Journal of Computer Science

Original Research Paper

On the Enlargement of Robust Region of Chaotic Tent Map for the Use in Key Based Substitution-Box (S-Box)

Muhammad Asif Khan and Varun Jeoti

Department of Electrical and Electronics Engineering, Universiti Teknologi PETRONAS,
Darul Ridzuan, 31750 Perak, Malaysia

Article history
Received: 12-03-2014
Revised: 13-04-2014
Accepted: 26-01-2015

Corresponding Author:
Muhammad Asif Khan
Department of Electrical and Electronics Engineering,
Universiti Teknologi PETRONAS, Darul Ridzuan,
31750 Perak, Malaysia
Email: asif48@gmail.com

Abstract: Robust chaotic maps with wide robust region are favored in cryptography as it extends the key length. Chaotic tent map has robust chaos for control parameter $\mu = 2$. Perturbation of control parameter values beyond control parameter 2, results in orbit diverging towards infinity and trajectories vanish. Thus, to avoid trajectories diverging to infinity and to keep trajectories chaotic beyond parameter value 2, a new technique is proposed that makes use of modulo and scaling operators. The parameter space of non-smooth maps is never considered for enlargement. Herein, modified tent map results in larger parameter space that in turn can be used to design key based S-box. The recently published chaotic key based S-box with chaotic map's parameter space does not achieve large key space. For modified tent map, the modulo operation keeps trajectories in domain (0, 1) while scaling allows for uniform distribution of points in domain (0, 1). These operations keep chaotic orbits globally stable and robust. In results, the robustness of chaotic tent map and modified chaotic tent map is compared using bifurcation diagram. The improved robust region of tent map justifies the effectiveness of proposed method that results to design key based S-box.

Keywords: Substitution Box, Nonlinear Dynamics, Robust Chaos, Tent Map, Piecewise Non-Smooth Maps

Introduction

Chaos is, though deterministic in nature, a random like phenomenon in dynamical systems. In past decade, chaos has been considered for information security because it exhibits properties such as extreme sensitive to initial parameters, random like nature and ergodicity. Chaos shows great similarities with cryptography and great amount of work has been published on chaos based cryptography (Kocarev, 2001; Kocarev and Jakimoski, 2001; Amigó *et al*., 2007). An S-box is a cryptographic element that introduces 'confusion' in the cryptosystem (Schneier, 1996). It is the only nonlinear component in a cryptosystem, hence it remains an active and fertile research area (Wang *et al*., 2009; Özkaynak and Özer, 2010; Yong *et al*., 2010). Chaos based design of S-box is also a very active research area (Adams and Tavares, 1990; Wang *et al*., 2011; Peng *et al*., 2012).

Recently, various methods have been proposed to design chaos based S-box. The chaos based S-box was first presented by Jakimoski and Kocarev (2001). In this study, S-boxes were generated using discretized exponential and logistic map. The initial parameters and number of iterations served as a key. Moreover, it also argued that key based S-box can enhance resistance against linear and differential attacks (Biham and Shamir, 1991; Matsui, 1994). Towards this end, in (Tang and Liao, 2005) method has been proposed to design dynamic S-boxes using discretized skew tent map. The key space achieved in this study is about 2^{13}. Moreover, they space of 2^6 is achieved in (Kocarev and Jakimoski, 2001). In (Yin *et al*., 2009) authors used logistic map to design a key based S-box. The key space of 2^{40} is achieved with reasonable correlation among S-boxes. Logistic map is known to have chaotic behavior beyond control parameter 3.57. However, the chaotic region is not robust in the chaotic region [3.57, 4] because of the presence of

Science Publications

periodic windows in that region. Thus it limit the useable robust region used in (Yin *et al*., 2009) with the range [3.9, 4]. For key based S-box, robust chaotic map with larger parameter space is desirable. The choice of map and key is vital in designing key based S-boxes. A good key based S-box requires larger key space which in turn requires a chaotic map with larger parameter space. Previously, the modification of robust region for large parameter space is only limited to continuous map. Recently, in (Hwang *et al*., 2008), author proposed a method to improve the robust region of continuous map. The modified region can be used to generate key based S-box. The design of chaotic key based S-box is an active research area. Recent chaotic key based S-box without modified parameter space does not achieve large key space.

In this study, we extend the concept presented in (Hwang *et al*., 2008) and we carefully analyze and propose the enlargement of the parameter space of non-smooth tent map. The parameter domain extension for tent map has not been studied before. The modified tent map is shown to have much larger parameter space as compared to traditional tent map. The methodology of modified tent presented in this study can be used to design key based S-boxes. The proposed modified tent map achieves larger parameter space, while maintaining robust chaotic trajectories. As in (Hwang *et al*., 2008) the modified tent map uses modulo and scaling operator to extend the robust region.

The rest of the paper is organized as follows. Section 2 covers the design methodology of proposed technique. Section 3 discusses the results related to proposed scheme. Section 4 covers the discussions of proposed scheme and section 5 concludes this study.

Proposed Technique

This section introduces the proposed modified chaotic tent map. The tent map is introduced in next section followed by the detailed description of modified tent map utilizing the operations of modulo and scaling.

Chaotic Tent Map

The chaotic tent map is defined as Equation 1:

$$x_{n+1} = \begin{cases} \mu x_n & x_n \ < \ 1/2 \\ \mu(1-x_n) & 1/2 \ \leq \ x_n \end{cases} \qquad (1)$$

where, the initial condition of chaotic tent map is x_n and μ is the control parameter that lies in the range of [0, 2].

The tent map is a piecewise non-smooth chaotic map. It shows chaotic behavior at $\mu = 2$. The tent map that is defined in (1) is shown in Fig. 1. The bifurcation diagram of chaotic tent map with varying control parameter value is shown in Fig. 2. The bifurcation diagram analyzes the behavior of dynamics, whether the trajectories are periodic or chaotic. The x-axis is control parameter ∊ (0, 2) and y-axis is the chaotic tent map domain ∊ (0, 1).

Modified Chaotic Tent Map

This study is the study of whether tent map's robust region can be enlarged while keeping the map robust in that region. The modified chaotic tent map is derived from classic tent map. To keep the chaotic tent map amplitude at '1' when $x_n = 1/2$ and to keep the map chaotic for μ>2, modification is required. The operations of modulo and scaling are employed.

The operations of modulo and scaling extends the robust region of chaotic tent map beyond control parameter value 2. The bifurcation diagram in Fig. 2 shows that when 1<μ≤2, there exists periodic and non-periodic attractors. With μ>2, there still exists periodic and non-periodic orbit of any length but orbits diverge towards negative infinity. The detail of modulo and scaling operator is discussed in detail in next subsection.

Modulo Operation

In order to avoid divergence of orbits when control parameter value μ>2, the modulo-1 operator is applied on tent map so as to keep amplitude within range [0, 1]. In order to analyze change in tent map without modulo, the value of μ of tent map is varied from 2 and to 2.5. It is evident from the plot that the map amplitude is increased from 1 to 1.2. Now, the modified tent map with modulo operation is given in Equation 2:

$$x_{n+1} = \begin{cases} \mu x_n (\mathrm{mod} 1) & x_n < 1/2 \\ \mu(1-x_n)(\mathrm{mod} 1) & x_n \geq 1/2 \end{cases} \qquad (2)$$

The effect of modulo operation on the tent with μ = 2.5 is shown in Fig. 3b. The portion [1, 1.2] appears at bottom of the center and covers the range [0, 0.2] approximately. As we vary μ, the height and width of the central potion changes. To demonstrate the change in height of the portion, the modified tent map with modulo operation with μ values of 2.5, 3 and 3.8 is plotted in the Fig. 3b-d respectively. It can be seen from the plot that the amplitude of the map is changing at the centre, thus it results in non-uniform distribution of points. In order to tackle this, scaling operator is employed on tent map.

Scaling

For scaling operation, the challenge is to first define the portion of domain ∊ (0, 1). Later, this portion is normalized using scaling operation. As compared to logistic map, proportion of scaling portion with varying control parameter is different because the shape of the map is different. The portion $I_{in} = [n_1, n_2]$ is shown in the Fig. 4 with arrow lines. For scaling of this portion, the portion I_{in} for given μ is required to be known precisely. It is because the width of this portion expands and contracts with changes in μ.

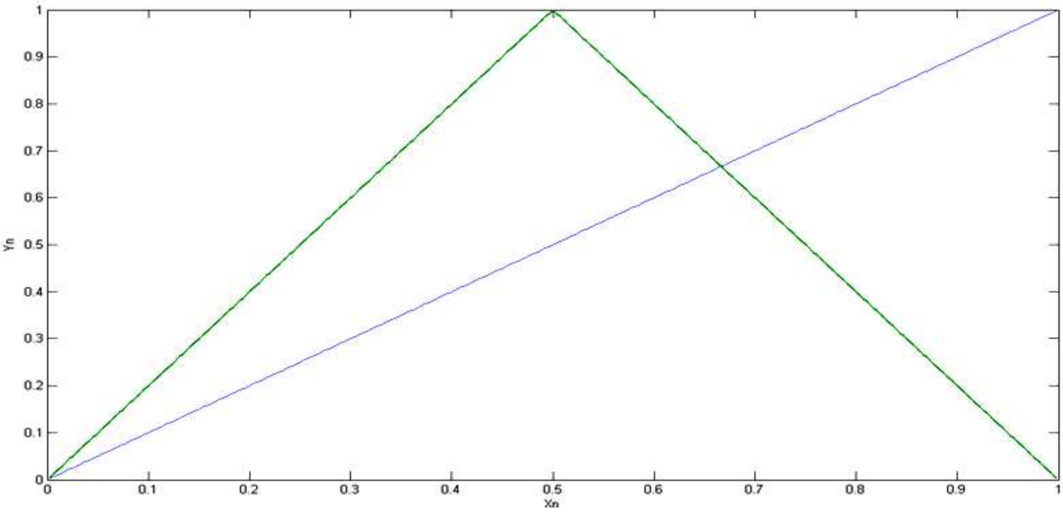


Fig. 1. Tent map (x-axis: Parameter space ∊ (0,1), y-axis: Chaotic range ∊ (0, 1))

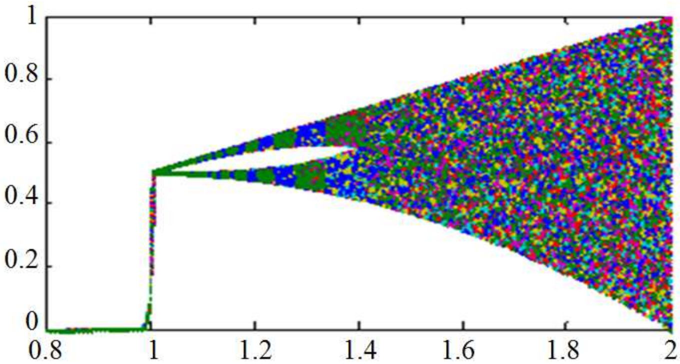
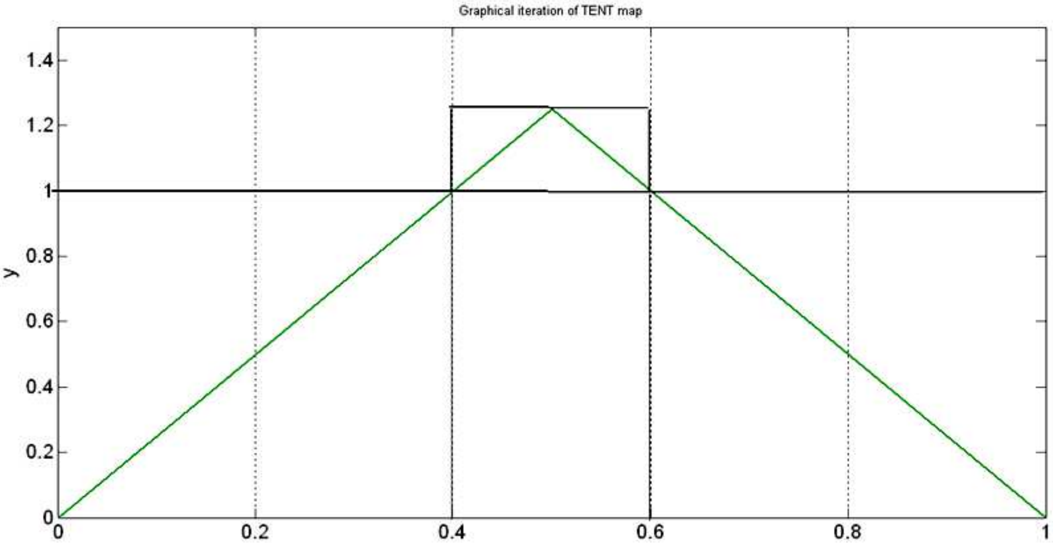
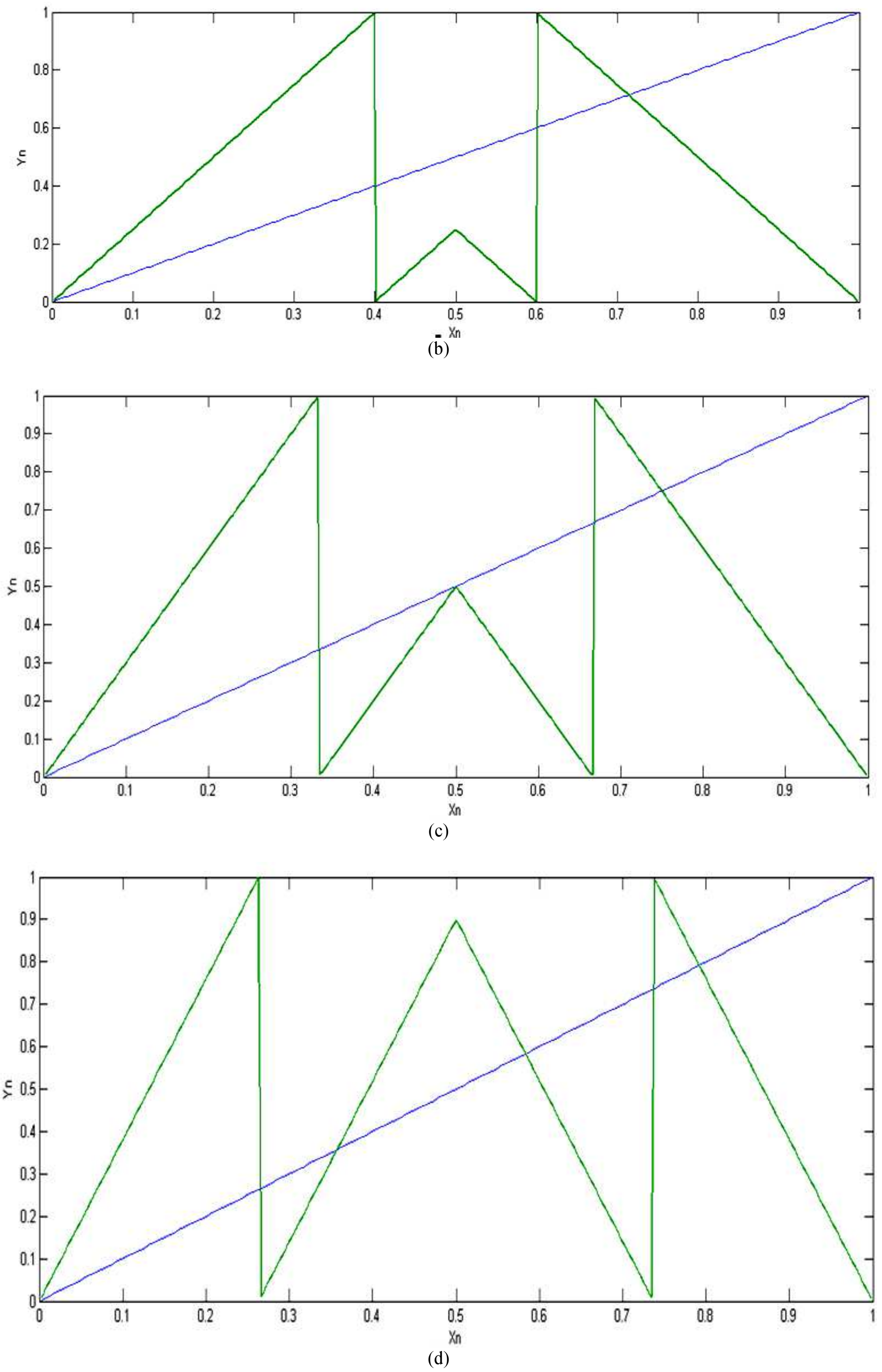


Fig. 2. Bifurcation diagram of tent map (x-axis: Control parameter μ, y-axis: Chaotic domain ∊ (0, 1))



(a)



(b)

(c)

(d)

Fig. 3. (a) Tent map (x-axis: Parameter space ∈ (0,1), y-axis: Chaotic range ∈ (0, 1) with μ = 2.5 (b) Modified Tent map with modulo opration (x-axis: Parameter space ∈ (0,1), y-axis: Chaotic range ∈ (0, 1) with μ = 2.5 (c) Modified Tent map with modulo opration (x-axis: Parameter space ∈ (0,1), y-axis: Chaotic range ∈ (0, 1) with μ = 3 (d) Modified Tent map with modulo operation (x-axis: Parameter space ∈ (0,1), y-axis: Chaotic range ∈ (0, 1) with μ=3.8

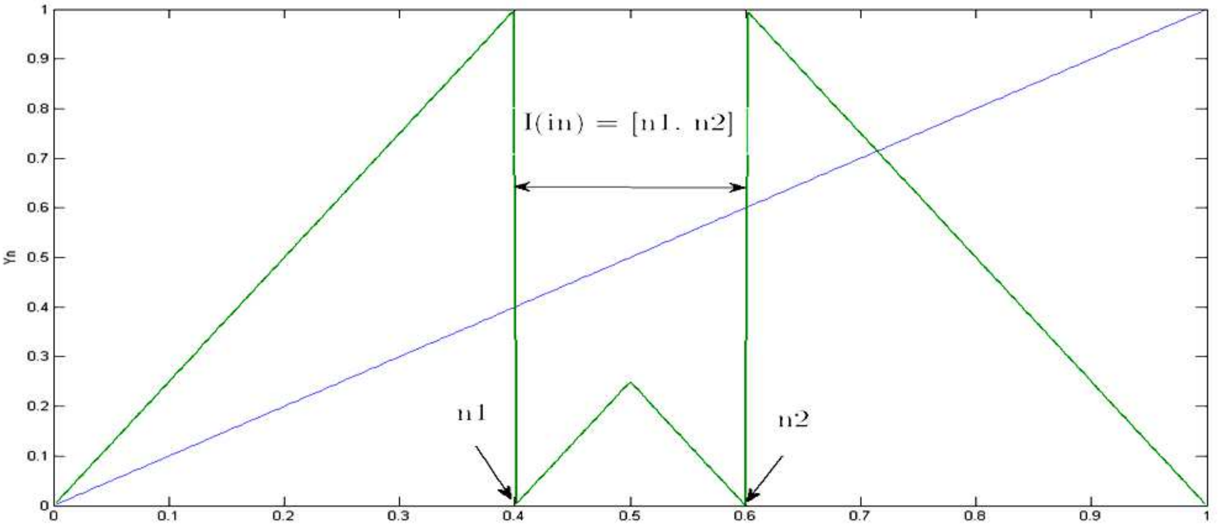


Fig. 4. Modified Tent map with modulo operation (x-axis: Parameter space ∊ (0,1), y-axis: Chaotic range ∊ (0, 1) with μ = 2.5

In order to scale this portion, two equations are defined for [n_1, n_2] as follows:

$$n_1 = \frac{1}{2} - \frac{\mu\left(\frac{1}{2}\right)\text{mod}1}{\mu}, \quad n_2 = \frac{1}{2} + \frac{\mu\left(\frac{1}{2}\right)\text{mod}1}{\mu} \tag{3}$$

These two equations estimate the portion I_{in} required for scaling of tent map. For the modification of chaotic tent map using both modulo and scaling operation, the domain is divided into two subspaces. The two subspaces are inner portion I_{in} of range [0, 1] and rest of the domain [0, 1] excluding I_{in}. The initial condition or initial parameter selected to iterate tent map is checked for its position to know where it lies. If it lies in the range covered by I_{in} then (4) will iterate the map, else (5) will. In the subsequent iterations of the map, each point is checked where it falls and appropriate equation is used to iterate the map:

$$x_{n+1} = \begin{cases} \dfrac{(\mu x_n)(\text{mod}1)}{\left(\mu/2\right)(\text{mod}1)} & x_n < 1/2 \\[2ex] \dfrac{\left(\mu(1-x_n)\right)(\text{mod}1)}{\left(\mu/2\right)(\text{mod}1)} & x_n \geq 1/2 \end{cases} \tag{4}$$

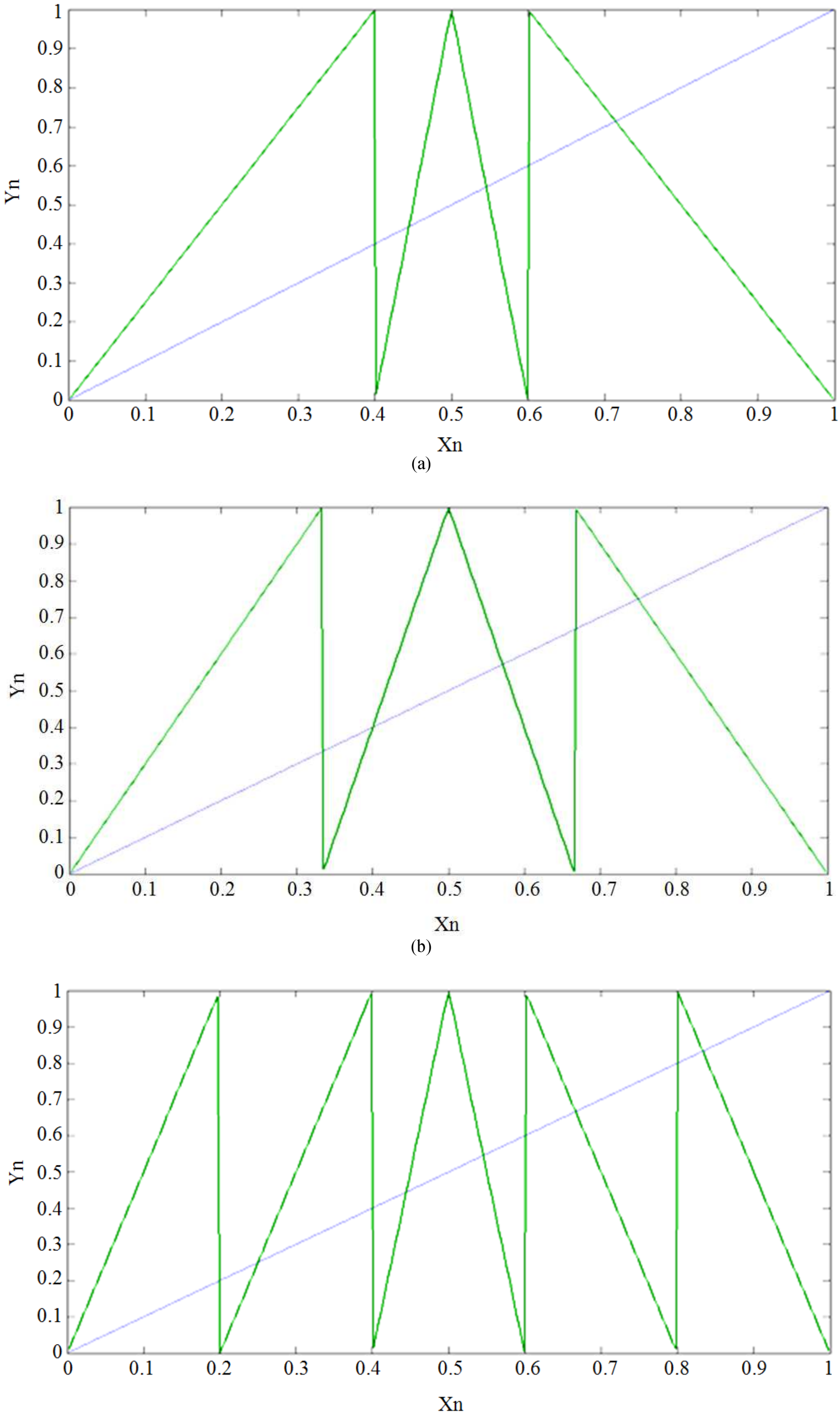
$$x_{n+1} = \begin{cases} \mu x_n(\text{mod}1) & x_n < 1/2 \\ \mu(1-x_n)(\text{mod}1) & x_n \geq 1/2 \end{cases} \tag{5}$$

The Equation 3 to 5 define the complete modified chaotic tent map.

Results

This section analyzes the proposed modified chaotic tent map and discusses the results. For the analysis of modified tent map, the values of μ are varied from 2 to 6 for experiment and corresponding Tent Maps are shown in Fig. 5. The modified tent map with μ values of 2, 3, 5 and 6 are plotted in Fig. 5a to d. It is evident from the plots that the portion for scaling is precisely defined. Moreover, it is also evident from the figure that the portion width is stretched as μ value is varied from 2 to 4. The portion again has minimum width as μ is slightly varied from 4 and portion again has stretching behavior as μ is varied to 6. It is obvious from the plot that tent map can be modified for larger parameter space. The map covers the complete phase domain with modulo and scaling operator. However, the behavior of modified tent map with varying μ can be analyzed using its bifurcation diagram. The bifurcation theory is well established and recognized theory to analyze the behavior of nonlinear dynamical systems. The bifurcation diagram analyzes the behavior of dynamics, whether the trajectories are periodic or chaotic. The modified tent map is chaotic beyond parameter value 2 with positive Lyapunov exponent and covers arbitrarily large parameter space.

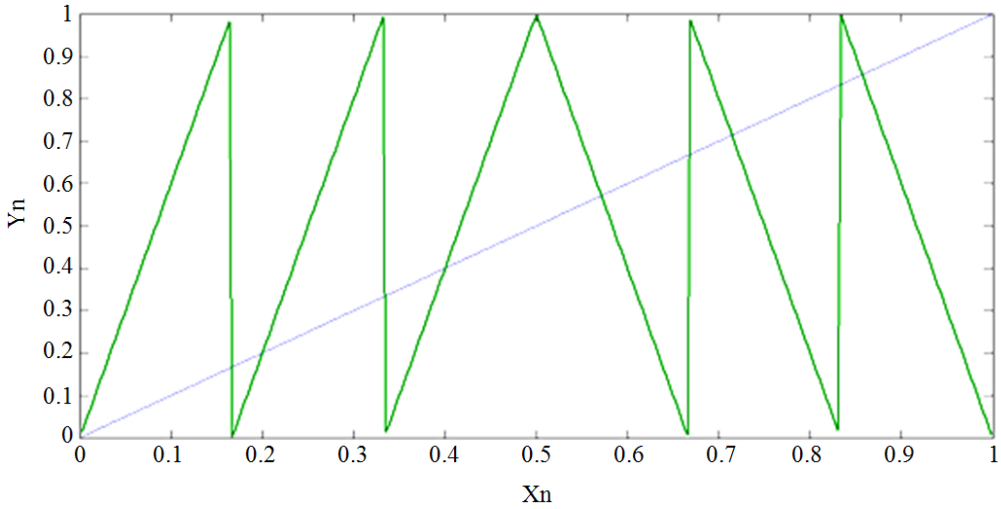
The bifurcation of modified chaotic tent map is shown in Fig. 6. The bifurcation diagram shows no periodic orbits in parameter space and covers the complete domain ∊ (0, 1) using the scaling operation. The Fig. 6 shows that the chaotic trajectories are dense and indeed robust without the presence of periodic windows. It is evident that modified chaotic tent map covers larger parameter space as compared to typical tent map. Moreover, trajectories are covering complete phase domain.



(a)

(b)

(c)



(d)

Fig. 5. (a) Modified Tent map with modulo and scaling operation (x-axis: Parameter space ∊ (0,1), y-axis: Chaotic range ∊ (0, 1) with μ = 2.5 (b) Modified Tent map with modulo and scaling operation (x-axis: Parameter space ∊ (0,1), y-axis: Chaotic range ∊ (0, 1) with μ = 3 (c) Modified Tent map with modulo and scaling operation (x-axis: Parameter space ∊ (0,1), y-axis: Chaotic range ∊ (0, 1) with μ = 5 (d) Modified Tent map with modulo and scaling operation (x-axis: Parameter space ∊ (0,1), y-axis: Chaotic range ∊ (0, 1) with μ = 6

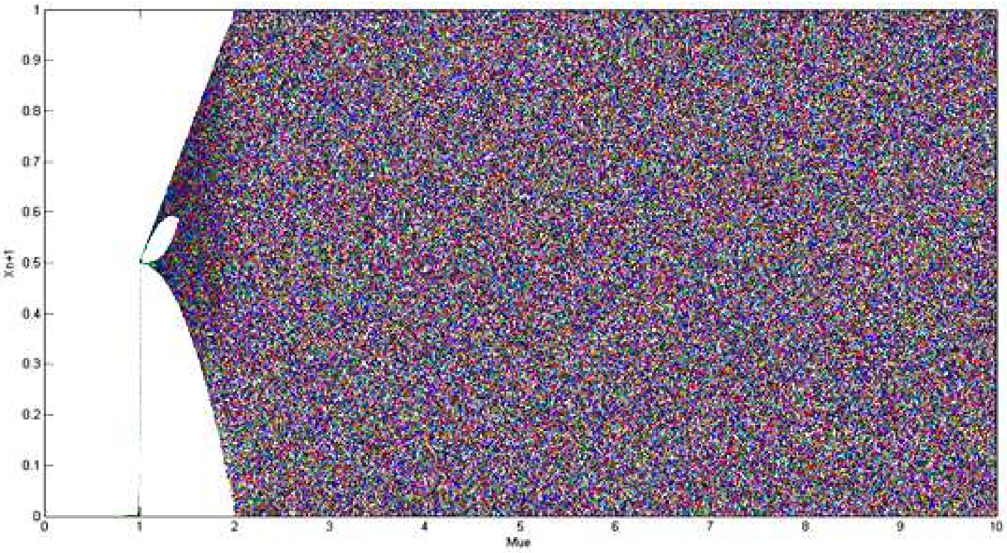


Fig. 6. Bifurcation diagram of chaotic tent map with x-axis: Control parameter μ, y-axis: Chaotic domain ∊ (0, 1)

Case Study: Key Length of Key Based Substitution-Box (S-Box)

This section analyzes the key space extension that is achieved using chaotic tent map. We use same methodology presented in (Yin *et al*., 2009) to study the achieved key space and key length. For analysis of modified tent map, parameter space is $\mu \in [2, 6]$. However, the key based S-box design using modified chaotic and its analysis is considered as the scope for future work. In Yin *et al*. (2009) proposed a key based S-box using discretized chaotic logistic map. The modified chaotic logistic key parameter:

$$x_n = (3.9 + k)x(1 - x) \tag{6}$$

where, $K \in (0, 1)$ and x is used as a key.

The chaotic logistic map has chaotic behavior for control parameter lying in the range [3.57, 4]. But, the chaotic behavior is not considered robust due to periodic windows. Instead, the range 3.9 to 4 is used by the author of (Yin *et al*., 2009) for key based S-box. However, chaotic logistic map cover compete phase space of [0, 1] at control parameter value 4. The key space and correlation between S-box generated with small perturbation of key $K \in [3.9, 4]$ are analyzed as follows:

For the key length of L bits, the possible keys space that can be achieved is 2^L. The perturbation of key $\Delta K = 2^{-L}$ is set in such a way so that it gives near optimal correlation values. The key length L is chosen and correlation between S-boxes is measured by setting K parameter in (6) derived from $K_j = jK^{-L} \in [0,1]$, $j = 1,2,\ldots 2^L$. The correlation between S-boxes is measured with K_j and K_j-ΔK. The key length $L = 40$ gives key space of 2^{40} with perturbation of key $\Delta K = 2^{-40}$ and correlation coefficient of 0.52. The correlation coefficient value is improved at the cost of increasing ΔK. The correlation coefficient value of 0.2058 is achieved when key length is set to $L = 8$. The detailed analysis with varying number of iterations, key length and achieved key space is given in (Yin *et al*., 2009).

Discussion

It is apparent from the Fig. 5 that modified tent map covers the complete phase space. The scaling of tent map is precisely defined using (3) and (4). The proposed modification shows notable parameter extension as compared to chaotic tent map, where trajectories vanishes with μ value beyond 2.

Previously non-smooth maps are never considered for the modification of parameter space. Thus, we explore the suitability of non- smooth chaotic tent map specifically for the application to design key based S-box. As discussed earlier that only notable work exist that is using smooth chaotic logistic map, where parameter space is modified for secure communication. We extended the study to explore and proposed a method to enlarge non-smooth tent maps. As discussed earlier that smooth and non-smooth maps shapes are different. Therefore, changing the parameter of modified version requires completely different mathematical equation to estimate the modified region. Previous method of designing key based S-box uses existed smooth and non-smooth chaotic maps without parameter space modification.

To study the achieved improvement in key space if key based S Box is designed using modified tent map with robust region $\in (2, 6)$, the similar approach is adopted. The robust region from 2 to 3 gives roughly 10 times improvement in key space as compared to recently published well known work (Yin *et al*., 2009). The achieved improvement considering $\mu = (2, 6)$ gives key length of $L = 2^{40\times40}$ with key space of $2^{40\times40}$, $\Delta K = 2^{-(40\times40)}$ and correlation coefficient of 0.52. Moreover, if we improve correlation coefficient to 0.2058 on the cost of ΔK, then the values are as follows, $L = 2^{40\times14}$, key space $2^{40\times14}$, $\Delta K = 2^{-(40\times14)}$. The analysis shows that the proposed method gives a lot of space to design key based S-box.

Conclusion and Future Work

Chaos based key dependent S-box requires larger parameter space with robust region. However, the key based S-boxes given in literature do not seems to have large key space. In this study, we propose modified chaotic tent map with improved robust region. Chaotic tent map is piecewise non-smooth map that shows robust chaotic behavior with control parameter $\mu = 2$. Therefore, for tent maps to have robust region beyond 2, modulo and suitable scaling are employed. The results show that the modified chaotic tent map shows robust chaotic trajectories for $\mu > 2$. The modified tent map covers complete phase space and shows no periodic windows in robust region. Moreover, the improvement in key space with modified tent map is studied and presented. The analysis shows that proposed improved chaotic tent map gives great amount of improvement for designing key based S-box. This study can be extended for the enlargement of other non-smooth chaotic maps. Moreover, study requires exploring other fields of engineering and science where these modified maps can be utilized and it is still considered an open problem.

Funding Information

The authors have no support or funding to report.

Author's Contributions

All authors equally contributed in this work.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Adams, C. and S. Tavares, 1990. Good s-boxes are easy to find. Proceedings of the 9th Annual International Cryptology Conference, Aug. 20-24, Santa Barbara, California, USA, pp: 612-615. DOI: 10.1007/0-387-34805-0_56

Amigó, J.M., L. Kocarev and J. Szczepanski, 2007. Theory and practice of chaotic cryptography. Phys. Lett. A, 366: 211-216. DOI: 10.1016/j.physleta.2007.02.021

Biham, E. and A. Shamir, 1991. Differential cryptanalysis of DES-like cryptosystems. Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology, (CAC' 91), Springer, pp: 2-21. DOI: 10.1007/3-540-38424-3_1

Hwang, T., S.M. Chang, W.W. Lin and T. Hwang, 2008. Digital secure-communication using robust hyper-chaotic systems. Int. J. Bifurcat. Chaos, 18: 3325-3339. DOI: 10.1142/S0218127408022408

Jakimoski, G. and L. Kocarev, 2001. Chaos and cryptography: Block encryption ciphers based on chaotic maps. IEEE Trans. Circuits Syst. I: Fundamental Theory Applic., 48: 163-169. DOI: 10.1109/81.904880

Kocarev, L., 2001. Chaos-based cryptography: A brief overview. IEEE Circuits Syst. Magaz., 1: 6-21. DOI: 10.1109/7384.963463

Kocarev, L. and G. Jakimoski, 2001. Logistic map as a block encryption algorithm. Phys. Lett. A, 289: 199-206. DOI: 10.1016/s0375-9601(01)00609-0

Matsui, M., 1994. Linear cryptanalysis method for DES cipher. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, May 23-27, Springer, Norway, pp: 386-397. DOI: 10.1007/3-540-48285-7_33

Özkaynak, F. and A.B. Özer, 2010. A method for designing strong S-Boxes based on chaotic Lorenz system. Phys. Lett. A, 374: 3733-3738. DOI: 10.1016/j.physleta.2010.07.019

Peng, J., X. Liao and X. Liao, 2012. A novel approach for designing dynamical S-Boxes using hyperchaotic system. Int. J. Cogn. Inform. Nat. Intell., 6: 100-119. DOI: 10.4018/jcini.2012010105

Schneier, B., 1996. Applied Cryptography: Protocols, Algorithms and Source Code in C. 1st Edn., John Wiley and Sons, Inc., New York, ISBN-10: 0471128457.

Tang, G. and X. Liao, 2005. A method for designing dynamical S-boxes based on discretized chaotic map. Chaos, Solitons Fractals, 23: 1901-1909. DOI: 10.1016/j.chaos.2004.07.033

Wang, Y., K.W. Wong, Xiaofeng Liao and G. Chen, 2011. A new chaos-based fast image encryption algorithm. Applied Soft Comput., 11: 514-522. DOI: 10.1016/j.asoc.2009.12.011

Wang, Y., K.W. Wong, X. Liao and T. Xiang, 2009. A block cipher with dynamic S-boxes based on tent map. Commun. Nonlinear Sci. Numerical Simulat., 14: 3089-3099. DOI: 10.1016/j.cnsns.2008.12.005

Yin, R., J. Yuan, J. Wang, X. Shan and X. Wang, 2009. Designing key-dependent chaotic S-box with larger key space. Chaos Solitons Fractals, 42: 2582-2589. DOI: 10.1016/j.chaos.2009.03.201

Yong, W., Y. Li, M. Li and S. Song, 2010. A method for designing S-box based on chaotic neural network. Proceedings of the 6th International Conference on Natural Computation, Aug. 10-12, IEEE Xplore press, Yantai, Shandong, pp: 1033-1037. DOI: 10.1109/icnc.2010.5582968