https://doi.org/10.26682/csjuod.2023.26.2.48

Journal of University of Duhok., Vol. 26, No.2 (Pure and Engineering Sciences), Pp 533 - 540, 2023
4th International Conference on Recent Innovations in Engineering (ICRIE 2023) (Special issue)

DESIGNING AN ENCRYPTION FUNCTION FOR CHAOTIC-BASED MODEL WITH BIFURCATION SHIFTING IN SECURITY COMMUNICATE

BUSHRA **H**USSIEN **A**LIWI
Dept. of Mathematics, Education College for Pure Sciences, University of Babylon-Iraq

(Accepted for Publication: November 27, 2023)

ABSTRACT

A new design for a function(s) developed in the encryption stage on secret communications by shifting of the bifurcation for Quadratic map that is chaotic with one parameter. These functions approach the values for parameters on the real axis. Each new value for a chaotic map will add to the generated real values super increasing sequence toward negative infinity, and then modify the ciphertext. Bifurcation shifting computed through different functions shifting the bifurcation function such as triangular and exponential function. A modified ciphertext applied in the terms of a fuzzy chaotic based model. This encryption stage will be applied in communication models or as a part of the master-slave system. Then we provide the algorithms to recover the performance steps of the designed method. Finally, the process of numerical implementation is discussed to verify the effectiveness of the method with primary results.

***KEYWORD*: -** Bifurcation, Fuzzy chaotic, Logistic map, Quadratic family, Takagi-Sugeno Model.

INTRODUCTION

Most works on communication aim for security and affectivity. The chaos-based cryptography schemes were designed for digital communication.

The interactions between chaos theory and fuzzy logic gain an interesting and importance. For the past 30 years have many directions in research such as fuzzy modeling of chaotic systems with Takagi-Sugeno TS fuzzy models, models with linguistic descriptions of chaotic systems, fuzzy control systems of chaos models, and a combination between fuzzy control technology and chaos models in engineering technology and chaos theory [1]. The fuzzy model-based synchronization approaches on a chaotic systems are implemented for a chaos-based secure communication system (SCS)[2]. A systematic control design for multivariable TS fuzzy system through control algorithms are approached with relaxed stabilization conditions that were derived and solved by linear matrix inequality LMI. A fuzzy controller designed to control performance problem with parametric uncertainties in TS fuzzy model [3].

As integrating between fuzzy logic and chaos theory in [4], through introduce a fuzzy model-based chaotic cryptosystem used use the Lur´e type discrete-time chaotic systems. The model represented by TS fuzzy models with a super increasing sequence using a chaotic signal. Output of the TS fuzzy chaotic drive system, or any state in performed to synchronization error in cryptosystem, and the message is encrypted using the superincreasing sequence at the drive system. The ciphertext embedded in scalar signal is sent to the response system [5].

A triangle functions such sine and cosine were implemented with chaotification and chaotic maps as in [6] and [7], since these functions are nonlinear continuous and periodic function and simple in computations.

A Fuzzy modeling and fuzzy prediction-based feedback control schemes applied on unstable chaotic dynamical systems [8]. And the fuzzy models were established by input–output data pairwise. That led to ensuring the chaotic state was stable with constant targets, at fixed points or unstable periodic orbits in phase plane [8].

Perform the applications of Nonlinear Systems using MATLAB is powerful especially in dealing with chaotic systems [9]. The book introduces industrial applications in a real-world context, with some examples of systems.

The remainder of the paper is organized as follows. In Sec. 2, the essential designing of fuzzy chaotic-based model is presented for a general autonomous dynamical system with diagram of work, and in Sec. 3, the suggested fuzzy chaotic encryption terminology is derived with steps of details. In Sec. 4, a masking signal process with two subsections for designing the master system as chaotic fuzzy model, and bifurcation shifting

pure.bushra.hus@uobabylon.edu.iq

for masking the signal. For this bifurcation for quadratic map considered using MATLAB. Finally, a conclusion is summarized for this work.

1. Fuzzy Chaotic-Based Model

The TS fuzzy chaotic master model started with a n-dimension chaotic system. A chaotic system has a primitive variable that makes the nonlinear terms in the system.

For explaining the details: Consider a discrete-time nonlinear control chaotic system as:

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

This system with an input term, where the vector $x(t) = [x_1(t)\ \ x_2(t)\ \ ....\ \ x_n(t)]^T \in R^n$, is state vector, functions $f\big(x(t)\big)$ and $g(x(t)) \in R^n$ are nonlinear vector functions defined on $x(t)$, a vector $u(t) \in R^m$ is a control input vector for m dimension (may be $m < n$), determine m based on nonlinear equations number in the chaotic system. Firstly, the TS fuzzy model is composed as a set of fuzzy rules ;

$$Plant\ Rule\ i{:}\ IF\ x_1(t)\ is\ \mathrm{L}_1^i\ and\ x_2(t)\ is\ L_2^i\ and\ ....\ and\ x_n(t)\ is\ \mathrm{L}_n^i$$

$$THEN\ x(t+1) = D_i x(t) + H_i u(t),\ i = 1, 2, \ldots, q \qquad (2)$$

For $(t+1)$ is index of time steps, q is rules number of this TS fuzzy model, L_j^i are fuzzy sets for values of $x_j(t)$ and $j = 1,2, \ldots n$, $D_i \in R^{n\times n}$ is a discrete-time control system matrix (system matrix), $H_i \in R^m$ is an bias matrix. $x_1(t), x_2(t), \ldots, x_n(t)$ are premise variables, that is variables make the nonlinear terms in the chaotic system, which consist of state values in states space for the chaotic system. The membership functions for fuzzy sets could be selected with any form, since choosing membership function in these fuzzy sets will diverge with so little values that will not affect the computed values, generally it is chosen as a triangular fuzzy number (triangular membership function with real values).

The essential feature for the TS model is expressing the local dynamics of each fuzzy implication through a linear state-space system. Then model the fuzzy system through fuzzy blending of the local linear system models by some appropriate membership functions. Rules number depends on the fuzzy set numbers for the primitive variables values .

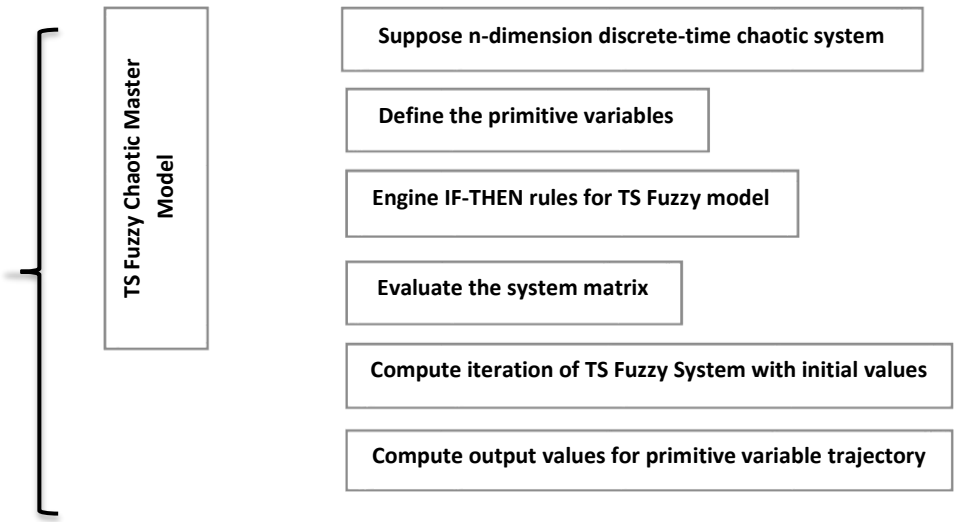


Fig.(1):- The discrete-time TS fuzzy model for nd-chaotic system

2. The Suggested Fuzzy Chaotic Encryption Terminology

The structure of the suggested chaotic encryption represented by TS fuzzy model through the essential terminologies and definitions;

▪ Use the plaintext M to transmitted as a composite message vector
$M = [m_1 m_2 \dots m_l]$, the message $m_i \in \{0,1\}$, $i = 1, \dots, l$, i is index of messages.
▪ The positive real value superincreasing sequence S_i, such that;

$S(t) = [S_1(t) S_2(t) \dots . S_l(t)]$, and add it to the increasing sequence μ_n, $n = 1, \dots, \infty$, converges, as $n \to \infty$, that will encode text M.
▪ Encryption function for encode the plaintext to be ciphertext is $E(.)$ using the key K, through combines the plaintext with the superincreasing sequence formed by the sequence of key signal as in following form;

$$K(t) = [k(t-0)k(t-1), \dots, k(t-l+1)]$$
$$= [x_1(t-0)x_1(t-1), \dots, x_1(t-l+1)] \quad (3)$$
$$S_1(t) = |k(t)| + \tau \quad \text{and} \quad S_j(t) = \sum_{i=1}^{l-1} S_i(t) + |k(t-l+1)| + \tau \quad (4)$$
$$E\big(M(t), K(t-i)\big) = (S(t) + \mu_n) M(t)^T = E(t) \quad (5)$$
$$\text{for } i = 0,1, \dots l-1 \text{ , and } n = 1, \dots, l \text{ .}$$

M is $E = \{c1, \dots, cl\}$, where E is an encryption function.
▪ Next, the second user modify the encryption function C to the $\xi(t)$;

▪ First user compute $c_i = \sum_{j=1}^{s} m_{ij} b_j$ where c_i is a ciphertext that corresponds to the plaintext m_i, with s elements. So, the ciphertext for a plaintext

$$\xi(t) = \left(\frac{2E}{T} - 1)\right) / \rho$$

for ρ is a small scalar put $\xi(t) \in (-0.01, 0.01)$. The ciphertext $\xi(t)$will sends to the first user.

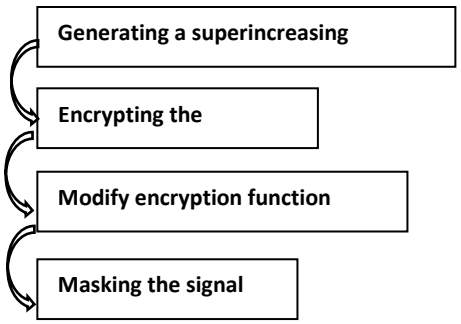


Fig.(2):- Diagram of generating the ciphertext in encryption function

3. MASKING SIGNAL PROCESS

The steps for masking signals with embedded messages must start by designing a TS fuzzy model as master (transmitter) Then make a mask for the signal they will use. Later the fuzzy inferred results transmitted to TS fuzzy response system (slave).

4.1 Designing the Ts Fuzzy Master System with Fuzzy Chaos Model

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.

For modulation process the masking signal is injected into the chaotic transmitter that expressed as a TS fuzzy model transmitter. So, to extract the transmitter from the primitive variable say $x_1(t)$ from $x_1(t)$ or $x_2(t)$

$$plant\ Rule\ i: IF\ x_1(t)\ is\ L_i$$
$$THEN\ x(t+1) = D_i x(t) + H_i(t) u(t) + \Gamma_i \xi(t) \quad (6)$$
with the masking mechanism by rule;

$$Masking\ Rule\ ij: IF x_1(t)\ is\ L_i$$
$$THEN\ \bar{y}(t) = \hat{E}x(t) + \hat{M}_j\xi(t),\ i = 1,2,\dots,r\ , j = 1,2,\dots,z \qquad (7)$$

$j = 1,2,\dots,z$ is index of mask values in bifurcation columns, $\bar{y}(t)$ is the coupling masked signal, and $\hat{M} \in R$, is the public output masking key, The value of $\hat{M} \neq 0,1$, added complexity to the work, 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:

$$Tranmitter\ Rule\ ij: IF\ \bar{y}(t)\ is\ L_i$$
$$THEN\ x(t+1) = D_i x(t) + H_i(t)u(t) + \Gamma_i\hat{M}_j\xi(t) \qquad (8)$$

$$\bar{y}(t) = \hat{E}x(t) + \hat{M}_j\xi(t),\ i = 1,2,\dots,r \qquad (9)$$

where $\Gamma_i\ , i = 1,2,\dots,r$ are gain matrices, The embedded message and the masked signal are sent to the fuzzy chaotic receiver (slave system). The overall fuzzy inferred result for the fuzzy chaotic transmitter system is derived by

$$x(t+1) = \sum_{i=1}^{r}\mu_i\big(\bar{y}(t)\big)\{\bar{D}_i x(t) + H_i(t) + \Gamma_i\bar{y}(t)\} \qquad (10)$$

$$\bar{y}(t) = \hat{E}x(t) + \hat{M}_j\xi(t), \text{ for } i = 1,2,\dots,r,\ , j = 1,2,\dots,z \qquad (11)$$

where $\bar{D}_i = D_i - \Gamma_i\hat{E}$, and $y(t)$ as the output of the drive system with $\hat{M} \neq 1$, since it means nothing with the value 1.

$$\hat{M}_j = \frac{\bar{y}(t) - \hat{E}x(t)}{\xi(t)} \qquad (12)$$

If $\hat{M}_j = 1$ then $\xi(t) = \bar{y}(t) - \hat{E}x(t),\ j = 1,2,\dots,z$.

4.2Masking the Signal with Shifting Bifurcation

For masking a signal, we need to make one. The mask that is supposed here is by embedding the signal with the bifurcation of the quadratic map shown in Fig.3. The bifurcation data will also be modified by shifting data. Bifurcation shifting computed with different functions that shift the bifurcation data. The triangular functions such as; Sine, Cosine, Tan, in addition to Exponential functions. A modified data explained by figures for each function in comparison with the essential bifurcation.

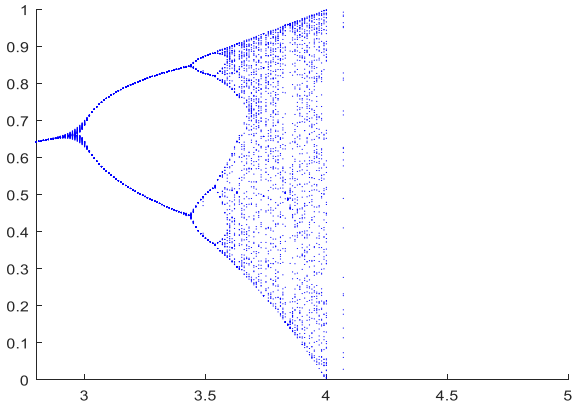


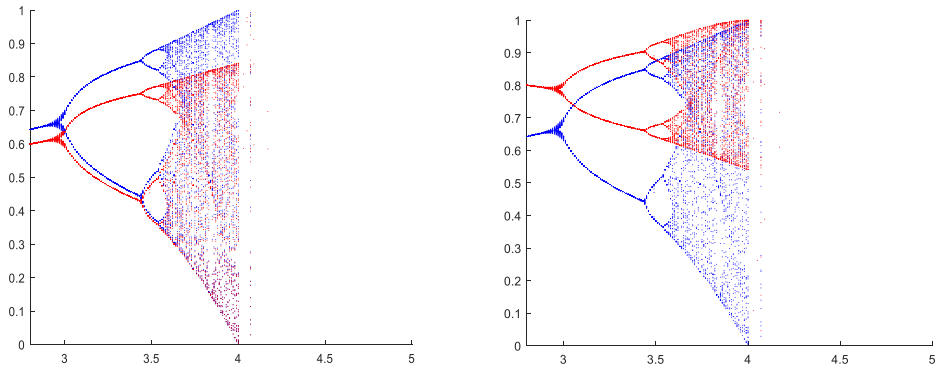
Fig.(3):- Bifurcation for quadratic map

The reason for choosing the bifurcation process since the numerical studies on Quadratic map show that there exists an increasing sequence of bifurcation values μ_n at which an attracting periodic orbit of period 2^n for f_μ loses stability and an attracting periodic orbit of period 2^{n+1} is born.

The sequence μ_n converges, as $n \to \infty$, to a limit μ_∞, as the Feigenbaum constant ω [10],

$$\lim_{n\to\infty} \frac{\mu_\infty - \mu_{n-1}}{\mu_\infty - \mu_n} = \omega = 4.669201609 \qquad (13)$$

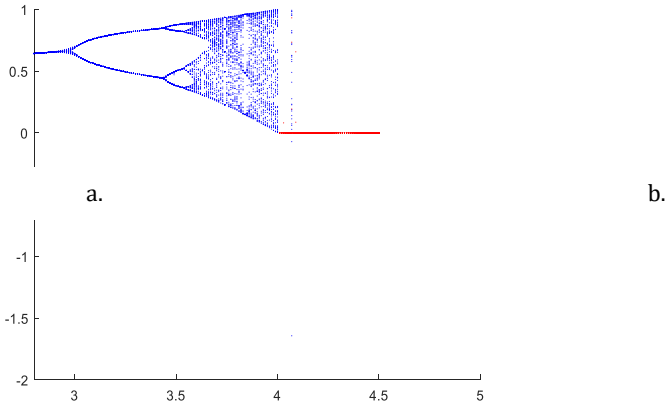
The resulted constant ω is called the Feigenbaum constant. The Feigenbaum constant appears for many other one-parameter families.



(a) (b)

Fig. (4):-Bifurcation shfting for quadratic map with other functions.(red dotted line). a. $\boldsymbol{sin}(\boldsymbol{x})$ b. $\boldsymbol{cos}(\boldsymbol{x})$

The two triangle functions don't introduce a good result as explained in Fig. 4. So, the values for bifurcation for shifting with sine and cosine function aren't used. The complexity and similarity in some values are not suitable for masking the signal. So, the experiment uses an exponential function which is also not suitable.



a. b.

Fig. (5):-Bifurcation shfting for quadratic map with $\boldsymbol{exp}(\boldsymbol{x})$ (red dotted line).

Fig. explain that an exponential function $exp(x)$ doesn't have any complexity on bifurcation shifting, so its values are not used also. A good result obtained with $tan(x)$ function as will shown in Fig. 6.

pure.bushra.hus@uobabylon.edu.iq

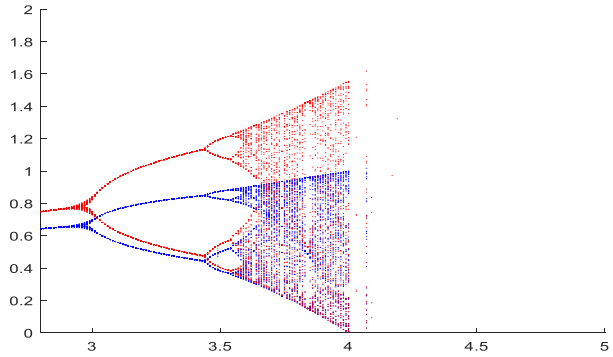


Fig. (6):-Bifurcation shfting for quadratic map $tan(x)$(red dotted line).

The bifurcation shifting values explained in Table 1. The shifting values started closely in interval [0.6, 0.8] and throughout to decay in shifting the rest bifurcation values. The minimum shifting value is 0.01 at value 6 in columns 115 through 133, while the maximum value is 1.6176 at value 14 in the same columns. Note that some bifurcation shifting values are identical with some bifurcation values, because the process is on the same intervals and the bound for the parameter in the quadratic map is the same for some values.

The numerical values on shifting bifurcation of the Quadratic map show that in encrypting the message the sequence μ_n is also converges, as $n \to \infty$, to a limit μ_∞, and the Feigenbaum constant ω is still at value close to 4.669201609

In encrypting the message this work will composing the increasing sequence μ_n in columns 39 through 57 and columns 58 through 76.

Table (1):- bifurcation shifting values for quadratic map with $tan(x)$ for 171 column

No.	Columns 1 through 19	Columns 20 through 38	Columns 39 through 57	Columns 58 through 76	Columns 77 through 95	Columns 96 through 114	Columns 115 through 133	Columns 134 through 152	Columns 153 through 171
1	0.749	0.8156	1.0166	0.4951	0.3923	1.2695	0.898	NaN	NaN
2	0.751	0.831	1.0226	0.4918	0.3821	1.0019	0.0808	NaN	NaN
3	0.753	0.8482	1.0285	0.4886	0.3878	0.2096	0.193	NaN	NaN
4	0.7549	0.8654	1.0342	0.4855	0.3449	1.2825	1.2536	NaN	NaN
5	0.7569	0.8815	1.0398	0.4822	0.6487	1.1915	0.5975	NaN	NaN
6	0.7588	0.8959	1.0452	0.4789	0.4687	0.2809	0.01	NaN	NaN
7	0.7608	0.9088	1.0504	0.4761	0.3306	1.1662	0.3329	NaN	NaN
8	0.7627	0.9205	1.0556	0.4788	0.7495	0.2362	NaN	NaN	NaN
9	0.7647	0.9312	1.0606	0.4903	0.6866	1.1377	NaN	NaN	NaN
10	0.7666	0.9411	1.0655	0.5054	0.3995	0.5321	NaN	NaN	NaN
11	0.7686	0.9504	1.0702	0.5188	0.7214	1.4214	NaN	NaN	NaN
12	0.7707	0.9592	1.0749	0.5297	0.6366	1.3748	NaN	NaN	NaN
13	0.7729	0.9675	1.0795	0.5391	0.338	0.4376	NaN	NaN	NaN
14	0.7754	0.9754	1.084	0.4027	1.1211	1.4379	1.6176	NaN	NaN
15	0.7784	0.9829	1.0883	0.3968	0.3143	0.182	NaN	NaN	NaN
16	0.7821	0.9902	1.0926	0.3914	0.6412	0.1166	NaN	NaN	NaN
17	0.787	0.9971	0.5053	0.3865	0.8196	0.0997	NaN	NaN	NaN
18	0.7938	1.0038	0.5018	0.383	0.7638	0.375	NaN	NaN	NaN
19	0.8031	1.0103	0.4984	0.3882	1.3548	0.3675	NaN	NaN	NaN

pure.bushra.hus@uobabylon.edu.iq

The values computed by MATLAB R2018b, all data represented as sequences in columns. Note that, these values stopped in the columns 115 through 133 and above.

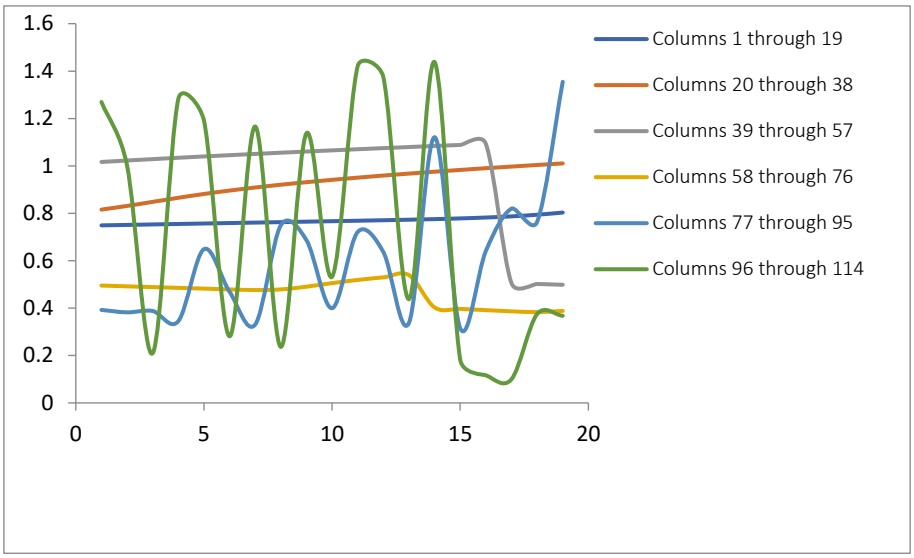


Fig. (7):-Columns values for bifurcation for the first 114 value

From the Fig. 7. the most complexvector values is at coulmn 96 through 114, the values be different in good maner not increasing or decreasing. So the best choice for mask values will be by these values.Since the of values chosen column will add step by step with each rule as in ()of values. In each coulmn the values number in this method is 19 value, while columns number is 9. In last two columns the values go to invinity so symboliced by (NaN).

4. CONCLUSION

The designing of an encryption function(s) in secret communications systems is developed by bifurcation shifting of the nonlinear chaotic map with one parameter a quadratic map. The parameters values approach the real axis and the shifting bifurcation by triangular and exponential function. Best results are with values of shifting by tan function. A new value for a Quadratic map bifurcation shifting will add to the generated real values super increasing sequence toward negative infinity. The ciphertext will be modified through the master fuzzy chaotic model, though the encryption stage will be applied in communication models as a part of the master-slave system. The Quadratic map bifurcation shifted values will add to the signal as a mask, The numerical values on shifting bifurcation of the Quadratic map show that in encrypting the message the sequence μ_n is also converges, as $n \to \infty$, to a limit μ_∞,. That mask chosen as the complex column from the set of columns for the bifurcation shifted values. Some columns show an increasing manner, other show the infinite. The robust of method is cleared through choosing the chaotic map to generate a super increasing sequence, also using the master slave model for modify and masking signals and then through choose another nonlinear chaotic map to generate the mask for signals with complex manner, and randomly in choosing parameters and real values for chaotic maps in the two steps. All previous points add security and complexity for communications.

Acknowledgment
The author would like to thank Maher Kadhum Abd for his support in working and planning on this paper.

REFERENCES

Romuel F. Machado a, Murilo S. Baptista , and C. Grebogi , "Cryptography with Chaos at the Physical Level", Chaos, Solitons and Fractals ,vol. 21, (2004) 1265–1269

Hao-Gong Chou, Chun-Fu Chuang, and Wen-June Wang, "A Fuzzy-Model-Based Chaotic Synchronization, and Its Implementation on a Secure Communication System", *IEEE Transactions on Information Forensics and*

Security, Vol. 8, No. 12, 2013,doi:10.1109/TIFS.2013.2286268

Chen-Sheng Ting "Stability Analysis and Design of Takagi–Sugeno Fuzzy Systems", Information Sciences 176 (2006) 2817–2845

Z. Li, Wolfgang A. Halang, and G. Chen, "Integration of Fuzzy Logic and Chaos Theory", Springer-Verlag Berlin Heidelberg Printed in The Netherlands, 2006, pp.(507–525)

Zhong Li, "Fuzzy Chaotic Systems Modeling, Control, and Applications", Stud Fuzz 199, Springer-Verlag Berlin Heidelberg , pp. 275–283, 2006

Z.Y. Hua, B.H. Zhou, and Y.C. Zhou, "Sine Chaotification Model for Enhancing Chaos and its Hardware Implementation", IEEE Trans. Ind. Electron. 99, (2018), 1-1.

Z. Hua, Y. Zhou and H. Huang, "Cosine-Transform-Based Chaotic System for Image Encryption", Elsevier Inc., Information Sciences 480, 403–419, 2018.

Naim Mekircha, Abdelkrim Boukabou and Noura Mansour,"Fuzzy Control of Unstable Chaotic Systems", Journal of Automation & Systems Engineering 6-1 (2012): 11-19, https://doi.org/10.1063/5.0143923

Jian Zhang, Akshya Kumar Swain, and Sing Kiong Nguang, "Robust Observer-Based Fault Diagnosis for Nonlinear Systems Using MATLAB", Springer International Publishing Switzerland, 2016, pgs. (203-221)

R. L. Devaney, "An Introduction to Chaotic Dynamical systems,"(Second Edition), Addison-Wesley Studies in Nonlinearity, pp. 31-102, 1989

Bushra Hussien Aliwi, and Ruma Kareem K. Ajeena, "A Performed Knapsack Problem on the Fuzzy Chaos Cryptosystem with Cosine Lozi Chaotic Map", AIP Conference Proceedings, 2414, 040047, (2023), https://doi.org/10.1063/5.0114840