Chaotic Modeling and Simulation (CMSIM) **3: 197-203, 2020**

A New Substitution Box Structure Based on Nose–Hoover Chaotic System

Yaşar Selim Bahçeci[1], Fatih Özkaynak[2]

[1] Department of Software Engineering Fırat University, 23119, Elazig, Turkey
(E-mail: yasarselimbahceci@gmail.com)
[2] Department of Software Engineering Fırat University, 23119, Elazig, Turkey
(E-mail: ozkaynak@firat.edu.tr)

Abstract. A cryptographic protocol should provide two basic requirements for secure communication. These requirements are known as diffusion and confusion. Substitution box structures are needed in order to provide the confusion requirement in block encryption algorithms. These cryptographic blocks must have a nonlinear structure to meet the confusion requirement. Various designs based on chaotic systems have been proposed to ensure the nonlinearity requirement. In this study, a new substitution box structure based on Nose–Hoover Chaotic System is proposed. Successful analysis results showed that the proposed new chaos based substitution box structure could be an alternative to the other three degree chaos based substitution box structures.

Keywords: chaos, cryptography, substitution box, image encryption.

1 Introduction

Our security requirements have changed as everything in our world has changed. The concept of knowledge has become increasingly important in this change [1]. As the concept of knowledge gained importance, the security problem of this information emerged. Researchers have developed many different encryption algorithms to solve this problem. These encryption algorithms must meet various requirements. These requirements are known as diffusion and confusion. Substitution box structures are needed in order to provide the confusion requirement in block encryption algorithms [2]. These cryptographic blocks must have a nonlinear structure to meet the confusion requirement.

Many encryption algorithms use substitution box structures to provide the confusion requirement [3-15]. Although there are many methods for substitution box structures, a design approach that has attracted attention in recent years has been the design approach using chaotic systems. In this study, a substitution box structures approach based on chaotic systems is proposed. The application of this proposed cryptographic structure is shown on an image encryption algorithm.

Received: 25 June 2020 / Accepted: 27 July 2020

ISSN 2241-0503

The rest of the study is organized as follows. In the Section 2, a brief literature summary about chaos based s-box design is given. In the Section 3, the Nose-Hoover chaotic system is introduced. In the Section 4, the proposed new s-box structure is explained and analysis results are given The last section summarizes the study.

2 Related Works

Chaos-based s-box studies have been a remarkable research topic in the last two decades. One of the most important reasons behind this increase in interest in research topic is the developments in cryptanalysis studies. In particular, application attacks allow the attacker to make various inferences about cryptographic protocols using a variety of side channel information. Although designs based on mathematical transformation do not contain weaknesses in terms of performance criteria, their well-defined features allow this side channel information to be easily obtained. Therefore, new searches for alternative s-box structures based on mathematical transformation have accelerated. An important design technique in this aim is chaos based s-box designs.

Chaos based s-box design was first encountered in 2001 [16]. In this study, a s-box design has been realized by using discrete time logistic map and this structure has been used in a block encryption algorithm architecture. Between 2001 and 2010 [17, 18], it has been aimed to improve the performance of s-box structures by using different chaotic maps. However, the performance characteristics of the AES s-box structure could not be approached in these studies. Therefore, performance parameters have been improved with various optimization algorithms [19]. However, the additional transaction costs in these studies have emerged as another problem to be solved .

In 2010, the idea of using continuous time chaotic systems in the design process as an alternative to discrete time chaotic systems has been proposed [20]. The aim of these design studies is to increase the complexity of the chaotic system and improve the nonlinearity properties of s-box designs. Following these studies, several studies aimed at improving performance by using more complex chaotic systems have been proposed. Among these studies, design studies based on hyper chaotic systems [21], time delayed chaotic systems [22] and fractional order chaotic systems [23] draw attention.In chaos based s-box designs, the effect of using only different chaotic systems on performance has not been investigated. In addition to selecting chaotic systems as an entropy source, it is aimed to increase the quality of the entropy source by using various additional procedures [23-30].

In this study, an algorithm based on continuous time chaotic systems has been proposed. The most important aspect of the study is that the system selected as chaotic system does not need any control parameters. This feature of the selected system will have several advantages in the design process of the cryptographic protocol, especially in the process of sharing the secret key of the algorithm (key distribution).

3 Nose–Hoover Chaotic System

Chaos theory is an exciting science. Because it points out that the randomness behind the events have actually mathematical equations. Chaotic behavior first emerged by showing that reason of randomness in weather forecasts modeled by various differential equations is the internal structure of the system. In the literature, the simplest differential equation models in which chaotic behavior is observed are known as systems like Lorenz, Chua, Chen. The common features of these systems are expressed in third order differential equations.

Nose–Hoover system [31] is a third-order system like the systems mentioned above. The definition using ordinary differential equations is given in Eq. (1). The system in which Eq. (1) is expressed has three initial conditions.

$$\begin{aligned} dx/dt &= y \\ dy/dt &= y * z - x \\ dz/dt &= 1 - y*y \end{aligned} \tag{1}$$

The phase space graphs showing the variation of the state variables of the Nose – Hoover system are shown in Figure 1.

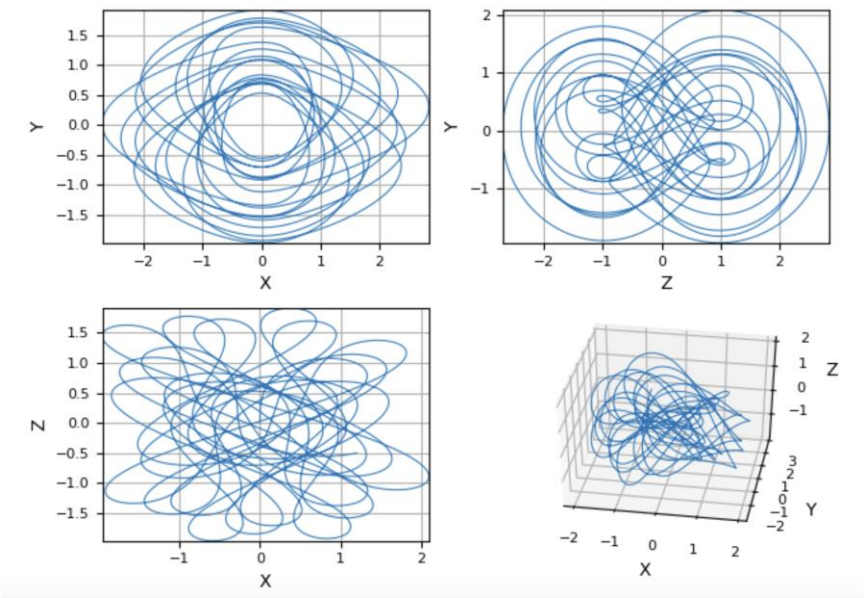

Fig. 1. Phase-space analysis of Nose–Hoover system

4 Proposed S-Box Design Algorithm

The innovative aspect of the study is the chosen chaotic system class. This is the first study in the literature using Nose–Hoover chaotic system in substitution box design. For substitution box design, the recommended method in Ref. [14] is used. The details of the used method can be examined in detail. A program can be produced different substitution box design by running the program repeatedly at different times. The program has a user-friendly design. There is also an introductory video on how to use the program. There is also an interface for the performance tests of the substitution box structures produced in the program. There are five widely accepted criterion in the literature. These tests are:

- Bijective criterion,
- Nonlinearity criterion,
- Bit independence criterion (BIC),
- Strict avalanche criterion
- Input/output XOR distribution criteria

A sample substitution box structure and performance criteria produced using the proposed chaotic system are given in Table 1. Since the method used for substitution box design automatically provides bijective, this criterion is not included in Table 1.

Table 1. Proposed substitution box structure

	s-box															
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	19	100	82	169	62	29	131	137	16	49	240	105	155	43	152	73
1	36	171	57	18	237	81	247	136	98	9	195	97	228	17	235	165
2	224	218	193	232	177	229	147	227	35	71	46	54	216	58	238	53
3	23	175	139	75	151	33	129	163	252	248	96	61	225	254	68	40
4	21	250	176	78	253	4	200	183	162	66	145	188	243	28	166	64
5	255	22	133	161	39	55	197	191	143	173	104	63	206	83	233	50
6	220	106	154	205	146	181	24	67	25	90	48	111	239	77	101	226
7	74	164	102	204	44	14	87	217	236	91	168	158	120	65	122	119
8	142	10	76	244	189	37	222	207	56	246	174	84	214	60	230	42
9	79	182	221	126	1	2	198	38	245	180	251	116	88	89	134	5
A	231	112	190	69	201	0	72	215	31	167	234	113	209	199	109	186
B	196	95	178	86	52	20	132	128	41	7	13	156	202	3	123	212
C	12	213	160	223	51	93	70	203	242	110	15	125	118	30	80	184
D	187	47	115	208	45	121	210	6	194	108	144	117	138	85	211	148
E	141	192	107	103	124	172	11	241	219	130	159	185	26	170	149	27
F	127	34	99	153	135	140	179	114	59	157	94	92	8	249	32	150

The cryptographic features of the proposed substitution-box structure are given in Table 2.

Table 2. Cryptographic properties of proposed substitution box structure

s-box structure				
Nonlinearity Average	**Strict Avalanche Criterion Average**	**Bit Independence Creation**		**Input / Output XOR Distribution**
		BIC-SAC	**BIC-Nonlinearity**	**Max**
104.25	0.5044	0.502	103.93	10

5 Conclusions

In this study, a substitution box design has been performed which could be an alternative to chaos based substitution box structures in the literature. The innovative aspect of the proposed method is the chaotic system used in the design process. The most important feature that distinguishes this Nose–Hoover system from others is that it does not need any control parameters. The results of the analysis showed that a successful substitution box structure can be obtained.

Acknowledgments

This study is supported by the Firat University Scientific Research Project (TEKF.19.18).

References

1. C. Wu and D. Feng, Boolean Functions and Their Applications in Cryptography. Berlin, Germany: Springer, 2016.
2. M. S. Açikkapi, F. Özkaynak, and A. B. Özer, "Side-channel analysis of chaos-based substitution box structures", IEEE Access, vol. 7, pp. 79030–79043, 2019. doi: 10.1109/ACCESS.2019.2921708.
3. D. Lambić, ''S-box design method based on improved one-dimensional discrete chaotic map,'' J. Inf. Telecommun., vol. 2, no. 2, pp. 181–191, 2018.
4. H. A. Ahmed, M. F. Zolkipli, M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map", Neural Computing and Applications, vol. xx, no. x, pp. xx-yy, May 2018.
5. K. M. Ali and M. Khan, "Application based construction and optimization of substitution boxes over 2D mixed chaotic maps", Int. J. Theor. Phys., pp. 1–27, 2019. doi: 10.1007/s10773-019-04188-3.
6. A. H. Zahid and M. J. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping", Symmetry, vol. 11, no. 3, p. 437, 2019. doi: 10.3390/sym11030437.

7. M. F. Khan, A. Ahmed, K. Saleem, and T. Shah, “A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system”, IEEE Access, vol. 7, pp. 84980–84991, 2019. doi: 10.1109/ACCESS.2019.2925081..
8. F. Özkaynak, ‘‘From biometric data to cryptographic primitives: A new method for generation of substitution boxes,’’ in Proc. ACM Int. Conf. Biomed. Eng. Bioinformat., Bangkok, Thailand, Sep. 2017, pp. 27–33. doi: 10.1145/3143344.3143355.
9. L. Liu, Y. Zhang, and X. Wang, “A novel method for constructing the S- box based on spatiotemporal chaotic dynamics”, Appl. Sci., vol. 8, no. 12, p. 2650, 2018. doi: 10.3390/app8122650.
10. F. Özkaynak, “An analysis and generation toolbox for chaotic substitu- tion boxes: A case study based on chaotic labyrinth rene thomas system”, Iranian J. Sci. Technol.-Trans. Elect. Eng., pp. 1–10, 2019. doi: 10.1007/s40998-019-00230-6.
11. M. F. Khan, A. Ahmed, and K. Saleem, “A novel cryptographic substitution box design using Gaussian distribution”, IEEE Access, vol. 7, pp. 15999–16007, 2019. doi: 10.1109/ACCESS.2019.2893176.
12. T. Ye and L. Zhimao, “Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling”, Nonlinear Dyn. vol. 94, no. 3, pp. 2115–2126, 2018. doi: 10.1007/s11071-018- 4478-5.
13. A. H. Zahid, M. J. Arshad, M. Ahmad, (2019). “A Novel Construction of Efficient Substitution-Boxes Using Cubic Fractional Transformation”. Entropy, 21(3), 245.
14. F. Özkaynak, “Construction of robust substitution boxes based on chaotic systems”, Neural Comput. Appl., pp. 1–10, 2017. doi: 10.1007/s00521- 017-3287-y.
15. E. Tanyildizi, F. Özkaynak, A New Chaotic S-Box Generation Method Using Parameter Optimization of One Dimensional Chaotic Maps, IEEE Access, Volume 7, Page(s): 117829 - 117838, DOI: 10.1109/ACCESS.2019.2936447
16. G. Jakimoski, L. Kocarev, ‘‘Chaos and cryptography: Block encryption ciphers based on chaotic maps,’’ IEEE Trans. Circuits Syst. I. Fundam. Theory Appl., vol. 48, no. 2, pp. 163–169, Feb. 2001.
17. F. Özkaynak,, (2020) On the Effect of Chaotic System in Performance Characteristics of Chaos Based S-box Designs, Physica A: Statistical Mechanics and its Applications, Volume 550, 124072, https://doi.org/10.1016/j.physa.2019.124072.
18. G. Tang and X. Liao, ‘‘A method for designing dynamical S-boxes based on discretized chaotic map,’’ Chaos Solitons Fractals, vol. 23, no. 5, pp. 1901–1909, 2005.
19. Z. M. Z. Muhammad, F. Özkaynak, (2020) A Cryptographic Confusion Primitive Based on Lotka–Volterra Chaotic System and Its Practical Applications in Image Encryption, IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 25-29 February 2020, Slavske, Ukraine.
20. F. Özkaynak and A. B. Özer, “A method for designing strong S-boxes based on chaotic Lorenz system”, Phys. Lett. A, vol. 374, no. 36, pp. 3733–3738, 2010.
21. E. A. Solami, M. Ahmad, C. Volos, M. N. Doja, and M. M. S. Beg, ‘”Anew hyperchaotic system-based design for efficient bijective substitution- boxes”, Entropy, vol. 20, no. 7, p. 525, 2018. doi: 10.3390/e20070525.

22. F. Artuğer, F. Özkaynak, (2020) A Novel Method for Performance Improvement of Chaos-Based Substitution Boxes, Symmetry 2020, 12, 571, doi:10.3390/sym12040571.
23. A. Belazi, A. A. A. El-Latif, A.-V.Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms", Opt. Lasers Eng., vol. 88, pp. 37–50, Jan. 2017.
24. Ahmad, M. [2018] "Random search based efficient chaotic substitution box design for image encryption," Int. J. Rough Sets Data Anal. 5(2), 131–147, doi: 10.4018/IJRSDA.2018040107.
25. Ahmed, H.A., Zolkipli, M. F., Ahmad, M. [2018] "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map", Neural Comput. Appl. 3, 1-10.
26. Alzaidi, A.A., Ahmad, M., Doja, M.N., Solami, E.A., Beg, M.M.S.[2018] "A New 1D Chaotic Map and beta-Hill Climbing for Generating Substitution-Boxes", IEEE Access 6, 55405-55418.
27. Alzaidi, A.A., Ahmad, M., Ahmed, H.S., AlSolami, E. [2018] "Sine-Cosine Optimization Based Bijective Substitution-boxes Construction Using Enhanced Dynamics of Chaotic Map", Complexity, 2018.
28. Farah, M.A.B., Guesmi, R., Kachouri, A. et al. A new design of cryptosystem based on S-box and chaotic permutation. Multimed Tools Appl (2020). https://doi.org/10.1007/s11042-020-08718-8
29. S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan and I. Hussain, "Construction of Cryptographic S-Boxes Based on Mobius Transformation and Chaotic Tent-Sine System," in IEEE Access, vol. 7, pp. 173273-173285, 2019.
30. M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar and A. Razaq, "Comparison of Pre and Post-Action of a Finite Abelian Group Over Certain Nonlinear Schemes," in IEEE Access, vol. 8, pp. 39781-39792, 2020.
31. R. Hao, X. Ma (2019) Dynamical Analysis of Nose-Hoover Continuous Chaotic System Based on Gingerbreadman Discrete Chaotic Sequence. In: Jin J., Li P., Fan L. (eds) Green Energy and Networking. GreeNets 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 282. Springer, Cham