ ٣١ قَالُوا
سُبْحَانَكَ لاَ عِلْمَ لَنَا إِلاَّ مَا عَلَّمْتَنَا إِنَّكَ أَنتَ الْعَلِيمُ الْحَكِيمُ ٣٢

صدق الله العظيم

من سورة البقرة

# Declaration

*Aware of legal liability I hereby declare that I have written this dissertation myself and all the contents of the dissertation have been obtained by legal means.*

*Signature:*

*Name:* ***Bushra Hussien Aliwi Nasser***

*Date :     /     /2022*

# Supervisor's Certification

*I certify that this dissertation "* **Cryptosystem Based Fuzzy Chaotic Models** *" by student "**Bushra Hussien Aliwi Nasser** " was prepared under my supervision at the University of Babylon, College of Education for Pure Sciences, in a partial fulfillment of requirements for the degree of Doctor of Philosophy in Education / Mathematics*

Signature:

Name: ***Dr. Ruma Kareem K. Ajeena***

Title: Asst. Prof.

Date: / / 2022

*In view of available recommendations, I forward this thesis for debate by the examining committee.*

Signature:

Name: ***Dr. Azal Jaafar Musa***

Title: Asst. Prof.

Head of Mathematics Department, College of Education for Pure Sciences, University of Babylon

Date: / / 2022

# Certification of Linguistic Expert

I certify that I have read this dissertation entitled " **The Fuzzy Chaotic Models for Encryption Schemes**" and corrected its grammatical mistakes; therefore, it has qualified for debate.

Signature: Mayuuf

Name: Dr. Hussain H. Mayuuf

Title: Asst. Prof.

Date: / /2021

## Certification of Scientific Expert

I certify that I have read the scientific content of this thesis **"The Fuzzy Chaotic Models for Encryption Schemes "** and I have approved this dissertation is qualified for debate.

**Signature:** Dheia G.S

**Name:** ~~Dr~~Prof. PhD. Dheia G. Salih Al-Khafajy

**Title:** Dept. of Math., College of Science, University of Al-Qadisiyah.

**Date:** 31-10-2021

## Certification of Scientific Expert

I certify that I have read the scientific content of this thesis **"The Fuzzy Chaotic Models for Encryption Schemes "** and I have approved this dissertation is qualified for debate.

**Signature:**

**Name: Dr.** Ali H. Kashmar

**Title:** Assist. prof

**Date:** 2021/11/16

# Examining Committee Certification

We are the chairman and members of the examination committee; We certify that we have read this dissertation (**Cryptosystem Based Fuzzy Chaotic Models** ) as Examining committee, examined the student (**Bushra Hussien Aliwi Nasser)** in its contents and its qualified as dissertation for the degree of Doctor of Philosophy in Education / Mathematics.

*Signature:*
*Name:* ***Dr. Ayad A. Abdulsalam***
*Title: Professor*
*Date: / 2 /2022*
***( Chairman )***

*Signature:*
*Name:* ***Dr. Iftichar Mudhar. Alsharaa***
*Title: Professor*
*Date: / 2 /2022*
***( Member )***

*Signature:*
*Name:* ***Dr. Hassan Rashed Yassein***
*Title: Professor*
*Date: / 2 /2022*
***( Member )***

*Signature:*
*Name:* ***Dr. Najlae Falah Hameed AlSaffar***
*Title: Asst. Prof.*
*Date: / 2 /2022*
***( Member )***

*Signature:*
*Name:* ***Dr. Enas Hamood Al-Saadi***
*Title: Asst. Prof.*
*Date: / 2 /2022*
***( Member )***

*Signature:*
*Name:* ***Dr. Ruma Kareem K. Ajeena***
*Title: Asst. Prof.*
*Date: / 2 /2022*
***(Supervisor )***

***Approved by the Dean of the College of Education for Pure Sciences, University of Babylon***

*Signature:*
*Name:* ***Dr. Bahaa Hussien Salih Rabee***
*Title: Professor*
*Date: / /2022*
*Address:* ***Dean of the College of Education for Pure Sciences****.*

# Publications

1. Bushra Hussien Aliwi, Ruma Kareem K. Ajeena, A Performed Knapsack Problem on the Fuzzy Chaos Cryptosystem with Cosine Lozi Chaotic Map, Accepted in AIP Publishing Conference Proceedings, ICCEPS-2021.
2. Bushra Hussien Aliwi, Ruma Kareem K. Ajeena, The Knapsack Fuzzy Chaos Cryptosystem, Accepted in AIP Publishing Conference Proceedings, ICARPAS 2021.
3. Bushra Hussien Aliwi, Ruma Kareem K. Ajeena, The Knapsack Fuzzy Chaos Cryptosystem Based on Sine Lozi Chaotic Map, Accepted for publication in Proceedings of the IEEE.

# Abstract

The Knapsack Fuzzy Chaotic Cryptosystem was suggested as a combination between the Knapsack problem and Fuzzy Chaos based cryptosystem. That is through applying the Knapsack problem in the Takagi-Sugeno fuzzy model on a discrete-time chaotic system and then decrypting the message. The system modified by using a discrete chaotic map to be a seed map within a continuous map. The cosine and sine map were performed.

Finally, The Knapsack problem in the Takagi-Sugeno fuzzy model was implemented as the driver system for the fuzzy chaotic system in encrypting the ciphertext and as a response system in decrypting ciphertext. The synchronization signal with feedback gains between the drive-response system is achieved at the error dynamic that is exactly linearized to ensure stability. By solving the LMI problem the system could decrypt the message.

The suggested systems were implemented on 2D and 3D discrete-time chaotic systems. The iteratiation of the chaotic system affects the length of the superincreasing sequence, which is also increased by modifying the system. The computios were by hand and Microsoft Excel 2010, and some figures were drawn by MATHLAB R2018b.

# Acknowledgements

First and foremost, I thank my God for all things.

I thank my PhD advisor, Dr. Ruma Kareem K. Ajeena, for her guidances. I thank the Head of Mathematics Department Dr. Azal Mera for her unreserved support during the work on thesis. I thank my PhD thesis committee members, for their time, their roles, and their insightful comments. I thank all the amazing doctoral students for year 2018-2019, for their supports, laughter and tears. I thank my mentors outside my PhD program, my brothers and sisters Dr. Ali H., Dr.Amal H., and Lecturer. F. H. Aliwi for their enlightenment on my career path. I thank my housband Mr. Maher K. for his significant role in my life, and my roses, my children for making me proud of what I have accomplished and who I am. Finally, I thank my family all thank, especially my mom, the most loving and courageous woman, and my brothers with their families, the most diligent and righteous men, and for their unconditional love.

# Dedication

*To My Family*

*And My Father, I am not Forget you ever*

*To My Mam*

*To My Hausband and myChilidren*

*To My Brothers and Sisters and their sons*

*Bushra*

# Contents

## Chapter Three: The Suggested Knapsack Fuzzy Chaos-Based Cryptosystem

## Chapter Four: Numerical Schemes Examples and Results Discussions of Cases Study for Suggested Systems

## Chapter Five: Conclusions and Future Works

# List of Tables

# List of Figures

# List of Algorithems

# List of Symbols

| | |
|---|---|
| $\mu,$ | membership function , |
| $\mu(.)$ | membership degree |
| $U\ ,V$ | universal sets |
| $\Gamma$ | fuzzy set |
| $A, B, D, E, \ldots$ | Matrices |
| $x(t), \ldots$ | vector variables |
| $x_1(t),\ x_2(t)$ | State vector values |
| $sup$ | Least upper bound |
| $\lim\limits_{u \to (.)} \mu_A(u)$ | limit of membership function $\mu_A(u)$ |
| $C$ | Ciphertext |
| $\xi(.)$ | Modified Ciphertext |
| $X^T$ | transpose of matrix (vector) |
| $H$ | Hawrtuiz Matrix |
| $\Delta$ | changing (difference) |
| b(t) | bias term |
| u(t) | Control input vector |
| $t$ | Time variable |
| $\hat{x}(t), \hat{y}(t)$ | Estimated values |
| $es_x(t), es_y(t)$ | Errors signals |
| $\alpha, \beta, \ldots$ | Parameters |
| $C(.)$ | Sine map |
| $G(.)$ | Cosine map |

# List of Abbreviations

| | |
|---|---|
| TS | Takagi-Sugeno |
| FIS | Fuzzy inference system |
| PDC | Parallel Distributed Composition |
| EL | Exact Linearization |
| KFCC | Knapsack Fuzzy Chaotic Cryptosystem |
| LMIs | Linear Matrix Inequality Problems |
| M | Plaintext\Message |
| EL | Exact Linearization technique |
| FL | Fuzzy Logic |
| T | Time variable |
| CLZ | Cosine Lozi map |
| SLZ | Sine Lozi map |
| MF | Membership Function |
| CFS | Continuous-time fuzzy systems |
| DFS | Discrete -time fuzzy systems |
| DTF-3DCS | Discrete-time TS fuzzy model of 3D chaotic system |
| CTF-3DCS | Continuous-time TS fuzzy model of 3D chaotic system |
| KDT-FCC | Knapsack Discrete-time TS fuzzy chaotic cryptosystem |
| KCT-FCC | Knapsack Continuous-time TS fuzzy chaotic cryptosystem |
| DTFC | Discrete-Time Fuzzy Chaotic |
| KFCCMS | Knapsack Fuzzy Chaotic Cryptosystem with Master Slave |

# Chapter One

# General Introduction

## 1.1 Background

Cryptography could be defined as the science that studies secret writing, concerning the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers, or other methods, so that only certain people can see the real messages.

The science of cryptography is very old, and can be traced to Ancient Egypt. From Julius Caesar to Mary, Queen of Scots, to Abraham Lincoln's Civil War ciphers, cryptography has been a part of history. At that time, cryptography was concerned only by those associated with the military, the diplomatic service and government in general, and was used as a tool to protect national secrets and strategies. In 1949, Shannon [1] talk in his seminal paper "Communication Theory of Secrecy Systems“, about mixing transformation for many concepts such chaos .

Since 1990's, Some researchers referred to existing an interesting relationship between the chaos and cryptosystem [2,3]. Many chaotic systems properties corresponding to the cryptographic properties, such sensitivity to initial conditions, control parameters, mixing property, and ergodicity, and others, that correspond to the confusion and diffusion, for cryptographies schemes.

There are studies that have been developed for stability analysis of continuous or discrete time model based fuzzy control system such Takagi- Sugeno TS. It found many applications for modeling complex and nonlinear systems [4]. Also many works on chaos-based cryptosystems are failed through proposed schemes in explaining or possessing a cryptosystems.

## 1.2 Problem Statement

The suggested method has been proposed to design a new fuzzy chaotic cryptosystem. That through designing an alternative versions of the Knapsack public key cryptosystem based on the TS fuzzy chaotic models as the Knapsack Fuzzy Chaotic Cryptosystem (KFCC). These models are Discrete-Time TS Fuzzy model of 3D Chaotic System (DTF-3DCS) and Continuous-Time TS Fuzzy model of 3D Chaotic System (CTF-3DCS).

## 1.3 Objective of the Thesis

The objective of this thesis is to develop the Fuzzy Chaos-Based Cryptosystem, that has little works on since than 2006 due to its complexity in numerical experiments. Usage of the common features between unpredictability of chaotic and cryptosystems, fuzzy models with its rules bases and inferred results, this with the practical Knapsack problem. That all, in order to eliminate the drawbacks of each model alone.

## 1.4 Literature Review

In 2002, Palacios and Juarez in [5] implement the cryptography with chaos. He recover in his work the possibility to encrypt the plaintext using the ergodic property for the simple low-dimensional and chaotic logistic equation, that each character encrypted as the integer number of iterations of the logistic equation. The trajectory transformed from an initial condition towards an $\epsilon -$interval in the logistic chaotic attractor.

In 2005, Zhong Li and et.al in [6] designed the chaos-based cryptography and chaotic pseudo-random number generators (CPRNGs) for stream cipher and their chip implementation.

In 2006, a suggested guideline were introduced in [3], to assisting the designers to synthesis a cryptosystems with chaos as chaos-based cryptosystem. The guide were through three main issues; implementation, key management, and security analysis. That helpful in designing the cryptosystem requirements in more systematic and rigorous ways.

In 2006, Zhang Li in [2] combined a TS fuzzy model with chaotic model to modulate a cryptosystem performed on Lure type with discrete time chaotic systems. That to generate a superincreasing sequence formed by chaotic signal in drive system side. The model is with flexibility in choosing whether the ciphertext is embedded in the output of the drive system. The response system side receives the embedded ciphertext scalar signal. Two sides achieve and then solving a chaotic synchronization problem by solving the LMIs problem .

Later in the same year 2006, Zhang Li in [7] introduces two ways in creating sequence of the key secure either to be as output of the TS fuzzy chaotic drive system or any state in which the synchronization error approaches zero. In synchronization state the same superincreasing sequence could be regenerated and then recover the ciphertext at response system end. By decrypt it using a regenerated superincreasing sequence it could be get the message. In both cases state or output drive system in [2,7] the models implemented on Henon map.

In 2006, in [8], Chang-Ho Hyun and others propose an alternative indirect adaptive fuzzy observer based on synchronization design scheme and applying it in secure communication of chaotic systems. This scheme performed by assuming that the chaotic systems states are immeasurable and their parameters are unknown. They use TS fuzzy model to represent the chaotic system and the observer structure. While the adaptive law is derived by use a Lyapunov stability theory to estimate the unknown parameters values and guarantee the system stability, and then achieving the asymptotically synchronization of the chaotic system. The output $y(t)$ of the model is used as a primitive variable instead of the one in the used chaotic system.

In 2008, Gwo-Ruey Yu in [9] presents a robust design for chaotic cryptosystems. That combines cryptograph with chaotic synchronization to synchronize the hyperchaotic signals between the encryption and the decryption processes based on observer gains. He used the linear matrix inequality (LMI) technique to compute gains.

In 2009, Precup and Tomescu in [10] proposed a stability analysis method for TS fuzzy model (FLCs) used to control the nonlinear processes. The stability done by Lyapunov's direct method instead of Lyapunove's theorem, by sufficient conditions for stability and it introduce an illustrative example for inverted pendulum. They conclude that this method could be used for approaching stability for the system that has an equilibrium point not as origin.

In 2011, Ababneh and et. al in [11] present a new systematic method on robust synchronization for uncertain chaos systems as a control problem. That by designing a digital response system drive by a continuous time chaotic drive system and synchronize with it. The fuzzy model used for modeling the chaotic dynamic system is a TS fuzzy model. The uncertain chaotic system could be written as a set of local linear models with additional disturbed input. Synchronization between receiver and transmitter system was very closely. They use a piecewise linear and nonlinear even with uncertain parameters on uncertain Chua circuits. But the continuous time chaotic is not were used in cryptography.

In 2011, Kocarev and Lian in [12] refer to spirit both cryptography and chaos theory than other researchers treated way with the subject. They introduce a chaos-based public key cryptography through many theorems, algorithms, and applications. In their work they based on Chebyshev polynomials in generating a public key cryptosystems performed on integer numbers with some chaotic properties, to use in both encryption and digital signature. Also the ElGamal-like and RSA-like algorithms when using Chebyshev polynomials on integer numbers are secure in encryption algorithms.

In 2012, Makris and Antoniou in [13] develop and implement the program of Shannon in cryptography with chaos on three Tours

Automorphisms are: Baker map, Horseshoe map, and Cat map. The developed algorithms applied to encryption and creating keys on picture and text in real time. While the decryption require the reverse application of algorithms. Practical implementation of the encryption and decryption depend on the text size while the key length doesn't.

In 2014 , Saad M. Darwish and et. al in [14] works on database encryption that proposed system utilizes a chaotic encryption method based on cellular automata to realize higher complexity of crypt-analytical attacks ,and generate a symmetric key. A fuzzy observer based scheme for synchronizing chaotic keys of encrypted signal is employed to enhance key distribution. This method used in confusion, diffusion, a large number of passwords helped in building of symmetric private key.

In 2017, Merah and et.al in [15] refer to that most conventional ciphers such; DES, AES, IDEA, with the used computing power in that time, though are not suitable for image or video encryption due to their speed is very slow due to the data volume is large and also the correlation among image pixels is strong. So the significant interest in exploit chaotic dynamics in cryptography is increased

In 2018, Hamdy M. Mousa in [16] propose iterative Chaotic Genetic-fuzzy Encryption Technique (C-GET) in order to enhance secured encryption technique and less predictable.

Also in 2018, Kocarev and Lian in [17] use a similarity between chaotic systems and cryptosystem. Since they describe a technique for transformation of digital information by using a pseudo chaotic carrier, and use a pseudo chaotic sequences as a key to encrypt a digital message through spreading codes that to encode each user's message. The decryption of messages could be done also by spreading of chaotic sequences again by the orthogonal property at the receiver. The pseudo chaotic sequence generators are in class of Non Linear Feedback Shift Registers(NLFSR).

In 2019, Alroubaie and others in [18] apply the chaos based stream cipher by using synchronized fixed point chaotic map for encryption speech system, known as synchronized fixed-point chaotic map based stream ciphers (SFPCM-SC). The chaotic maps that used were synchronized through master-slave synchronization technique, and use it to Pseudo Random Bit Generator (PRBG).That introduce XOR-ed with digitized speech signal that create an encrypted signal, by use fixed point. A same map in slave that synchronize with master one used to recognize the original speech signal. Consequently the resulted error between the master and slave systems after a small period become zero and successfully recovered the original speech signal with real time environment.

In the same year 2019, Alwida and et. al in [19] used the digital cosine chaotic map as a chaotification method for chaotic map in chaotic based cryptographic algorithm. This method were used to avoid the negative affect in chaotic systems and cryptography, in spite it have many similar characteristics in adding the security to the systems. This chaotification uses a cosine function alongside a chaotic map as seed map before analyzing its chaotic properties, that were performed to enhance the Logistic map and Henon map. As consequent the new chaotic maps have a chaotic properties from the essential one such as it have a wide chaotic range, elevated sensitive to slight changes in initial conditions, complex characteristics, high nonlinearity, and extend the cycle length in comparison with the original chaotic maps and other chaotic maps.

In 2020, Chandrashekhar Meshramand and et. al in [20] introduced a conversion process to transfer cryptosystems using Chebyshev's chaotic maps to a subtree-based protocol for fuzzy user data sharing. They opposed to reconnecting a different structure. In their design conversion process, there is no need to adjust the original cryptosystem based on chaotic maps.

## 1.5 The Outlines of the Dissertation

In Chapter 2, a mathematical background for the text subjects were presented, terms, definitions, and models in the suggested method. These are the fuzzy logic and TS fuzzy model, chaos and dynamical systems, cryptosystem and chaos. The Knapsack problem details were also discussed in Chapter 2.

Next, in Chapters 3, a hybrid methods for the Knapsack problem were presented with the TS fuzzy chaotic model in cryptosystem, and consider these methods through two directions. First, named as Knapsack fuzzy chaotic cryptosystem (KFCC). That works on 2D and (3D) discrete-time and continuous-time TS fuzzy chaotic models as (KDT-FCC) and (KCT-FCC), respectively. The KDT-FCC model was discretized to get KDT-FCC. Next, the (KDT-FCC) method was modified through add modification on chaotic maps, by using chaotic maps as seed maps in the cosine map once and in the sine map in others. Also another direction were proposed in hybrid the KFCC through using the master-slave system in decryption the ciphertext stage as KFCCMS method, that demonstrated theoretically to achieve synchronization.

Then, in Chapter 4, numerical applications were investigated for KDT-FCC and KCT-FCC. The KDT-FCC were performed on the Lozi map which is 2D discrete-time chaotic map in TS fuzzy model. The modification by cosine and sine map were performed also Lozi map as cosine Lozi map CLM and sine Lozi map SLM. The best results were at performing the CLM. Unlike the previous performance, the KCT-FCC were considered with the Lorenz map, as a 3D continuous-time strange attractor, with the TS fuzzy model. In order to applied in cryptosystem there is need to discretize it at some time step parameter to get KDT-FCC.

Finally, The conclusions of the thesis were presented in Chapter 5.

# Chapter Two

# Mathematical Background of Fuzzy Logic, Chaos and Cryptography

## 2.1 Introduction

In mathematics the crisp logic is deals with propositions can be true on one occasion has truth value 1, and false on other has failed value 0 [21]. FL is a multivalued logic [22], and it is translate the fuzziness of linguistic variables into form that computers can understand and manipulate it [23]. Linguistics such; rather good, or very fast, can be formulated and processed by computers [24].

The truth value of a proposition is widely used in control problems, through IF-THEN rules in subject to fuzzy rules. Since most of its applications involves construction and processing of fuzzy rules [22] .

Dynamical systems is the study of the long-term behavior of evolving systems, either be discrete or continuous dynamical system (flow) [25]. Chaotic behavior by chaotic properties has found numerous applications in communication engineering, and information technologies [12]. The chaotic signals and the theories of chaos synchronization were since 1900. Todays, the modeling of communication channels using chaotic cryptography [16].

Cryptography has been used for thousands of years to help to provide confidential communications between mutually trusted parties [26]. The cryptosystem constitutes a complete specification of the keys and how they are used to encrypt and decrypt information.

Chaos-based cryptography [12] is a new research field that across two fields; chaos through nonlinear dynamic system and cryptography.

In fuzzy model based chaotic cryptosystem. The encrypting process were by using chaotic signal in TS fuzzy model to get the ciphertext. The ciphertext is embedded either to the output [2] or to the state of the drive system [7]. Retrieving the plaintext is through synthesis the signal synchronization. Using the Linear Matrix Inequality problem (LMI) to solve the chaotic synchronization problem. The TS fuzzy model were exact represented for the well-known Lure type discrete–time [7] and continuous-time chaotic systems [5,6].

For essential subjects in mathematical background, firstly a fuzzy logic and fuzzy set theory and some basic concepts were described in Section 2.2. Section 2.5 was introduced a dynamical system, chaos and some chaotic maps. Section 2.6 was introduced a cryptosystem and Knapsack problem. Section 2.7 described the fuzzy model based chaotic cryptosystems and TS fuzzy chaotic model and other models, and presented the chaotic synchronization and stability conditions and LMI. and described some draw backs of the previous models.

## 2.2 Fuzzy Logic

Fuzzy Logic FL is a multivalued logic [27], with intermediate values in $[0, 1]$. In mathematical strength of fuzzy logic, there are two different meanings for FL [2] ; A narrow and a broad (wide) sense. In its narrow sense, FL is a system of logical operators [22]. But in a wider (broad) sense, which is in predominant used today, describing a family of classes with unsharp boundaries in which membership is a matter of degree [28] .

The fuzzy set is basic idea in fuzzy set theory and FL [29]. That is it operate with a mathematical formulas, words, and terms of natural language beside the numeric values for linguistic variables.

Systems of FL, specially rule-based system, rules play a central role in applications [28]. But on other hand, other systems such as ; control system depends on consequents and antecedents part of the rules.

FL can views as a methodology for computing with words rather than numbers, and a control system [22]. Inference engine as its mechanism main parts, that enable approximate human reasoning capabilities to be applied to knowledge based systems [24].

From essential characteristics of FL which recognize it than other logical systems [30, 31] ;

1. Any logical system can be Fuzzified .
2. In FL, everything is a matter of degree .
3. FL could be controlled nonlinear systems that are difficult or impossible to module mathematically [2].
4. Inference is view as process of propagation of elastic constraints [24].
5. A major challenge to FL is the translation of the information contained implicitly in a collection of data points to linguistically interpretable fuzzy rules [31] .
6. FL provides a bridge between the continuous world of our perceptions and the digital world of computers. Since it can translate linguistic variables by rules into numerical variables correspond it without jettisoning partial truth that allows us to construct vastly improved models of human reasoning and expert knowledge [32].

## 2.3 Fuzzy Set Theory and Some Fundamental Concepts

A fuzzy set theory which is an extension of a classical set theory [33], deals with two kinds of variables; linguistic variables and numerical variables.

In classical mathematic, we are familiar with crisp sets [21].In fuzzy logic this different and we deals with fuzzy sets [27]. In crisp sets an element is either a member in a set or not (True or False) (1 or 0) [35]. Fuzzy sets on the other hand allow members (elements) to be partially in a set with some degree .

The shapes of fuzzy sets are generated by its certain accepted MFs [36], and then in values of these functions on members of sets. These shapes have adopted several conventions influence on fuzzy sets;

**Definition 2.3.1 (Fuzzy Set) [33]**: Let $U$ a nonempty set be the universal set (universe of discourse), and let a function $\mu_F: U \to [0, 1]$, for $u \in U$, called a membership function MF, its value which represent the degree of belonging $u$ to a set $U$. Then the fuzzy set $F$ is defined on $U$ to be a set of ordered pairs of a member (element) in the universal set $U$ and the value of a membership function at that member(element) which is called a membership degree and denoted by $\mu_F(u)$, for a member $u \in U$ .

So $F$ could be written as [37];

$$F = \{(u, \mu_F(u)) : u \in U\} \qquad \ldots(2.1)$$

that is, it is characterized by its MF [24] .

The elements of a fuzzy set are ordered pairs in form $(u, \mu_F(u))$ [38], first side is member included in the set $A$ (satisfies its conditions) while second part refer to degree of this inclusion (value between 0 and 1). The idea of fuzzy sets proposed to represent data information that possess non statistical uncertainty [39] ,or vague values [33].

A fuzzy set can have a finite or an infinite number of elements depending on the universal set [22], if it is a set of real, integers, or other situations and a membership function. These reflect on the support of a fuzzy set. It is clear that if one only allowed the extreme membership values of 0 and 1 [35] , that is would actually be equivalent to crisp set .This is wide in discrete membership function. So fuzzy set can be expressed as [2]:

1. Discrete case : When the universe of discourse $U$ is finite set :

$U = \{u_1, u_2, \ldots, u_n\}$. A fuzzy set $F$ on $U$ can be written as;

$$F = \mu_F(u_1)/\,u_1 + \mu_F(u_2)/\,u_2 + \cdots + \mu_F(u_n)/\,u_n$$
$$= \textstyle\sum_{i=1}^{n} \mu_F(u_i)/\,u_i \qquad \ldots(2.2)$$

2. Continuous case: When the universe of discourse $U$ is infinite set: A fuzzy set $F$ on $U$ can be written as;

$$F = \int_u \mu_F(u_i)/\,u_i \qquad \ldots(2.3)$$

**Example 2.3.1[22]:** Let $R$ be a universal set ,the fuzzy set $F$ on $R$ is set of all and only real numbers which "near zero" and that between -1 and 1.

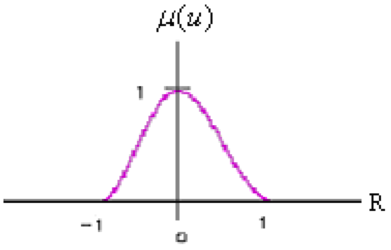


FIGURE 2.1: A fuzzy set "near zero" [22]

This fuzzy set will be infinite if we take it on real numbers without giving determined domain ,i.e. the domain will be R .

**Definition 2.3.2 (Empty Fuzzy Set) [24]:** The empty fuzzy set of universal (nonempty) set $U$,is defined as the fuzzy subset $\emptyset$ of $U$, such that $\mu(u) = 0$ for each $u \in U$, or sometimes denoted as $\emptyset(u)$, see Figure (2.2) .

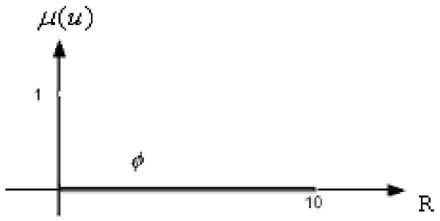


FIGURE 2.2: Empty fuzzy set in $U = [0,10]$. [24]

**Definition 2.3.3 (Universal Fuzzy Set) [33]:** The larges fuzzy set in universal set $U$, is called "universal fuzzy set", and it denoted by $1_U$ ,and defined as ; $\mu_{1_U} = 1$, for each $u \in U$. As example on universal set $U = R$, define universal fuzzy set on interval $[0, 10]$, then $1_U$ can written with membership degree equal to 1 for each member in $[0, 10]$.

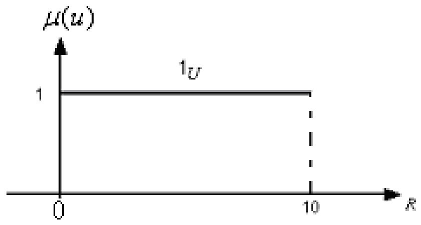


FIGURE 2.3: Universal fuzzy set in $u = [0,10]$ [24]

**Definition 2.3.4 (Normal Fuzzy Set) [39]:** A fuzzy set $F$ in a universe of discourse $U$, is said to be normal fuzzy set if $\exists\ u' \in U$, and $\mu_F(u') = 1$,that is max $\mu_F(u) = 1$, for $u \in U$.

**Definition 2.3.5 (Subnormal)[36]:** A fuzzy set F, is subnormal if it is not normal [2], that is, $\nexists\, u' \in U$, and $\mu_F(u') = 1$,that is $\max \mu_F(u) \neq 1$, for $u \in U$.

**Definition 2.3.6 (Convex Fuzzy Set) [36]:** A fuzzy set $F$, is said to be convex fuzzy set, if and only if all of its $\alpha - cut$ $(levels)$ are convex in classical sense, that is for each $\alpha - cut$ $(level)$ $F_\alpha$,for any $r, s \in F_\alpha$,and any $\lambda \in [0,1\,]$,then

$$\lambda r + (1 - \lambda)s \in F_\alpha \qquad \ldots(2.4)$$

Convex means that any $\alpha - cut$ $(level)$, which parallel to the horizontal axis is through interval [22].

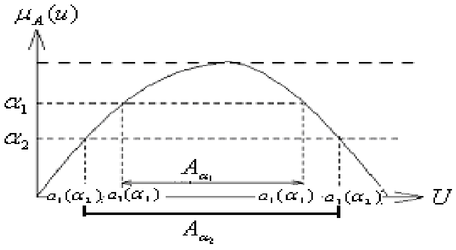


FIGURE 2.4: Convex Fuzzy set [36]

The intervals[1] on real axis which represent $\alpha - cut$ sets are nested if fuzzy set is convex and normal [22]. So a fuzzy set can be considered as a series of $\alpha - cut$ sets which are represented by interval determined on real axis, that is a fuzzy set(fuzzy number) is a union of $\alpha - cut$ sets .

**Definition 2.3.7(level Set (Cut Set)) [33]:** The set of elements that belongs to fuzzy set $A$ on universal set $U$, at least to degree $\alpha$ is called $\alpha - level$ or $\alpha - cut$ set, and defined as;

$$A_\alpha = \{u \in U : \mu_A(u) \geq \alpha \text{ , for } \alpha \in [0, 1] \qquad \ldots(2.5)$$

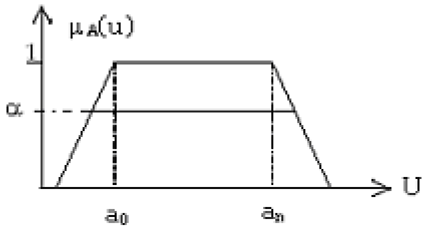


FIGURE 2.5: Level Set [22]

[1] These intervals called **intervals of confidence** [22] .

**Definition 2.3.8 Support of a Fuzzy Set [2]:** Let F be a fuzzy set on universal set $U$, then support of $F$ ,denoted by $supp(F)$ or $F_{sup}$, is the crisp set of all members of the universal set $U$, for which a members have non zero membership degree in $F$, and written as ;

$$supp(F) = \{u \in U: \mu_A(u) > 0\} \qquad \ldots(2.6)$$

**Definition 2.3.9 Singleton [2] :** A fuzzy set $F$ whose support $suppA$ contains a single point $u$ in $U$ with $\mu_F(u) = 1,$ is referred to as a fuzzy (set) singleton.

Sometimes called a fuzzy point as in [24], which is a single real number [2] That is say for fuzzy set $F$;

$$F_\alpha = [u, u] = \{u\}, \forall\ \alpha\ \in [0, 1] \qquad \ldots(2.7)$$

A function which define this point is with a unity value at this one particular point and zero everywhere else called a singleton function [28].

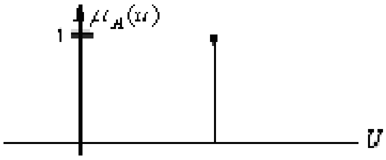


FIGURE 2.6: Singleton [33]

**Definition 2.3.10 (Fuzzy Numbers)[22]:** A fuzzy set $F$ on real line $R$ as a universal set with a normal, (fuzzy) convex, and continuous membership function $\mu_F(.)$ of bounded support finite set is said to be a fuzzy number. In some references we note that fuzzy numbers are denoted by uppercase letters with tildes such as ; $\widetilde{A}, \widetilde{B}$ ,…,etc.[2], or use numeric symbols for variables.

**Example 2.3.2:** Let the equation $y = \tilde{5}x_1 + \widetilde{10}x_2$, where $\tilde{5}$ and $\widetilde{10}$ are fuzzy numbers *"about five"* and *"about ten"*, respectively, defined by MFs instead of use exact values, and defined on real axis $R$ with triangular MFs [40].

[2] The uppercase letters is refer to uncertainty values for variable see [28,44].

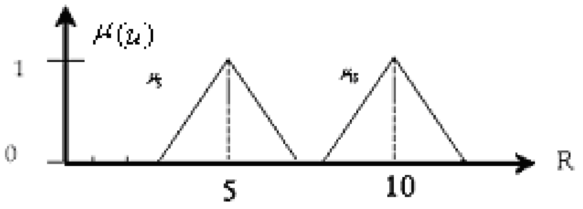


FIGURE 2.7: Examples of  fuzzy number [40]

**Definition 2.3.11 Not Fuzzy Number [24]:** A set $F$ is not fuzzy number if there exists $\beta$, such that $\beta \epsilon [0,1]$, that $F_\beta$ *level* set is not convex subset of $R$. That is not satisfies condition for a set to be convex, in spite of it is continuous MF (on a set), and normality satisfied in this situation .

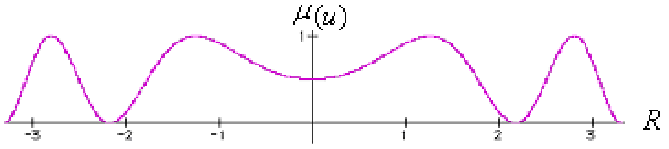


FIGURE 2.8: Not fuzzy number [24]

**Definition 2.3.12** (**Quasi-Fuzzy Number**) **[24]:** A fuzzy set $F$ on real line $R$ with a normal, fuzzy convex, and continuous membership function satisfies the limiting conditions as ;

$$\lim_{u \to \infty} \mu_F(u) = 0, \quad \lim\nolimits_{u \to -\infty} \mu_F(u) = 0 \qquad \ldots(2.8)$$

called  a quasi-fuzzy number.

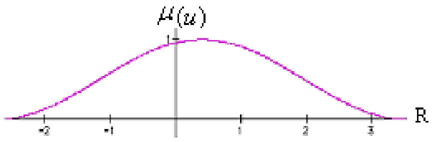


FIGURE 2.9: A quasi fuzzy number [24]

**Definition 2.3.13 (Triangular Fuzzy Number TFN) [41]:** It is a fuzzy number represented with three points as follows : given by three ordinary numbers $\tilde{A} = (a_1, a_2, a_3)$ [42] :

$$\mu(a) = \left\{ \begin{array}{cc} 0 \quad , & a < a_1 \\ \frac{a-a_1}{a_2-a_1} \quad , & a_1 \le a \le a_2 \\ \frac{a_3-a}{a_3-a_2} \quad , & a_2 \le a \le a_3 \\ 0 \quad , & a > a_3 \end{array} \right\} \qquad \ldots(2.9)$$

**Definition 2.3.14 (Trapezoidal Fuzzy Number TrFN) [43]:** To represent the Trapezoidal Fuzzy Number (TrFN) ,if $\tilde{B} = (b_1, b_2, b_3, b_4)$, where $-\infty < b_1 \leq b_2 \leq b_3 \leq b_4 < +\infty$, called TrFN. When $b_1 > 0$ it be positive trapezoidal fuzzy number, but when $b_2 = b_3$ the TrFN change into TFN. Its interval is represented by two end points $b_1$ and $b_4$ and a two peak points $b_2, b_3$ as $(b_1, b_2, b_3, b_4)$. The MF of TrFN as [48];

$$\mu(b) = \begin{cases} \dfrac{b - b_1}{b_2 - b_1} & , \quad b_1 \leq b < b_2 \\ 1 & , \quad b_2 \leq b \leq b_3 \\ \dfrac{b - b_4}{b_3 - b_4} & , \quad b_3 < b \leq b_4 \\ 0 & , \quad other \end{cases} \qquad \ldots.(2{,}10)$$

**Definition 2.3.15 (Fuzzy Relation) [2]:** A vague relationships like $x\ and\ y\ are\ closed"$, and $"x\ is\ much\ more\ smart\ than\ y"$ are difficult to expressed in ordinary relations. Fuzzy relations are appropriate to express such relations [2].

Let $U$ and $V$ be two universes of discourse. A fuzzy relation R is a fuzzy set in the product space $U \times V$ , which is characterized by a MF $\mu_{\mathrm{R}}$ , $\mu_{\mathrm{R}}: U \times V \rightarrow [0, 1]$.

When $U = V$, $R$ is known as a fuzzy relation on $U$. For generalization of fuzzy relations, the $n - ary$ fuzzy relation $R$ in $U_1 \times \ldots \times U_n$ is ;

$$R = \int_{U_1 \times \ldots \times U_n} \mu_{\mathrm{R}}\,(x_1, \ldots, x_n) /\,(x_1, \ldots, x_n),\ x_i \in U_i \qquad \ldots(2.11)$$

where $\mu_{\mathrm{R}}: U_1 \times \ldots \times U_n \rightarrow [0, 1]$.

**Definition 2.3.16 (Fuzzy Implication) [2]:** Let $A$ and $B$ be fuzzy sets on $U$ and $V$, respectively. A fuzzy implication, denoted by $A \rightarrow B$, is a special kind of fuzzy relation on $U \times V$ satisfying the conditions of t-norm, such ;

*Boolean logic implication:* $\mu_{A \rightarrow B}(x, y) = (1 - \mu_A(x)) \vee \mu_B(y)$ …(2.12)

*Mamdani's method :* $\mu_{A \rightarrow B}(x, y) = \mu_A(x) \wedge \mu_B(y)$ …(2.13)

*Algebraic product :* $\mu_{A \rightarrow B}(x, y) = \mu_A(x) \,.\, \mu_B(y)$ …(2.14)

*Bounded product:* $\mu_{A \rightarrow B}(x, y) = 0 \vee (\mu_A(x) + \mu_B(y) - 1)$ …(2.15)

## 2.4 Fuzzy Rule Base

Fuzzy implication is performed with inference rules, that are expressed by IF-THEN form, called fuzzy IF-THEN rules. A fuzzy rule base is composed as a collection of fuzzy IF-THEN rules. Fuzzy rule consist of the antecedents (premise) inputs with fuzzy sets and a consequent part that either fuzzy or function. Most popular fuzzy rules are Takagi-Sugeno (TS) fuzzy rules and Mamdani fuzzy rules. Here, we will focus on TS fuzzy rules since it will used in the work [43].

**2.4.1 Takagi-Sugeno (TS) Fuzzy Rules:** The TS fuzzy rules use a linear function between variables in the consequent part instead of using fuzzy sets in the consequence part. That represent input-output relation. A TS fuzzy rule is formed as [2];

$$R_{TS}^{l}: IF\ x_1 is\ F_1^l and\ \dots and\ x_n is\ F_n^l$$

$$THEN\ y^l = a_0^l + a_1^l x_1 + \cdots + a_n^l x_n \text{ , for } l = 1, 2, \dots, q \qquad \dots(2.16)$$

Where $F_i^l$ are fuzzy sets, $a_i^l$ are real-valued parameters for rule $l$, and $y^l$ is the system output.

### 2.4.2 Fuzzy Rule Based Inference

A Fuzzy Inference System (FIS) is the process that formulating the mapping from inputs to an output using fuzzy logic by fuzzy set theory [7]. Fuzzy inference is sometimes called reasoning or approximate reasoning. It is used in a fuzzy rule to determine the rule output from the inputs [7][22]. The fuzzy rule based inference algorithm consists of some steps as follows;

1. Fuzzification: that fuzzify the input variables by calculating the membership degree to which the input data match the condition of the fuzzy IF-THEN rule.
2. Inference: that calculate the rules conclusion based on its matching degree either by clipping or scaling method. That inferred outcome by suppressing the MF of the consequent part in fuzzy rule

3. Combination: that combine the outcome inferred by all the fuzzy rules into the final conclusion based on max fuzzy disjunction operator to multiple possibility
4. Defuzzification: that used to convert a fuzzy conclusion into a crisp output.

### 2.4.3 Fuzzification

Fuzzification is a mathematical process for converting an element in the universe of discourse to the membership value with membership degree of the fuzzy set [7].

A mapping from universal set into determined set (a closed interval $I = [0, 1]$). This operation called the fuzzification ,when it is mapping a crisp set from universal set into $[0, 1]$. For any subset in universal set ,a MF is not unique [50].We can choose many types for same set(range) ,in spite of that they different in its values of degree for same member(element) ,(see this example). These MFs can be chose from a wide set, which is called a *"dictionary of* MFs*"* [31,44] .

**Example 2.4.1[35]:** A set of real numbers is a universal set, fuzzy sets NL= numbers that are negative large, NM= numbers that are negative medium, NS= numbers that are negative small, Z = numbers that are near zero, PS= numbers that are positive small, PM= numbers that are positive medium, and PL= numbers that are positive large .

The shape of these classes is in Figure (2.10). Note the MF is same for all classes in the middle, and different in classes PL and NL .

**Note:** We can take it on the set of integer numbers .

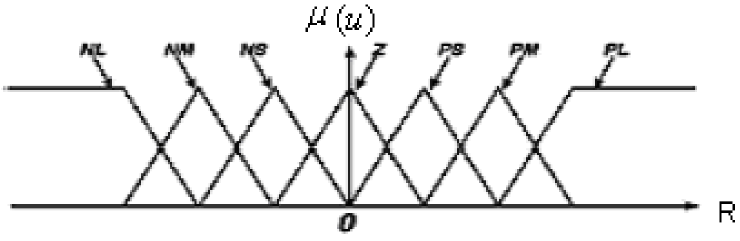


FIGURE 2.10: Membership Function for the set of all numbers R (N=Negative, P=Positive, L=Large, M=Medium, S=Small) [35]

Now depending on the influence of fuzzy MF in fuzzy sets. It must carefully choose a general parameters which determine a MF ,a number of classes to describe all values of (linguistic)variable on universal set [35], position of different MFs on universal set, width ,and concrete parameters . A classes has different ranges of values in spite it is same universal set or same MF, or it is overlaps. For fuzzifier that performs a map from a crisp point $x = (x_1, \dots, x_n)^T$ in vector field $U$ into a fuzzy set $F$ on $U$ [2].

1. **Singleton fuzzifier:** $F$ is a fuzzy singleton with support $x$, with $\mu_F(x') = 1$ for $x' = x$ and $\mu_F(x') = 0$ with $x' \neq x$ for all other $x$in $U$
2. **Nonsingleton fuzzifier:** $\mu_F(x) = 1$ decreases from 1 as $x'$ moves away from $x$, such as [2], $\mu_F(x') = exp\left(-\frac{(x'-x)^T(x'-x)}{\sigma^2}\right)$, where $\sigma$ is a parameter characterizing the shape of $\mu_F(x')$ .

### 2.4.4 Defuzzifier

Defuzzification is a mathematical process that convert a fuzzy set or sets to a real number (crisp value) [7]. A defuzzifier performs a map from fuzzy sets in $V$ to a crisp point in $V$. There are many defuzzifier formulas such as[28]; center of area, height method, mean of maximum, …etc. From most popular is the center-average defuzzifier, which maps the fuzzy set $F°R$ in $V$ to a crisp point [2];

$$y = \frac{\sum_{l=1}^{M} y_l \mu_{F°R}(y_l)}{\sum_{l}^{M} \mu_{F°R}} \qquad \dots(2.17)$$

where $y_l$ is a point in $V$.

### 2.4.5 Fuzzy Inference Engine

A fuzzy inference (reasoning), is a process for the fuzzy IF-THEN rules in the fuzzy rule base by converting it to a map from a fuzzy set in $U$ to fuzzy set(s) in $V$. The TS fuzzy rules and Mamdani fuzzy rules are with different fuzzy inference approaches [22].

### 1. Takagi-Sugeno (TS) Inference Method

In many control systems the inputs and outputs of the system are real-valued variables. So a TS fuzzy model proposes a solution to deals with such systems. A fuzzy reasoning is performed by the weighted mean as [2],

$$y(x) = \frac{\sum_{l=1}^{M} y_l w_l}{\sum_{l}^{M} w_l} \qquad \ldots(2.18)$$

Where $w_l$is the overall truth value of the premise variable of the input rule $R_{TS}^{l}$, and formulated as;

$$w_l = \prod_{i=1}^{n} \mu_{F_i^l}(x_i) \qquad \ldots(2.19)$$

Where $\mu_{F_i^l}(x_i)$ is a membership degree of the fuzzy set $F_i^l$.

### 2. Mamdani Fuzzy inference

A fuzzy IF-THEN rule is interpreted as a fuzzy implication $F_1^l \times \ldots \times F_n^l \rightarrow E^l$ on $U \times V$. From disadvantages of Mamdani inference is that its inputs and outputs are fuzzy sets [2].

So we will focus on the TS fuzzy model instead of the Mamdani fuzzy model.

### 2.4.6 Quantization and Normalization

In fuzzy systems, we use fuzzy sets to refers to the uncertain information. The processing of fuzzy sets via digital computer processor needs to discretize of a universes which means quantization [7];

- If a universe is discrete it is easy to deals with.
- If a universe is continuous it discretized into segments .

1. Quantization [2] : means discretizes a universe into a certain number of segments called quantization levels. A quantization levels labeled by a generic elements each one of it assigns to a grade-of-membership value in [0,1] as fuzzy sets.

2. Normalization of universe [7]: means mapping a physical values of inputs and outputs into a normalized domain through scaling or multiplication by a normalization factor. In many cases we choose a fuzzy sets are symmetrical on equal support length.

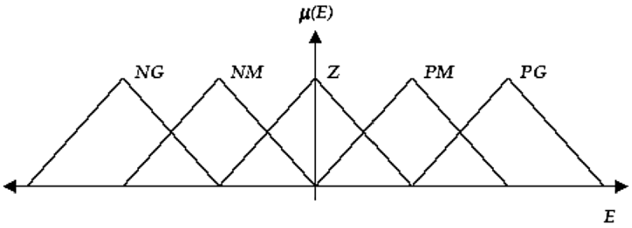
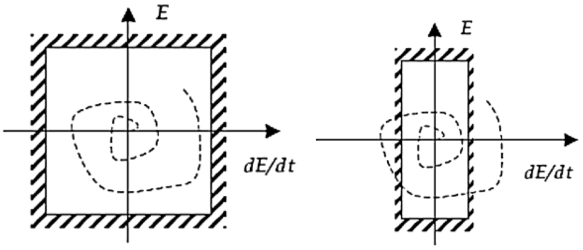


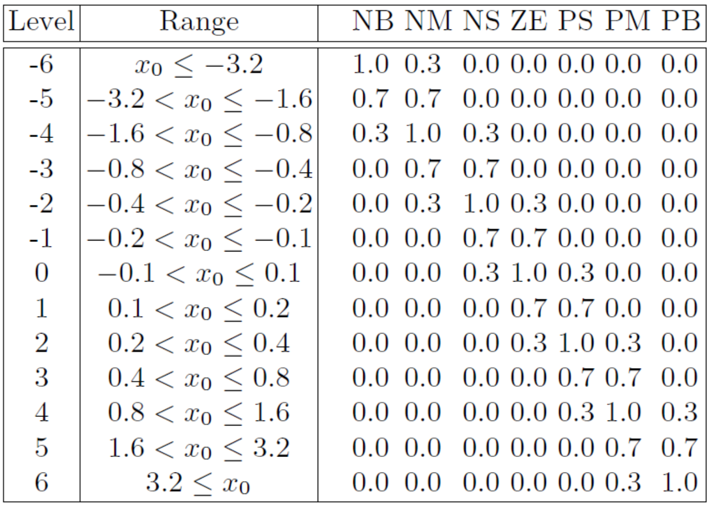
FIGURE (2.11): Symmetric partitioning of universe in fuzzy sets for input variable error E [2].



(a) (b)

FIGURE (2.12) : Scales adjustment in the phase plane. (a) correct gain ; (b) incorrect gain [7]

TABLE (2.1): An example of quantization and normalization on [-6,6] [2]



| Level | Range | NB | NM | NS | ZE | PS | PM | PB |
|---|---|---|---|---|---|---|---|---|
| -6 | $x_0 \leq -3.2$ | 1.0 | 0.3 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| -5 | $-3.2 < x_0 \leq -1.6$ | 0.7 | 0.7 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| -4 | $-1.6 < x_0 \leq -0.8$ | 0.3 | 1.0 | 0.3 | 0.0 | 0.0 | 0.0 | 0.0 |
| -3 | $-0.8 < x_0 \leq -0.4$ | 0.0 | 0.7 | 0.7 | 0.0 | 0.0 | 0.0 | 0.0 |
| -2 | $-0.4 < x_0 \leq -0.2$ | 0.0 | 0.3 | 1.0 | 0.3 | 0.0 | 0.0 | 0.0 |
| -1 | $-0.2 < x_0 \leq -0.1$ | 0.0 | 0.0 | 0.7 | 0.7 | 0.0 | 0.0 | 0.0 |
| 0 | $-0.1 < x_0 \leq 0.1$ | 0.0 | 0.0 | 0.3 | 1.0 | 0.3 | 0.0 | 0.0 |
| 1 | $0.1 < x_0 \leq 0.2$ | 0.0 | 0.0 | 0.0 | 0.7 | 0.7 | 0.0 | 0.0 |
| 2 | $0.2 < x_0 \leq 0.4$ | 0.0 | 0.0 | 0.0 | 0.3 | 1.0 | 0.3 | 0.0 |
| 3 | $0.4 < x_0 \leq 0.8$ | 0.0 | 0.0 | 0.0 | 0.0 | 0.7 | 0.7 | 0.0 |
| 4 | $0.8 < x_0 \leq 1.6$ | 0.0 | 0.0 | 0.0 | 0.0 | 0.3 | 1.0 | 0.3 |
| 5 | $1.6 < x_0 \leq 3.2$ | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.7 | 0.7 |
| 6 | $3.2 \leq x_0$ | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.3 | 1.0 |

where N, B, M, P, Z, E, and S are fuzzy sets. They are Linguistic variables with meaning : N as "Negative", P as "Positive", Z as "Zero", B as "Big", M as "Medium", S as "Small", E as "Error", the combination of these defined as ; NB refers "Negative Big" means not exists positive values in level, NM refers "Negative Medium", NS refers "Negative Small", ZE refers "Zero Error", PS refers "Positive Small", PM refers "Positive Medium", PB refers "Positive Big" means not exists negative values in level.

**Note 1**: The increasing in number of quantization levels gives an adequate approximation.

**Note 2:**We can use different values in normalization and in quantization for more accuracy.

**Note 3**: The advantage of normalization is in fuzzification, rule firing, and defuzzification to design the physical domains of input and output variables is independent.

3. Phase plane [7]: that acts when there are a little experience is available on the process, were the process dynamics and control actions based on intuitive ideas. By looking to the transient waveform of the controlled variable it is possible to divide it in time segments where the variable and its derivative have the same sign as shown in Figure 2.13, It is very important to define a critical points.

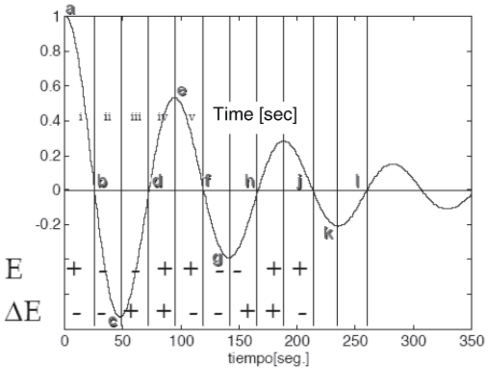


FIGURE 2.13: Transient response to inputs and time discrete for rules[7]

From the normalization, it could use the data division as table for inference the rules base consequents. Table (2.2) refer compute the consequent for each rule.

TABLE 2.2: Normalization for compute the rules consequents

| | NB | NM | NS | Z | PS | PM | PB |
|---|---|---|---|---|---|---|---|
| **PB** | Z | PS | PM | PB | PB | PB | PB |
| **PM** | NS | Z | PS | PM | PB | PB | PB |
| **PS** | NM | NS | Z | PS | PM | PB | PB |
| **ZE** | NB | NM | NS | Z | PS | PM | PB |
| **NS** | NB | NB | NM | NS | Z | PS | PM |
| **NM** | NB | NB | NB | NM | NS | Z | PS |
| **NB** | NB | NB | NB | NB | NM | NS | Z |

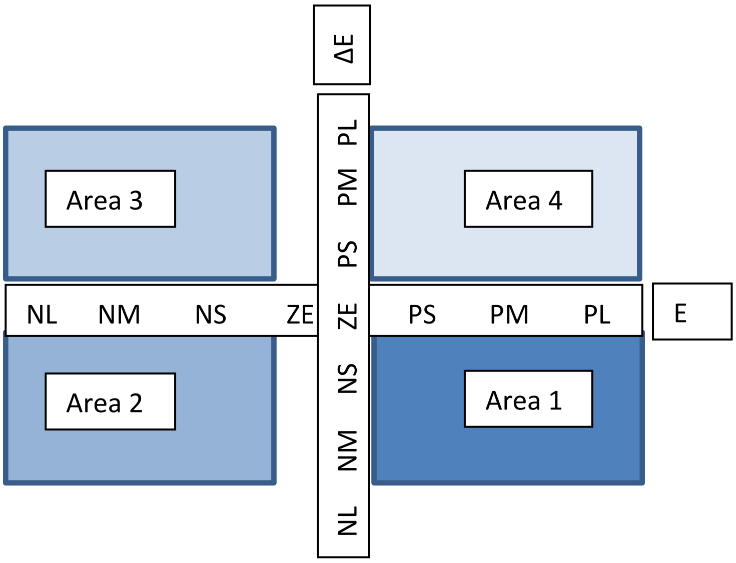


FIGURE 2.14: Phase plane for the regions determined by fuzzy inference

The axis for $E$ and $\Delta E$, with central value at ZE.

The phase plane were divided into four areas: Area 1, for positive and negative. Area 2, for negative and negative. Area 3, for negative and positive. Area 4, for positive and positive.

The regions that were coloring in dark to the low color level that mean converge to inference solution.

## 2.5 Introduction to Chaos Theory

In this section some important concepts of the chaos theory are discussed as follows

**Definition 2.5.1 (Dynamical System) [45]:** Given a continuous function $f\colon J \to J$ on a finite closed interval $J \subseteq R$,

For some essential terms in one dimensional discrete dynamical system;

Consider that ; $x_{n+1} = f^k(x_n)$, $k = 0,1,2,\dots$ , where $x, x_k \in J$, then $f^0(x) = x$, and $f^{n+1}(x) = f\big(f^n(x)\big) = fof^n(x)$ , for $n = 0,1,2,\dots$

**Definition 2.5.2 (Fixed and Periodic Points) [45]:** The point $x$ is said to fixed point for $f$ if $f(x) = x$. The point $x$ be a periodic point of period $n$ if $f^n(x) = x,$ for some $n \geq 1$.

**Definition 2.5.3 (Topological Transitive) [45]:** The map $f\colon J \to J$ is said to be topologically transitive, if for any pair of nonempty open sets $U, V \subset J$, there exists an integer $k > 0$, such that $f^k(U) \cap V \neq \emptyset$ .

Through this definition it could be known this map has a point(s) which eventually move from one arbitrarily small neighborhood to any other neighborhood through iteration processes. So the dynamical system can't be decomposed into two disjoint open sets $U$and $V$, which are invariant under the map $f(U) \cap f(V) = \emptyset$. Note that the map with dense orbit is topologically transitive [50].

**Definition 2.5.4 (Sensitive Dependence on Initial Conditions) [45]:** The map $f\colon J \to J$ is has sensitive dependence on initial conditions, if there exists a real number $\delta > 0$, such that for any point $x \in J$ and for any neighborhood $D$ of $x$, there exists a point $y \in D$ and $k \geq 0$ such that;

$$d\left(f^k(x), f^k(y)\right) > \delta \qquad \dots(2.20)$$

That means a sensitivity to initial conditions of the map $f$ on the set $J$, if there exist a point(s) which arbitrary close to $x$ (initial condition), which eventually away from $x$ in at least with distance $\delta$ under iterative process for $f$, and not all points near $x$ need eventually separate from $x$ under iteration, but must there exists at least one such point in every neighborhood of $x$. In some dynamical systems the dynamic of a map $f$ defy numerical computations.

**Definition 2.5.5 (Attractor) [25]:** Let $X$ be a compact topological space, and $f: X \to X$ be a continuous map. Generalizing the notion of an attracting fixed point, we say that a compact set $C \subset X$ is an attractor if there is an open set $U$containing $C$, such that $f\,(\bar{U}\,) \subset U$, $\bar{U}$ is the closure of $U$, and $C = \bigcap_{n \geq 0} f^n(U)$ …(2.24)

The forward orbit of any point $x \in U$ converges to $C$, i.e., for any open set $V$ containing $C$, there is some $N > 0$, such that $f^{\,n}(x) \in V$ for all $n \geq N$.

**Definition 2.5.6 (Strange Attractors) [25]**: From the nonlinear systems that have attractors are chaotic with sensitive dependence on initial conditions but not hyperbolic are called strange attractors, such as: Henon attractor and the Lorenz attractor.

### 2.5.1 Some Chaotic Maps

From the chaotic maps that will use in practical implementation are:

**1. Lozi Map**

Rene Lozi in 1978 gave an example of a family of piecewise linear mappings of the plane into itself [46],

$$x_1(t) = 1 + x_2(t) - a\,|x_1(t)|$$
$$x_2(t) = b\,x_1(t) \qquad \ldots(2.25)$$

known as Lozi map [15]. That is a discrete-time chaotic Lozi system its chaotic behavior exhibited in a single scroll, since it is well-known two-dimensional map on the interval [0,1]. The Lozi map as implicational example for theoretical derivative is like the Henon map but with absolute formulate the dynamical equations. for some set of values of the parameters. for some set of values of the parameters, the Lozi mappings have strange attractors [54]. See Figure (2.1), a numerical evidence of chaotic behavior of Lozi map with $a = 1.4$ and $b = 0.3$ [15].

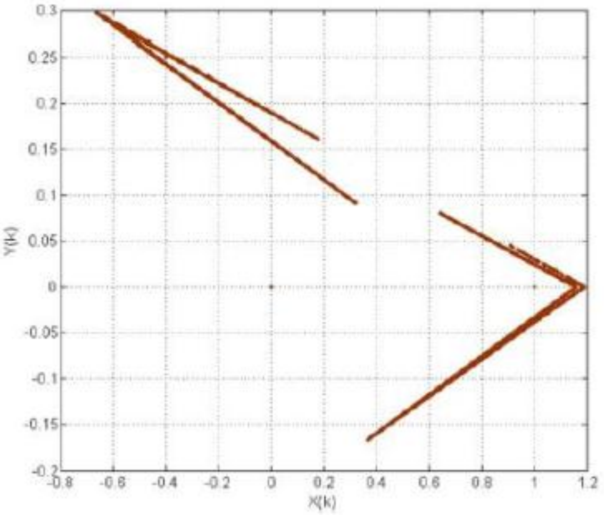


FIGURE 2.16: Chaotic Lozi map [15]

## 2. Lorenz Map

The chaotic Lorenz system for continuous-time is defined as a system with parameters values are [25]: $a$=10, $b$=8/3 and $r$=28, so the system is given by;

$$\begin{aligned} \dot{x_1} &= -10x_1 + 10x_2 \\ \dot{x_2} &= 28x_1 - x_2 - x_1x_3 \\ \dot{x_3} &= x_1x_2 - 8/3x_3. \end{aligned} \qquad \ldots(2.26)$$

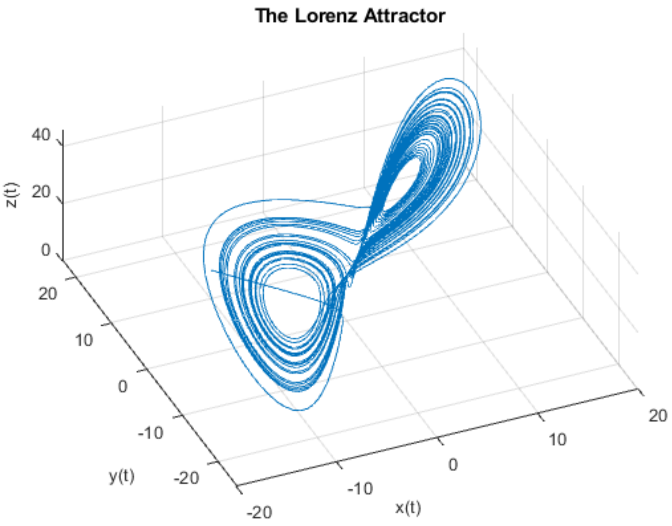


FIGURE 2.17: Chaotic Lorenz Map

The Figure (2.17) were drawn by using MATLAB Toolbox R2018b.

### 2.5.2 Chaotic Signals:

The definition of chaotic signals often unclear [45]. Standardly a chaotic signal is the output of chaotic system. So there are three consequences;

First: the apparent irregularity of chaotic signals is reduced to the source of randomness in the chaotic system, and this what depended in the suggested cryptosystem.

Second: the signal inherits the stationary and ergodic properties from the underlying chaotic system(this not in studying region)

Third: chaos relevant signal properties are defined in terms of the underlying dynamical system. Estimation of such properties, includes a phase space reconstruction step for revealing the system dynamics.

At using the chaotic signal it is loss the predictability in applications due to chaos theory, and the initial conditions for chaotic system are affective on chaotic signal.

### 2.5.3 Hurwitz Matrix and Hurwitz Stable

Consider the $n$-dimensional linear differential equations with real constant coefficients:

$$\frac{dx}{dt} = Ax \ , \ \ x = (x_1, \dots, x_n)^T \qquad \dots(2.27)$$

$$A \ = \ (aij\ )_{n\times n} \ \in R^{n\times n} \qquad \dots(2.28)$$

Put $\lambda(A)$ to be the eigenvalue of the matrix $A \ = \ (aij\ )_{n\times n}$

For the matrix $A = (aij\ )_{n\times n}$ ,If all eigenvalues are in the open left side of complex plane, that is $Re\,\lambda i(A) < 0$,for $i = 1, \dots, n$, then $A$ is said to be Hurwitz stable. But if all eigenvalues of $A$ lie in the closed left side of complex plane, that is $Re\,\lambda i(A) \leq 0$ for $i \ = \ 1, \dots, n$ and if $Re\,\lambda_{j0}(A) = 0$, for $\lambda_{j0}$ correspond to simple elementary divisor of $A$, then $A$ is said to be quasi-stable.

we need this theorem for proving the matrix to be Hurwitz matrix.

**Example 2.5.3.1[46]:** The matrix $\boldsymbol{A} = \begin{bmatrix} \mathbf{-6} & \mathbf{3} & \mathbf{1/8} & \mathbf{-1/8} \\ \mathbf{-5} & \mathbf{2} & \mathbf{1/7} & \mathbf{-1/7} \\ \mathbf{1/2} & \mathbf{1} & \mathbf{-4} & \mathbf{1} \\ \mathbf{1} & \mathbf{1/2} & \mathbf{1} & \mathbf{-4} \end{bmatrix}$ is Hurwitz matrix.

## 2.6 Cryptosystem

Fundamentally, cryptography is science of studying enabling two people, usually refer as Alice and Bob, to communicate over an insecure channel [2]. Eve, cannot understand what is being said. The information that Alice wants to send to Bob, called "plaintext," may be text or numerical data, its structure is completely arbitrary. Alice encrypts the plaintext, using a predetermined key, and sends it as ciphertext over the public channel. Eve, see the ciphertext but cannot recover the plaintext. But Bob knows the encryption key, so he can decrypt the ciphertext and retrieve the plaintext.

**Definition 2.6.1 Cryptosystem [26]:** A cryptosystem is a five-tuple (M, C,K, E,D), with these conditions are satisfied:

1. $M$ is a finite set of possible plaintexts (message).
2. $C$ is a finite set of possible ciphertext.
3. $K$, the keyspace, is a finite set of possible keys.
4. For each $k \in K$, there is an encryption rule $e_k \in E$ and a corresponding decryption rule $d_k \in D$. Each $e_k: M \to C$ and $d_k: C \to M$, are functions such that:

$$d_k\big(e_k(x)\big) = x, \text{ for every plaintext element } x \in M \qquad \ldots(2.29)$$

**Definition 2.6.2 (Super increasing Sequence) [47]:**A sequence of positive real numbers $s_1, s_2, \ldots$is called superincreasing if every element of the sequence is greater than the sum of all preceding (previous) elements in the sequence. In other words ;

$$s_{n+1} > \sum_{i=1}^{n} s_i \qquad \ldots(2.30)$$

That is $s_n > s_1 + s_2 + \cdots + s_{n-1}$.

If $n = 5$, then $s_5 > s_1 + s_2 + s_3 + s_4$.

A simple example of the super-increasing sequence

**Example 2.6.1:** The sequence $(0, 1, 3, 5, 11, 21, 42, 85)$ is a superincreasing sequence, but $(0, 1, 3, 4, 5, 7, 11, 19)$ is not super-increasing sequence.

**Example 2.6.2:** The sequence $(0,\ 0.4532\ ,\ 0.5,\ 1,\ 2.331,\ 5,\ 10.3119,\ 21)$ is a superincreasing sequence, but $(0, 0.4532,\ 0.4533,\ 0.53,\ 1, 2.3, 7.44,\ 11.8,\ 21)$ is not super-increasing sequence.

## 2.6.1 Knapsack Problem

In spite the use of superincresasing sequence in cryptosystem back to 1978 by R.Makle and M. Helman, this method used in fuzzy models based cryptosystems [47].

A problem, that in which a public-key cryptosystem based on the classic problem combinatory or known as the knapsack problem, or the subset sum problem. This problem could be stated as follows: Given a knapsack of volume $V$ the sum as;

$$V = a_1x_1 + a_2x_2 + \cdots + a_nx_n \qquad \ldots(2.31)$$

for $n$ items the of various volumes $a_1, a_2, \ldots, a_n$ positive integers, where $x_i = 0$ or $x_i = 1$, for $i = 1, 2, \ldots, n$.

The problem is to solve the previous equation if the sequence of integers $a_1, a_2, \ldots, a_n$ have some special properties to be a superincreasing sequence. The user started by choosing a superincreasing sequence $a_1, a_2, \ldots, a_n$. Then select a modulus $N > 2a_n$ a multiplier $a$ with $0 < a < N$ , and $gcd(a, N) = 1$ this led to $ax \equiv 1(mod\ N)$ has a unique solution say $x \equiv c(mod\ N)$. Finally from the sequence of integers $b_1, b_2, \ldots, b_n$, $b_i = a_i(modN), i = 1, 2, \ldots, n$ , and $0 < b_i < N$ .

Carrying out this transformation generally destroys the superincreasing property of $a_i$. To keep secret of the system the sequence $a_1, a_2, \ldots, a_n$ and $m$ and $a$ are secret, while $b_1, b_2, \ldots, b_n$be publish in public directory.

Note that, anyone wishing to send a message to the user employs the publicly available sequence (public encrypting sequence) as the encryption key.

The sequence $b_1, b_2, \dots, b_n$ is not necessary superincreasing, that add difficult to the problem, since no one without private key can change the difficult of the knapsack problem into easy.

$$S = b_1x_1 + b_2x_2 + \cdots + b_nx_n \qquad \dots(2.32)$$

$S$ is hidden information that the sender transmits over a communication channel which presume to be insecure. So that the private and public sequence differ by several transformations.

**Note:** To increase security the knapsack should contain at least 250 items to choose from.

**Note:** The system can be made somewhat more secure by iterating the modular multiplications in the method with different values of $a$ .

### 2.6.2 Knapsack Cryptosystem

An easy knapsack problem is a problem in which the input set of positive integers $S = \{s_1, s_2, \dots, s_n\}$ is a superincreasing sequence and $N > 2s_n$ [47]. In superincreasing sequence each $S_i$ term is larger than the sum of all preceding terms, such that ;

$$s_2 > s_1\ ,\ s_3 > s_1 + s_2\ ,\ s_n > s_1 + s_2 + \dots + s_{n-1} \qquad \dots(2.33)$$

The polynomial time algorithm start with inputting a superincreasing $S$ and the value $N$ ,if there is a subset of $S$ sums to $E$ ,the output is True. At the algorithm, outputs binary array $P$ of n elements where $P[i] = 1$ if and only if $s_i \in X$, else the algorithm returns False.Knapsack problems that based on superincreasing sequence have unique solution where they are solvable at all. A public cryptosystem based on the knapsack problem work as follows: A typical user of the system will [48];

1. Chooses a superincreasing sequence $S = \{s_1, s_2, \dots, s_n\}$
2. Selects a modulus $N > 2s_n$ to be a privative key .

3. Calculates $T = \sum_{i=1}^{n} s_i$
4. Chooses a multiplier $W$ with $2 \leq W \leq N$, and $gcd(W, N) = 1$. That ensure the congruence $Wx \equiv 1(mod\, N)$ has a unique solution.
5. Computes a public(hard) knapsack from a sequence of integers $B = \{b_1, b_2, \dots, b_n\}$ defines as $b_i \equiv Ws_i\ (mod\, N)$, for $i = 1, \dots, n$, and $0 < b_i < N$.

Finally, the user keeps private key $T, N$, and $W$. The user publishes public key $B$ in a public directory.

## 2.7 Fuzzy Chaotic Model and Designing a Model for Fuzzy Chaotic Cryptosystem

An important difference between chaos and cryptography lies on the fact that systems used in chaos are defined on real numbers, while cryptography deals with systems defined on finite numbers of integers. Nevertheless, it is believed that the two disciplines can benefit from each other .

### 2.7.1 Fuzzy Model Based Chaotic Cryptosystem

This cryptosystem encrypting the plaintext by using a superincreasing sequence formed by chaotic signal by TS fuzzy model to get the ciphertext [7]. The ciphertext is embedded either to the state [2] or output of the drive system [7], and then sent to the response system. The retrieving of the plain text is through synthesis performed for signal synchronization. By using the LMI to solve the chaotic synchronization problem. The TS fuzzy model were be exactly represented for discrete–time [2], and continuous-time chaotic systems [5]. The fuzzy model based chaotic were implemented with T fuzzy model and Mamdani fuzzy model, in this work only the TS fuzzy model were studied.

### 2.7.2 TS Fuzzy Model of Nonlinear Systems

The TS fuzzy model dynamic models which originates from Takagi and Sugeno [9], are described by fuzzy (If-Then) rules in which the consequent parts represent local linear models. These rules utilized to exactly representing nonlinear systems in a region of interest [6], the methodology is applied to a large class of chaotic systems; continuous and discrete [6].

A compact fuzzy model can be obtained by a careful selection of rule number and parameters;

### 2.7.3 Takagi-Sugeno Fuzzy Representation of nonlinear Systems

To construct a TS fuzzy model that exact represents the nonlinearities [6];

$$sx(t) = f\big(x(t)\big) + g\big(x(t)\big)u(t) \qquad \ldots(2.34)$$

Where $sx(t)$ is $\dot{x}(t)$ for continuous-time system and $x(t+1)$ for discrete-time system. $x \in R^n$ is a state vector, and $u \in R^p$is a control input vector, $x(t) = [x_1(t),\ x_2(t), \ldots, x_n(t)]^T$, $f(.)$ and $g(.)$ are nonlinear functions with appropriate dimension.

The characteristic nonlinearities are first expressed as fuzzy inferred outputs by specifying the fuzzy membership functions in premise parts of the rules and associated coefficients matrices $A_i, B_i$ in the consequence parts of the rules. Then the fuzzy model is composed of the rules [5].

$$\boldsymbol{Plant\ Rule\ i}\text{: } IF z_1(t)\ is\ \Gamma_{1i}\ and\ z_2(t) is\ \Gamma_{2i}\ and\ \ldots and\ z_g(t) is\ \Gamma_{gi}$$

$$Then\ sx(t) = A_i x(t) + B_i u(t) + b_i(t) \qquad \ldots(2.35)$$

for $i = 1,2, \ldots, r$

where $z_1(t) \sim z_g(t)$ are the premise variables, which would consists of the states of the system, $\Gamma_{ji}, j = 1,2, \ldots, g$ are fuzzy sets, $r$ is the number of fuzzy rules, and $A_i, B_i$ are system matrices with appropriate dimensions, $b_i(t)$ is bias term(s) which generated by the exact fuzzy model producer.

Denote the continuous-time fuzzy systems CFS, and the discrete-time fuzzy systems DFS. The overall outputs of the fuzzy systems are inferred by the singleton fuzzifier, product fuzzy inference and weighted average defuzzifier as;

$$sx(t) = \textstyle\sum_{i=1}^{r} \mu_i\big(z(t)\big)\{A_i x(t) + B_i u(t) + b_i(t)\} \qquad \ldots(2.36)$$

where $z(t) = [z_1(t) \quad z_2(t) \cdots \quad z_g(t)]^T$, and

$\mu_i\big(z(t)\big) = w_i(z(t)) / \sum_{i=1}^{r} w_i(z(t))$ , with ;

$$w_i\big(z(t)\big) = \prod_{j=1}^{g} F_{ij}(z_j(t)) \qquad \ldots(2.37)$$

where $\sum_{i=1}^{r} \mu_i\big(z(t)\big) = 1$ for all $t$, and $\mu_i\big(z(t)\big) \geq 0$, for $i = 1, \ldots, r$ are normalized weights. The nonlinear term in the system and its associated fuzzy representation are emphasized in the system [5].

A fuzzy modeling methods are proposed for three cases;

1) Nonlinear terms with only one dependent variable [5].
2) Nonlinear terms with multiple dependent variable [6].
3) Multiple nonlinear terms in the system [5].

**Case 1 [5]**: Only one dependent variable in a nonlinear term;

Consider a single scalar nonlinear function $f(x_l)$, which depends only on a state variable $x_l$. Let the nonlinear term $f(x_l)$ takes the form $\emptyset(x_l)x_m$ with $x_m$ is ;

$$x_m = \begin{cases} x_l & , \ if \ \lim_{x_l \to 0} \frac{f(x_l)}{x_l} \ \ exists \ and \ \ in \ L_\infty \\ 1 & , \quad other \ wise \end{cases} \qquad \ldots(2.38)$$

Then the function $\emptyset(x_l)$ is well-defined function. Take $x_l$ which forms the function $\emptyset(x_l)$ as the premise variable, then the fuzzy representation is the composed of the following fuzzy rules;

$\boldsymbol{Rule \ i}$: $IF x_l \ is \ \Gamma_i$

$$Then \ \hat{f} = d_i x_m \ , i = 1, 2, \ldots, r \qquad \ldots(2.39)$$

where $\Gamma_i$ is fuzzy set, $\hat{f}$ is a fuzzy representation of $f(x_l)$, and $d_i$ is constant coefficient to be determined. $r$ is the number of fuzzy rules.

The fuzzy inferred output is written as;

$$\hat{f}(x_l) = \frac{\sum_{i=1}^{r} w_i(x_l) d_i}{\sum_{i=1}^{r} w_i(x_l)} \ x_m = \sum_{i=l}^{r} w_i(x_l) d_i \ x_m \qquad \ldots(2.40)$$

with $w_i(x_l) = \Gamma_i(x_l) \geq 0$, which must be equal to $\emptyset(x_l)x_m$.

$w_i(x_l)$ is regards as a normalized weight which is require that $\sum_{i=1}^{r} w_i(x_l) = 1$, that further yields $\emptyset(x_l) = \sum_{i=1}^{r} w_i(x_l)\, d_i$

Thus $f(x_l)$ can be exactly represented by a fuzzy system $\hat{f}(x_l)$ by suitably assigning $\Gamma_i(x_l)$ and $d_i$ in the region of the system trajectory $\Omega$ .

The other linear terms such $\Theta x_k$ is with the consequent part $\hat{f} = \Theta x_k$, then the inferred output is;

$$\hat{f} = \frac{\sum_{i=1}^{r} w_i(x_l)\Theta x_k}{\sum_{i=1}^{r} w_i(x_l)} = \Theta x_k \qquad \ldots(2.41)$$

Which exactly equal $\Theta x_k$ ,here $d_i = \Theta$ for variable $x_k$

For demonstration in [6], Let $r = 2$ and then specify the MFs

The general form of TS fuzzy chaotic model is written as [7]:

$$\boldsymbol{Plant\ Rule\ i}: IF\ y(t) is\ \Gamma_i$$

$$THEN\ x(t + 1) = A_i x(t) + b_i(t), \qquad \ldots(2.42)$$

for $i = 1, 2, \ldots, r$ ,where the scalar variable $y(t)$ is the output signal.

The overall inferred output signal can be written as

$$x(t+1) = \sum_{i=1}^{r} \mu_i(y(t))\ [A_i x(t) + b_i(t)]\,,$$

$$y(t) = Cx(t) \qquad \ldots(2.43)$$

Where

$$\mu_i\big(y(t)\big) = \frac{\omega_i\big(y(t)\big)}{\sum_{i=1}^{r} \omega_i\big(y(t)\big)}\,, \qquad \ldots(2.44)$$

with $\omega_i\big(y(t)\big) = \Gamma_i\big(y(t)\big) \geq 0.$

### 2.7.4 Cryptosystem with Discrete-time TS Fuzzy Chaotic System

The ciphertext from TS fuzzy chaotic based model could be masked by one from two different ways. In the both ways the modulation process is carried out by injecting the masking signal into the fuzzy chaotic transmitter. Then the resulted masked signal is transmit to the fuzzy chaotic receiver, where the ciphertext is extracted according to the masking methods [7].

### 2.7.5 Ciphertext Masked by a State of a Chaotic System

The user could encrypts the messages by the algorithm of chaotic encryption to get the embedded ciphertext $\xi$, see the reference fort the algorithm [7]. In this form the fuzzy chaotic transmitter(driver) be as;

$\boldsymbol{Transmitter\ Rule\ i}: IF\ y(t)\ is\ \Gamma_i$

$$THEN\ x(t+1) = A_i\bar{x}(t) + b_i(t)$$

$$\bar{x}(t) = x(t) + M_s\xi(t)$$

$$\bar{y}(t) = C\bar{x}(t) \qquad \ldots(2.45)$$

that is $\bar{y}(t) = Cx(t) + CM_s\xi(t)$

where $\bar{x}(t) \in R^n$ is the composed states that mask the ciphertext $\xi$, $M_s = [m_1 \ldots m_n]^T \in R^n$, for $m_j \in [0,1]$, for $j = 1,2,\ldots,n$, is the public state masking key, that specifies the state used for masking the ciphertext, and $y(t)$ represents the coupling signal. Then $y(t)$ will transmitted into the fuzzy chaotic receiver throughout a public channel. The inferred output of the transmitter is;

$$x(t+1) = \sum_{i=1}^{r} \mu_i(\bar{y}(t))\,[A_i x(t) + b_i(t) + A_i M_s \xi(t)]\,,$$

$$\bar{y}(t) = Cx(t) + CM_s\xi(t)] \qquad \ldots(2.46)$$

that is;

$$x(t+1) = \textstyle\sum_{i=1}^{r} \mu_i(\bar{y}(t))\,[A_i(x(t) + M_s\xi(t)) + b_i(t)]\,,$$

$$\bar{y}(t) = C[x(t) + M_s\xi(t)] \qquad \ldots(2.47)$$

To recover the message, the fuzzy chaotic receiver(response) is formed as;

$\boldsymbol{Receiver\ Rule\ i}: IF\ \bar{y}(t)\ is\ \Gamma_i$

$$THEN\ \hat{x}(t+1) = A_i x(t) + bi(t) + L_i(\bar{y}(t) - \hat{y}(t))$$

$$\hat{y}(t) = C\hat{x}(t)\,, \qquad \ldots(2.48)$$

where $\hat{x}(t)$ is the estimate of state $x(t)$, and $\hat{y}(t)$ is the estimate of $y(t)$. $L_i \in R^n$ denotes the design gain vector.

The fuzzy chaotic inferred receiver can be expressed in the form

$$\hat{x}(t+1) = \sum_{i=1}^{r} \mu_i\big(\bar{y}(t)\big)[\,A_i\hat{x}(t) + bi(t) + L_i(\bar{y}(t) - \hat{y}(t))$$

$$\hat{y}(t) = \ C\hat{x}(t), \qquad \ldots(2.49)$$

This system use different theorem for synchronization and stability of signal than the system use the output of chaotic system for theses theorems see the literatures [5,6,7].

In our work the masking by output will depended, so we will focuses on.

### 2.7.6 Ciphertext Masked by Output of the Chaotic System

The ciphertext $\xi(t)$ added directly to the output of the chaotic system. The TS fuzzy chaotic transmitter is formulated as [2];

$\boldsymbol{Transmitter\ Rule\ i}: IF\ \bar{y}(t) is\ \Gamma_i$

$$THEN\ x(t+1) = A_i x(t) + b_i(t) + L_i M_o \xi(t)$$

$$\bar{y}(t) = Cx(t) + M_o\xi(t), \qquad \ldots(2.50)$$

for $i\ =\ 1, 2, \ldots, r$,where the gains matrices $L_i$, will be determined later, and $M_o$ is a public output masking key, described in previous masked way, $M_o$ masks the ciphertext by a constant.

The fuzzy inferred output for the transmitter is;

$$x(t+1) = \textstyle\sum_{i=1}^{r} \mu_i(\bar{y}(t))\,[\bar{A}_i x(t) + bi(t) + L_i\bar{y}(t)]\,,$$

$$\bar{y}(t) = \ Cx(t) + \ M_o\xi(t) \qquad \ldots(2.51)$$

where $\bar{A}_i = A_i - L_i C$,

For recovering the ciphertext, the chaotic fuzzy receiver is designed as

$\boldsymbol{Receiver\ Rule\ i}: \ IF\ \bar{y}(t)\ is\ \Gamma_i$

$$THEN\ \hat{x}(t+1) = A_i\hat{x}(t) + bi(t) + L_i(\bar{y}(t) - \hat{y}(t))$$

$$\hat{y}(t) \ = \ C\hat{x}(t)\,, \qquad \ldots(2.52)$$

where $\hat{x}(t)$ is estimate of state $x(t)$, and $\hat{y}(t)$ is estimate of $y(t)$. $L_i \in R^n$ denotes the design gain vector.

The overall fuzzy chaotic inferred receiver is expressed as;

$$\hat{x}(t+1) = \sum_{i=1}^{r} \mu_i(\bar{y}(t))[A_i x(t) + b_i(t) + L_i(\bar{y}(t) - \hat{y}(t))$$

$$\hat{y}(t) = C\hat{x}(t), \qquad \ldots(2.53)$$

Now, define the error signals $e_x(t) \equiv x(t) - \hat{x}(t)$ and $e_y(t) \equiv \bar{y}(t) - \hat{y}(t)$. From (2.52) and (2.53), the error dynamics for error signals are as;

$$e_x(t+1) = \sum_{i=1}^{r} \mu_i\,(\bar{y}(t))(Ai - L_i C)e_x(t) \qquad \ldots(2.54)$$

$$e_y(t) = Ce_x(t) + M_o\xi(t) \qquad \ldots(2.55)$$

The stability condition for (2.55) is satisfied by the Lyapunov method in this theorem. For theorems that satisfy stability and synchronization see literature [2,4]

**Theorem 2.7.1[1]:**In the chaotic transmitter in equation (2.51) and receiver in equation (2.53), the ciphertext can be recovered from $\xi(t) = \frac{1}{M_o} e_y(t)$, and all states of chaotic transmitter and receiver are synchronized in an asymptotic manner if there exist a matrix $P$, where $P$ is common positive-definite and gains $L_i$, for $i = 1, 2, \ldots, r$, such that the following LMIs are satisfied:

$$\begin{bmatrix} P & (PA_i - W_i C)^T \\ PA_i - W_i C & P \end{bmatrix} > 0\,, \quad for\ all\ i, \qquad \ldots(2.56)$$

where $W_i = PL_i$ .

The complete proof occurred in the references [2].

As a result for theorem the synchronization error $e_x(t) \to 0$, as $t \to \infty$, Thus $e_y(t) \to M\xi(t)$, as $t \to \infty$. Since the convergent rate of the synchronization error :$x(t)$ affects the

transmission performance, the decay rate design for chaotic cryptosystems can be performed by solving LMIs problems as follows:

*Chaotic Cryptosystem with decay rate* :

$$\underset{P,W_i}{minimize}\ \beta$$

$$subject\ \ to\ P > 0, \beta\epsilon(0,1)$$

$$\begin{bmatrix} \beta P & (PA_i \; - W_i C)^T \\ PA_i \; - W_i C & P \end{bmatrix} > 0 \;, \quad for\ all\ i, \qquad \ldots(2.57)$$

Where $W_i = PL_i$. Then by form of $\Delta V\big(e_x(t)\big)$, the constrain will be $\Delta V\big(e_x(t)\big) \leq -(1-\beta)Ve_x(t)$ with parameter $\beta$ tuning the decay rate. By LMI form the conditions will be solved to compute $L_i$.

### 2.7.7 Chaos Synchronization and Stabilization Problem

Christian Huygens in 1965 discovers the synchronization of two weakly coupled pendulum clocks(that hanging on the same beam) [2]. Later many systems in biology, optics, chemistry, physics, and electrical and mechanical engineering, proved its ability to synchronize. It is closely related to chaos in addition to the stabilization [7]. Synchrony can be commonly observed in coupled systems, networks, or arrays that can be chaotic or periodic [14]. The chaotic systems have the property to be sensitive to initial conditions that defy the synchronization between the two coupled chaotic systems.

Importantly in approaches systems is to consider the synchronization problem through control theory [2]. At which synchronization achieved by a drive chaotic system coupled with response chaotic system [2]. The so called drive(reference) system that unidirectionally drive the second system that called response system. So the synchronization problem is to design two systems started from different initial inputs, such that the controlled system archives asymptotic synchronization with the drive system.

The drive system and control system are chosen with the same chaotic oscillator ,while controlled system has control input(s). Pecora and carol in [49] introduce a basic idea through taking two identical 3D dynamical systems, the designing of the synchronization of the system described as;

Let $\dot{x} = f(x)$ , for $x = (x_1, x_2, x_3)^T$ and $f(x)$ being a vector field. One of these systems used as a drive system $\dot{x}_d = f(x_d)$, that unidirectional drive the response system $\dot{x}_r = f(x_r)$, by a suitable replacement of the dynamical variables in the response system. Suppose $e(t)$ a dynamical error as ;

$$e(t) =: x_d - x_r, \text{ if } e(t) \to 0 \text{ as } t \to \infty \qquad \ldots(2.58)$$

The dynamics of the response system approaches the time evolution of the drive system and synchronization of these two system is achieved.

There are two cases for synchronization depend on the cancelation problem [2];

**Case 1:** The cancelation problem is feasible.

**Case 2:** The cancelation problem is infeasible .

This work will use first case for feasible solution, and will apply the same chaotic maps with two oscillating points.

By ensure stability of the systems it could be archive synchronization.

The stability may be though bounded input bounded output BIBO [7], or through LMI problems [2]

Chaos synchronization were approaches in Lurie systems and then discuss the stability of its error dynamics [50].

Consider a uni-directional feedback-controlled chaos synchronization system with form [46]:

$$\frac{dx}{dt} = A_1 x + B_1 f\,(c^T x, t)$$

$$\frac{dy}{dt} = A_2 x + B_2 f\,(c^T y, t) - K(x - y) - g(y, t) \qquad \ldots(2.59)$$

where $x(t), y(t), c \in R^n, A_i, B_i, K \in R^{n \times n}$, and $f \in C[R \times (t_0, \infty), R]$.

Let synchronization error be : $e = x - y$.

Substituted in the equation, Then the system reformed as;

$$\frac{de}{dt} = A_1 x - A_2 y + B_1 f\,(c^T x, t) - B_2 f\,(c^T y, t)) + Ke - g(y, t) \qquad \ldots(2.60)$$

Choose the constant feedback gain $K$ and a simplest possible control signal $g(y, t)$ such that $e(t) \to 0$ as $t \to \infty$, that achieving the synchronization $y(t) \to x(t)$ as $t \to \infty$.

Note that in system for synchronization purpose the control term $g(y,t)$ is only a function of the $y$ signal but not the $x$ signal [46]. Therefore, this setting can be easily implemented as a component of the response (receiver), which usually has the same structure as the drive (transmitter).

**Lemma 2.7.1[46]**: For the chaos synchronization system there always exist a constant feedback gain $K$ and a control signal $g(y,t)$ such that the error dynamics can be rewritten in the classical Lurie system form as follows:

$$\frac{de}{dt} = (A_1 + K)e + B_1 F(c^T e, t), \qquad \dots(2.61)$$

where $F(\sigma, t) := \ f(c^T x, t) - f(c^T y, t)$, For the variable $\sigma$

### 2.7.8 Parallel Distributed Compensation Technique

The Parallel Distributed Compensation (PDC) is a model-based design procedure, introduced in work by Wang in 1995 [4]. Mainly it is a technique employed for determining the structure of a fuzzy controller using TS fuzzy model.

PDC technique**,** employed to construct the fuzzy controller from the given fuzzy model [51]. It works firstly from the given nonlinear plant that represented by the TS fuzzy model. Since it express the joint dynamics of each fuzzy rule by a linear system model. The TS fuzzy systems is done by fuzzy IF-THEN rules, which linear input-output relations of a system. Each plant rule corresponding to control rule, that is each control rule is constructed from the corresponding plant rule of the TS fuzzy model. As shown in references [52], the designed fuzzy controller shares the same number of rules, the same fuzzy sets, and the same MFs with the rules of in premise part of the fuzzy rules in TS fuzzy model. Fuzzy control rules structure that constructed from PDC technique formulated as [52]:

$$\boldsymbol{Control\ Rule\ i}:\ \ IF\ x_1(t) is\ \Gamma_1^i\ and \dots and\ \ x_n(t)\ is\ \Gamma_n^i$$

$$THEN\ u_n(t) = F_i x(t), i = 1,2,\dots,q. \qquad \dots(2.62)$$

where $\{F_i\}_{i=1}^{q}$ are constant feedback gain matrices to be determined.

A fuzzy combination of the stabilizing state feedback gains $F_i, i = 1, \dots, q$ associated with every linear subsystem is used as the overall state feedback controller [4].

A fuzzy control rules by PDC have linear state feedback laws in the consequent parts. So the overall inference fuzzy controller as [2];

$$u(t) = \frac{-1}{\sum_{i=1}^{q} \omega_i(t)} \; \sum_{i=1}^{q} \omega_i(t)\, F_i x(t) \equiv -\sum_{i=1}^{q} h_i(t)\, F_i x(t) \qquad \dots(2.63)$$

For practically, there requisite that the control gain matrices $\{F_i\}_{i=1}^{q}$ be uniformly bounded as follows [4]:

$$\mathrm{sup}_{1\leq \mathrm{i} \leq \mathrm{q}} \|F_i\| \leq M < \infty \qquad \dots(2.64)$$

for some constant $M > 0$ .

The fuzzy control system by PDC is constructed by substituting overall fuzzy controller into the defuzzified output of TS fuzzy system. To be formulated as [2];

$$\dot{x}(t) = \sum_{i=1}^{q} \mu_i(x(t))\,(A_i x(t) + (B_i u(t)) \qquad \dots(2.65)$$

By substituting $u(t)$ in the defuzzified output of TS, that is mean the fuzzy model and fuzzy controller connected through closed loop as:

$sx(t) = \dot{x}(t)$ for continuous time TS fuzzy systems CFS

$sx(t) = x(t+1)$ for discrete time TS fuzzy systems DFS

To be for $i = j$ and for $i < j$ as;

$$sx(t) = \sum_{i=1}^{q} \sum_{j=1}^{q} h_i(t)\, h_j(t) [A_i + B_i F_j] x(t) \qquad \dots(2.66)$$

$$= \sum_{i=1}^{q} \mu_i(x(t))\,(A_i x(t) + (B_i \sum_{i=1}^{q} h_i(t)\, F_i x(t))$$

$$= \sum_{i=1}^{q} \mu_i(x(t))\,(A_i x(t) + (B_i \sum_{i=1}^{q} \frac{\omega_i(t)}{\sum_{i=1}^{q} \omega_i(t))} F_i x(t))$$

$$= \sum_{i=1}^{q} (\frac{\omega_i\big(x(t)\big)}{\sum_{i=1}^{q} \omega_i\big(x(t)\big)})\,(A_i x(t)) + (B_i \frac{\sum_{i=1}^{q} \omega_i(t) F_i x(t))}{\sum_{i=1}^{q} \omega_i(t)})$$

$$x(t+1) = \sum_{i=1}^{q} \sum_{j=1}^{q} \; h_i(t) h_j(t)\,(A_i + B_i F_j) x(t) \qquad \dots(2.67)$$

where $h_i(t) = \frac{\omega_i(t)}{\sum_{i=1}^{q}\omega_i(t)}$ , and $h_j(t) = \frac{\omega_j(t)}{\sum_{j=1}^{q}\omega_j(t)}$ , for $i,j = 1,\dots,q$

We can added the property from [33]

$$\sum_{i=1}^{q}\sum_{j=1}^{q} h_i(t)h_j(t) = 1 \qquad \dots(2.68)$$

Since $\mu_i(x(t)) = \frac{\omega_i(x(t))}{\sum_{i=1}^{q}\omega_i(x(t))}$ and $\omega_i(x(t)) = \prod_{j=1}^{n}\Gamma_j^{\,i}(x_j(t))$

$\Gamma_j^{\,i}(x_j(t)$ are the grades of MF(membership degree) of $x_j(t)$ in fuzzy set $\Gamma_j^i$. When the approach of sharing the premise MFs of the rules produce complicated fuzzy controller structure this mean the MFs of TS fuzzy model is complicated.

Also there are some constrains for $\omega_i(x(t))$:

$$\omega_i(x(t)) \geq 0, \text{ and } \sum_{i=1}^{q}\omega_i(x(t)) > 0, \qquad \dots(2.69)$$

that is must be positive or zero so its summation must be positive for all $i = 1,\dots,q$ . So $\mu_i(x(t)) \geq 0$, and $\sum_{i=1}^{q}\mu_i(x(t)) = 1$, for all $i = 1,\dots,q$. We can write $sx(t)$ after spreading values that equaled for $i$ and $j$;

$$sx(t) = \sum_{i=1}^{q} h_i(t)h_i(t)\,(A_i{+}B_iF_i)x(t) + 2\sum_{i<j}^{q} h_i(t)h_j(t)\ \frac{(A_i+B_iF_j)+(A_j+B_jF_i)}{2}\ x(t) \qquad \dots(2.70)$$

Let $G_{ii} = (A_i{+}B_iF_i)$, $G_{ij} = (A_i{+}B_iF_j)$, and $G_{ji} = (A_j{+}B_jF_i)$, $i,j = 1,\dots,q$. Then ;

$$x(t+1) = \sum_{i=1}^{q} h_i(t)h_i(t)\,G_{ii}x(t) + 2\sum_{i<j}^{q} h_i(t)h_j(t)\ \left(\frac{G_{ij}+G_{ji}}{2}\right) x(t) \qquad \dots(2.71)$$

### 2.7.9 Stability for Fuzzy Controller System

The stability conditions and control design for TS fuzzy model could be formulated in a Lyapunov stability conditions that can be derived in terms of the Lyapunov direct method for CFS and DFS in form of LMIs [2] or in the form of PDC [4].

The work on cryptography systems led to focus on the discrete case, to see the theorem on the continuous case see [6]:

**Theorem 2.7.2[4]:** The equilibrium of the discrete TS fuzzy system:

$$x(t+1) = \sum_{i=1}^{q} h_i(z(t))\,(A_i x(t) + B_i u(t)) \qquad \ldots(2.71)$$

with $u(t) = 0$ is globally asymptotically stable if there exists a common positive definite matrix $P$such that :

$$A_i{}^T P A_i - P < 0, i = 1, 2, \ldots, r \qquad \ldots(2.72)$$

That is, a common $P$ has to exists for all subsystems.

Now, the next theorem is for $u(t) \neq 0$ .

**Theorem 2.7.3 [4]:** The equilibrium of the discrete TS fuzzy system:

$$x(t+1) = \sum_{i=1}^{q} h_i(t) h_i(t)\, G_{ii} x(t) + 2\, \sum_{i<j}^{q}\, h_i(t) h_j(t)\, \left(\frac{G_{ij}+G_{ji}}{2}\right) x(t) \qquad \ldots(2.73)$$

is globally asymptotically stable if there exists a common positive definite matrix $P$such that :

$$G_{ii}{}^T P G_{ii} - P < 0, i = 1, 2, \ldots, r \qquad \ldots(2.74)$$

$$\left(\frac{G_{ij}+G_{ji}}{2}\right)^T P \left(\frac{G_{ij}+G_{ji}}{2}\right) - P \leq 0 \qquad \ldots(2.75)$$

$i < j$ such that $h_i \cap h_j \neq \emptyset$ .

That is $\mu_i(x(t)).\mu_j(x(t)) = 0,\ \forall\, t$

The task of fuzzy controller design is to find $F_j, i = 1, 2, \ldots, q$ satisfying stability conditions in theorem for a positive definite matrix $P$.

The complete proof for these theorems found in [1].

### 2.7.10 Solving Stability Conditions

By solving stability conditions using Math lab LMI control Toolbox could be find the matrices $F_1, F_2, \ldots, F_q,\ P$ that refer to the response of the system and control effort, there are two cases [4] :

Case1: Stable Controller Design.

Case 2: The Decay Rate , that will use in this work.

The decay rate is associated with speed of system response. The decay rate fuzzy controller design used to calculate feedback gains matrices, that provide better settling time [4], for continuous fuzzy chaotic CFC, and discrete fuzzy chaotic DFC

The condition that; $\Delta V(x(t)) \leq (\alpha^2 - 1)V(x(t))$ for all $x(t)$ can formulated as;

$$G_{ii}{}^{T} P G_{ii} - \alpha^2 P < 0, i = 1, 2, \dots, r \qquad \dots(2.76)$$

$$\left(\frac{G_{ij}+G_{ji}}{2}\right)^{T} P \left(\frac{G_{ij}+G_{ji}}{2}\right) - \alpha^2 P \leq 0 \qquad \dots(2.77)$$

$i < j$ such that $h_i \cap h_j \neq \emptyset$ and $\alpha < 1$ .

## 2.7.11 Linear Matrix Inequality Problems

A Linear Matrix Inequalities (LMIs) [53], which are linear or affine in a set of matrix variables. These inequalities are essentially convex constraints, so there are many problems of optimization solution with convex objective functions and LMI constraints can easily be solved efficiently using programing in many existing software [54]. Since a wide variety of control problems can be formulated as LMI problems, this method be popular among control engineers in recent years.

**Definition 2.7.1** [53]: The formula of LMI be as $F(x) > 0$, that is;

$$\begin{aligned} F(x) &= F_0 + x_1 F_1 + \cdot\cdot\cdot + x_n F_n \\ &= F_0 + \sum_{i=1}^{n} x_i F_i > 0 \end{aligned} \qquad \dots(2.78)$$

for $i = 1, \dots, n$,

Even though the first term $F_0 = 0$, where $x \in R^m$ is the vector of decision variables. $F_0, F_1, \cdot\cdot\cdot, F_n$ are given constant symmetric real matrices, that is, $F_i = F_i{}^T$, $i = 0, \dots, n$, the inequality symbol $(> 0)$ in equation above means that $F(x)$ is positive definite.

The positive definite means that $u^T F(x)u > 0$ for all nonzero vector $u \in R^n$. The matrix inequality is linear in the variables $x_i$.

**Definition 2.7.2 [55]**: The Lyapunov inequality formulated as;

$$A^T P + PA < 0 \qquad \ldots(2.79)$$

where $A \in R^{n\times n}$ is a given matrix, and $X = X^T$ is the decision variable that can be expressed in the formula of LMI.

Let $P_1, P_2, \ldots, P_l$ be a basis for the symmetric $n \times n$ matrices, and $m$ computed as $(l = \frac{n(n+1)}{2})$.

By taking $F_0 = 0$ and $F_i = A^T P_i + P_i A$, that means basis for the vector space of $n \times n$ symmetric matrices with these conditions.

The symmetric matrices have arbitrary elements on both sides with respect to the diagonal. The number of elements on each side of the diagonal is determined as $(\frac{n(n-1)}{2})$. The number of diagonal elements be $n$. Therefore, the dimension of the vector space of all $n \times n$ symmetric matrices computed as;

$$(number\ of\ elements\ in\ each\ sid + number\ of\ diagonal\ elements)$$

$$\equiv \left(\frac{n(n-1)}{2} + n\right)$$

$$= \frac{n(n+1)}{2} \qquad \ldots(2.80)$$

That is, there are $(\frac{n(n+1)}{2})$ matrices in a basis for the vector space of $n \times n$ symmetric matrices. For example, for $n = 2$ there is a basis contains three matrices: $l_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, l_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, l_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

### 2.7.12 Some Drawbacks of the Previous Fuzzy Chaotic Cryptosystems and Knapsack Problem

From the previous system for fuzzy chaos-based cryptosystem, and from studying the Knapsack problem and previous cryptosystem by Chian and Kuang, we found that there are some drawbacks such:

- The fuzzy modeling technique couldn't extended to more general nonlinear system.
- The technique used with most well-known continuous and discrete-time chaotic systems that have at most two nonlinear terms such Henon Map.
- In Knapsack problem for increasing its security is under condition containing at least 250 items to choose from.
- In Knapsack problem the system could be work in somewhat more secure by iterating the modular multiplications in the method with different values of a multiplier $a$ and a modulus $N$, that selected as $N > 2a_n$, with $0 < a < N$, and $gcd(a, N) = 1$ .

# Chapter Three

# The Suggested Knapsack Fuzzy Chaos-Based Cryptosystem

## 3.1 Introduction

The suggested method we named it Knapsack Fuzzy Chaos-Based Cryptosystem (KFCC) works through three directions in decrypting the ciphertext, and recovering the message. First one is to apply the Knapsack inside the TS fuzzy chaotic system on a discrete-time chaotic system and recover the message through the algorithm of Knapsack problem as, and a second side is on a continuous-time chaotic system. While the other direction is to implement the Knapsack problem inside the TS fuzzy chaotic model as driver system for the TS fuzzy chaotic as response system. By achieving the synchronization between the drive-response system the error dynamic can be exactly linearized by exact linearization technique EL to ensure stability, so by solving the LMI problem it could recover the message.

The first suggested direction system could be performed on both 2D and 3D discrete-time or continuous-time chaotic systems that could be represented exactly by TS fuzzy model under some conditions. Firstly, we introduce the designing cryptosystem for discrete-time TS fuzzy chaotic systems. In same direction and under needs to improve system, we were modify the chaotic map by use it as seed map within the cosine map, and then within sine map, that also exact represented by TS fuzzy model, these performed on Lozi map. Later, we introduce a designing cryptosystem by implementing a 3D continuous-time that needs to be discretized (by any step time) and then represented by a TS fuzzy model, performed on Lorenz map, as will be seen in Numerical examples in Chapter 5.

In this work, the masking message by output of the TS fuzzy model state values for vector variables will depend, so it will focus on. The method adds an enhancement to the implementation of chaos based cryptosystem through designing the chaotic map as chaotification for cosine and sine functions to get cosine chaotic and sine chaotic maps, respectively, also using the knapsack method. The enhancement on key, by depending on a superincreasing sequence from the primitive variable trajectory.

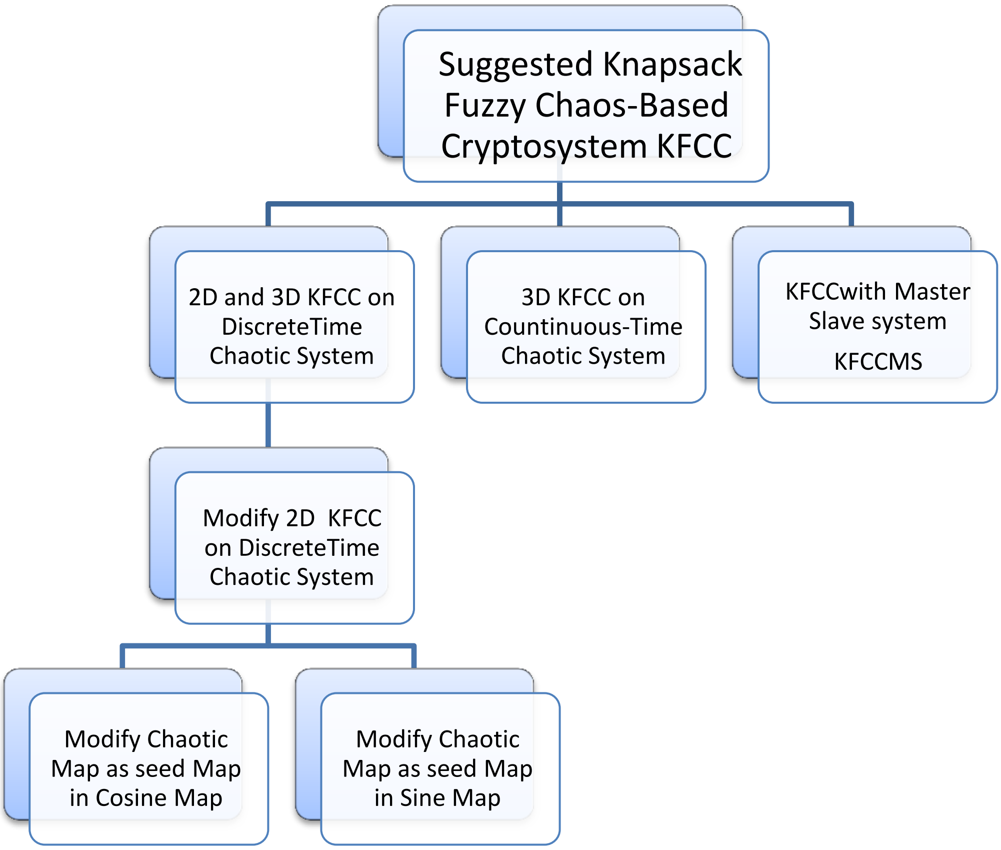

Suggested Knapsack Fuzzy Chaos-Based Cryptosystem KFCC
2D and 3D KFCC on DiscreteTime Chaotic System
3D KFCC on Countinuous-Time Chaotic System
KFCCwith Master Slave system KFCCMS
Modify 2D KFCC on DiscreteTime Chaotic System
Modify Chaotic Map as seed Map in Cosine Map
Modify Chaotic Map as seed Map in Sine Map

FIGURE 3.1: Diagram of the work on the suggested KFCC

## 3.2 The Knapsack Fuzzy Chaotic Cryptosystem

In this section, new contributions have been proposed to design an alternative versions of the Knapsack public key cryptosystem based on the TS fuzzy chaotic models as the Knapsack fuzzy chaotic system (KFCC). These models are discrete-time TS fuzzy model of 3D chaotic system (DTF-3DCS) and continuous-time TS fuzzy model of 3D chaotic system (CTF-3DCS). In designing the fuzzy chaotic cryptosystem, two types of the TS fuzzy models for the chaotic systems are determined, which are the discrete-time and continuous-time TS fuzzy models that are discussed as;

### 3.2.1 The TS Fuzzy Model for a 3D-Discrete Time Chaotic System

This model works on the discrete-time type with 2D or 3D, so generally it can refer by 3D. The aim of using the discrete-time TS fuzzy model is to get a trajectory of a point in the phase space of the chaotic system. The discrete-time fuzzy chaotic (DTFC) model is explained in the following steps:

Step 1: Suppose a 3D discrete-time chaotic system with a control input vector that is depended on the number of nonlinear equations of the chaotic system as input, or without the control input vector.

Step 2: Determining the primitive variables in a discrete-time chaotic system $x_1(t),\ x_2(t),\ x_3(t)$.

Step 3: Designing the TS fuzzy model through if-then rules of the of primitive variable values that gives a nonlinear property for the discrete-time chaotic system such, $x_1(t)$ on the interval $[-d, d]$.

Step 4: Evaluating the chaotic system parameters and the values of variables to get the chaotic system matrix at chaotic behavior. The iterations number could be determined by the user. In this work, the iterations number selected until 40 iterations.

Step 5: Calculating the values for iterations of the TS fuzzy chaotic system starting with initial values $x_1(0), x_2(0), x_3(0)$ at $t = 0$ to find the phase trajectory.

Step 6: Determining the output values that represent the trajectory for $x_1(t)$ in the phase trajectory.

The TS fuzzy model for the 3D discrete-time chaotic system can be shown in Figure (3.2).

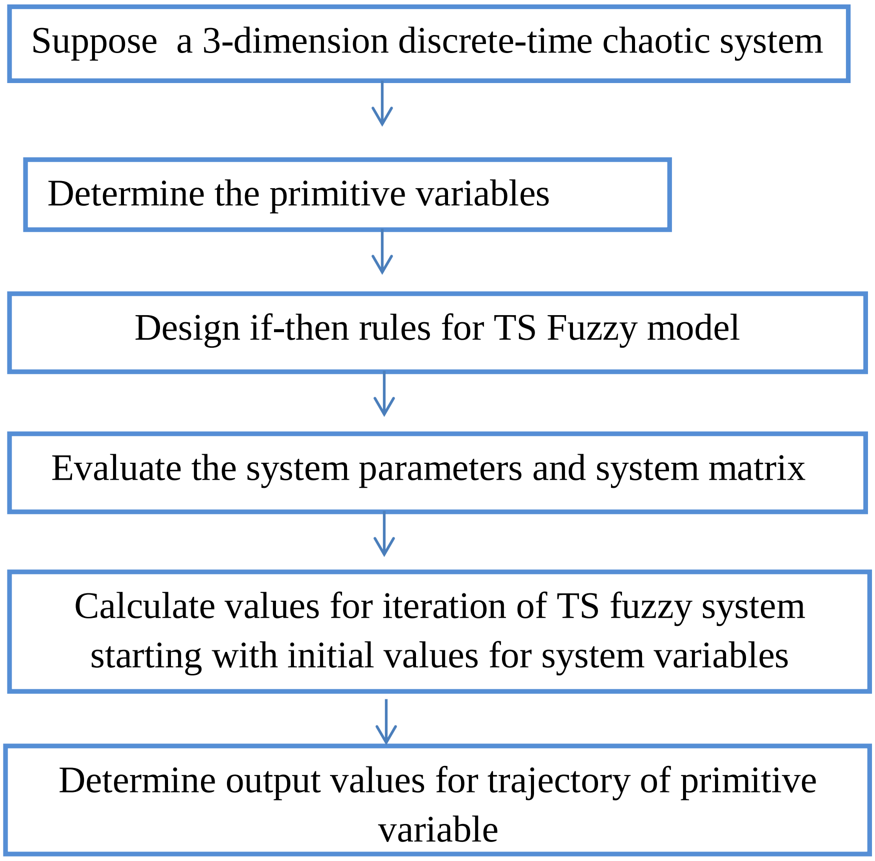

Suppose a 3-dimension discrete-time chaotic system
Determine the primitive variables
Design if-then rules for TS Fuzzy model
Evaluate the system parameters and system matrix
Calculate values for iteration of TS fuzzy system starting with initial values for system variables
Determine output values for trajectory of primitive variable

FIGURE 3.2: Designing the discrete-time TS fuzzy model for 3D-chaotic system

These steps can be explained in more details. Consider a class of discrete-time nonlinear control chaotic system with an input term expressed by

$$x(t+1) = f\big(x(t)\big) + g\big(x(t)\big)u(t) \qquad \ldots(3.1)$$

where $x(t) = [x_1(t) \ \ x_2(t) \ \ x_3(t)]^T \in R^3$, which is a state vector, the functions $f\big(x(t)\big)$ and $g(x(t)) \in R^3$are nonlinear vector functions defined on $x(t)$, a vector $u(t) \in R^m$ is a control input vector for $m$ dimension is determined based on the number of nonlinear equations in the chaotic system and $x(t+1)$ refers to the discrete case of the chaotic system. First the TS fuzzy model is composed for the rules as a set of fuzzy rules

$\boldsymbol{Plant\ Rule\ i}$: $IF\ x_1(t)\ is\ \Gamma_1^i\ and\ x_2(t)\ is\ \Gamma_2^i\ and\ x_3(t)\ is\ \Gamma_3^i$

$$THEN\ x(t+1) = D_i x(t) + E_i u(t),\ i\ =\ 1,2,\dots,q \qquad \dots(3.2)$$

where $(t+1)$ is an index of time steps, $q$ is the number of rules of this TS fuzzy model, $\Gamma_j^i$are fuzzy sets for $x_j(t)$ and $j = 1,2,3$, $D_i \in R^{3\times 3}$ is a discrete-time control system matrix, $E_i \in R^m$ is an input matrix. $x_1(t), x_2(t), x_3(t)$ are the premise variables which consist of the state values in states space for the system. The membership functions for fuzzy sets can be selected with any form, since the choosing of the membership function in this fuzzy sets will change in so little values that will not effect on the computed values, but in general it chosen as a triangular membership function**.**

These rules characterize local relation(s) of the chosen chaotic system in the state space. Mainly, the essential feature for TS model is expressed the local dynamics of each fuzzy implication through a linear state-space system. The fuzzy system is then modeled through fuzzy blending of the local linear system models by some appropriate membership functions.

In some applications, the discrete-time chaotic nonlinear control system is constructed without input term by

$$x(t+1) = f(x(t)) \qquad \dots(3.3)$$

where $x(t) \in R^3$ is the state vector and $f(x(t))$ is a nonlinear function with appropriate dimension defined on $x(t)$. The TS fuzzy model here is composed for the rules as:

$\boldsymbol{Plant\ Rule\ i}$: $IF\ x_1(t)\ is\ \Gamma_1^i\ and\ x_2(t)\ is\ \Gamma_2^i\ and\ x_3(t)\ is\ \Gamma_3^i$

$$THEN\ x(t+1) = D_i x(t) + b_i(t), \text{ for } i\ =\ 1,2,\dots,r \qquad \dots(3.4)$$

where $D_i \in R^{3\times 3}$ is a system matrix for $i\ =\ 1,2,\dots,r$, and $b_i(t) \in R^2$ which refers to the bias vectors.

It is important to note that the number of primitive variables is a number of variables that make the nonlinear terms in the chaotic system.

Whereas, the number of rules depends on a number of the fuzzy sets for the primitive variables values .

### 3.2.2 The Knapsack Discrete Time Fuzzy Chaotic Cryptosystem

In this section, the alternative Knapsack public key cryptosystem is proposed based on the 3D discrete-time TS fuzzy chaotic model as Knapsack fuzzy chaotic cryptosystem (3D-KDT-FCC).

The Knapsack problem easily is the input sets of positive integers that from the super-increasing sequences as discussed in Chapter (2). A fuzzy model, especially TS model is applied on Lorenz chaotic map, and a positive real super-increasing sequence, are employed to give an alternative hybrid version of Knapsack public key cryptosystem. The proposed 3D KDT-FCC processes that could employed on 2D are explained as follows;

### 3.2.3 The 3D-KDT-FCC: Key Generation Process

Using the primitive variable $x_1(t)$ in a vector variable $x(t) = [x_1(t), x_2(t), x_3(t)]^T$at nonlinear terms which is the output of TS fuzzy chaotic model for initial values and trajectory for primitive variable in interval $[-d, d]$, that generate a secure ephemeral key $k(t)$. The prative and public keys of 3D KDT-FCC are generated by Lemma (3.2.2.1.1).

**Proposition 3.1**: Suppose $x_1(t)$ is a primitive variable of a vector variable $x(t)$, where $x(t) = [x_1(t), x_2(t), x_3(t)]^T$. Then the keys of 3D-KFCC are $B$ and $(S, W, N)$, which consider as the public and private keys respectively.

Proof: Suppose a primitive variable $x_1(t) \in x(t) = [x_1(t), x_2(t), x_3(t)]^T$ at nonlinear terms which is the output of TS fuzzy chaotic model for initial values and trajectory for primitive variable in interval $[-d, d]$, that generate a secure ephemeral key $k(t)$, by

$$k(t) = [k(t-0), k(t-1), \dots, k(t-j+1)]$$

$$=[x_1(t-0), x_1(t-1), \dots, x_1(t-j+1)] \quad \dots(3.5)$$

Now a positive real valued super-increasing sequence $S_i$ for $i = 1, 2, \ldots, l$, is generated through the following computations as:

The terms of sequence are

$$S_1(t) = |k(t-1+1)| + \tau S_1(t) = |k(t)| + \tau$$

$$S_2(t) = |k(t-2+1)| + \tau = |k(t-1)| + \tau$$

$$S_3(t) = |k(t-3+1)| + \tau = |k(t-2)| + \tau$$

and so on until $S_j(t) = |k(t-j+1)| + \tau$.

In general, $S_1(t) = |k(t)| + \tau$, and

$$S_j(t) = \sum_{i=1}^{j-1} S_i(t) + |k(t-j+1)| + \tau \qquad \ldots(3.6)$$

for $j = 2, 3, 4, \ldots, l$ , and $\tau > 0$.

The super-increasing sequence $S = \{S_1, S_2, \ldots, S_l\}$ is computed secretly by first user.

Also he/she(first user) computes $S_1 + S_2 + \cdots + S_l = T$ and he/she chooses prime secret $N \ni N > T$.

Then, he/she selects $W \in [2, N-1]$ and $gcd(W, N) = 1$. This ensures that the element $W$ (prime secret) has a multiplicative inverse $(mod\ N)$. Later, first user computes the public hard Knapsack $B = \{\ b_1, \ldots, b_l\}$, with $b_i = WS_i(mod\ N)$, for $i = 1,2, \ldots, l$.

Finally, he/she keeps $(S, W, N)$ as his/her private key and $B$ as his/her public key. ■

For more implementation results, use Algorithm (31).

**Algorithm 3.1. The 3D-KDT-FCC: Keys Generation Process.**

**First user:**

**Input.** A positive integer $n$ and the vector variable $x(t) = [x_1(t), x_2(t), x_3(t)]^T$

**Output.** A private key $(S, W, N)$ and a public key $B$.

```
t=1
While $t < n$
    For $j = 0,1,2,\dots,l-1$
        Compute $k(t) = x_1(t-j+1)$ .
    End for
    $t = t+1$
End while
Return a secure ephemeral key $k(t) = [x_1(0)x_1(1),\dots,x_1(l-1)]$.
Selected randomly $\tau > 0$
Computes $S_1(t) = |k(t)| + \tau$
For $i = 2,3,\dots,l,$
    For $j = 2,3,4,\dots,l$
        Generates a super-increasing sequence
            $S_j(t) = \sum_{i=1}^{j-1} S_i(t) + |k(t-j+1)| + \tau$
    End for
End for
Return $S_j(t)$
Computes $S1 + S2 + \cdots + Sl = T$
Chooses randomly $N > T$
Selects $W$ in $[2, N-1]$, with $gcd(W,N) = 1$
    For $i = 1,2,\dots,l$
    Computes $b_i = WS_i(mod\ N)$
    End for
Return a public hard knapsack $B = \{b_1, b_2, \dots, b_l\}$
Return a private key $(S, W, N)$ and a public key $B$ .
```

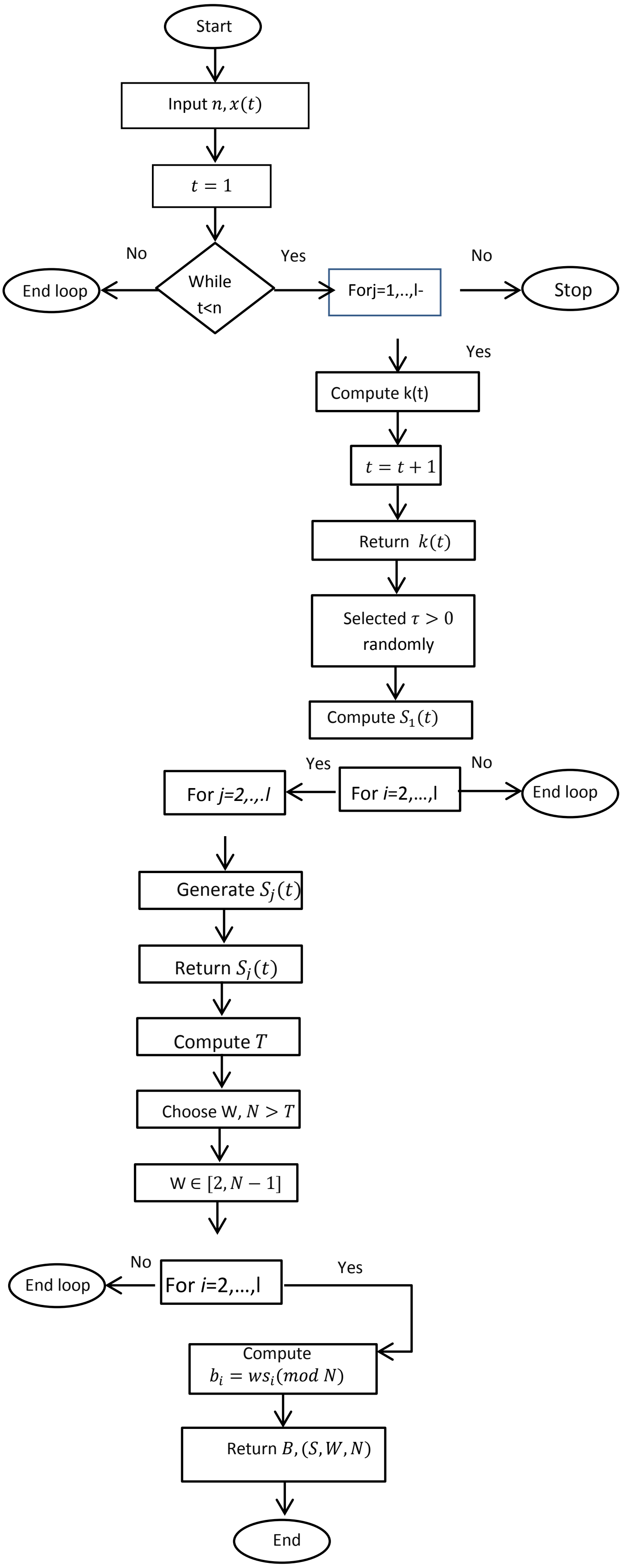


FIGURE 3.3: Diagram of the 3D-KDT-FCC keys generation process.

### 3.2.4 The 3D-KDT-FCC: Encryption Process

In encryption process, the second user wants to encrypt his/her plaintext $M$ which is a binary string. This string breaks up into $l$ blocks, each one consists of $s$ elements, namely $M = \{m_1, \dots, m_l\}$ with $m_i$ has length is equal to $s$, for all $i$. For each block $m_i$, the user computes

$$c_i = \sum_{j=1}^{l} m_{ij} b_j, \qquad \dots(3.7)$$

where $c_i$ is a ciphertext that corresponds to plaintext $m_i$.

So, the ciphertext $C = \{c_1, \dots, c_l\}$ for plaintext $M$, which considers as an encryption function. This function namely $C$ is modified into $\xi(t)$, that computed by

$$\xi(t) = \left(C - \frac{T}{2}\right) / \left(\frac{\gamma T}{2}\right) \qquad \dots(3.8)$$

where $\gamma$ is a small scalar makes $\xi(t) \in (-0.01, 0.01)$ . The ciphertext $\xi(t)$ will sends to the first user.

Algorithm (3.2) is used to compute several numerical results of the ciphertext of the proposed 3D-KDT-FCC.

**Algorithm 3.2. The 3D-KDT-FCC: Encryption process**

**Second user:**

**Input.** A public key $B = \{b_1, b_2, \dots, b_l\}$, a positive integer $s$, small real.

**Output.** The modified ciphertext $\xi(t)$

```
Chooses randomly the small real numbers $\gamma$ and $T$ in secret way.
A plaintext $M = \{m_1, \dots, m_l\}$ has been selected randomly, where $m_i \in \{0,1\}$ and the length of any $m_i$ is $s$.
For $i = 2, 3, \dots, l$.
    For $j = 1,2, \dots, s$.
        Compute $m_{ij} b_{ij}$
    End for
End for
Return $m_{ij} b_{ij}$
For $i = 2, 3, \dots, l$,
    For $j = 1,2, \dots, s$.
        Compute $c_i = \sum_{j=1}^{s} m_{ij}\, b_{ij}$
    End for
End for
Return the ciphertext $C = \{c_1, \dots, c_l\}$.
Computes modified ciphertext $\xi = (C - \frac{T}{2})/(\frac{\gamma T}{2})$
Return $\xi(t)$
```

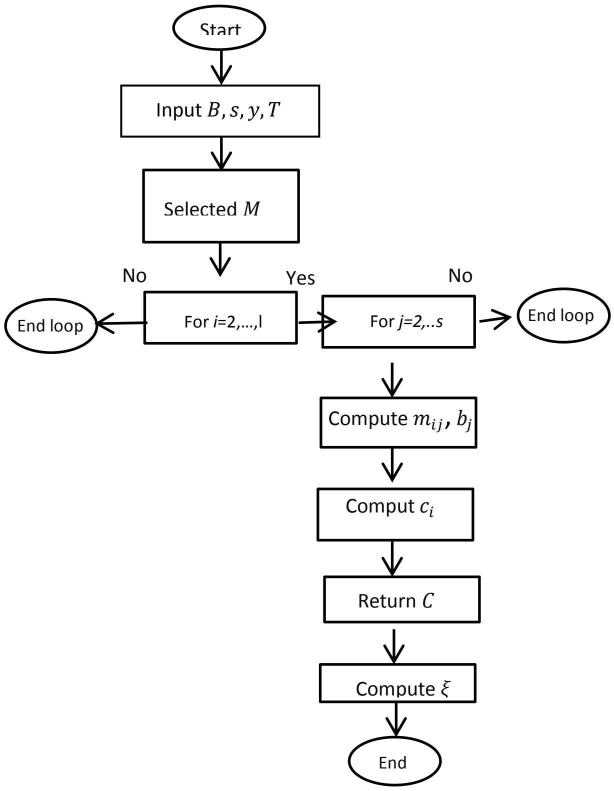


FIGURE 3.4: The diagram of 3D-KDT-FCC encryption process.

### 3.2.5 The 3D-KDT-FCC: Decryption Process

Upon receiving the ciphertext to first user, he/she tries to decrypt ciphertext $\xi(t)$ and recover the original plaintext by computing

$$C = (\gamma\xi(t) + 1)T/2. \qquad \ldots(3.9)$$

Then, he/she computes $v$ as a multiplicative inverse of $W$, namely $vW \equiv 1\ (mod\ N)$. Now, computing $vb_i \equiv S_i(mod\ N)$, for $i = 1,2, \ldots, n$, has been done. After that, a parameter $Z_i$, for each $c_i$, is computed by $Z_i \equiv vc_i(mod\ N)$.

If $Z_i < N$ and $N > T$, then the formula of finding a plaintext $M$ is;

$$Z_i = \sum_{j=1}^{n} m_{ij} S_j \qquad \ldots(3.10)$$

The decryption process of the 3D-KDT-FCC is proved by proposition (3.2).

**Proposition 3.2:** Suppose the modified ciphertext $\xi(t)$ of the ciphertext $C$ in the 3D-KDT-FCC is computed by

$$C = \frac{(\gamma\xi(t) + 1)T}{2}$$

where $\gamma$ is a small real number and $T$ is a public key.

Then, the original plaintext $M$ computed by

$$M = Z_i = \sum_{j=1}^{n} m_{ij} S_j$$

Proof: Since the first user receives $\xi(t)$ and he\she knows the value $T$, so the parameter $C$ is computed by

$$C = \frac{(\gamma\xi(t) + 1)T}{2} = \{c_1, \dots, c_l\}.$$

He\She computes the multiplies inverse $v$ of $W$.

Now, based on his\her private key computes

$$vb_i \equiv S_i (mod\ N), \text{ for } i = 1,2, \dots, n,$$

The parameter $Z_i$, is computed by

$$Z_i \equiv v \sum_{j=1}^{n} m_{ij} b_j \ (mod\ N)$$

$$\equiv \sum_{j=1}^{n} m_{ij}\ v\ b_j \ (mod\ N)$$

$$\equiv \sum_{j=1}^{n} m_{ij}\ \ S_j \ (mod\ N)$$

If $Z_i < N$ and $N > T$, then

$$M = Z_i = \sum_{j=1}^{n} m_{ij} S_j.$$

Otherwise, $M \neq Z_i$. ■

Algorithm (3.3) is used for more numerical results of the decryption process of the 3D-KFCC.

**Algorithm 3.3. The 3D-KFCC: Decryption process.**

**Input.** The ciphertext $\xi$ a small real number $\gamma, T$ and $N$

**Output.** Original plaintext $M$.

```
Compute $C = (\gamma\xi(t) + 1)T/2$
Compute $v$ through the relation $vW \equiv 1(modN)$
For $i = 2, 3, \dots, l$.
Compute $vb_i \equiv S_i(mod\ N)$
End for
  For $i = 2, 3, \dots, l$.
      For $j = 1,2, \dots, l$.
Compute $m_{ij}S_j$
      End for
  End for
Return $m_{ij}S_j$
For $i = 2, 3, \dots, l$.
      For $j = 1,2, \dots, l$.
Compute $Z_i = \sum_{j=1}^{n} m_{ij}S_j(modN)$.
      End for
  End for
  For $i = 1,2, \dots, l$.
 If $Z_i < N$ and $N > T$
      Then $M[i] = 1$ and $Z_i = Z_i - S_j$
         Else $M[i] = 0$
  End if
 If $Z_i = 0$ , Then Return (False and there is no solution).
         Else Return ($M[1], M[2], \dots, M[n]$).
 End if
End for
```

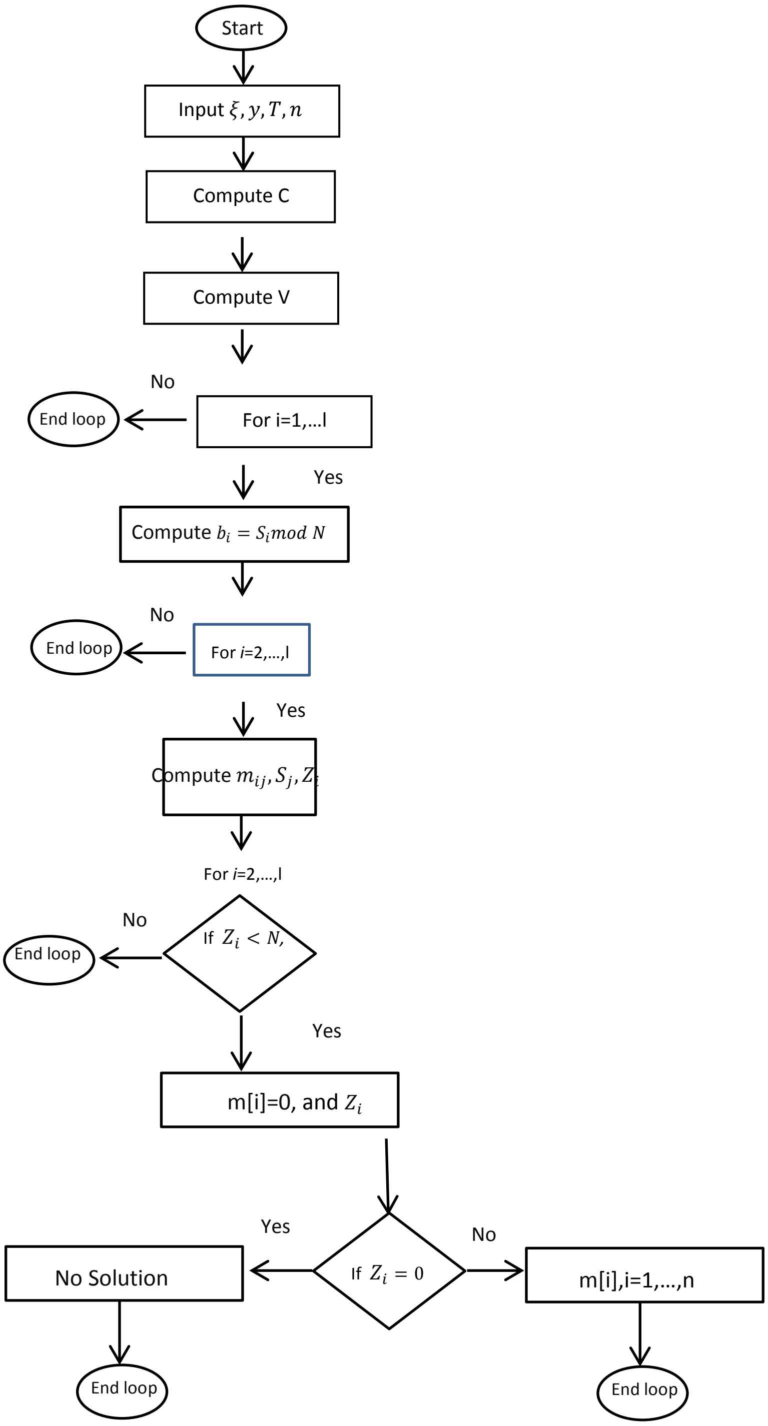


FIGURE 3.5: The Diagram of 3D-KDT-FCC decryption process .

Depending on the number of increasing terms in the super increasing sequence it could be determine the number of symbols in each term if it three, four , five or six as will see in the examples. Furthermore number of elements in plain text $M$.

## 3.3 Modify the 2D-KFCC with Continuous Map

The suggested method on discrete-time ward to study another cases for more robust security and complicated through hybrid two cases: first using chaotic map as a seed map in cosine map, and the second using chaotic map as a seed map in sine map in generation a secrete key .

### 3.3.1 The TS Fuzzy Model for Modify Chaotic System by Cosine and Sine Map

The TS fuzzy modeling of cosine chaotic systems for continuous-time and discrete-time TS fuzzy model will discussed here. Our work in this case focuses on the discrete-time type with two dimension. The idea is to use the discrete-time model to get a trajectory for point(s) in phase space of chaotic system for a prime variable. The reason for using this modification on based chaotic system in the fuzzy model, since there is not capably to modify the TS fuzzy model.

Details of the design and the algorithm for the fuzzy chaotic cryptosystem is explained in the following steps:

Step1: Suppose a 2-dimensional discrete-time chaotic system $x(t) = [x_1(t),\ x_2(t)]$.

Step2: Determine which the primitive variables in the system $x_1(t),\ x_2(t)$

Step3: Design the TS fuzzy model through if-then rules on values of primitive variable at the chaotic system such; $x_1(t)$ in $[-d, d]$.

Step4: Calculate the table values for iterations of the TS system implemented on initial values $x_1(0), x_2(0)$ to find the phase trajectory.

Step 5: Perform the cosine (sine) function alongside a chaotic map as a seed map.

Step 6: Formulate the resulted map cosine chaotic system on $x(t) = [x_1(t),$ $x_2(t)]$.

Step 7: Evaluate the parameters in the system and the values of variables to get the system matrix $D_i$.

Step 8: Determine the output values that represent the trajectory for $x_1(t)$ in the phase trajectory after $t$ iteration .

Consider a class of discrete-time nonlinear control system without input term constructed as in equation (3.3) but for $x(t) \in R^2$, $[x_1(t) \;\; x_2(t)]^T$ is the state vector and $f\big(x(t)\big) \in R^2$ is a nonlinear function with appropriate dimension defined on $x(t)$, where $(t+1)$ is an index of time steps in the discrete case of the system. The TS fuzzy model here is composed for the rules as a set of rules (fuzzy implications):

$\boldsymbol{Plant\ Rule\ i}$: $IF\ x_1(t)\ is\ \Gamma_1^i\ and\ x_2(t)\ is\ \Gamma_2^i$

$$THEN\ x(t+1) = A_i x(t) + b_i(t) \qquad \ldots(3.11)$$

for $i = 1, 2, \ldots, q$. The premise variables $x_1(t),\ x_2(t)$ consist of the state values in states space for the system, $q$ is the number of rules of this TS fuzzy model, $\Gamma_j^i$ are fuzzy sets for $x_j(t)$ and $j = 1,2$. $A_i \in R^{2\times 2}$ is a discrete-time control system matrix and $b_i(t) \in R$ denotes to the bias terms. The membership functions as in the first case are with any form since the choosing of the membership function in this fuzzy sets will change in so little values that will not effect on the computed values, but in general it chosen as triangular membership function**.**

These fuzzy rules characterize local relation(s) of the chosen system in the state space. Mainly, the essential feature for TS model is the expression of the local dynamics of each fuzzy implication through a linear state-space system model. The fuzzy system is then modeled through fuzzy blending of the local linear system models by some appropriate membership functions.

### 3.3.2The TS Fuzzy Chaotic Model for Generating the Secret Keys

The initial values $x(t)$ for vector states considers as an input to the system. From the vector variable $x(t) = [x_1(t) \quad x_2(t)]^T$, the $x_1(t)$ is to be the output that is used to generate a secure ephemeral key $k(t)$. In the other words, first user computes the key $k(t)$ by form (3.5), and he/she computes

$$cos\big(x_1(t)\big) = [\cos(x_1(t-0)), \quad \cos(x_1(t-1)), \quad \cdots, \quad \cos(x_1(t-j+1))] \quad \ldots(3.12)$$

Symbolize the vector for the absolute values as

$$\big|cos\big(x_1(t)\big)\big| = [|\cos(x_1(t-0))|, \quad |\cos(x_1(t-1))|, \quad \cdots, \quad |\cos(x_1(t-j+1))|] \quad \ldots(3.13)$$

But at using sine map the computing keys,

$$sin\big(x_1(t)\big) = [sin(x_1(t-0)), \quad sin(x_1(t-1)), \quad \cdots, \quad sin(x_1(t-j+1))] \quad \ldots(3.14)$$

Now, a super-increasing sequence $S_i$, for $i = 1, 2, \ldots, l$, that generated for cosine as:

$$S_1(t) = |cos(x_1(t-0))| + \tau, \text{ and ;}$$

$$S_j(t) = \sum_{i=1}^{j-1} S_i(t) + |\cos(x_1(t-j+1))| + \tau \quad \ldots(3.15)$$

And for sine as:

$$S_1(t) = |sin(x_1(t-0))| + \tau, \text{ and ;}$$

$$S_j(t) = \sum_{i=1}^{j-1} S_i(t) + |\sin(x_1(t-j+1))| + \tau \quad \ldots(3.16)$$

Then the sequence is

$$\{|s(t-0)|, \quad |s(t-1)|, \quad \cdots, \quad |s(t-j+1)|\} \quad \ldots(3.17)$$

Now, a super-increasing sequence $S_i$, for $i$ =1, 2, ..., $l$, is generated easily $S_1(t) = |s(t)| + \tau$, and the j-th item be as;

$$S_j(t) = \sum_{i=1}^{j-1} S_i(t) + |s(t-j+1)| + \tau \quad \ldots(3.18)$$

for $j = 2, 3, \ldots, l$ and $\tau > 0$. The absolute values here ensure that all the terms in the sequence are positive though the positive real super-increasing sequence $S = \{ S_1, S_2, \dots, S_l \}$ which are computed secretly. Also, a first user computes $T = \sum_{j=1}^{l} S_j$, and will chooses $N > T$. Then a parameter $W$ selects from $[2, N-1]$ and $gcd(W, N) = 1$. That is, $W$ and $N$ are relatively prime to ensure that $W$ has multiplicative inverse $modN$. First user computes a public hard knapsack $B = \{ b_1, b_2, \dots, b_l\}$, where $b_i = WS_i(mod\, N)$ for $i = 1,2, \dots, l$. Finally, $(S, W, N)$ are keeping as a private key and $B$ as public key.

### 3.3.3 Encryption Stage to Generate the Ciphertext

Assume that the other user(s) would encrypt the plaintext $M$ and send the ciphertext to first user, by choose a binary plaintext $M$ breaks up into $l$ sets each of $t$ elements long, namely $M = \{m_1, \dots, m_l\}$. For each set $m_i \in \{0,1\}$ from message. Now, compute

$$c_i = \sum_{j=1}^{t} m_{ij} b_j \qquad \dots(3.19)$$

where $c_i$ is a ciphertext that corresponds to the plaintext $n_i$. So the ciphertext for a plaintext $M$ is $C = \{c_1, \dots, c_l\}$, Next, the second user will modify the encryption function into $\xi(t)$ as another formulation for equation (3.8), to be as;

$$\xi(t) = \left(\frac{2C-T}{\gamma T}\right) \qquad \dots(3.20)$$

for a scalar $\gamma$ with $\xi(t) \in (-0.01, 0.01)$. The user will publishes the modified form $\xi(t)$ and $\gamma$ into public channel, to first user for decryption.

The proposed cryptosystem is mainly used the TS fuzzy model that is employed using a chaotic map. Using one state from the vector variable $x(t) = [x_1(t) \;\; x_2(t)]^T$ to be the output that uses to generate the secure key $K(t)$ in the system.

### 3.3.4 Decryption Stage for the Suggested System

At this stage the first user receives the values $\xi(t)$and $\gamma$ and he/she will try to recover ciphertext $C$ through implementing the steps:

Step 1: The user know the value T.

Step 2: Demodify ξ(t) into the form (3.9).

Step 3: Compute $v$ as a multiplicative inverse for $W\,mod\,N$, as; $vW \equiv 1(mod\ N)$

Through the connection between hard and easy knapsacks which could be defined as; $vb_i = S_i(mod\ N)$, For $i = 1, \dots, n$

Step 4: Calculate $Z_i$ for each $c_i$,by applying the form ; $Z_i = vc_i(mod\ N)$

By substituting the values of $c_i$, the form be

$$Z_i = v\sum_{j=1}^{n} n_{ij}\, b_j(mod\ N) = \sum_{j=1}^{n} m_{ij}\, vb_j(mod\ N)$$

$$Z_i = \sum_{j=1}^{n} m_{ij}\, S_j(mod\ N) \qquad \dots(3.21)$$

Step 5: Testing condition: if that $Z_i < N$ and $N > T$, then the formula for finding plaintext

$$Z_i = \sum_{j=1}^{n} m_{ij}\, S_j \qquad \dots(3.22)$$

Step 6: Applying the polynomial time algorithm since $S$ is an easy Knapsack.

## 3.4 The Continuous Time TS Fuzzy Chaotic Model

The designing of the continuous time TS fuzzy chaotic model somewhat different on the previous model in Sections (3.1,3.2), the steps are :

### 3.4.1 The TS Fuzzy Chaotic Model Design for 3D-Countinuous Chaotic System

The work with the continuous-time type of 3D, is firstly to use the continuous-time TS fuzzy chaotic model and then discretize it to the discrete-time TS fuzzy chaotic model theoretically presented to get a trajectory of a point in the phase space of the chaotic system. The continuous-time fuzzy chaotic model is explained in the following steps :

Step 1: Suppose a 3-dimensional continuous-time chaotic system.

Step 2: Determining the primitive variables in a fuzzy chaotic system $x_1(t),\ x_2(t),\ x_3(t)$

Step 3: Designing the continuous-time TS fuzzy model through if-then rules of the of primitive variable values that gives a nonlinear property for the chaotic system such, $x_1(t)$ on the closed interval $[-d, d]$.

Step 4: Evaluating the parameters in the fuzzy chaotic model and the values of variables to get the system matrix.

Step 5: Discretizing the continuous-time TS fuzzy model, through suppose $T_s$ second as a sampling time value that discrete the time and to get a new system matrix for discrete –time version from continuous TS fuzzy model.

Step 6: Calculating the values for iteration of the TS fuzzy chaotic model starting with initial values $x_1(0),\ x_2(0),\ x_3(0)$ at $t = 0$ to find the phase trajectory.

Step 7: Determining the output values that represent the trajectory for $x_1(t)$ in the phase trajectory as a table.

For a continuous-time TS fuzzy model, consider a class of continuous-time nonlinear control system with an input term as;

$$\dot{x}(t) = f\big(x(t)\big) + g\big(x(t)\big)u(t) \qquad \ldots(3.23)$$

where $x(t) \in R^3$, $[x_1(t)\ \ x_2(t)\ \ x_3(t)]^T$ is the state vector and $f\big(x(t)\big), g(x(t)) \in R^3$ are nonlinear vector function with appropriate dimension defined on $x(t)$. $u(t) \in R^m$ is the control input vector for $m$ is a number of nonlinear equations in the system. $\dot{x}(t)$ is refer to the continuous case of the system. The TS fuzzy model here is composed for the rules as a set of rules (fuzzy implications) :

$\boldsymbol{Plant\ Rule\ i}$: $IF\ x_1(t)\ is\ \Gamma_1^i\ and\ x_2(t)\ is\ \Gamma_2^i\ and\ x_3(t)\ is\ \Gamma_3^i$

$$THEN\ \dot{x}(t) = A_i x(t) + B_i u(t) \qquad \ldots(3.24)$$

for $i = 1, 2, \ldots, q$. where $q$ is the number of rules of this TS fuzzy model, $\Gamma_j^i$ are fuzzy sets for $x_j(t)$ and $j = 1,2,3$. $A_i \in R^{3\times3}$ is a continuous-time control system matrix, and $B_i \in R^m$ is the input matrix. These rules characterize local relation(s) of the chosen system in the state space.

Mainly, the essential feature for TS model is expressing the local dynamics of each fuzzy implication through a linear state-space system model. The fuzzy system is then modeled through fuzzy blending of the local linear system models by some appropriate membership functions.

For a discrete-time TS fuzzy model, a discrete-time nonlinear control system as considered as in form (3.1), with $(t+1)$ is index of time steps. The discrete-time TS fuzzy model is constructed in form of rules (3.2), that we need to convert the model to it.

### 3.4.2. Converting the Continuous-Time TS Fuzzy Model into a Discrete-Time

Some applications of TS fuzzy model require converting the continuous model into the discrete model through discretization such as continuous-time for Rossler's system, Chua's circuit, and chaotic Lorenz system. This converting will employ on the continuous-time for chaotic Lorenz system as will be seen later in the experiments. For the discretization process Theorem (3.1) can be applied for the process. This theorem is stated by;

**Theorem 3.1** [2]: A continuous-time TS fuzzy model with a continuous-time plant rule $i$ is

$\boldsymbol{Plant\ Rule\ i}$: $IF\ x_1(t)\ is\ \Gamma_1^i\ and\ \ldots\ and\ x_n(t)\ is\ \Gamma_n^i$

$$THEN\ \dot{x}(t) = A_i x(t) + B_i u(t) \qquad \ldots(3.25)$$

could be converted into the discrete-time TS fuzzy model with a discrete-time plant rule $i$ which is given by

$\boldsymbol{Plant\ Rule\ i}$: $IF\ x_1(t)\ is\ \Gamma_1^i\ and\ \ldots\ and\ x_n(t)\ is\ \Gamma_n^i$

$$THEN\ x(t+1) = D_i x(t) + E_i u(t) \qquad \ldots(3.26)$$

where $D_i = exp(A_i T_s) = I + A_i T_s + {A_i}^2 \frac{{T_s}^2}{2!} + \cdots,$ $\ldots(3.27)$

$$E_i = \int_0^{T_s} exp(A_i \tau)B_i d\tau = (D_i - I){A_i}^{-1} B_i \qquad \ldots(3.28)$$

and $T_s$ is the sampling time step.

Proof: The complete proof  can be seen in [2]

### 3.4.3 The 3-Dimension Knapsack Fuzzy Chaotic Cryptosystem (3D-KFCC) for Continuous Chaotic Map

An easy Knapsack problem with inputs as sets of positive integers as super-increasing sequences. For more details about the Knapsack cryptosystem, one can see [57]. Alternative version of the Knapsack cryptosystem has been proposed in this work. This version employed the fuzzy model, especially TS model applied on Lorenz chaotic map, and a positive real super-increasing sequence.

### 3.4.4 The 3D-KFCC Key Generation Process

Using $x_1(t)$ in vector variable at nonlinear terms $x(t) = [x_1(t)\ \ x_2(t)\ \ x_2(t)]^T$, as the output to generates a secure key $k(t)$. Here the user will computes the key $k(t)$ by using the same form in (3.5).

A super-increasing sequence $S_i$, for $i\ = 1, 2, . . . , l$, is generated through the computations: $S_1 = |k(t)| + \tau$, and the equation (3.6).

Now, the super-increasing sequence $S = \{S_1, S_2, \dots, S_l\}$ computed secretly.

Also, the first user computes $S_1 +\ S_2\ \dots +\ S_l = T$, and he/she chooses $N > T$.

Later, selects $W$ in closed interval $[2, N - 1]$ and $gcd(W, N) = 1$. $W$and $N$ are prime numbers, ensuring $W$ has multiplicative inverse $mod\ N$. First user computes public hard knapsack $B = \{\ b_1, \dots, b_l\}$, with;

$$b_i = WS_i(mod\ N), \text{ for } i = 1,2, \dots, l.$$

Finally, he/she keeps $(S, W, N)$ as a private key and $B$ as public key, these all through using Algorithm (3.1).

### 3.4.5 The 3D-KFCC Encryption Process

Assume that second user would like to encrypt his/her plaintext $M$ which is a binary string. This string breaks up into $l$ sets each one consists $s$ elements, namely $M = \{m_1, \dots, m_l\}$. For each set $m_i$, the user computes $c_i = \sum_{j=1}^{l} m_{ij} b_j$, where $c_i$ is a ciphertext that corresponds to plaintext $m_i$. So the ciphertext for plaintext $M$ is $C = \{c_1, \dots, c_l\}$, where $C$ is an encryption function. Next, the second user will modify the encryption function $C$ into $\xi(t)$ by using the form (3.8),with keep on using the scalar $\gamma$ with small value making $\xi(t) \in (-0.01, 0.01)$.

The ciphertext $\xi(t)$ will sends to the first user. All steps are in Algorithm (3.2).

### 3.4.6 The 3D-KFCC Decryption Process

At this stage first user try recovering ciphertext $\xi(t)$ by computing $C$. Next, he/she computes $v$ as multiplicative inverse of $W$ by formula $vW \equiv 1\ (mod\ N)$. Now, the connection of easy and hard knapsack problems is by computing;

$$vb_i \equiv S_i(mod\ N), \qquad \text{for } i = 1, 2, \dots, n\ . \qquad \dots(3.29)$$

Later $Z_i$, for each $c_i$ is computed by; $Z_i \equiv vc_i(mod\ N)$.

Substituting the value $c_i$ ;

$$Z_i = v \sum_{j=1}^{n} m_{ij} b_j (mod\ N) = \sum_{j=1}^{n} m_{ij} v b_j (mod\ N) \qquad \dots(3.30)$$

Testing conditions if that $Z_i < N$ and $N > T$. Then the formula to find the plaintext $M$ has been as summation bellow;

$$Z_i = \sum_{j=1}^{n} m_{ij} S_j (mod\ N) \qquad \dots(3.31)$$

The Algorithm (3.3) is used for more implementing numerical results for decrypting process of the 3D-KFCC.

## 3.5 Designing the Discrete Time Knapsack Fuzzy Chaotic Cryptosystem with Master Slave System (KFCCMS)

This Section presented as a complementation to work on another direction, that through implementing KFCC with Master Slave system as KFCCMS. That inside the TS fuzzy chaotic model as a driver system for the TS fuzzy chaotic model and also as a response system in decrypting the ciphertext. Achieving the synchronization signal with feedback gains between the drive-response system means that the error dynamic can be exactly linearized by exact linearization technique EL to ensure stability, so by solving the LMI problem it could recover the message this model designed for 2D discrete-time chaotic systems.

The design started in similar manner to the first direction in Section 3.2, so the idea and algorithms are the same. Second direction started depending on the Knapsack problem to encrypt the message but not in the decryption of it. Decryption of the message by the suggested Knapsack Fuzzy Chaotic in fuzzy chaos based synchronization**.**

The fuzzy chaotic model based-cryptosystem here used to enhance and prove some advantages ; that is the ciphertext is embedded in output of TS fuzzy chaotic model in the drive system. Different values are used as the states values, some other values as a masking the plaintext, and other for estimated values. Synchronization is achieved between fuzzy chaotic drive and response systems in cryptosystem with error converge to zero.

A multi users are capable to employ this cryptosystem. The systematic design with high level of security .

Figure (3.6, 3.7) show the diagram of KFCCMS and Knapsack problem with fuzzy chaos cryptography, respectively .

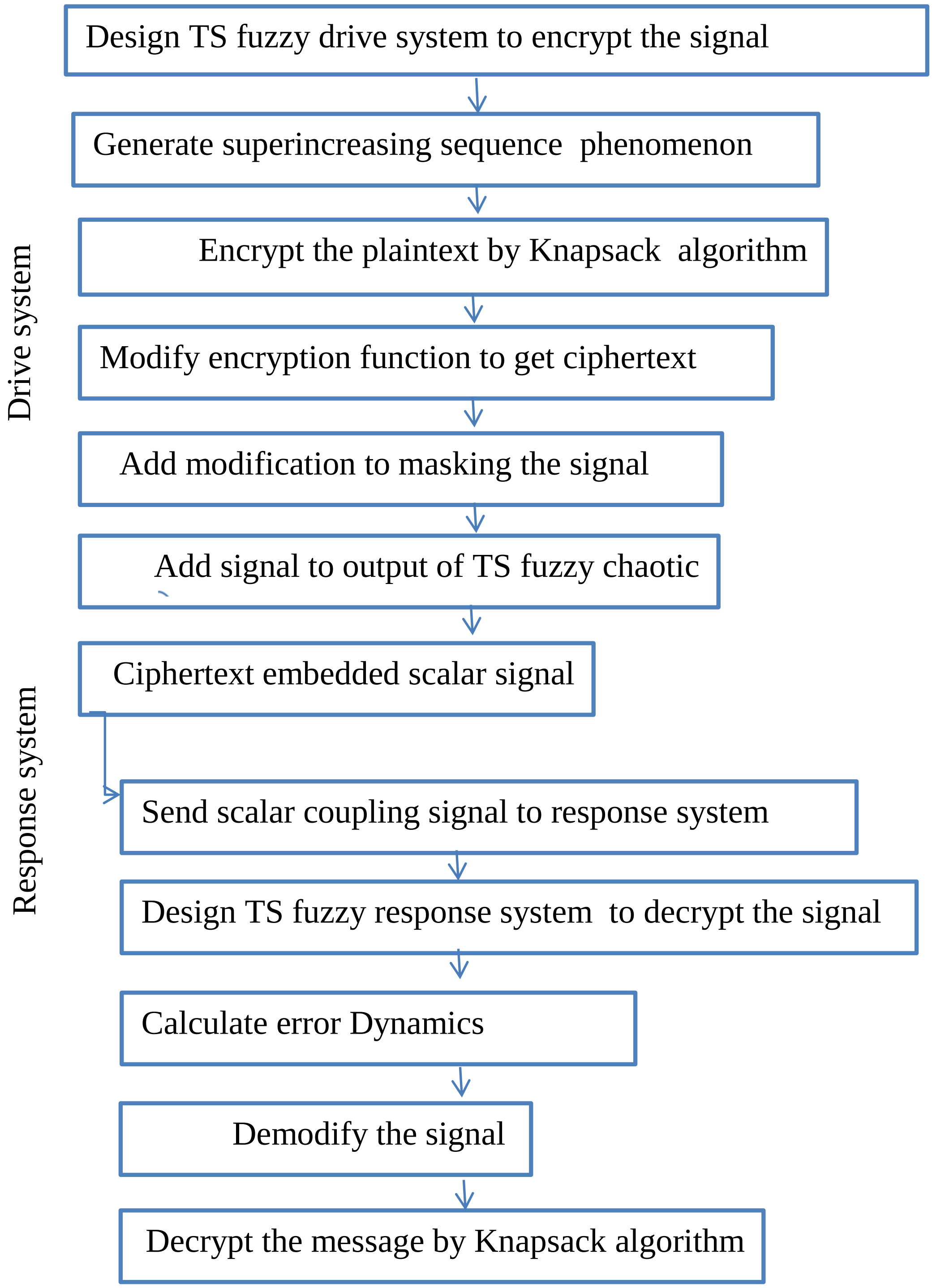

Design TS fuzzy drive system to encrypt the signal
Generate superincreasing sequence phenomenon
Encrypt the plaintext by Knapsack algorithm
Modify encryption function to get ciphertext
Add modification to masking the signal
Add signal to output of TS fuzzy chaotic
Ciphertext embedded scalar signal
Send scalar coupling signal to response system
Design TS fuzzy response system to decrypt the signal
Calculate error Dynamics
Demodify the signal
Decrypt the message by Knapsack algorithm
Drive system
Response system

FIGURE 3.6: Chaotic cryptography with Knapsack

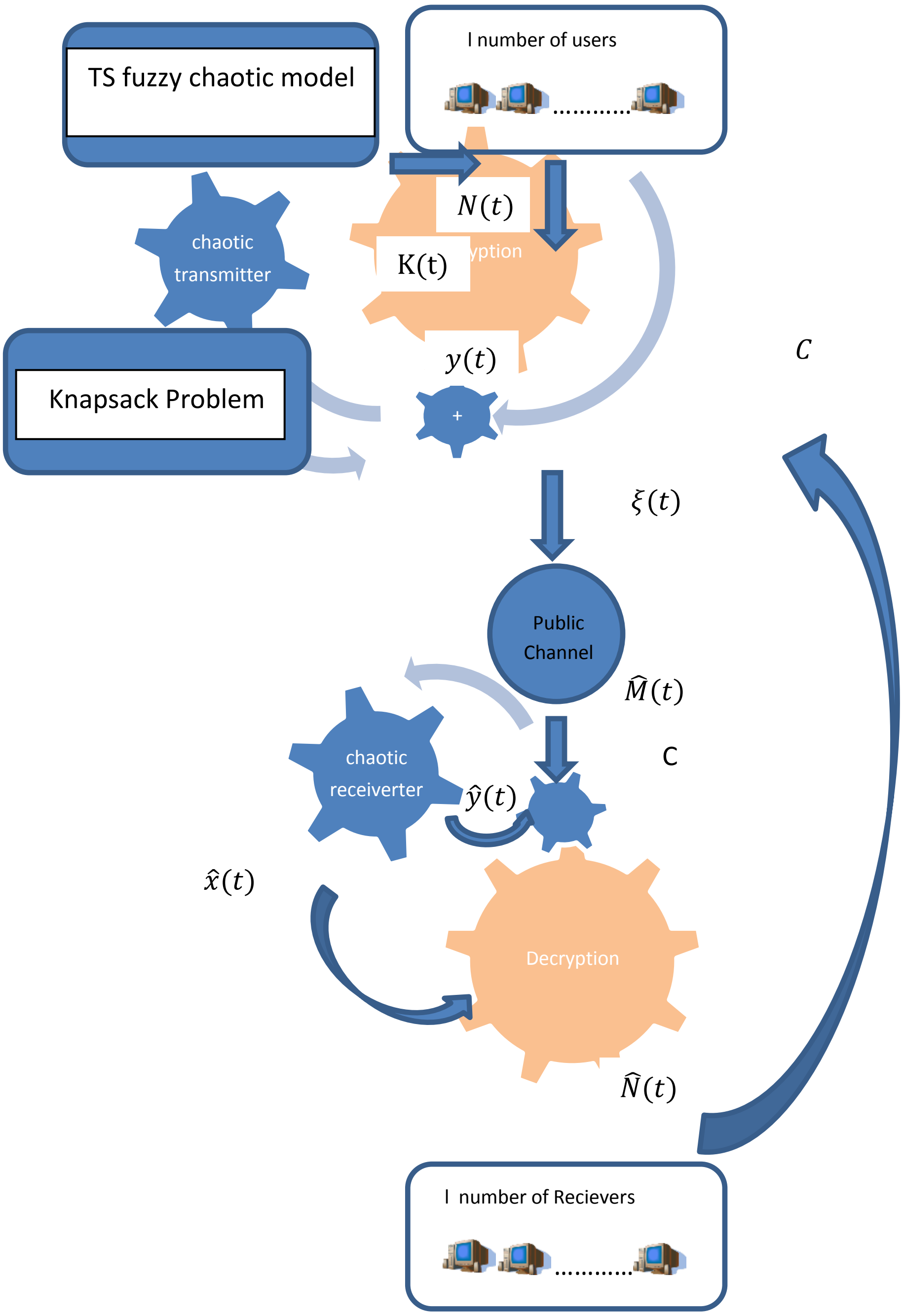


FIGURE 3.7: Chaotic cryptography with Knapsack

### 3.5.1The TS Fuzzy Model Design as Master System for 2D or 3D Discrete Chaotic System

Designing the TS fuzzy modeling as a master system for the chaotic system(s) is the same for the chaotic system in Section (3.2). The 2D discrete-time TS fuzzy model is supposed since the cryptosystems works on with this type and with 3D and determine the primitive variable from the variables $x_1(t), x_2(t) \in R$ at $t = 0$.

The stages of designing KFCC with discrete-time chaotic system with 2D started as

### 3.5.2 The 2D or 3D Knapsack Fuzzy Chaotic Cryptosystem Generation Process (2D-KFCC) or (3D-KFCC)

Knapsack problem with inputs as sets of positive integers as super-increasing sequences. This version employed the fuzzy model, especially TS model applied on a chaotic map, and a positive real super-increasing sequence.

### 3.5.3 The KFCC Key Generation Process as Output of TS Fuzzy Model

In same steps for first direction to employ the Knapsack for TS fuzzy model it will done here. In most Lure type discrete time chaotic systems, the primitive variable is $x_1(t)$ in vector variable $x(t)$ at nonlinear terms, as the output of TS fuzzy chaotic model in interval $[-d, d]$, that generate key $k(t)$. User will compute $k(t)$ by equation (3.5).

A positive real valued super-increasing sequence $S_i$, for $i = 1,2, \dots, l$, will generated as equation (3.6). The super-increasing sequence $S = \{S_1, S_2, \dots, S_l\}$ computed secretly. Compute the summation of terms T as;

$$T = S_1 + S_2 + \cdots + S_l$$

and chooses $N > T$.

Select $2 \leq W \leq N - 1$ and $gcd(W, N) = 1$. $W$ and $N$ are prime numbers, ensuring $W$ has multiplicative inverse $modN$.

First user will computes public hard knapsack $B = \{ b_1, \dots, b_l\}$, with $b_i = WS_i(modN)$, for $i = 1,2, \dots, l$.

Finally, $(S, W, N)$ is a private key must kept securely, and $B$ is a public key shared through public channel. See Algorithm ( 3.1) .

### 3.5.4 The KFCC Encryption Process

The second user would encrypt the plaintext $M$ which with a binary string breaks up into $l$ sets each one consists $s$ elements, say $M = \{m_1, \dots, m_l\}$. For each set $m_i$ compute $c_i = \sum_{j=1}^{l} m_{ij} b_j$, where $c_i$ is a ciphertext that corresponds to plaintext $m_i$. So the ciphertext for plaintext $M$ is $C = \{c_1, \dots, c_l\}$, where $C$ is an encryption function.

Next, another user will modify the encryption function $C$ to $\xi(t)$ as in equation (3.8), with $2C - T > 0$, or $2C > T$, more accuracy, $C > \frac{T}{2}$. For $\gamma \in R$ , is small scalar makes $\xi(t) \in (-0.01, 0.01)$. The ciphertext $\xi(t)$will sends to the first user. Algorithm (3.2) introduced all steps. A plaintext $M = \{m_1, \dots, m_l\}$ were selected, with each $m_i \in \{0,1\}$, and the length of any $m_i$ is $\boldsymbol{s}$.

### 3.5.5 Design the TS Fuzzy Driver System for Knapsack Problem with Fuzzy Chaos Cryptography

Designing the TS fuzzy model driver system as a fuzzy chaotic transmitter, to recover the signal from synchronization between the drive (master) and the response (slave) system. $\xi(t)$ will add to the masking signal and send a scalar coupling signal to the slave. That is the ciphertext is added directly into the output of the chaotic system to be masked.

To carry out the modulation process the masking signal is injected into the chaotic transmitter that expressed as a TS fuzzy model transmitter;

To extract the transmitter from the primitive variable say $x_1(t)$ from $x_1(t)\ \ x_2(t)$

$\boldsymbol{Rule\ i}: IF\ x_1(t)\ is\ \Gamma_i$

$$THEN\ x(t+1) = D_i x(t) + b_i(t) + L_i M \xi(t) \qquad \dots(3.32)$$

with the masking mechanism by rule ;

$\boldsymbol{Masking\ Rule\ i}: IF x_1(t)\ is\ \Gamma_i$

$$THEN\ \bar{y}(t) = \hat{C}x(t) + \widehat{M}\xi(t),\ i\ =\ 1,2,\dots,r \qquad \dots(3.33)$$

$\bar{y}(t)$ is the coupling masked signal, and $\widehat{M} \in R$, is the public output masking key, which masks the ciphertext by a constant value and could be set by the user. So the transmitters rules could be extracted depending on $\bar{y}(t)$ as

$\boldsymbol{Tranmitter\ Rule\ i}$: $IF\ \bar{y}(t)\ is\ \Gamma_i$

$$THEN\ x(t+1) = D_i x(t) + b_i(t) + L_i \widehat{M} \xi(t) \qquad \ldots(3.34)$$

$$\bar{y}(t) = \hat{C}x(t) + \widehat{M}\xi(t), \qquad i = 1, 2, \ldots, r$$

where $L_i, i = 1,2, \ldots, r$ are gain matrices to be determined later, The masked signal and the embedded message is sent to the fuzzy chaotic receiver.

It can note that the value of $\widehat{M} \neq 0{,}1$, also could added the complexity or simplicity to the work.

The overall fuzzy inferred result for the fuzzy chaotic transmitter system is derived by

$$x(t+1) = \sum_{i=1}^{r} \mu_i\big(\bar{y}(t)\big) \{\bar{D}_i x(t) + b_i(t) + L_i \bar{y}(t)\} \qquad \ldots(3.35)$$

$$\bar{y}(t) = \hat{C}x(t) + \widehat{M}\xi(t) \quad \ldots(1)$$

for $i = 1, 2, \ldots, r$

where $\bar{D}_i = D_i - L_i\hat{C}$, and $y(t)$ as the output of the drive system $\widehat{M}$ which do not chosen equal to 1, since it means nothing with the value 1.

$$\widehat{M} = \frac{\bar{y}(t) - \hat{C}x(t)}{\xi(t)} \qquad \ldots(3.36)$$

If $\widehat{M} = 1$, then the ciphertext be

$$\xi(t) = \bar{y}(t) - \hat{C}x(t) \qquad \ldots(3.37)$$

### 3.5.6 Design a TS Fuzzy Response System for Knapsack Problem with Fuzzy Chaos Cryptography

To recover the ciphertext that masked by the output of fuzzy chaotic system. The TS fuzzy chaotic response (receiver)system is designed with signal masking $\bar{y}(t)$ as;

$\boldsymbol{Responser\ Rule\ i}$: $IF\ \bar{y}(t)\ is\ \Gamma_i$

$$THEN\ \hat{x}(t+1) = D_i\hat{x}(t) + b_i(t) + L_i(\bar{y}(t) - \hat{y}(t)) \quad ...(3.38)$$

$$\hat{y}(t) = \hat{C}\hat{x}(t),\ \ i = 1, 2, \ldots, r$$

where $\hat{x}(t)$, and $\hat{y}(t)$ is denote the estimate for state $x(t)$, and output $\hat{y}(t)$, respectively. The overall fuzzy receiver inferred result for the fuzzy chaotic receiver system is formed as;

$$\hat{x}(t+1) = \sum_{i=1}^{r} \mu_i\big(\bar{y}(t)\big)\{D_i x(t) + b_i(t) + L_i(\bar{y}(t) - \hat{y}(t)\} \quad \ldots(3.39)$$

$$\hat{y}(t) = \hat{C}\hat{x}(t), \qquad i = 1, 2, \ldots, r$$

**Theorem 3.2:** The ratio between the estimated value $\hat{y}(t)$ and estimated value $\hat{x}(t)$ for the vector variables is equal to the coupled $\hat{C}$ vector for vector variables, and equal to $\frac{\bar{y}(t)-\hat{C}x(t)}{\xi(t)}$, if $\widehat{M} = 1$ .

**Proof:** From the equation (4.3) of transmitter rule as

$$\bar{y}(t) = \hat{C}x(t) + \widehat{M}\xi(t)$$

Modify respect to $\widehat{M}$

$$\widehat{M} = \frac{\bar{y}(t) - \hat{C}x(t)}{\xi(t)}$$

if $\widehat{M} = 1$, then

$$\xi(t) = \bar{y}(t) - \hat{C}x(t)$$

Modify respect to $\hat{C}$ from

$$\hat{C}x(t) = \bar{y}(t) - \xi(t)$$

So the vector

$$\hat{C} = \frac{\bar{y}(t) - \xi(t)}{x(t)} \qquad \dots(3.40)$$

From the equation (4.7 ) of the response system and rules

$$\hat{y}(t) = \hat{C}x(t)$$

Modify respect to $\hat{C}$ also,

$$\hat{C} = \frac{\hat{y}(t)}{\hat{x}(t)} \qquad \dots(3.41)$$

End of first part of the proof.

From equations (4.9) and (4.10), we get the second part of proof ,

$$\frac{\bar{y}(t) - \xi(t)}{x(t)} = \frac{\hat{y}(t)}{\hat{x}(t)}$$

■

**Theorem 3.3:** The estimated value $\hat{y}(t)$ and the coupling masked signal $\bar{y}(t)$ to be equaled, if $\widehat{M}$ =0 .

**Proof:** Suppose $\widehat{M} = 0$, so the equation (4.5) be

$$\frac{\bar{y}(t) - \hat{C}x(t)}{\xi(t)} = 0$$

Then $\bar{y}(t) = \hat{C}x(t)$ ... (3.42)

From the equation of the response system and rules;

$$\hat{y}(t) = \hat{C}x(t) \qquad \dots(3.43)$$

From equations (3.42) and (3.43), we get, $\bar{y}(t) = \hat{y}(t)$

This means the receiver knows the transmitted value and then expected value transmitted to the receiver through a communication channel. So the system will be with no ciphertext and no need to synchronization, and then nothing to work on. ■

The values of terms in $\hat{C}$ are in $\{0,1\}$, and both $\hat{C}\hat{x}(t)$ and $\hat{C}x(t)$ are real.

### 3.5.7 Synchronization of Drive and Response Systems (Master-Slave Systems Synchronization)

An achieving the signal synchronization between the drive and response system need to compute the dynamic error for all over system as synchronization error until converge to zero. Firstly, calculate the error signals from both driver and response systems.

Let error signals from transmitter and receiver given by;

$$es_x(t) \equiv x(t) - \hat{x}(t) \qquad \ldots(3.44)$$

$$es_y(t) \equiv \bar{y}(t) - \hat{y}(t) \qquad \ldots(3.45)$$

From equations (1) and (2), the error dynamics system of error signals $es_x(t)$ and $es_y(t)$ are formulated by

$$es_x(t+1) = \sum_{i=1}^{r} \mu_i \left(\bar{y}(t)\right)(D_i - L_i C) es_x(t) \qquad \ldots(3.46)$$

$$es_y(t) = \hat{C} es_x(t) + \widehat{M}\, \xi(t) \qquad \ldots(3.47)$$

the error $es_y(t)$ depends on the $es_x(t)$ on synchronization, since

$$\begin{aligned} es_y(t) &\equiv \bar{y}(t) - \hat{y}(t) \\ &= \hat{C}x(t) + \widehat{M}\, \xi(t) - \hat{C}\hat{x}(t) \\ &= \hat{C}\left(x(t) - \hat{x}(t)\right) + \widehat{M}\, \xi(t) \\ &= \hat{C} es_x(t) + \widehat{M}\, \xi(t) \end{aligned}$$

Then

$$\xi(t) = \frac{es_y(t) - \hat{C} es_x(t)}{\widehat{M}} \qquad \ldots(3.48)$$

The aim of the synchronization is to make $\hat{C} es_x(t) \equiv 0$, that is $es_x(t) \rightarrow 0$, at $t \rightarrow \infty$. So, the ciphertext in recovering depends on the value of error $es_y(t)$ and $\widehat{M}$ which gives

$$\xi(t) = \frac{es_y(t)}{\widehat{M}} \qquad \ldots(3.49)$$

### 3.5.8 The Synchronizations Theorem of the Designed Method

The theorem that ensures the synchronization of the two systems is depended on the theorem introduced in previous works in literature [12].

**Theorem 3.4**: In the discrete time fuzzy chaotic system DFS, consider the chaotic transmitter (4.3) and receiver (4.7), the ciphertext can be recovered from $\xi(t) = 1/M_o \ \tilde{y}(t)$, and all states of chaotic transmitter and receiver are synchronized in an asymptotic manner if there exist a common positive-definite Hurwitz stable matrix $H$, and gains $Li$, for $i = 1, 2, \dots, r$, such that the following LMIs, with $W_i \equiv HL_i$ , have feasible solutions;

$$\begin{bmatrix} H & (HA_i \ - W_iC)^T \\ HA_i \ - W_iC & H \end{bmatrix} > 0\ , \quad \text{for all } i, \qquad \dots(3.50)$$

**Proof**: The proof here is similar to the theorem in [2]. Depending on Given a Lyapunov function candidate for DFS by

$$V\big(es_x(t)\big) = es_x^T(t)\, H\, es_x(t) > 0$$

We have difference of $V(t)$ as along the error dynamics $ed_x(t)$ yields

$$\Delta V\big(es_x(t)\big) = V\ \big(es_x(t+1)\big)\ - V\big(es_x(t)\big) \qquad \dots(3.51)$$

$$= \ \big(es_x(t+1)\big)^T H\big(es_x(t+1)\big) - [\big(es_x(t)\big)^T H\big(es_x(t)\big)]$$

$$= \left[\sum_{j=1}^{r} \mu_j(\bar{y}(t))\ (A_i - L_iF_i)^T es_x^T(t)\right] H \left[\sum_{i=1}^{r} \mu_i(\bar{y}(t))\ (A_i + L_iF_i) es_x(t)\right]$$

$$-es_x^T(t) H es_x(t)$$

Put $\bar{A}_i = A_i - L_iC$

$$= \left[\sum_{i=1}^{r} \mu_i(\bar{y}(t))\mu_i(\bar{y}(t))\ es_x^T(t)\big(\bar{A}_i^T H \bar{A}_i - H\big)\right] es_x(t)$$

$$+ 2\left[\sum_{i<j}^{r} \mu_i(\bar{y}(t))\mu_j(\bar{y}(t))\ es_x^T(t) \frac{\big(\bar{A}_i^T H \bar{A}_j - H\big) + \big(\bar{A}_j^T H \bar{A}_i - H\big)}{2}) es_x(t)\right]$$

$$= \left[\sum_{i=1}^{r} \mu_i(\bar{y}(t))\mu_i(\bar{y}(t))\, es_x^T(t)(\bar{A}_i^T H\bar{A}_i - H)\right] es_x(t)$$

$$+ \left[\sum_{i<j}^{r} \mu_i(\bar{y}(t))\mu_j(\bar{y}(t))\, es_x^T(t)(\bar{A}_i^T H\bar{A}_j + \bar{A}_j^T H\bar{A}_i - 2H)es_x(t)\right]$$

where $H > 0$. From the conditions of proof in [61][66],

If $\bar{A}_i^T H\bar{A}_i - H < 0$, then $\bar{A}_i^T H\bar{A}_j + \bar{A}_j^T H\bar{A}_i - 2H$ …(3.52)

This means that if there are H and L such that the conditions are held, then by Schur complement get $\bar{A}_i^T H\bar{A}_i - H < 0$ .

To prove $\Delta V\big(es_x(t)\big) < 0$, Let $-Q$ be denotes to the maximum negative definite matrix of $\bar{A}_i^T H\bar{A}_i - H$ for all i.

Then $\Delta V\,\big(es_x(t)\big) < -es_x^T\,(t)\,Q\,es_x(t) < 0$, and the synchronization error asymptotically converges to zero, $es_x(t) \to 0$ as $t \to \infty$.

According to the equation (4.14) of error for $y(t)$, $es_y(t)$ converges to $M\xi(t)$ as $es_x(t) \to 0$, and as $t \to \infty$. ■

Since the convergence rate of the synchronization error $es_x(t)$ affects the transmission performance, and under the condition of Hurwitz stable matrix $H$, that $Re\,\lambda i(A) < 0$.

The decay rate design uses $-Re\,\lambda i(A)$ to determine the decay rate that is to be minimized for chaotic cryptosystems which can be carried out to minimize by solving LMIs problems as follows

*Chaotic Cryptosystem with Decay rate :*

$$\underset{H,W_i}{minimize}\ \delta$$

$$subject\ \ to\ H > 0, 0 < \delta < \ 1$$

$$\begin{bmatrix} \delta H & (HA_i\ - W_iC)^T \\ HA_i\ - W_iC & H \end{bmatrix} > 0\ ,\quad for\ all\ i, \qquad \ldots(3.53)$$

where $W_i = HL_i$. Then $\Delta V\big(es_x(t)\big) < -(1-\delta)Ved_x(t)$ with parameter $\delta$ tuning the decay rate. If $-Re\,\lambda i(A) > 1$, put $-Re\,\lambda_l(A) = \delta_l$, for $l$ is a number of eigenvalues for H, turned to use the formula $\delta_l = \frac{\delta_{l-1}}{\delta_l}$ for $l = 1, \ldots, k$, $k$ is a number of turning trails.

One can use $Re\,\lambda_l(H)$ of H to determine the decay rate that can be minimized.

If there exists the feedback gains matrices $L_i$, satisfying the stability conditions, the stability of error dynamics system is guaranteed near the equilibrium points, that is $\left\|es_y(t)\right\| \leq \delta$.

The feedback gains can be computed by solving the design problem by fuzzy controller design for exact linearization EL on discrete-time fuzzy system DFS, that could be formed by a stable fuzzy controller for EL-DES

*Stable Fuzzy Controller Design for EL-DES*

$$\underset{H,S,W_1,W_2,\ldots,\,W_r}{\text{Minimize}}\ \beta$$

$$subject\ to\ \ H > 0, \beta > 0, S > 0$$

$$\begin{bmatrix} I & S \\ S & I \end{bmatrix} > 0$$

$$\begin{bmatrix} X & XA_i - W_i^TB^T \\ A_iX - BM_i & X \end{bmatrix} > 0, \qquad i = 1, 2, \ldots, r$$

$$\begin{bmatrix} \beta S & [(A_1X - BM_1) - (A_iX - BM_i)]^T \\ [(A_1X - BM_1) - (A_iX - BM_i)] & I \end{bmatrix} > 0$$

$$\ldots(3.54)$$

for $i = 1, 2, \dots, r$, where $X = H^{-1}$ , and $M_i = F_i X$.

This system will solved by LMIs, in which if all entries in Matrix $\beta.S \approx 0$ are close to zero, the fuzzy controller design could be solved for EL condition. Then ELs for stable fuzzy controller design is feasible. So by EL technique get on $G = A_i - BM_i$ for all $i$ and $G$ is stable Matrix. Since the matrix $G$ is not always stable.

### 3.5.9 The 3D-KFCC Decryption Process

Similarly to first direction in Section 3.2. At this stage the first user try to recovering the ciphertext $\xi(t)$ that were received. The recovering is by demodify the ciphertext by computing $C$ as;

$$C = (\gamma\xi(t) + 1)\frac{T}{2} \qquad \dots(3.55)$$

The user computes $v$ as multiplicative inverse of $W$ for $modN$, as ; $vW \equiv 1\ (modN)$, since $W$ is known for him. By connecting the easy and hard knapsack problems through computing ; $vb_i \equiv S_i(modN)$, for $i = 1,2, \dots, n$.

After that, computing the parameter $Z_i$ can be done, for each $c_i$, by substituting the value $c_i$ for $i$ by; $Z_i \equiv vc_i(modN)$.

$$Z_i = \sum_{j=1}^{n} m_{ij} S_j (modN) \qquad \dots(3.56)$$

Now, test conditions if $Z_i < N$, and $N > T$, then the formula to find a plaintext $M$, as in Algorithm (3.3).

Note that the formula for modification and demodification is with same form in all cases in KFCC and KFCCMS, but we change its view.

# Chapter Four

# Numerical Schemes Examples and Results Discussions of Cases Study for Suggested Systems

## 4.1 Results of Experimental and Numerical Discussion

The suggested system in this thesis could be performed on the 2D discrete-time and 3D continuous-time chaotic systems. In this chapter, we will give examples on 2D discrete-time, and then perform the example by the modification respect to using cosine map in one example and use sine map in other example these all implemented on the Lozi Map that could be exact represented by TS fuzzy model. Later, we introduce an example on 3D continuous-time by implementing the Lorenz map, which is a continuous map that needs to be discretized and exact represented by TS fuzzy model. Description of experimental results and the numerical results that extracted from system, discussion and comparison between experimental results and computational results has been introduced, in order to study and investigate the study cases.

### 4.1.1 Simulation Example for Study Case on the Discrete-time 2d-KFCC

In this simulation, we will consider the chaotic Lozi map [20] in a chaotic cryptosystem. That is a discrete-time chaotic Lozi system in view of step by step of performing the suggested system. Its chaotic behavior exhibited in a single scroll, since it is well-known two-dimensional map on the interval [0,1], the Lozi map as implicational example for theoretical derivative is like the Henon map but with absolute formulate the dynamical equations as the equation system bellow:

$$x_1(t+1) = -1.8\,|x_1(t)| + x_2(t) + 3$$

$$x_2(t+1) = 0.25x_1(t) \qquad \ldots(4.1)$$

The Lozi Map with one variable in the nonlinear term [12] has the nonlinear term $|x_1(t)|$. Since$|x_1(t)|$ is not well defined at $x_1(t) = 0$, let $\varphi(x_1(t)) = |x_1(t)|$ and choose $x_1(t)$ to be the premise variable.

The equivalent fuzzy model can be constructed with the system matrices as:

$$D_1 = D_2 = \begin{bmatrix} 0 & 1 \\ 0.25 & 0 \end{bmatrix} \qquad \ldots(4.2)$$

The system matrices evaluated to be equaled, and with non-common bias terms as

$$b_1 = \begin{bmatrix} 3 - 1.8d \\ 0 \end{bmatrix},\ b_2 = \begin{bmatrix} 3 \\ 0 \end{bmatrix} \qquad \ldots(4.3)$$

The fuzzy sets for prime variable values are determined through the membership functions as;

$$\Gamma_1(x_1(t)) = (|x_1(t)|/d),\ \ \Gamma_2(x_1(t)) = 1 - (|x_1(t)|/d) \qquad \ldots(4.4)$$

with $d = 3.5$, so $x_1(t) \in [-3.5, 3.5]$ . Then a general TS-fuzzy model of discrete time chaotic system at Lozi map with dynamical equations can be written as follows, [10] ;

$\boldsymbol{Rule\ i}$: $IF\ x_1(t) is\ \Gamma_i$

$$THEN\ x(t+1) = D_i x(t)\ +\ bi(t), \text{for } i = 1,2,\ldots,r \qquad \ldots(5.5)$$

where the premise variable $x_1(t)$ is a proper state variable, and $\Gamma_1, \Gamma_2$ are fuzzy sets "$about\ -3.5$", and "$about$ 3.5", respectively.

TABLE 4.1: The membership degrees of fuzzy set $\Gamma_1, \Gamma_2$ within [-3.5, 3.5]

| $x_1(t)$ | $\mu_1(x_1(t))$ | $x_1(t)$ | $\mu_1(x_1(t))$ |
|---|---|---|---|
| -3.5 | 1 | -3.5 | 0 |
| -3 | 0.857142857 | -3 | 0.142857143 |
| -2.5 | 0.714285714 | -2.5 | 0.285714286 |
| -2 | 0.571428571 | -2 | 0.428571429 |
| -1.5 | 0.428571429 | -1.5 | 0.571428571 |
| -1 | 0.285714286 | -1 | 0.714285714 |
| -0.5 | 0.142857143 | -0.5 | 0.857142857 |
| 0 | 0 | 0 | 1 |
| 0.5 | 0.142857143 | 0.5 | 0.857142857 |
| 1 | 0.285714286 | 1 | 0.714285714 |
| 1.5 | 0.428571429 | 1.5 | 0.571428571 |
| 2 | 0.571428571 | 2 | 0.428571429 |
| 2.5 | 0.714285714 | 2.5 | 0.285714286 |
| 3 | 0.857142857 | 3 | 0.142857143 |
| 3.5 | 1 | 3.5 | 0 |

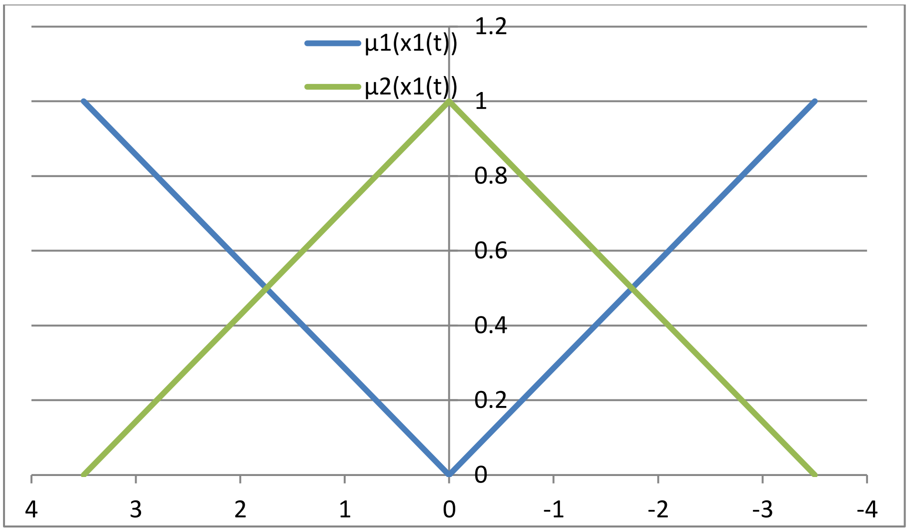


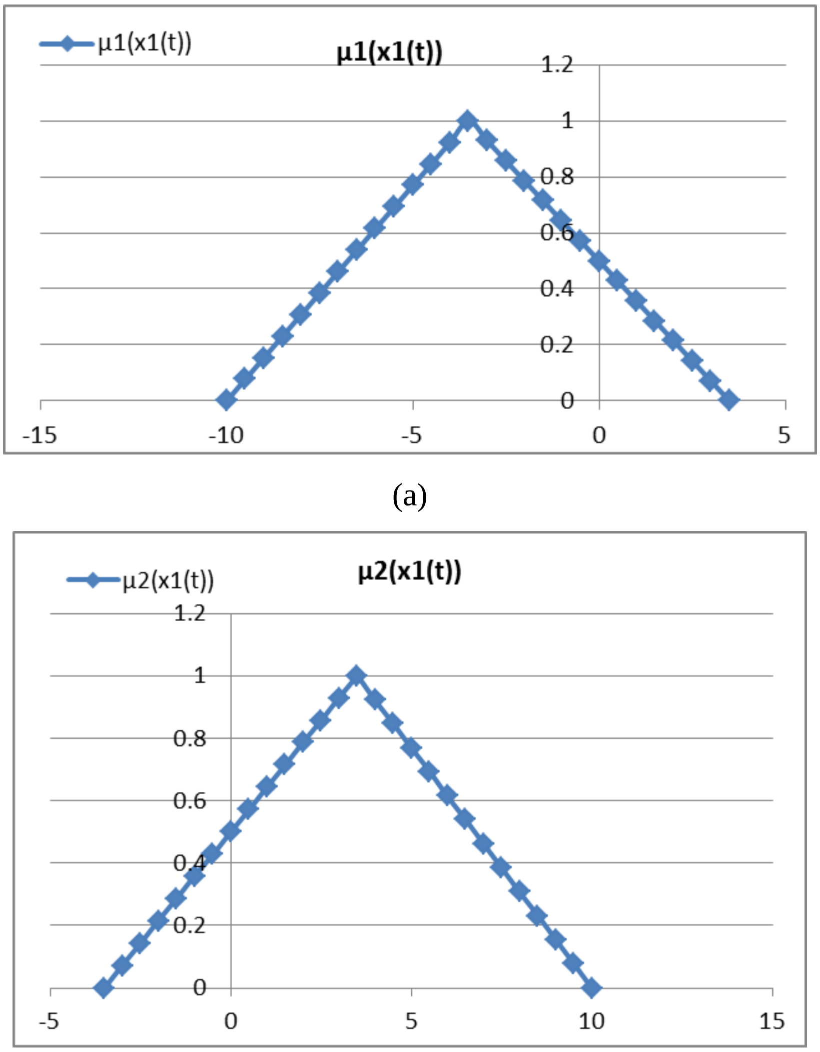
FIGURE 4.1 Membership degrees for fuzzy sets $\Gamma_1, \Gamma_2$ within [-3.5, 3.5]

Note that these fuzzy sets corresponding the triangular fuzzy sets fuzzy sets "$about\ -3.5$", and "$about$ 3.5", respectively, in the Fuzzy Logic.

TABLE 4.2: Membership degrees for fuzzy sets "about -3.5" , "about 3.5"

| $x_1(t)$ | $\mu_1(x_1(t))$ | $x_1(t)$ | $\mu_1(x_1(t))$ |
|---|---|---|---|
| -10 | 0 | -3.5 | 0 |
| -9.5 | 0.076923077 | -3 | 0.071428571 |
| -9 | 0.153846154 | -2.5 | 0.142857143 |
| -8.5 | 0.230769231 | -2 | 0.214285714 |
| -8 | 0.307692308 | -1.5 | 0.285714286 |
| -7.5 | 0.384615385 | -1 | 0.357142857 |
| -7 | 0.461538462 | -0.5 | 0.428571429 |
| -6.5 | 0.538461538 | 0 | 0.5 |
| -6 | 0.615384615 | 0.5 | 0.571428571 |
| -5.5 | 0.692307692 | 1 | 0.642857143 |
| -5 | 0.769230769 | 1.5 | 0.714285714 |
| -4.5 | 0.846153846 | 2 | 0.785714286 |
| -4 | 0.923076923 | 2.5 | 0.857142857 |
| -3.5 | 1 | 3 | 0.928571429 |
| -3 | 0.928571429 | 3.5 | 1 |
| -2.5 | 0.857142857 | 4 | 0.923076923 |
| -2 | 0.785714286 | 4.5 | 0.846153846 |
| -1.5 | 0.714285714 | 5 | 0.769230769 |
| -1 | 0.642857143 | 5.5 | 0.692307692 |
| -0.5 | 0.571428571 | 6 | 0.615384615 |
| 0 | 0.5 | 6.5 | 0.538461538 |
| 0.5 | 0.428571429 | 7 | 0.461538462 |
| 1 | 0.357142857 | 7.5 | 0.384615385 |
| 1.5 | 0.285714286 | 8 | 0.307692308 |
| 2 | 0.214285714 | 8.5 | 0.230769231 |
| 2.5 | 0.142857143 | 9 | 0.153846154 |
| 3 | 0.071428571 | 9.5 | 0.076923077 |
| 3.5 | 0 | 10 | 0 |

Figure 4.2. shows the normal triangular fuzzy sets for the primitive variable $x_1(t)$ with $\mu(-3.5) = 1 = \mu(3.5)$. with initial value in $[-3.5, 3.5]$.



(a)

(b)

FIGURE 4.2: (a) The fuzzy set "about -3.5". (b) The fuzzy set "about 3.5"

### 4.1.2 Implement TS fuzzy Model and Discuss its Effect

At this step we implement the chaotic map with initial values at $x_1(t) = -1$ and $x_2(t) = 0.25$, with $\tau = 18$. To extract the super increasing sequence we compute the absolute value and then find the summation with $\tau$, and for 40 iterations. The associated figures recover the variance in values.

TABLE 5.3: The values of state with initial $x_1(t) = -1$ and $x_2(t) = 0.25$

| time t | $x_1(t)$ | $x_2(t)$ | $\|k(t)\| + \tau$ |
|---|---|---|---|
| 0 | -1 | 0.25 | 19 |
| 1 | 1.45 | 0.3625 | 19.45 |
| 2 | 0.7525 | 0.188125 | 18.7525 |
| 3 | 1.833625 | 0.458406 | 19.83363 |
| 4 | 0.15788125 | 0.03947 | 18.15788 |
| 5 | 2.755284063 | 0.688821 | 20.75528 |
| 6 | -1.270690297 | -0.31767 | 19.27069 |
| 7 | 0.395084891 | 0.098771 | 18.39508 |
| 8 | 2.387618418 | 0.596905 | 20.38762 |
| 9 | -0.700808548 | -0.1752 | 18.70081 |
| 10 | 1.563342476 | 0.390836 | 19.56334 |
| 11 | 0.576819163 | 0.144205 | 18.57682 |
| 12 | 2.105930298 | 0.526483 | 20.10593 |
| 13 | -0.264191962 | -0.06605 | 18.26419 |
| 14 | 2.458406478 | 0.614602 | 20.45841 |
| 15 | -0.810530041 | -0.20263 | 18.81053 |
| 16 | 1.338413417 | 0.334603 | 19.33841 |
| 17 | 0.925459204 | 0.231365 | 18.92546 |
| 18 | 1.565538233 | 0.391385 | 19.56554 |
| 19 | 0.573415738 | 0.143354 | 18.57342 |
| 20 | 2.111205606 | 0.527801 | 20.11121 |
| 21 | -0.272368689 | -0.06809 | 18.27237 |
| 22 | 2.441644188 | 0.610411 | 20.44164 |
| 23 | -0.784548491 | -0.19614 | 18.78455 |
| 24 | 1.391675594 | 0.347919 | 19.39168 |
| 25 | 0.842902829 | 0.210726 | 18.8429 |
| 26 | 1.693500614 | 0.423375 | 19.6935 |

| | | | |
|---|---|---|---|
| 27 | 0.375074048 | 0.093769 | 18.37507 |
| 28 | 2.418635226 | 0.604659 | 20.41864 |
| 29 | -0.748884601 | -0.18722 | 18.74888 |
| 30 | 1.464786569 | 0.366197 | 19.46479 |
| 31 | 0.729580818 | 0.182395 | 18.72958 |
| 32 | 1.869149732 | 0.467287 | 19.86915 |
| 33 | 0.102817916 | 0.025704 | 18.10282 |
| 34 | 2.84063223 | 0.710158 | 20.84063 |
| 35 | -1.402979956 | -0.35074 | 19.40298 |
| 36 | 0.123891089 | 0.030973 | 18.12389 |
| 37 | 2.807968812 | 0.701992 | 20.80797 |
| 38 | -1.352351658 | -0.33809 | 19.35235 |
| 39 | 0.227679101 | 0.05692 | 18.22768 |
| 40 | 2.647097394 | 0.661774 | 20.6471 |

Note that after 40 iteration, we get a super increasing sequence with only two items. These result will not encourage us to work on it, since it not let to complicity and then unsecure. Figures (4.2.-4.5) illustrate the graphing of values in Table (4.2)

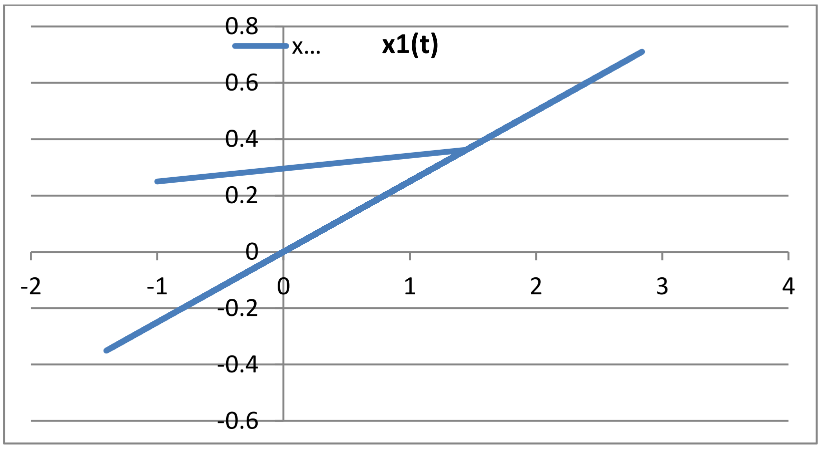


FIGURE 4.3: Graphing of $x_1(t)$ and $x_2(t)$ by Lozi map for Table 4.2

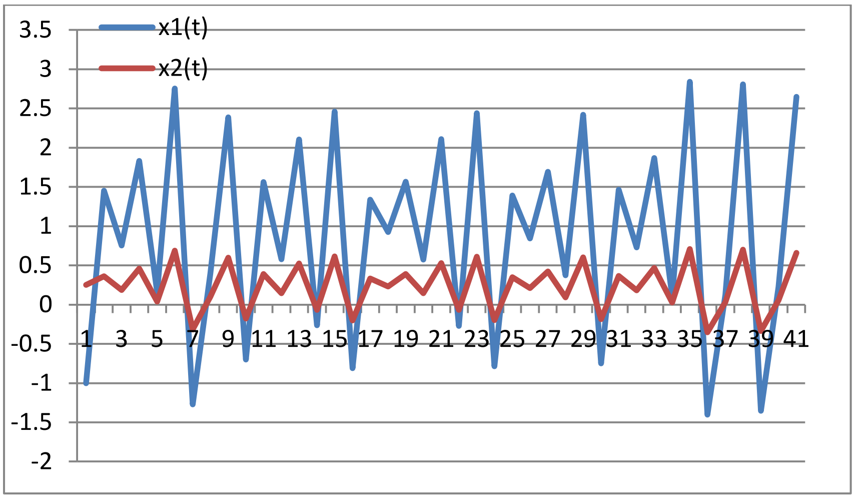
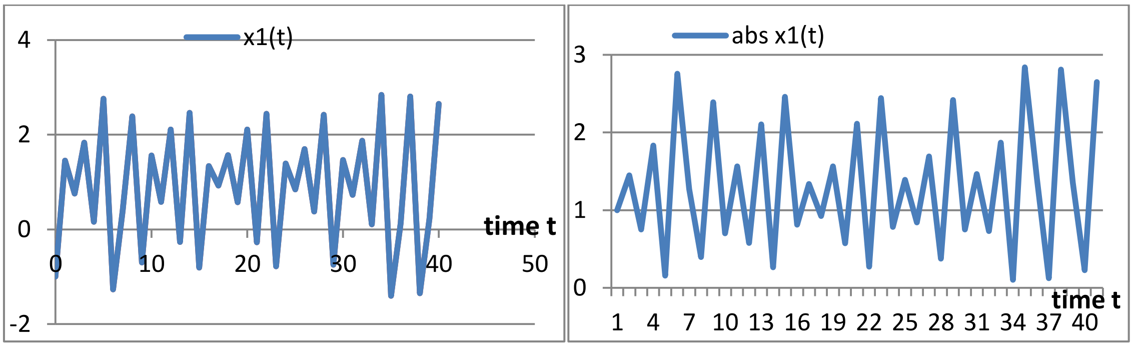


FIGURE 4.4: Illustration of divergence between initial conditions as state values of variables in Table 4.2



(a) (b)

FIGURE 4.5: (a)Primitive variable values (b) Absolute value

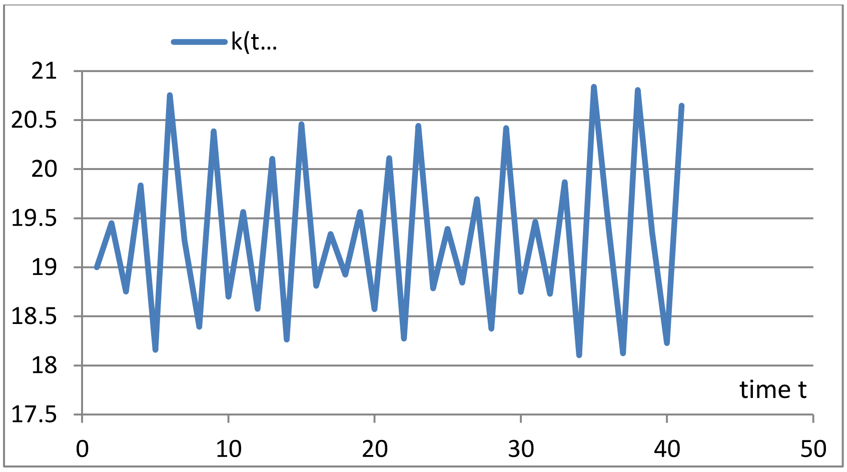


FIGURE 4.6: Primitive variables with parameter $\tau$ to construct $k(t)$

To improve the previous result that declared, We implement the TS fuzzy model that exact representing the Lozi map that inferred with rules numbers $r = 2$.

$\boldsymbol{Rule\ 1}$: $IF\ x_1(t)\ is\ \Gamma_1\ THEN\ x(t+1) = D_1 x(t) + b_1(t)$ …(4.6)

and $\boldsymbol{Rule\ 2}$: $IF\ x_1(t)\ is\ \Gamma_2\ THEN\ x(t+1) = D_2 x(t) + b_2(t)$ …(4.7)

So,

$\boldsymbol{Rule\ 1}$: $IF\ x_1(t) is\ "about - 3.5"$

$$THEN\ x(t+1) = \begin{bmatrix} 0 & 1 \\ 0.25 & 0 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} x(t) + \begin{bmatrix} -3.3 \\ 0 \end{bmatrix} \quad \text{…(4.8)}$$

$\boldsymbol{Rule\ 2}$: $IF\ x_1(t) is\ "about\ 3.5"$

$$THEN\ x(t+1) = \begin{bmatrix} 0 & 1 \\ 0.25 & 0 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + \begin{bmatrix} 3 \\ 0 \end{bmatrix} \quad \text{…(4.9)}$$

The TS fuzzy model is with tiny difference in values at bias terms. From the observation of bias terms, the systems Lozi map system have non-common bias terms, while there are other systems have common bias terms in TS fuzzy models. Since

$$\varphi(x) = \sum_{i=1}^{2} \mu_i d_i \quad \text{…(4.10)}$$

, here $\varphi(x) = 1$.

TABLE 4.4: Exact representing of TS fuzzy model on Lozi map under constrains rules for values in Table 4.2.

| Time t | $x_1(t)$ | $x_2(t)$ | $\lvert x_1(t)\rvert$ | $\lvert x_1(t)\rvert + \tau$ |
|---|---|---|---|---|
| 0 | -3.05 | -0.25 | 3.05 | 21.05 |
| 1 | -2.9375 | 0.3625 | 2.9375 | 20.9375 |
| 2 | -3.111875 | 0.188125 | 3.111875 | 21.111875 |
| 3 | -2.84159375 | 0.45840625 | 2.84159375 | 20.84159375 |
| 4 | -3.260529688 | 0.039470313 | 3.260529688 | 21.26052969 |
| 5 | -2.611178984 | 0.688821016 | 2.611178984 | 20.61117898 |
| 6 | -3.617672574 | -0.317672574 | 3.617672574 | 21.61767257 |
| 7 | -3.201228777 | 0.098771223 | 3.201228777 | 21.20122878 |

| | | | | |
|---|---|---|---|---|
| 8 | -2.703095395 | 0.596904605 | 2.703095395 | 20.7030954 |
| 9 | -3.475202137 | -0.175202137 | 3.475202137 | 21.47520214 |
| 10 | -2.909164381 | 0.390835619 | 2.909164381 | 20.90916438 |
| 11 | -3.155795209 | 0.144204791 | 3.155795209 | 21.15579521 |
| 12 | -2.773517425 | 0.526482575 | 2.773517425 | 20.77351743 |
| 13 | -3.366047991 | -0.066047991 | 3.366047991 | 21.36604799 |
| 14 | -2.685398381 | 0.614601619 | 2.685398381 | 20.68539838 |
| 15 | -3.50263251 | -0.20263251 | 3.50263251 | 21.50263251 |
| 16 | -2.965396646 | 0.334603354 | 2.965396646 | 20.96539665 |
| 17 | -3.068635199 | 0.231364801 | 3.068635199 | 21.0686352 |
| 18 | -2.908615442 | 0.391384558 | 2.908615442 | 20.90861544 |
| 19 | -3.156646065 | 0.143353935 | 3.156646065 | 21.15664607 |
| 20 | -2.772198599 | 0.527801401 | 2.772198599 | 20.7721986 |
| 21 | -3.368092172 | -0.068092172 | 3.368092172 | 21.36809217 |
| 22 | -2.689588953 | 0.610411047 | 2.689588953 | 20.68958895 |
| 23 | -3.496137123 | -0.196137123 | 3.496137123 | 21.49613712 |
| 24 | -2.952081102 | 0.347918898 | 2.952081102 | 20.9520811 |
| 25 | -3.089274293 | 0.210725707 | 3.089274293 | 21.08927429 |
| 26 | -2.876624846 | 0.423375154 | 2.876624846 | 20.87662485 |
| 27 | -3.206231488 | 0.093768512 | 3.206231488 | 21.20623149 |
| 28 | -2.695341193 | 0.604658807 | 2.695341193 | 20.69534119 |
| 29 | -3.48722115 | -0.18722115 | 3.48722115 | 21.48722115 |
| 30 | -2.933803358 | 0.366196642 | 2.933803358 | 20.93380336 |
| 31 | -3.117604795 | 0.182395205 | 3.117604795 | 21.1176048 |
| 32 | -2.832712567 | 0.467287433 | 2.832712567 | 20.83271257 |
| 33 | -3.274295521 | 0.025704479 | 3.274295521 | 21.27429552 |
| 34 | -2.589841943 | 0.710158057 | 2.589841943 | 20.58984194 |
| 35 | -3.650744989 | -0.350744989 | 3.650744989 | 21.65074499 |
| 36 | -3.269027228 | 0.030972772 | 3.269027228 | 21.26902723 |

| | | | | |
|---|---|---|---|---|
| 37 | -2.598007797 | 0.701992203 | 2.598007797 | 20.5980078 |
| 38 | -3.638087915 | -0.338087915 | 3.638087915 | 21.63808791 |
| 39 | -3.243080225 | 0.056919775 | 3.243080225 | 21.24308022 |
| 40 | -2.638225652 | 0.661774348 | 2.638225652 | 20.63822565 |

Note that, also after 40 iteration, we get a super increasing sequence with only two items. In same manner these result will not helpful to work on it, since it not let to complicity and then unsecure. Figures (4.6.-4.8) illustrate the graphing of exact representing for TS fuzzy model for Lozi map and premise variables values as were stated in Table (4.3).

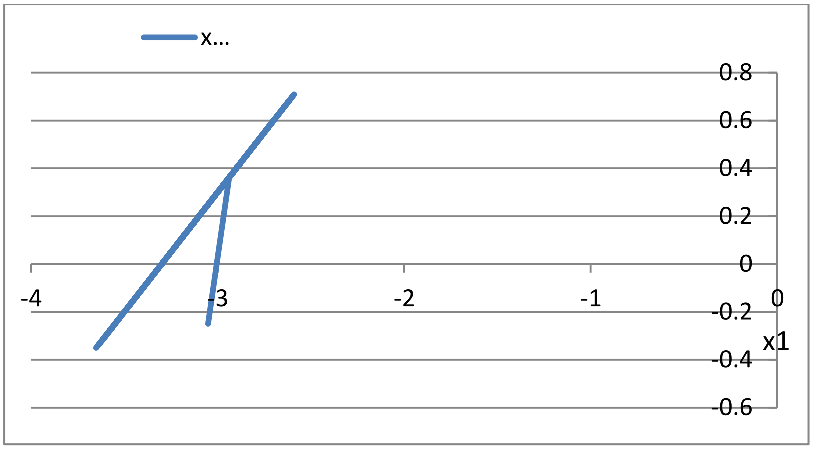


FIGURE 4.7: Graphing of $x_1(t)$ and $x_2(t)$ by TS fuzzy model on Lozi map for Table 4.3

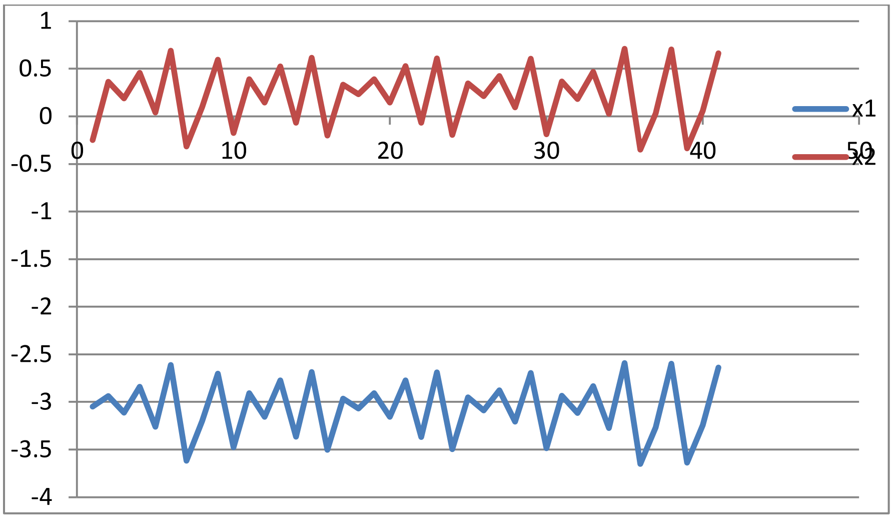
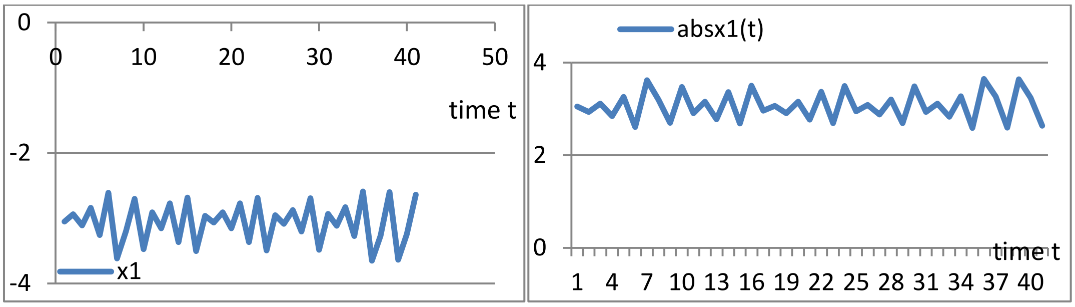


FIGURE 4.8: Divergence in initial conditions as state values of variables



(a) (b)

FIGURE 4.9: (a)Primitive variable values as results for TS Fuzzy Model (b) Absolute value for result of TS Fuzzy Model

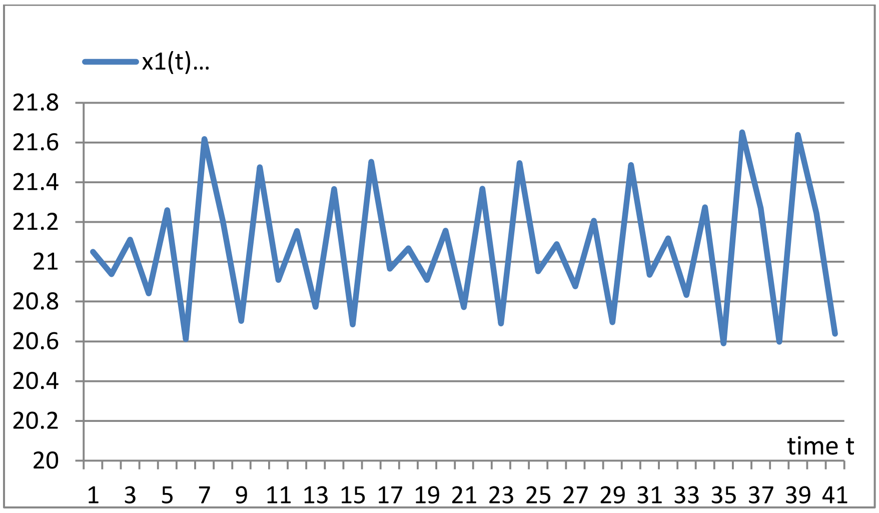


FIGURE 4.10: Primitive variables by TS fuzzy model with parameter $\tau$ to construct $k(t)$

We try to implement various values as initial conditions for Lozi map and if it be good we will perform it by exact representing by TS fuzzy model under standard situations for system matrix and non-common bias term. But the results were not best than previous one. In numerical experiments, initial value for Lozi chaotic map were supposed as; $x_1(t) = 2.5,$ and respect to values of $x_2(t) = -0.5$ with same vale of $\tau = 18$, and for 40 iterations. Table 4.4 and Figures (4.6-4.10) will illustrate the computational results that also led to nothing .

TABLE 4.5: Computations in numerical experiments are with different initial values than table (5.4)

| time t | $x_1(t)$ | $x_2(t)$ | $\|k(t)\| + \tau$ |
|---|---|---|---|
| 0 | 2.5 | -0.5 | 20.5 |
| 1 | -2 | 0.625 | 20 |
| 2 | 0.025 | -0.5 | 18.025 |
| 3 | 2.455 | 0.00625 | 20.455 |
| 4 | -1.41275 | 0.61375 | 19.41275 |
| 5 | 1.0708 | -0.35319 | 19.0708 |
| 6 | 0.7193725 | 0.2677 | 18.71937 |
| 7 | 1.9728295 | 0.179843 | 19.97283 |
| 8 | -0.371249975 | 0.493207 | 18.37125 |
| 9 | 2.82495742 | -0.09281 | 20.82496 |
| 10 | -2.17773585 | 0.706239 | 20.17774 |
| 11 | -0.213685175 | -0.54443 | 18.21369 |
| 12 | 2.070932723 | -0.05342 | 20.07093 |
| 13 | -0.781100196 | 0.517733 | 18.7811 |
| 14 | 2.111752829 | -0.19528 | 20.11175 |
| 15 | -0.99643014 | 0.527938 | 18.99643 |
| 16 | 1.734363955 | -0.24911 | 19.73436 |
| 17 | -0.370962653 | 0.433591 | 18.37096 |
| 18 | 2.765858213 | -0.09274 | 20.76586 |
| 19 | -2.071285446 | 0.691465 | 20.07129 |
| 20 | -0.03684925 | -0.51782 | 18.03685 |
| 21 | 2.415849988 | -0.00921 | 20.41585 |
| 22 | -1.35774229 | 0.603962 | 19.35774 |
| 23 | 1.160026374 | -0.33944 | 19.16003 |
| 24 | 0.572516954 | 0.290007 | 18.57252 |
| 25 | 2.259476076 | 0.143129 | 20.25948 |

|  |  |  |  |
|---|---|---|---|
| 26 | -0.923927699 | 0.564869 | 18.92393 |
| 27 | 1.901799161 | -0.23098 | 19.9018 |
| 28 | -0.654220415 | 0.47545 | 18.65422 |
| 29 | 2.297853044 | -0.16356 | 20.29785 |
| 30 | -1.299690582 | 0.574463 | 19.29969 |
| 31 | 1.235020213 | -0.32492 | 19.23502 |
| 32 | 0.452040971 | 0.308755 | 18.45204 |
| 33 | 2.495081306 | 0.11301 | 20.49508 |
| 34 | -1.378136107 | 0.62377 | 19.37814 |
| 35 | 1.143125333 | -0.34453 | 19.14313 |
| 36 | 0.597840373 | 0.285781 | 18.59784 |
| 37 | 2.209668662 | 0.14946 | 20.20967 |
| 38 | -0.827943498 | 0.552417 | 18.82794 |
| 39 | 2.06211887 | -0.20699 | 20.06212 |
| 40 | -0.91879984 | 0.51553 | 18.9188 |

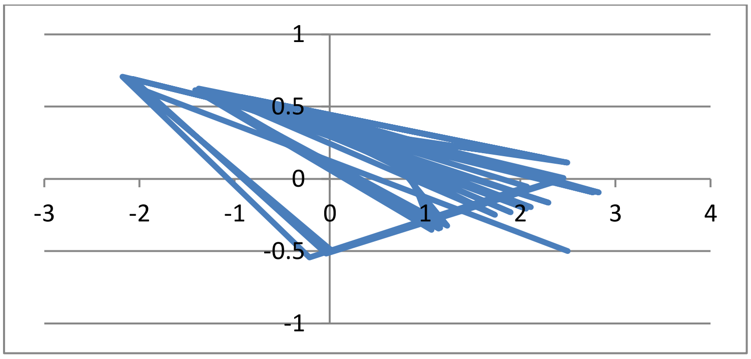


FIGURE 4.11: Graphing of  iterations values for $x_1(t)$  and $x_2(t)$

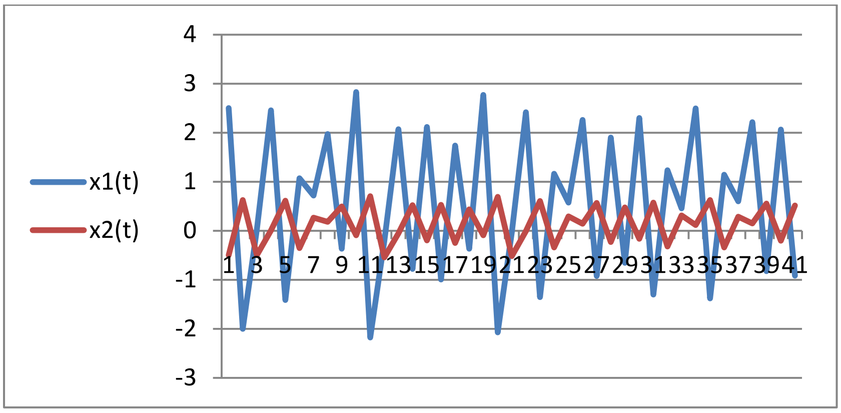
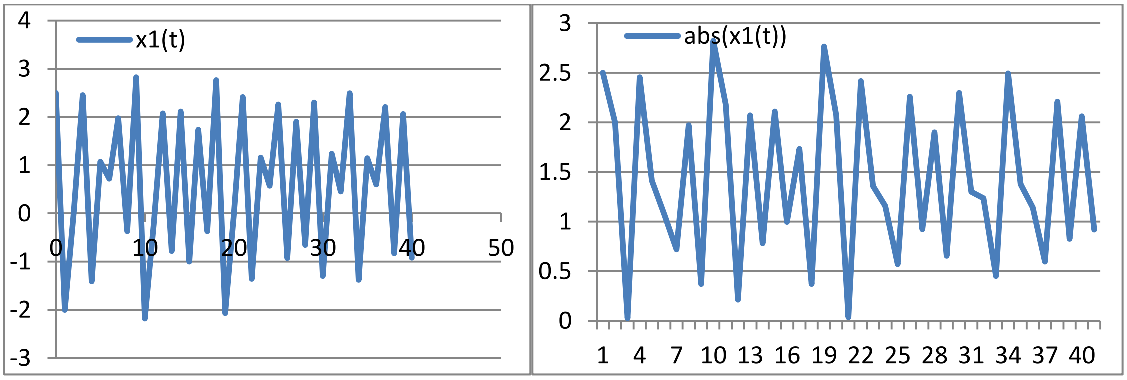


FIGURE 4.12: Divergence in initial conditions as state values of variables



(a) (b)

FIGURE 4.13: (a)Primitive variable values as results for TS Fuzzy Model

(b) Absolute value for result of TS Fuzzy Model

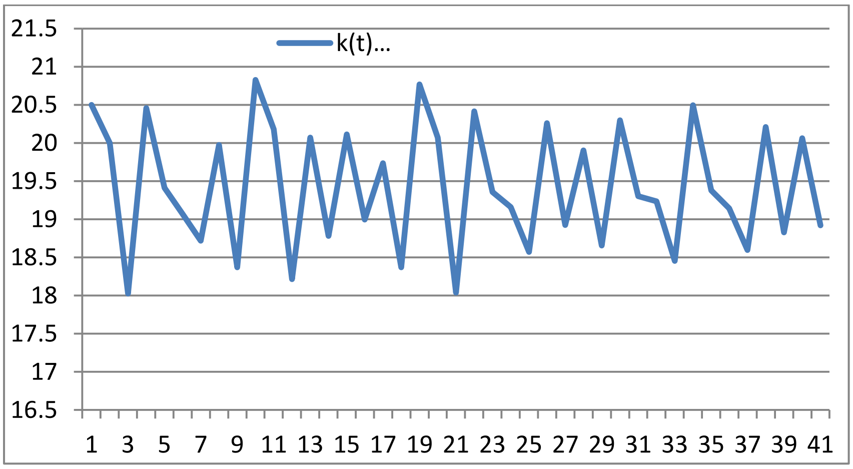


FIGURE 4.14: Primitive variables by TS fuzzy model with parameter $\tau$ to construct $k(t)$ terms to find the super increasing sequence

### 4.1.3 Conclusion for Discrete-time 2D KFCC

By this simulation experiments, we perform the Discrete-time 2d KFCC by implementing the chaotic Lozi. When performing the suggested system, that with one premise variable which $x_1(t)$ with the matrices system. Firstly, we implement TS fuzzy model at this step we implement the chaotic map with initial values at $x_1(t) = -1$ and $x_2(t) = 0.25$, with $\tau = 18$. To extract the super increasing sequence we compute the absolute value and then find the summation with $\tau$. After 40 iterations, we get a super increasing sequence with only two items. These result will not encourage us to work on it, since it not led to complicity and then unsecure.

Later, we try to implement various values as initial conditions for Lozi map $x_1(t) = 2.5,$ and respect to values of $x_2(t) = -0.5$, but the results were not the best. From the numerical experiments and its computational results we couldn't depend it in our work.

To improve the previous result that declared, We implement the TS fuzzy model that exact representing the Lozi map with non-common bias term and system matrix that inferred with only two rules. The TS fuzzy model was with tiny difference in values at bias terms, and with initial values at $x_1(t) = -1$, $x_2(t) = 0.25$, with $\tau = 18$.

Note that, also after 40 iteration, we get a super increasing sequence with only two items. In same manner these result will not help us to work on it, since it not let to complicity and then unsecure.

## 4.2 Simulation Example on the Suggested Fuzzy Cosine Chaotic Cryptosystem KFCC with 2D

In this simulation, we will also consider the chaotic map as Lozi map in equation (4.1). That is the discrete-time chaotic Lozi map will be a seed map in a cosine map in view of performing the suggested fuzzy cosine chaotic cryptosystem.

As were explained the Lozi Map has the nonlinear term $|x_1(t)|$, and choose $x_1(t)$ to be its premise variable. In same manner with Section 4.1, The exact representation for fuzzy model can be performed with the system matrices $D_1, D_2$ as in equations (4.2)-(4.4):

Prime variable values are with $d = 3.5$ , and $x_1(t) \in [-3.5, 3.5]$ too.

The general TS-fuzzy model of discrete time chaotic system at Lozi map with dynamical equations is the same in equation (5.5) with inferred rules $r = 2$, that on the proper state variable $x_1(t)$, and its fuzzy sets $\Gamma_1$, $\Gamma_2$ "$about\ -3.5$", and "$about\ 3.5$", respectively, with equations (4.6)-(4.9) .

### 4.2.1 The Cosine Lozi Chaotic map CLZ

The model performed on Lozi map as well known system that exact represented by TS fuzzy models on the vector variables $x(t) = [x_1(t)\ \ x_2(t)]^T$, where $x(t) \in R^2$, $x_1(t)$, $x_2(t)$ is the state vector. These features will help in encrypting the message in this work through composing the super-increasing sequence $S$

$$\begin{cases} x_1(t+1) = 3 - \alpha|x_1(t)| + x_2(t) \\ \quad x_2(t+1) = \beta\, x_1(t) \end{cases} \qquad \dots(4.11)$$

where $\alpha, \beta$ are the system parameters, such that $\alpha \in [1, 1.8]$, $\beta \in [0, 0.4]$, if we take some values for these parameters to view the chaotic behavior the dynamical system be as;

$$\begin{cases} x_1(t+1) = 3 - 1.8|x_1(t)| + x_2(t) \\ \quad x_2(t+1) = 0.25\, x_1(t) \end{cases} \qquad \dots(4.12)$$

The fuzzy sets that defined on values of premise variable $x_1(t)$ are as in equation (4.4), for $d \in R^+$. Also, suppose $d = 3.5$, and $x_1(t) \in [-d, d] = [-3.5, 3.5]$, and $\sum_{i=1}^{2} F_i = 1$. The system equaled matrices that associated with the equations system as in equation (4.2) .

Since there is no nonlinear terms in the system of equations, and so the bias terms $b$ on two rules will be as not equaled are as in equation (4.3) to control on $x_1(t)$ values. Since the system may be seen as

$$\begin{cases} x_1(t+1) = 3 - 1.8|x_1(t)| + 0\, x_1(t) + x_2(t) \\ x_2(t+1) = 0 \qquad\qquad\quad + 0.25\, x_1(t) + x_2(t) \end{cases} \qquad \ldots(4.13)$$

$x(t),\ b_i \in R^2,\ A_i \in R^{2\times 2},\ for\ i = 1, 2$. In designing the cosine Lozi map(CLZ) the system be;

$$F\big(x_n(t+1)\big) = G(2^{(k+F(x_n(t)))}) \qquad \ldots(4.14)$$

So ;

$$\begin{cases} x_1(t+1) = \cos(2^{\left(k+3-1.8|x_1(t)|+x_2(t)\right)}) \\ \quad x_2(t+1) = \cos(\,2^{(k+0.25\, x_1(t))}) \end{cases} \qquad \ldots(4.15)$$

where $G(x) = cos(x)$, and $k \in [10, 24]$. So then $x_1(t+1),\ x_2(t+1) \in [-1, 1]$, for initial conditions values $x(0) = [x_1(0) \quad x_2(0)]^T = [1 \quad 0.25]$.

### 4.2.2 Numerical Scheme Experiment for CLZ

The system performed with initial values for premise variables as; $x_1(0) = 1,\ x_2(0.25)$, and $k = 10$ after 40 iterations, to extract the secure key $k(t)$ from the state trajectory for the state $x_1(t)$. The sequence of cosine chaotic values be;

$$cos\big(x(t)\big) = \{-0.062147736, -0.10325421, -0.289280697, \\ -0.428048502, 0.996444258\} \qquad \ldots(4.16)$$

With value for $\tau = 6$, then $S_1(t) = |-0.062147736| + 6$, and so the 5-terms super-increasing sequence;

$$S = \{6.062147736, 6.10325421, 6.289280697, 6.428048502, \\ 6.996444258\} \qquad \ldots(4.17)$$

$$T = \sum_{j=1}^{5} S_j = 31.8791754 \qquad \ldots(4.18)$$

Put $N = 39 > T$. Select $W = 28$ in $[2,38]$ and $gcd(W, N) = 1$. Compute a public hard knapsack;

$B = \{187.9266, 189.2009, 194.9677, 199.2695, 216.8898\}$ …(4.19)

For each ($mod$ 39), so

$B = \{31.92658, 33.20088, 38.9677, 4.269504, 21.88977\}$ …(4.20)

where $(S, W, N)$ are a private key and $B$ as public key.

To encrypt the binary plaintext $M = \{00111, 11001, \ldots, m_l\}$ with five terms. For each set $m_i$ from message, compute for instance the set $m_1 = \{00111\}$, and using public key

$$C = 0 * 31.92658 + 0 * 33.20088 + 1 * 38.9677 + 1 * 4.269504 + 1 * 21.88977 \qquad \ldots(4.21)$$

Then $C = 65.126974$, modified into the ciphertext ;

$$\xi(t) = \left(\frac{2(65.126974) - 31.8791754}{\gamma(31.8791754)}\right)$$

$$= \frac{98.3747726}{\gamma(31.8791754)}$$

$$\xi(t) = \frac{3.085863149}{\gamma} \qquad \ldots(4.22)$$

Now, we need randomly take $\gamma \in R$ such that $\xi(t) \in (-0.01, 0.01)$. There are many values for instance $342.8736833$, and $617.1726299$, that $\xi(t) = 0.009$, and $\xi(t) = 0.005$, respectively.

To decrypt $\xi(t)$, by find the invertible of $W(mod\ N)$ as ;

$v28 = 1(mod\ 39)$,

Then $v = 7$. The user perform the connection between easy and hard knapsacks through computing ;

$vb_i = S_i(mod\ N)$, for $i = 1, \ldots, 5$ ...(4.23)

In the set;

$\{7 * 31.92658, 7 * 33.20088, 7 * 38.9677, 7 * 4.269504, 7 * 21.88977\}$ (mod 39)

$= \{31.9266, 33.2009, 38.9677, 4.2695, 21.8898\}$ ...(4.24)

Here, $Z_i$ for each $c_i$ for $i = 1, \dots, 5$ be as ;

$\{7 * 0 * 31.92658, 7 * 0 * \ 33.20088, 7 * 1 * \ 38.9677, 7 * 1 * 4.269504, 7 * 1 * 21.88977\}$ ...(4.25)

By substituting the values of $c_i$, testing condition ; if that $\mathrm{Z_i} < 39$ and $39 > \mathrm{T}$. The message is $M = \{00111\}$.

We were implement an experiment staring with different initial values and continued for 40 times, that refer to points in the phase trajectory instead continuous connected curve. The experiments are implemented with many initial values for $x_1(t)$ but the perfect values are in Table (4.6).

TABLE 4.6: Cosine function values on TS chaotic fuzzy model values for initial values $x_1(0) = 1,\ x_2(0.25)$, and $k = 1$

| *It.t* | *x₁(t)* | *x₂(t)* | $cos(x_1(t)$ | $\lvert cos(x_1(t))\rvert$ | $cos(x_2(t)$ |
|---|---|---|---|---|---|
| 0 | 1 | 0.25 | 0.949734335 | 0.949734335 | 0.371786285 |
| 1 | 1.45 | 0.3625 | -0.062147736 | 0.062147736 | -0.983815863 |
| 2 | 0.7525 | 0.188125 | -0.91777828 | 0.91777828 | -0.458953155 |
| 3 | 1.833625 | 0.45840625 | 0.782762288 | 0.782762288 | 0.907348575 |
| 4 | 0.15788125 | 0.039470313 | 0.438652235 | 0.438652235 | -0.999505732 |
| 5 | 2.755284063 | 0.688821016 | -0.734928136 | 0.734928136 | -0.251371903 |
| 6 | -1.270690297 | -0.317672574 | -0.957242733 | 0.957242733 | 0.093348315 |
| 7 | 0.395084891 | 0.098771223 | -0.396928379 | 0.396928379 | -0.989386445 |
| 8 | 2.387618418 | 0.596904605 | 0.507288872 | 0.507288872 | -0.999279544 |
| 9 | -0.700808548 | -0.175202137 | -0.10325421 | 0.10325421 | -0.522161811 |
| 10 | 1.563342476 | 0.390835619 | -0.579283623 | 0.579283623 | -0.399144929 |
| 11 | 0.576819163 | 0.144204791 | 0.857506858 | 0.857506858 | 0.783260782 |
| 12 | 2.105930298 | 0.526482575 | -0.916288522 | 0.916288522 | 0.005211442 |

| | | | | | |
|---|---|---|---|---|---|
| 13 | -0.264191962 | -0.066047991 | -0.289280697 | 0.289280697 | -0.415892367 |
| 14 | 2.458406478 | 0.614601619 | -0.163035987 | 0.163035987 | -0.974200403 |
| 15 | -0.810530041 | -0.20263251 | 0.887107061 | 0.887107061 | -0.73311434 |
| 16 | 1.338413417 | 0.334603354 | 0.733109641 | 0.733109641 | -0.994922343 |
| 17 | 0.925459204 | 0.231364801 | -0.974624774 | 0.974624774 | -0.444373778 |
| 18 | 1.565538233 | 0.391384558 | -0.751315142 | 0.751315142 | 0.100206045 |
| 19 | 0.573415738 | 0.143353935 | -0.996550037 | 0.996550037 | 0.999993187 |
| 20 | 2.111205606 | 0.527801401 | 0.658475385 | 0.658475385 | 0.976628256 |
| 21 | -0.272368689 | -0.068092172 | 0.921078603 | 0.921078603 | -0.970585909 |
| 22 | 2.441644188 | 0.610411047 | -0.7158617 | 0.7158617 | 0.382444482 |
| 23 | -0.784548491 | -0.196137123 | -0.761346353 | 0.761346353 | -0.050722046 |
| 24 | 1.391675594 | 0.347918898 | -0.736642093 | 0.736642093 | -0.881293834 |
| 25 | 0.842902829 | 0.210725707 | -0.428048502 | 0.428048502 | -0.787395664 |
| 26 | 1.693500614 | 0.423375154 | 0.701927972 | 0.701927972 | -0.93205506 |
| 27 | 0.375074048 | 0.093768512 | -0.651051176 | 0.651051176 | 0.873499428 |
| 28 | 2.418635226 | 0.604658807 | -0.677496327 | 0.677496327 | 0.439270707 |
| 29 | -0.748884601 | -0.18722115 | 0.992320921 | 0.992320921 | 0.637594091 |
| 30 | 1.464786569 | 0.366196642 | 0.572187642 | 0.572187642 | 0.914632719 |
| 31 | 0.729580818 | 0.182395205 | 0.077740594 | 0.077740594 | 0.925441838 |
| 32 | 1.869149732 | 0.467287433 | -0.704845572 | 0.704845572 | -0.389706697 |
| 33 | 0.102817916 | 0.025704479 | 0.996444258 | 0.996444258 | 0.824960125 |
| 34 | 2.84063223 | 0.710158057 | -0.936019998 | 0.936019998 | -0.712278863 |
| 35 | -1.402979956 | -0.350744989 | -0.691747192 | 0.691747192 | 0.316870053 |
| 36 | 0.123891089 | 0.030972772 | -0.849091659 | 0.849091659 | -0.997461672 |
| 37 | 2.807968812 | 0.701992203 | -0.357430422 | 0.357430422 | 0.733398462 |
| 38 | -1.352351658 | -0.338087915 | 0.479186383 | 0.479186383 | 0.897964692 |
| 39 | 0.227679101 | 0.056919775 | 0.509748836 | 0.509748836 | -0.978378087 |
| 40 | 2.647097394 | 0.661774348 | 0.740088972 | 0.740088972 | 0.483612249 |

In Figures 4.14, and 4.15, We were explain the trajectory of values for $x_1(t)$ implemented through the experiment staring with different initial values and continued for 40 times, that refer to points in the phase trajectory instead continuous connected curve. The experiments results are implemented with many initial values for $x_1(t)$ with values in Table (4.6).

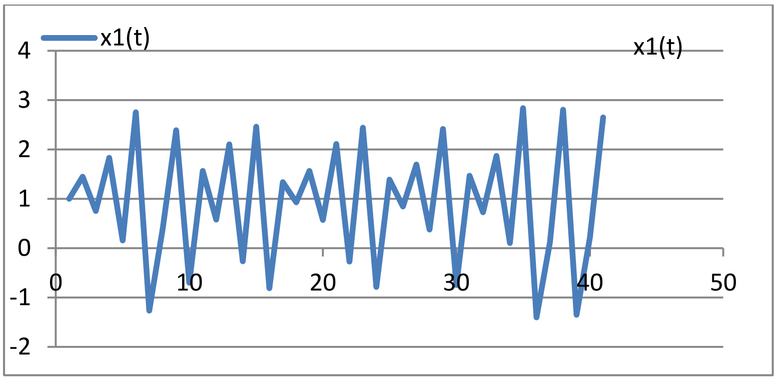


FIGURE 4.15: Values for $x_1(t)$ for iteration 40, as in Table (4.6)

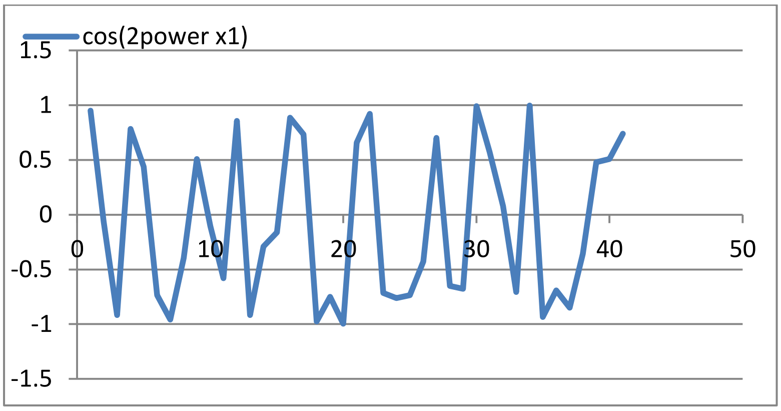


FIGURE 4.16: Cosine Chaotic values for $x_1(t)$ with It. 40, in Table (4.6)

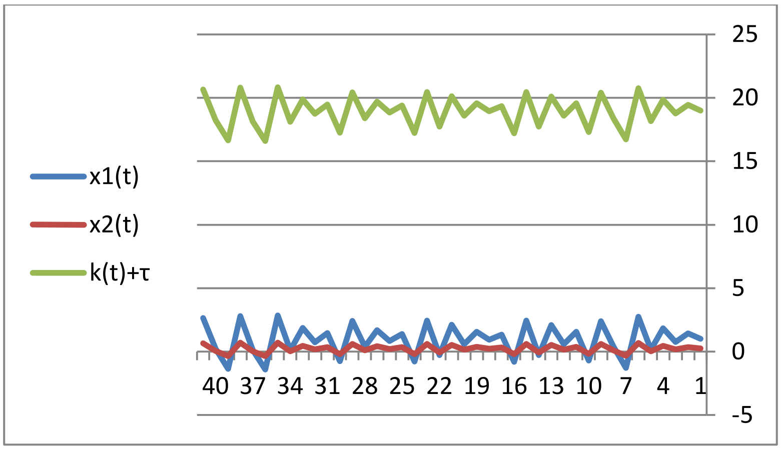


FIGURE 4.17: Trajectories for values in Table (4.6)

The primitive variable trajectory has more than one super increasing sequence after absolute value on cosine map, in the study case we discuss the standard one with the longer sequence with five terms.

### 4.2.3 Conclusions for Experiment on CLZ

The Knapsack problem is performed in combination with the TS fuzzy model for discrete-time chaotic systems, that are derived with only one premise variable. Following the cosine map implemented on the chaotic map at Lozi chaotic map, with non-common bias terms and the same premise variable and driving signal. In this fuzzy model-based on a cosine chaotic map applied with numerical data for chaotic behavior, parameters data and premise variable with initial values in interval $[-\mathbf{3.5}, \mathbf{3.5}]$. Were the trajectory of values for primitive variable that implemented through the experiment staring with  initial values and continued for 40 times. The advantage of this performance design is that all well-known chaotic systems stated achieved the results in more secure, since the trajectory values for premise variable, converted into values for cosine map in interval $[-\mathbf{1}, \mathbf{1}]$. Numerical simulations with  values in table and figures are shown to be consistent with theoretical design. The resulted trajectory values use to generate secret key by choosing super increasing sequence from the cosine values for trajectory from the chaotic map under TS model. After masking and modifying the ciphertext between the users, the ciphertext be ready to decrypted. A good result were gained and the security of the system shown in flexibility in changing the supposed values that will make the system behavior unpredictable. Also it could be extracted through; Employing a discrete chaotic map, and then compose the cosine map on it, and choosing the parameters values for chaotic map with chaotic behavior; Assume initial values randomly from closed interval in state space; Choosing the chaotic map is unpredictable.  Finding a super-increasing sequence from the trajectory(orbit) of points, with increase iterations for absolute value for cosine map for the seed chaotic map, the primitive variable trajectory has more than one super increasing sequence, we discussed the standard one with the longer sequence with five terms.

## 4.3 A Simulation Example on the Suggested Fuzzy Chaotic Cryptosystem Fuzzy Sine Chaotic Cryptosystem KFCC with 2D

At this simulation we will implemented the work on the chaotic Lozi map also in connection to Sections 4.1, 4.2 in a chaotic cryptosystem. That as discrete-time chaotic Lozi system in view of performing the suggested KFCC system by using the Lozi map as seed map in the sine map. The dynamical equations of Lozi system as in equation (4.1) with $x_1(t)$ to as the premise variable and the only one variable in the nonlinear term $|x_1(t)|$ as $\varphi(x_1(t)) = |x_1(t)|$. The equivalent TS fuzzy model for exact representing Lozi map were as in Section 4.1. That TS fuzzy model could be constructed with system matrices as in equation (4.2), that matrices evaluated to be equaled, and the non-common bias terms as in equation (4.3).

Also the fuzzy sets for premise and proper state variable $x_1(t)$ are determined through the membership functions as in equation (4.4), with $d = 3.5$, and $x_1(t) \in [-3.5, 3.5]$, with $\Gamma_1, \Gamma_2$ as fuzzy sets "about -3.5",and "about 3.5", respectively.

So the general TS fuzzy model of discrete time chaotic system at Lozi map were as in equation (4.5). with inferred rules $r = 2$ will also could be written as in equations (4.6)-(4.9).

The difference between this model and the suggested model in Sections 4.1 and 4.2 is through using sine map instead of using chaotic map directly or using cosine map.

### 4.3.1 The Sine Lozi Chaotic (SLC ) Map

The model performed on Lozi map that a well-known nonlinear system which exactly represented by the TS fuzzy model on $x_1(t),\ x_2(t)$ as the state vector in the vector variables $x(t) = [x_1(t)\ \ x_2(t)]^T$, where $x(t) \in R^2$, These features will be helpful in encryption stage for the message in KFCC through composing the increasing sequence $\mu_n$ with the super increasing sequence $S$. Basically, the model perfomed on the equation form for Lozi map in equation (4.11), with parameters system $\alpha \in [1, 1.8], \beta \in [0, 0.4]$, for some values for these parameters to view the chaotic behavior the dynamical system be as in equation (4.12).

The fuzzy sets that defined on values of premise variable $x_1(t)$ are as in equation (4.4), with positive real value for $d$ supposed at $d = 3.5$, that determine the interval of proper variable values $x_1(t) \in [-3.5, 3.5]$, and for $r = 2, \quad \sum_{i=1}^{2} F_i = 1$.

The equaled system matrices that associated with the equations (4.6) and (4.7) are in equation (4.2), and with bias terms $b_i$ on two rules as in equation (4.3).

To control on $x_1(t)$ values. As in the system seen in Section 4.2 in equation (4.14) also, for $x(t),\ b_i \in R^2,\ \ D_i \in R^{2\times 2}$, for $i = 1, 2$. In designing SLC map the system in equation (5.1) be;

$$f\big(x_n(t+1)\big) = C(2^{(s+F(x_n(t)))}) \qquad \ldots(4.26)$$

So
$$\begin{cases} x_1(t+1) = \sin(2^{\left(s+3-1.8|x_1(t)|+x_2(t)\right)}) \\ \quad x_2(t+1) = \sin(\ 2^{(s+0.25\, x_1(t))}) \end{cases} \qquad \ldots(4.27)$$

where $C(x) = sin(x)$, and $s \in [10, 25]$.

So $x_1(t+1),\ x_2(t+1) \in [-1, 1]$, for initial conditions let the values $x(0) = [1 \quad 0.25]$ .

### 4.3.2 The Numerical Scheme Experiment for SLC

The system performed with initial values for premise variables as; $x_1(0) = 1,\ x_2(0.25)$, and $s = 10$ after 40 iterations, to extract the secure key $k(t)$ from the state trajectory for the state $x_1(t)$.The sequence of sine chaotic be

$$sin\big(x(t)\big) = \{-0.123689894, 0.351946819, -0.528245544, 0.93393977\} \quad \text{…(4.28)}$$

With value for $\tau = 7$, then $S_1(t) = |-0.123689894| + 7$, and so the 4-terms super-increasing sequence;

$$S = \{7.123689894, 7.351946819, 7.528245544, 7.93393977\} \quad \text{…(4.29)}$$

$$T = \sum_{j=1}^{5} S_j = 29.93782203 \quad \text{…(4.30)}$$

Take $N = 39 > T$. Also select $W = 28$ in $[2, 38]$ and $gcd(W, N) = 1$. Compute a public hard knapsack; $O$ For each number with $(mod\ 39)$ be ;

$$O = \{4.463317032, 10.85451093, 15.79087523,27.15031356\} \quad \text{…(4.31)}$$

So $(S, W, M)$ are a private key and $B$ as public key. To encrypt the binary plaintext $M = \{0111,\ 1001, \dots, m_l\}$ with four terms. For each set $m_i$ from sender message, compute for instance the set $m_1 = \{0111\}$, and using public key;

$$E = 0 * 4.463317032 + 1 * 10.85451093 + 1 * 15.79087523 + 1 * 27.15031356 \quad \text{…(4.32)}$$

Then $E = 53.79569972$, Modify the ciphertext to;

$$\xi(t) = \left(\frac{2E - T}{\gamma T}\right)$$

$$\xi(t) = \left(\frac{2(53.79569972) - 29.93782203}{\gamma(29.93782203)}\right)$$

$$= \frac{77.65357741}{\gamma(29.93782203)}$$

$$\xi(t) = \frac{2.593828547}{\gamma} \quad \text{…. (4.33)}$$

Now, we need randomly take $\gamma \in R$ such that $\xi(t) \in (-0.01, 0.01)$, There are many values but here we will take only one, for instance; $288.2031719$, That $\xi(t) = 0.009$.

To decrypt $\xi(t)$, by find the invertible of $Wmod\ N$ as; $v28 = 1(mod\ 39)$, Then $v = 7$. The user perform the connection between easy and hard knapsacks through form ;

$vo_i = S_i(modN)$, for $i = 1, \dots, 5$ …(4.34)

In the set $\{7 * 4.463317032, 7 * 10.85451093, 7 * 15.79087523, 7 * 27.15031356\}$

Then $\{31.24322, 75.98158, 110.5361, 190.0522\}$

For $mod\ 39$ ;

$$\{31.24321922, 36.98157652, 32.53612662, 34.05219492\}$$

Here, $Z_i$ for each $e_i$ for $i = 1, \dots, 4$, and by substituting the values of $e_i$, testing condition; if that $\mathrm{Z_i} < 39$ and $\mathrm{T} < 39$. The message is $M = \{0111\}$.

TABLE 4.7: Sine map values on TS chaotic fuzzy model values

| *t* | *x1(t)* | *x2(t)* | *sin(2power x1)* | *abs sin x* | *sin(2power x2)* |
|---|---|---|---|---|---|
| 0 | 1 | 0.25 | -0.313057013 | 0.313057013 | -0.92831835 |
| 1 | 1.45 | 0.3625 | 0.998066961 | 0.998066961 | -0.179182443 |
| 2 | 0.7525 | 0.188125 | -0.397093223 | 0.397093223 | -0.888460467 |
| 3 | 1.833625 | 0.45840625 | -0.622320818 | 0.622320818 | -0.42037907 |
| 4 | 0.15788125 | 0.039470313 | -0.898656896 | 0.898656896 | 0.031437117 |
| 5 | 2.755284063 | 0.688821016 | 0.678144995 | 0.678144995 | -0.967890576 |
| 6 | -1.270690297 | -0.317672574 | -0.289285932 | 0.289285932 | -0.995633513 |
| 7 | 0.395084891 | 0.098771223 | 0.917849586 | 0.917849586 | -0.145308166 |
| 8 | 2.387618418 | 0.596904605 | -0.861776073 | 0.861776073 | 0.037952507 |
| 9 | -0.700808548 | -0.175202137 | 0.994655 | 0.994655 | 0.852846436 |
| 10 | 1.563342476 | 0.390835619 | -0.815126054 | 0.815126054 | -0.916887848 |
| 11 | 0.576819163 | 0.144204791 | 0.514472534 | 0.514472534 | 0.62169329 |
| 12 | 2.105930298 | 0.526482575 | -0.400518843 | 0.400518843 | -0.99998642 |

| | | | | | |
|---|---|---|---|---|---|
| 13 | -0.264191962 | -0.066047991 | -0.957244315 | 0.957244315 | -0.909413844 |
| 14 | 2.458406478 | 0.614601619 | -0.986620123 | 0.986620123 | -0.225684679 |
| 15 | -0.810530041 | -0.20263251 | -0.461563713 | 0.461563713 | -0.680105406 |
| 16 | 1.338413417 | 0.334603354 | 0.680110472 | 0.680110472 | -0.100645571 |
| 17 | 0.925459204 | 0.231364801 | -0.223844926 | 0.223844926 | 0.895841474 |
| 18 | 1.565538233 | 0.391384558 | 0.659943601 | 0.659943601 | -0.994966707 |
| 19 | 0.573415738 | 0.143353935 | -0.082994123 | 0.082994123 | 0.003691331 |
| 20 | 2.111205606 | 0.527801401 | 0.752602264 | 0.752602264 | -0.214935454 |
| 21 | -0.272368689 | -0.068092172 | -0.389376691 | 0.389376691 | 0.24075505 |
| 22 | 2.441644188 | 0.610411047 | 0.698242097 | 0.698242097 | -0.923978473 |
| 23 | -0.784548491 | -0.196137123 | -0.648345379 | 0.648345379 | 0.998712809 |
| 24 | 1.391675594 | 0.347918898 | -0.676282801 | 0.676282801 | 0.472568703 |
| 25 | 0.842902829 | 0.210725707 | 0.903755763 | 0.903755763 | -0.616447945 |
| 26 | 1.693500614 | 0.423375154 | 0.712247936 | 0.712247936 | -0.362316663 |
| 27 | 0.375074048 | 0.093768512 | 0.759033837 | 0.759033837 | -0.486825173 |
| 28 | 2.418635226 | 0.604658807 | 0.735526156 | 0.735526156 | -0.898354744 |
| 29 | -0.748884601 | -0.18722115 | -0.123689894 | 0.123689894 | 0.770372491 |
| 30 | 1.464786569 | 0.366196642 | -0.820122736 | 0.820122736 | 0.404285776 |
| 31 | 0.729580818 | 0.182395205 | 0.996973621 | 0.996973621 | -0.378889699 |
| 32 | 1.869149732 | 0.467287433 | 0.709360782 | 0.709360782 | 0.920939027 |
| 33 | 0.102817916 | 0.025704479 | 0.084254622 | 0.084254622 | -0.565190935 |
| 34 | 2.84063223 | 0.710158057 | 0.351946819 | 0.351946819 | -0.701896588 |
| 35 | -1.402979956 | -0.350744989 | -0.722139753 | 0.722139753 | -0.948468961 |
| 36 | 0.123891089 | 0.030972772 | -0.528245544 | 0.528245544 | -0.071205426 |
| 37 | 2.807968812 | 0.701992203 | 0.93393977 | 0.93393977 | 0.679799012 |
| 38 | -1.352351658 | -0.338087915 | -0.877713171 | 0.877713171 | -0.440067509 |
| 39 | 0.227679101 | 0.056919775 | -0.860323267 | 0.860323267 | -0.206824369 |
| 40 | 2.647097394 | 0.661774348 | -0.672508969 | 0.672508969 | -0.87528235 |

Figure 4.18 and the follows figures will illustrate the values for primitive variable, and other values in table (4.7).

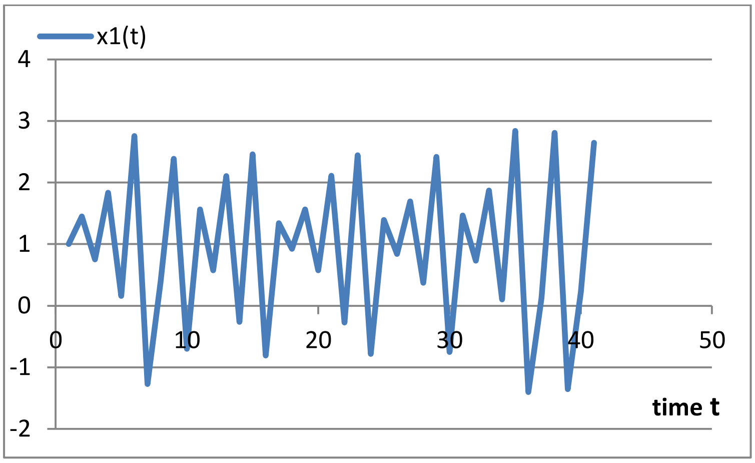


FIGURE 4.18: Values for $x_1(t)$ for iteration 40, as in table (4.7)

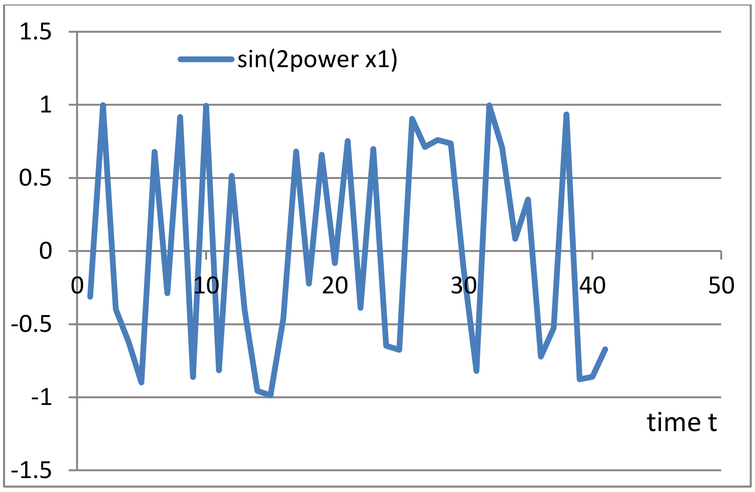


FIGURE 4.19: Sine Chaotic values for $x_1(t)$ with iteration 40 in table (4.7)

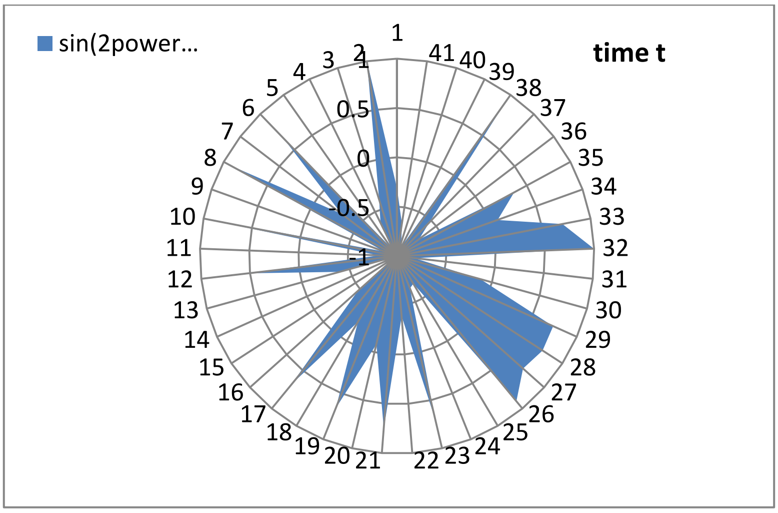


FIGURE 4.20: Sine Chaotic values for $x_1(t)$ with iteration 40 as circle

### 4.3.3 Conclusions for the Experiment on SLC

In this example, a designing of fuzzy model-based for chaotic map and cryptosystem has been proposed. The Knapsack problem was performed in combination with the T–S fuzzy model for discrete-time chaotic systems, that were exactly derived with only one premise variable. The sine map implemented on the chaotic map at Lozi chaotic map, with non-common bias terms and the same premise variable and driving signal. In this fuzzy model-based, a sine chaotic map were applied with numerical data for chaotic behavior, parameters data and premise variable with initial values in interval $[-3.5, 3.5]$. The advantage of this performance design is that all well-known chaotic systems stated achieved the results in more secure, since the trajectory values for premise variable, converted into values for sine map in interval $[-1, 1]$. Numerical simulations with the table and figures are shown to be consistent with theoretical design. The resulted trajectory values used to generate a secret key by choosing superincreasing sequence from the sine values for trajectory from the chaotic map under TS model. After masking and modifying the ciphertext between the users, the ciphertext be ready to decrypted. The security of the system shown in flexibility in changing the supposed values that will make the system behavior unpredictable. Also it could be extracted through; Employing a discrete chaotic map, and then compose the cosine map on it, and choosing the parameters values for chaotic map with chaotic behavior; Assume initial values randomly from closed interval in state space; Choosing the chaotic map is unpredictable; Finding a super-increasing sequence from the trajectory points, with increase iterations for absolute value for sine map for the seed chaotic map, the primitive variable trajectory has more than one super increasing sequence, we discussed the standard one with the longer sequence with four terms.

## 4.4 Example as Study Case on the 3D- Continuous KFCC:

### 4.4.1 Study Case on the 3D-KFCC

The chaotic Lorenz system for continuous-time is defined previously in Definition (2.3.1). The system with parameters values are: $a$=10, $b$=8/3 and $r$=28, so the system is given by;

$$\begin{aligned} \dot{x_1} &= -10x_1 + 10x_2 \\ \dot{x_2} &= 28x_1 - x_2 - x_1x_3 \\ \dot{x_3} &= x_1x_2 - 8/3x_3. \end{aligned} \qquad \ldots(4.35)$$

The equivalent fuzzy model constructed by ;

$\boldsymbol{Plant\ Rule\ i}$: $\boldsymbol{I}F\ x_1(t)\ is\ \ \Gamma_1^i\ THEN\ \dot{x}(t) = A_i x(t)$ …(4.36)

Thus, the rules are ;

$Plant\ Rule1$: $IF\ x_1(t)\ is$ about -d $THEN\ \dot{x}(t) = A_1x(t)$ …(4.37)

$Plant\ Rule2$: $IF\ x_1(t)\ is$ " $about\ \ d$ " $THEN\ \dot{x}(t) = A_2x(t)$ …(4.38)

where *"about d* " and *"about -d* " are fuzzy sets corresponding to $\Gamma_1^1, \Gamma_1^2$ in the rules system respectively. For values of $x_1(t)$, in the interval $[-d, d]$ with $d = 30$, the fuzzy sets defined with the triangular MFs by

*"about -d"*=$\Gamma_1^1\big(\,x_1(t)\big) = \frac{x_1(t)-(-d)}{d-(-d)} = \frac{x_1(t)+d}{2d}$ …(4.39)

*"about d"*= $\Gamma_1^2\big(\,x_1(t)\big) = \frac{d-x_1(t)}{d-(-d)} = \frac{d-x_1(t)}{2d}$ …(4.40)

Since $-d, d$ are controlled the non-linear terms in the system matrices which are given by

$$\mathrm{A}_1 = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & -d \\ 0 & d & -\frac{8}{3} \end{bmatrix}, \qquad \mathrm{A}_2 = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & d \\ 0 & -d & -\frac{8}{3} \end{bmatrix} \qquad \ldots(4.41)$$

The discretization of continuous-time chaotic Lorenz system depending on previous theorem (3.2) be;

$\boldsymbol{Plant\ Rule\ i}$: $IF\ x_1(t)\ is\ \ \Gamma_1^i\ THEN\ x(t+1) = D_i x(t)$ …(4.42)

Bias term as zero vector, with ;

$\boldsymbol{Plant\ Rule1}$: $IF\ x_1(t)\ is$ " $about\ -d$ " $THEN\ x(t+1) = D_1x(t)$

$\boldsymbol{Plant\ Rule2}$: $IF\ x_1(t)\ is$ " $about\ \ d$ " $\ THEN\ x(t+1) = D_2x(t)$

precisely could be written as ;

$\boldsymbol{Plant\ Rule1}$: $IF\ x_1(t)\ is$ "about -d " $THEN\ x(t+1) = D_1x(t)$

$\boldsymbol{Plant\ Rule2}$: $IF\ x_1(t)\ is\ "\ about\ \ d\ "\ \ THEN\ x(t+1) = D_2x(t)$

Where the matrices ;

$$\mathrm{D}_1 = \begin{bmatrix} 1-aT_s & aT_s & 0 \\ rT_s & 1-T_s & -dT_s \\ 0 & dT_s & 1-bdT_s \end{bmatrix}, \mathrm{D}_2 = \begin{bmatrix} 1-aT_s & aT_s & 0 \\ rT_s & 1-T_s & dT_s \\ 0 & -dT_s & 1-bdT_s \end{bmatrix}$$

$T_s$ values will supposed to be approvable with the chosen employing, in this paper takes $T_s = 0.003$ sec. with simulation calculations for $x_1(t) \in [-30, 30]$ the matrices be

$$\mathrm{D}_1 = \begin{bmatrix} 0.97 & 0.03 & 0 \\ 0.084 & 0.997 & 0.09 \\ 0 & -0.09 & 1.008 \end{bmatrix}, \qquad \mathrm{D}_2 = \begin{bmatrix} 0.97 & 0.03 & 0 \\ 0.084 & 0.997 & -0.09 \\ 0 & 0.09 & 1.008 \end{bmatrix}$$

We were implement an experiments staring with different initial values and continued for 40 times, that refer to points in the phase trajectory instead continuous connected curve.

### 4.4.2 The Experimental Result for the Example

The TS fuzzy model employed for Lorenz map with initial conditions $[-10 \quad 10 \quad 10]$ for vector state. The model iterated for 40 iteration to extract the secure key $k(t)$ from the state trajectory for state $x_1(t)$.

The value for $\tau$ assumed 18 since this value is with many factors$\{1, 2, 3, 6, 9, 18\}$. The Figures 4.20, 4.22, will explain the values in the table 4.8. While the Figure 4.21, will explain the using initial values $[-10 \quad 10 \quad 10]$, also for 40 iterations.

TABLE 4.8: TS chaotic fuzzy model values for continuous chaotic map

| t | $x_1(t)$ | $x_2(t)$ | $x_3(t)$ | $k(t) + \tau$ |
|---|---|---|---|---|
| 0 | -10 | 10 | 10 | 8 |
| 1 | -9.4 | 10.03 | 9.18 | 8.6 |
| 2 | -8.8171 | 10.03651 | 10.15614 | 9.1829 |
| 3 | -8.2514917 | 10.17981667 | 11.14067502 | 9.748508 |
| 4 | -7.698552449 | 10.45881267 | 12.14598392 | 10.30145 |
| 5 | -7.153831495 | 10.87389638 | 13.18444493 | 10.84617 |
| 6 | -6.612999659 | 11.42695289 | 14.26857117 | 11.387 |
| 7 | -6.071801083 | 12.12135146 | 15.41114549 | 11.9282 |
| 8 | -5.526006506 | 12.96195921 | 16.62535629 | 12.47399 |
| 9 | -4.971367535 | 13.95517085 | 17.92493547 | 13.02863 |
| 10 | -4.403571383 | 15.10895466 | 19.32430033 | 13.59643 |
| 11 | -3.818195602 | 16.43291483 | 20.83870065 | 14.1818 |
| 12 | -3.210662289 | 17.93837071 | 22.48437259 | 14.78934 |
| 13 | -2.576191299 | 19.6384535 | 24.27870094 | 15.42381 |
| 14 | -1.909751955 | 21.54822116 | 26.24039136 | 16.09025 |
| 15 | -1.206012762 | 23.68479255 | 28.38965439 | 16.79399 |
| 16 | -0.459288602 | 26.067502 | 30.74840296 | 17.54071 |
| 17 | 0.336515116 | 28.71807552 | 33.34046536 | 18.33652 |
| 18 | 1.187961928 | 31.66083044 | 36.19181588 | 19.18796 |
| 19 | 2.102147983 | 34.92290018 | 39.33082515 | 20.10215 |
| 20 | 3.086770549 | 38.53448617 | 42.78853277 | 21.08677 |
| 21 | 4.150202018 | 42.52913939 | 46.59894478 | 22.1502 |
| 22 | 5.301570139 | 46.94407397 | 50.79935889 | 23.30157 |
| 23 | 6.550845254 | 51.82051594 | 55.43072042 | 24.55085 |
| 24 | 7.908935375 | 57.20409023 | 60.53801261 | 25.90894 |
| 25 | 9.387790021 | 63.14524967 | 66.17068484 | 27.38779 |
| 26 | 11.00051381 | 69.69974992 | 72.38312279 | 29.00051 |

| | | | | |
|---|---|---|---|---|
| 27 | 12.76149089 | 76.92917488 | 79.23516526 | 30.76149 |
| 28 | 14.68652141 | 84.90151746 | 86.79267232 | 32.68652 |
| 29 | 16.79297129 | 93.69182122 | 95.12815027 | 34.79297 |
| 30 | 19.09993679 | 103.3828889 | 104.3214394 | 37.09994 |
| 31 | 21.62842535 | 114.0660644 | 114.4604709 | 39.62843 |
| 32 | 24.40155453 | 125.8420964 | 125.6421005 | 42.40155 |
| 33 | 27.44477078 | 138.8220897 | 137.9730259 | 45.44477 |
| 34 | 30.78609035 | 153.1285565 | 151.5707982 | 48.78609 |
| 35 | 34.45636433 | 168.8965743 | 166.5649347 | 52.45636 |
| 36 | 38.48957063 | 186.2750633 | 183.0981458 | 56.48957 |
| 37 | 42.92313541 | 205.4281951 | 201.3276867 | 60.92314 |
| 38 | 47.7982872 | 226.5369457 | 221.4268458 | 65.79829 |
| 39 | 53.16044696 | 249.8008071 | 243.5865856 | 71.16045 |
| 40 | 59.05965776 | 275.439675 | 268.017351 | 77.05966 |

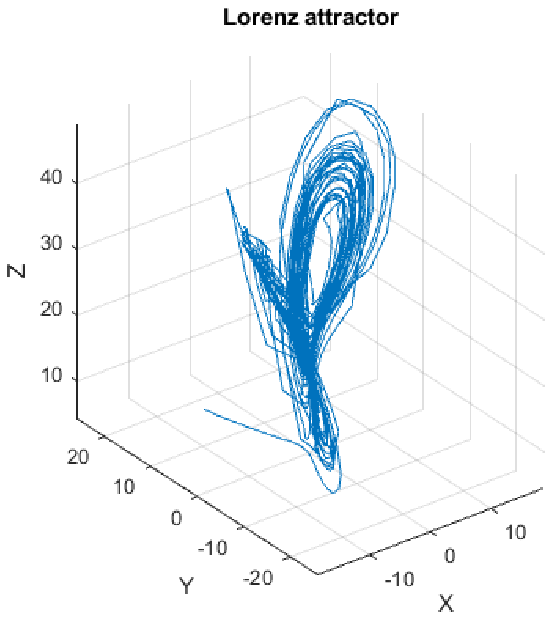


FIGURE 4.21: Lorenz attractor with initial value $[-10\ \ 10\ \ 10]$

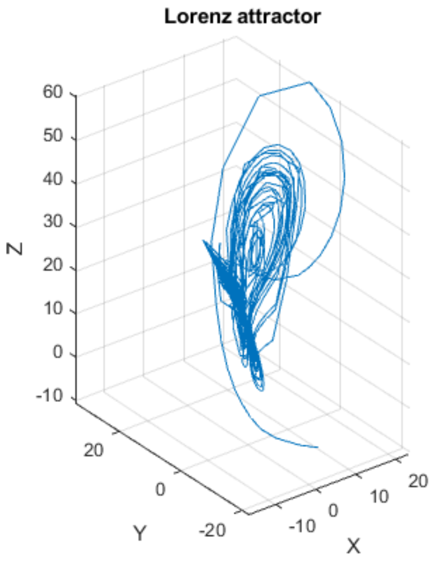
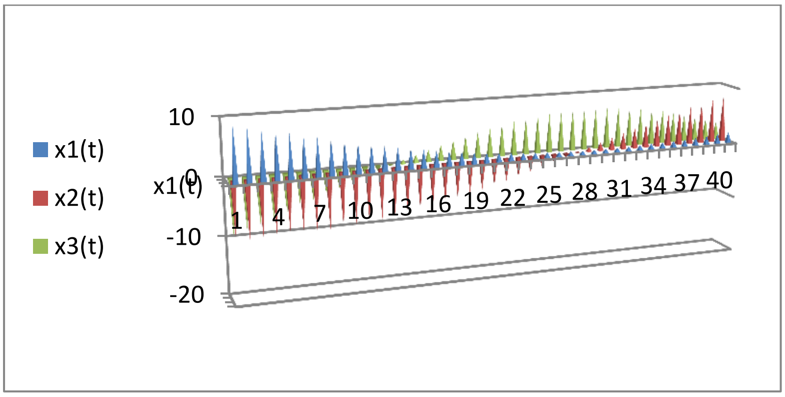
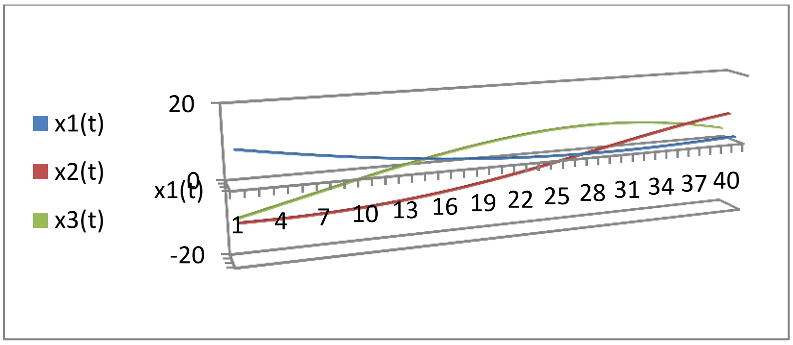


FIGURE 4.22: Lorenz attractor with initial value $[10\ -10\ -10]$

These figures were drawn by using MATHLAB R2018b, for iteration 40, and episode= 0.10000001, which represent the Ordinary differential equation solver precision in drawing the figure.



(a)



(b)

FIGURE 4.23: Trajectories for $x_1(t), x_2(t), x_3(t)$ in two different manner

We get a real values super-increasing sequences both with five terms, after 40 iterations as;

$S = \{8, 8.6, 16.79399, 34.79297, 71.16045\}$, then $T = 139.34741$.

Suppose *W=73*, *N=72*, for $bi = WSi\ (mod\ N)$,

then;

$b_i = \{584, 627.8, 1225.96127, 2539.88681, 5194.71285\}$.

Suppose a plaintext $M = [11100]$.

Compute $c_i = \sum_{j=1}^{s} m_{ij} b_j$, $Ci = \{8, 51.8, 1.96127, 0, 0\}$, then

$$C = 61.76127.$$

Now the modification will computes by $\gamma = 10^{-2}$to keeping in $(-0.01, 0.01)$, Then $\xi(t) = -0.001135641$.

That resented to first user to decrypt the ciphertext into $C = (\gamma\xi(t) + 1)T/2$. Since he/she knows the value $T$, and receive from public channel $\gamma$. Calculate $v$ an invers of $W(mod\ N)$, then $v = 71$.

Compute $vb_i = S_i(modN)$ as;

$vb_i(mod\ 74) = \{16, 17.2, 1.13398, 31.62394, 0.7509\}$,

then ;

$S_i(mod\ 72) = \{8, 8.6, 16.79399, 34.79297, 71.16045\}$,

for $i = 1, \dots, 5$. $m_i S_i = \{8, 8.6,\ 16.79399,\ 0, 0\}$, $Z_i = 33.39399$.

Then the message $M = \{11100\}$.

**Note** : The system implemented with initial state vector $[-10 \quad 10 \quad 10]$, we don't get super-increasing sequence even after 40 iteration.

### 4.4.3 Conclusions for the Experiment on the 3D Continuous KFCC

The proposed Knapsack fuzzy chaotic cryptosystem applied the Lorenz map that uses the TS-fuzzy model to generate a secret key to given another version of fuzzy chaotic cryptosystem.

The super-increasing sequence with positive real values added more complicated in computations and predictions. The study case implemented on continuous Lorenz map discrete theoretically by random time sample. A fuzzy model is implemented for 40 iterations on the chaotic system. The initial values assumed in two state vectors $[-10 \quad 10 \quad 10]$ and $[10 \quad -10 \quad -10]$.

All values and work performed on 1st vector while don't work with 2nd after 40 iterations. Resulted trajectory for a primitive variable are used to generate secret key by choosing a super-increasing sequence from data. A good results and flexibility for changing the supposed values made the system behavior is unpredictable.

The security of the proposed KFCC cryptosystem is determined through many points: Employing continuous chaotic map and then discrete it, using a random sample time in discretize, choosing the parameters values for chaotic map with chaotic behavior, assume initial values randomly from closed interval in state space, choosing chaotic map is unpredictable, finding a super-increasing sequence from the trajectory (orbit) of points, increasing of the iterations and when the trajectory has more than one super-increasing.

## 4.5 Comparison Between KFCC and the Design of Fuzzy Chaos-Based Cryptosystem

In comparition between the KFCC and the previous system for fuzzy chaos-based cryptosystem by Chian and Kuang in [1], it is clear there are good points such:

TABLE4.9:Comparition between KFCC and Fuzzy Chaos-Based Cryptosystem

| **Fuzzy Chaos-Based Cryptosystem** | **KFCC** |
|---|---|
| Applied on 2D discrete time chaotic systems | Applied on 2D and 3D discrete time chaotic systems |
| Applied on discrete time chaotic systems only | Applied on discrete and countinuous time chaotic systems |
| Length of superingreasing sequence determined by user | Length of superingreasing sequence Determined by user iterations number of performing chaotic system |
| Depends on the chaotic system parameter values | Depends on the chaotic system parameter values, the initial value for primitive variable, the random parameter and values in Knapsack problem. |
| Performed on Henon map only | Performed on Lozi map, and Lorenze map. |
| Depends on on superincreasing in the system | There are two or more super increasing in the iteration could be depend on it. |
| Could not modify chaotic system on TS | Could modify the chaotic system by countinuous map such sine and cosine map in TS. |
| Secure | More Secure because complexity |

# Chapter Five

# Conclusions and Future Works

## 5.1 Conclusions

The suggested system KFCC are introduced as a new method for combining TS fuzzy model and chaotic systems with knapsack problem, in crypto systems. In first, It were implemented on 2D and 3D discrete time chaotic map. The applied system on discrete time were modified by implementing discrete chaotic map as seed map in continuous maps such; cosine and sine map, and then implement TS fuzzy model. Next the system performed on continuous time chaotic map, that needs to discretize it to be applicable in cryptosystem.

The suggested system improved through apply a KFCC with Master-Slave systems as KFCCMS for chaotic systems to achieve the synchronization signal that effective in decrypt the ciphertext.

Performing the Discrete-time 2D KFCC led to low security through superincreasing sequence with only two items. These result do not help us to work on it, since it not led to complicity and then unsecure.

The modification on the system by seeding chaotic maps in cosine and sine map, in generating the superincreasing sequence for premise variable to create a secret key, and chaotic signal, that are used in modify the ciphertext. This led to produce a superincreasing sequence longer than previous, a superincreasing sequence with four and five items. The complexity and security of this were by the choosing arbitrary initial conditions for the map, in addition to the arbitrary parameters values within the performed Knapsack problem, and the iteration number by user.

An appropriate complexity and security for the suggested system were used when performing the 3D continuous-time chaotic map in KFCC and the discretize its trajectory for primitive variable. This performed using the Lorenz map. The complexity and security of this were by the choosing arbitrary initial conditions for the map, arbitrary parameter value that discretize the trajectory, in addition to the arbitrary parameters values within the performed Knapsack problem, number of superincreasing sequence items(control on length of box message), and the iteration number by user.

The performing of the KFCCMS. That improving the suggested system is by apply a KFCC with Master-Slave systems as KFCCMS for 2D chaotic systems to achieve the synchronization signal. That through performing the 2D discrete-time chaotic map in KFCC and use trajectory for primitive variable to generate the superincreasing sequence. This performed using the same example results that performed by KFCC on 2D chaotic map, and then work on it.

Security of KFCCMS are in addition to the points in previous direction such; choosing initial conditions, arbitrary parameters values within the performed Knapsack problem, number of superincreasing sequence items (control on length of box message), and the iteration number that needs to be increased to increase complexity and achieve synchronization. The designing a TS fuzzy model transmitter and receiver system for chaotic signal, play effective role in complexity. These systems need to introduce with estimated values (chosen arbitrary), and associated parameters vectors at masking and embedding the modified ciphertext.

## 5.2 The Security of the KFCC and KFCCMS

The main security features for the suggested system in its directions are listed below;

1. The based chaotic system in the fuzzy chaotic cryptography in this method could be changed, but must be represented exactly by a TS fuzzy model.
2. The apparent irregularity of chaotic signals is reduced to the source of randomness in the chaotic system, and this depends on the work.
3. The rules that characterize local relation(s) of the chosen system in the state space.
4. The essential feature for TS fuzzy model is expressing the local dynamics of each fuzzy implication through a linear state-space system model by some appropriate membership functions.
5. The randomness in choosing the initial values for chaotic systems, and other parameters used in the designing. Starting a fuzzy chaotic system, by choosing in some arbitrary way and different initial values for used chaotic systems with parameters ensures the chaoticity.
6. At the Knapsack encryption process, selecting the values for $N$ and $W$ randomly under some constraints, will also add security for the method through randomity values.
7. Generate a time varying superincreasing sequence and apply it in cryptosystem, depending on the chaotic behavior for the used chaotic discrete or continuous system, but in discrete situations for both.
8. Chaotic systems for some initial values contain more than one superincreasing sequence, which is helpful in choosing any one.
9. The number of fuzzy rules depends on the number of fuzzy sets for values of primitive variables.
10. In both fuzzy sets for values of premise variable $x_1(t)$ the masking rules for finding $\bar{y}(t)$ are same form but with different values.
11. Increasing iterations number will increase the terms number in the super increasing.

12. The number of terms of superincreasing sequence determines the length of the message by binary string to sets with a number of elements. The length used in this work is at least for four terms and above and eliminate the cases with two terms. So, a set with 4 or 5 numbers, such {0011, …}, or {10101,…}.
13. The ciphertext is embedded in the output of the TS fuzzy model for a chaotic system.
14. Capability in use different states values, and some other estimated values in masking the plaintext.
15. Add discretization time step parameter value for continuous chaotic map increase complexity.
16. Multi Users are capable of employing this cryptosystem
17. The KFCCMS system is designed depending on KFCC, so the security points also will inherited in this system.

From above points the chosen cryptosystem has a systematic design with a high level of security.

## 5.3 Future Works

This study has multiple unresolved issues and problems. We summarize the problems below as potential future works;

1. Regarding to the KFCC, perform the system on 3D continuous time chaotic map with large values for parameter time step.
2. Regarding to the KFCC, perform the system other 3D continuous time chaotic maps than Lorenz map.
3. Regarding to the KFCCMS, perform the system on 2D discrete time chaotic map.
4. Regarding to the KFCCMS, perform the system on 3D continuous time chaotic map.
5. Introduce a practical application for KFCC in real live.
6. Introduce a practical application for KFCCMS in real live.

# References

[1] C. E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, Vol. 28, 1949.

[2] Z. Li, Fuzzy Chaotic Systems, Springer-Verlag Berlin Heidelberg, Netherlands, 2006, pp. 275–283.

[3] Gonzalo Alvarez, Shujun Li, Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems, International Journal of Bifurcation and Chaos, vol. 16, no. 8, 2006, pp. 2129-2151.

[4] M. Seidi, Marzieh Hajiaghamemar, Bruce Segee, Fuzzy Control Systems: LMI-Based Design, INTECH, Creative Commons Attribution License, 2012.

[5] K. Y. Lian, T. S. Chiang, C. S. Chiu and P. Liu, Synthesis of Fuzzy Model-Based Designs to Synchronization and Secure Communications for Chaotic Systems, IEEE Transactions on Fuzzy Systems,MAN, AND CYBERNETICS—PART B: CYBERNETICS, Vol. 31, NO. 1, 2001, pp. 66 – 83.

[6] K. Y. Lian, C. S. Chiu, T. S. Chiang, P. Liu, LMI-Based Fuzzy Chaotic Synchronization and Communications, IEEE Transactions on Fuzzy Systems, Vol. 9, No. 4, 2001, pp. 539 –553.

[7] Z. Li, Wolfgang A. Halang, G. Chen, Integration of Fuzzy Logic and Chaos Theory, Springer-Verlag Berlin Heidelberg Printed in The Netherlands, 2006, pp.(507–525)

[8] Chang-Ho Hyun, Jae-Hun Kim, E. Kim, M. Park, Adaptive Fuzzy Observer Syncronization Design and Secure Communications of Chaotic Systems, Elsevier, Chaos Solutions and Fractals Vol. 27, 2006, pp.(930-940)

[9] Gwo-Ruey Yu, " Robust Chaotic Cryptosystems Based on T-S Fuzzy Model", The 17th World Congress Federation of Automatic Control Seoul, Korea, 2008.

[10] R.-Precup, M.-L. Tomescu, St. Preitl, Fuzzy Logic Control System Stability Analysis Based on Lyapunov's Direct Method, International Journal of Computers, Communications and Control, Vol. IV, No. 4, 2009, pp.(415-426)

[11] M. Ababneh, I. Etier, M. Smadi, J. Ghaeb, Synchronization of Chaos Systems Using Fuzzy Logic, Journal of Computer Science 7 (2), 2011, pp. 197-205.

[12] Ljupco Kocarev, Shiguo Lian, Chaos-Based CryptographyStudies in Computational Intelligence vol 354 Springer, 2011

[13] G. Makris , I. Antoniou, Cryptography with Chaos, Chaotic Modeling and Simulation (CMSIM) 1, 2013, pp.169-178.

[14] Saad M. Darwish, Adel A. El-Zoghabi, Mohammed A. Abdawi, 2014, Database Encryption Using Fuzzy Chaotic international Journal of Future Computer and Communications, Vol. 3, No. 6.

[15] Lahcene Merah, Adda Ali-Pacha, Naima Hadj-Said, Belkacem Mecheri, and Mustafa Dellassi, "FPGA Hardware Co-simulation of New Chaos-Based Stream Cipher Based on Lozi Map", International Journal of Engineering and Technology, Vol. 9, No. 5, 2017

[16] Hamdy M. Mousa, 2018, Chaos Genetic-fuzzy Encryption Technique, I.J. Computer Network and Information Security, DOI, 105815,04.02.

[17] L. Kocarev and S. Lian, Chaos-Based Cryptography Studies in Computational Intelligence Vol. 354 Springer, 2011, pp. 10–65.

[18] Zahraa M. Alroubaie, Muneer A. Hashem, Fadhil S. Hasan, FPGA Design of Encryption Speech System using Syncronized Fixed-

Point Chaotic Maps Based Stream Ciphers, International Journal of Engineering, 2019

[19] Moatsum Alawida, Azman Samsudin , Je Sen Teh , Wafa' Hamdan Alshoura,"Digital Cosine Chaotic Map for Cryptographic Applications", IEEE Access, Vol. 7, 2019.

[20] C. Meshram, C. Chi Lee, A. S. Ranadive, C. Ta Li, S. G. Meshram, J. V. Tembhurne, A Subtree-Based Transformation Model for Cryptosystem Using Chaotic Maps Under Cloud Computing Environment for Fuzzy User Data Sharing, John Wiley & Sons, Ltd, 2020.

[21] J. J. Buckley, E. Eslami, An Introduction to Fuzzy Logic and Fuzzy Sets, Springer 2002, pp.17-106

[22] L. Reznik, Fuzzy Controllers, Great Britain by Biddles Ltd, Guildford and King’s Lynn, pp.(1-57)(63-72) (124-152), 1997.

[23] T. Harvey, D. Mullins, Fuzzy Modeling and Control, Nova Science Publishers, NewYork, 2018, pp.(2-23)

[24] Robert F., Neural Fuzzy Systems, Abo Akademis tryckeri, Abo, 1995. pp. 249

[25] Michael Brin, Garrett Stuck, Introduction to Dynamical Systems, Cambridge University Press,2004.

[26] D. R. Stinson, M. B. Paterson, Cryptography Theory and Practice, Taylor & Francis Group, LLC, CRC Press, 2019

[27] P. Bauer, S. Nouak , R. Winkler, A brief course in Fuzzy Logic and Fuzzy Control, version 1.2, The FTP server FLLL , 1996

[28] W. Krabbs, S. Pickl, Dynamical systems :Stability,Controlability, and Chaotic Behavior, Springer, 2010, pp.163-172

[29] Z. Li, J Bae, Park, Y. Hoon Joo, Y. Ho Choi, G. Chen, Anticontrol of Chaos for Discrete TS Fuzzy Systems, IEEE Transaction on

Circuits and Systems-I: Fundamental Theory and Applications, Vol. 49, No. 2, 2002

[30] A. Ebrahimnejad, J. Luis Verdegay, Fuzzy Sets-Based Methods and Techniques for Modern Analytics, Springer, 2018, pp. 11-89.

[31] Z. Hua, Y. Zhou and H. Huang, "Cosine-transform-based chaotic system for image encryption", Elsevier Inc., Information Sciences 480, 403–419, 2018.

[32] H. O. Wang, K. Tanaka, M. F. Griffen, An Approach to Fuzzy Control of Nonlinear Systems: Stability and Design Issues, IEEE Transaction on Fuzzy Systems, Vol. 4, No. 1, 1996.

[33] Leondes C. T., Fuzzy Logic and Expert Systems Applications, ACADEMIC PRESS, 1998, pp.(1-5)(40-51)(60-77)

[34] R. Ezzati, R. Enayati, A. Mottaghi, and R. Saneifard ,"A New Method For Ranking Fuzzy Numbers Without Concerning Of Real Numbers" , TWMS Jour. Pure Appl. Math., vol.2, No..2, 2011, pp.256-270

[35] S. Mitra, Sankar K. Pal, Fuzzy sets in pattern recognition and machine intelligence, Fuzzy Sets and Systems, Elsevier, 156 ,2005

[36] Jonathan M. Garibaldi, Robert I. John, Choosing Membership Functions of Linguistic Terms, The IEEE International Conference on Fuzzy Systems, 2003.

[37] W. Wang, Y. Gan, B. Wang, X. Zhao, Q. Yang, Nonlinear Fuzzy Model Predictive Control of a Class of Chaotic Systems, IEEE, 2018

[38] H.-J. Zimmermann, Fuzzy Set Theory, John Wiley & Sons, Inc., Vol. 2, 2010.

[39] C. Chen H., Fuzzy Logic and Neural Networks Handbook , McGraw-Hill 1996 ,pp.(2-27) .

[40] Shih-Yu Li, Zheng- Ming Ge, Fuzzy Modeling and Synchronization of Two Totally Different Chaotic Systems via Novel Fuzzy Model, IEEE Transaction on Systems, Man, and Cybernetics-Part B: Cybernetics, Vol. 41, No. 4, 2011

[41] Reznik L. , “Fuzzy Controllers ” ,Great Britain by Biddles Ltd,Guildford and King’s Lynn ,1997

[42] Shang Gao, Zaiyue Zhang ,"Multiplication Operation on Fuzzy Numbers" ,Academy Publisher National Natural Science Foundation of China ,Journal of Software ,Vol. 4, NO. 4, JUNE 2009

[43] Sha Fu, Zhongli Liu, Hangjun Zhou, Dan Song and Yezhi Xiao,"Trapezoidal Fuzzy Number Attitude Indicators Group Decision Making Approaches Based on Fuzzy Language", Asian network for scientific Information ,Journal of Applied Sciences, 14: 2304-2308 ,2014 .

[44] Z. Li, J. Bae Park, Y. Hoon Joo, Y. Ho Choi, G. Chen, Anticontrol of Chaos for Discrete TS Fuzzy Systems, IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol. 49, No. 2, 2002

[45] R. L. Devaney, An Introduction To Chaotic Dynamical Systems, (Second Edition", Addison-Wesley Studies in Nonlinearity, 1989), pp. 17–159.

[46] Michar Misiurewicz, Strange Attractors For The Lozi Mappings, NYAS, 1980.

[47] D. M. Burton, Elementary Number Theory, seventh edition McGraw Hill Companies, 2011.

[48] J. Hoffstein, J. Pipher, J. H. Silverman, An Introduction to Mathematical Cryptography, Springer Science+Business Media, LLC, 2008

[49] Z. Hua, Y. Zhou, Hejiao Huang, Cosine-transform-based chaotic system for image encryption, Inc., Information Sciences 480, Elsevier, 2018, pp.(403–419)

[50] V. G. Ivancevic, T. T. Ivancevic, High-Dimensional Chaotic and Attractor Systems, springer, 2007, pp. (419-424)

[51] Hao Ying, Fuzzy Control and Modeling, IEEE Engineering in Medicine and Biology Society,2000

[52] V. Narsing Raol, K. Bhargavi, R. Reddy, An Approach for Secure Communication by Chaos-Based Cryptosystem, International Journal of Innovative Research in Technology IJIRT, Vol. 4, Iss.12, 2018.

[53] Jian Zhang, Akshya Kumar Swain, Sing Kiong Nguang, "Robust Observer-Based Fault Diagnosis for Nonlinear Systems Using MATLAB", Springer International Publishing Switzerland, 2016, pgs. (203-221)

[54] J. Zhang, A. Kumar Swain, S. Kiong Nuang, Robust Observer-Based Fault Diagnosis for Nonlinear Systems Using MATLAB, Springer, 2016, pp.(203-220)

[55] D. Zhang, B. Wei, Learning Control: Applications in Robotics and Complex Dynamical Systems, Elseiver Inc., 2021, pp. (93-102)

[56] Z. Hua, Y. Zhou and H. Huang, "Cosine-transform-based chaotic system for image encryption", Elsevier Inc., Information Sciences 480, 403–419, 2018

# الملخص

تم اقتراح نماذج نابساك فوضوية ضبابية القائمة على نظام التشفيركمزيج بين مشكلة النابساك ونظام التشفير المبني على الفوضى الضبابية. هذا من خلال تطبيق مشكلة النابساك في نموذج تاكاجي-سوجينو الضبابي القائم على نظام فوضوي متقطع ثم فك تشفير الرسالة. تم تعديل النظام باستخدام دالة فوضوية متقطعة لتكون دالة بذرة داخل دالة مستمرة. تم التعديل باستخدام دالتي الجيب والجيب.

بعد ذلك ، تم تنفيذ مشكلة النابساك في نموذج تاكاجي-سوجينو الضبابي كنظام محرك للنظام الفوضوي المستجيب في تشفير الرسالة وكنظام استجابة في فك تشفير الرسالة. يم تحقيق إشارة المزامنة مع مكاسب التغذية المرتدة بين نظام استجابة المحرك عند ديناميكية الخطأ التي تم تحديدها بدقة لضمان الاستقرار. من خلال حل مشكلة متباينة المصفوفات الخطي ليتمكن للنظام من فك تشفير الرسالة.

تم تنفيذ الأنظمة المقترحة على أنظمة الفوضى الزمنية المنفصلة ثنائية وثلاثية الأبعاد. يؤثر تكرار النظام الفوضوي على طول تسلسل الزيادة الفائقة ، والذي يزداد أيضًا عن طريق تعديل النظام. كانت الحواسيب يدويًا و Microsoft Excel 2010 ، وتم رسم بعض الأرقام بواسطة MATHLAB R2018b

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة بابل

كلية التربية للعلوم الصرفة

قسم الرياضيات

# نماذج فوضوية ضبابية قائمة على نظام التشفير

أطروحة

مقدمة إلى مجلس كلية التربية للعلوم الصرفة في جامعة بابل

كجزء من متطلبات نيل درجة الدكتوراه فلسفة في التربية / الرياضيات

من قبل

بشرى حسين عليوي ناصر

بأشراف

أ.م. د. رومى كريم خضير عجينة

٢٠٢٢م

١٤٤٣ هـ