Indian Journal of Science and Technology, *Vol 8(28), DOI: 10.17485/ijst/2015/v8i28/71759, October 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Application of Chaotic Functions for Construction of Strong Substitution Boxes

Arun Gautam[1*], Gurjot Singh Gaba[1], Rajan Miglani[1] and Ruchi Pasricha[2]

[1]Lovely Professional University, Jalandhar - 144411, Punjab, India; arungautam.ag@gmail.com, gurjot.17023@lpu.co.in, rajan.16957@lpu.co.in
[2]Chandigarh Engineering College, Mohali - 140307, Punjab, India; cecm.ece.rps@gmail.com

Abstract

In cryptography, the security of any algorithm relies on the strength of the key used and nonlinear mapping of the original information or data. It is desirable to have resistance against differential cryptanalysis, which assists in providing clues about the composition of keys, and linear secret system, where a simple approximation is created to copy the original cipher characteristics. The objective of the proposed work is to make the existing cipher techniques more prone to cryptanalysis by incorporating the proposed S-box in the design. In this paper, the use of nonlinear functional chaos-based substitution process is proposed which employs a set of differential equations called Lorenz equations with given initial parameters. The performance of the new substitution box is evaluated through simulation and data analytics tool. During testing, it has been found that the proposed technique produces high Standard Deviation (112.84) and negative correlation factor (-0.161) which makes it applicable where security against cryptanalysis is a major concern.

Keywords: Chaotic Function, Cipher, Cryptanalysis, Lorenz System, Substitution Box

1. Introduction

The purpose of providing security to the data is creating confusion to the eavesdropper via introduction of randomness in the data[16]. The random or non-linear behavior of chaotic systems exhibit demanding properties suitable for nonlinear dynamic systems such as the substitution process in a cipher without independent round keys. All such chaotic systems are highly sensitive to initial conditions and exhibit random behavior, which is deterministic if the initial information is available. If this initial information is absent, the system appears to be random to any observer or intruder. These properties are desirable and suitable in the design of cryptographic systems. The application of chaotic sequences to the construction of substitution boxes, used in various cipher schemes such as Advanced Encryption Standard (AES) etc., is capable of creating confusion and applying diffusion to the original data[4]. The substitution process in the AES encryption technique is the only nonlinear part, which creates confusion and secures the information. The substitution process is accomplished by the use of the Substitution-box (S-box) that is an array of size $n \times n$.

Chaotic ciphers are prone to attacks like denial of service and inability of resisting the privileged insider attack. These problems were formed as objective in their paper[5] and provided a security mechanism to fight against those attacks. But to fight against attacks, a large order of keys with novel approach to construct those keys is required[6]. It's not only the key who plays the vital role against cryptanalysis but strong substitution box is also recommended[7]. Different criteria's can be used for the evaluation of the Substitution boxes like Strict Avalanche Criterion, Bit Independent Criterion, nonlinear criterion etc. Further the constituted S-box from this principle can be used in AES and with other techniques to find its optimized allocation[8]. With these criteria's, one can calculate the algebraic and statistical encryption strength cum weakness of the S-box[9,10]. Variety of Substitution boxes are made over the time for different

**Author for correspondence*

applications. For image applications S_8 substitution boxes are NCA chaotic sequences are suggested which can provide security against classic attacks[11]. To analyze the strength of S-box in image encryption, root mean square error method[13] and majority logic criterion can be used[14].

Several methodologies for the construction of cryptographically strong S-boxes have been implemented in the past. One such method is devised as linear fractional transform method. After testing, it is found that it has more confusion creating capabilities as compared with the counterparts i.e. AES, Skipjack etc[17]. In[24], a method is proposed which relies on an in-depth search to construct a new S-box. Here the construction of new S-boxes with large values of n is computationally complex. Looking at the methods used by cryptanalysis[20], an S-box of size 5×5 was suggested in[3] with strong resistance to differential cryptanalysis. In today's era, the theory of chaos is also used for the construction of S-boxes. In another construction method based on this technique[2], a 3D chaotic Baker map is used to generate an 8×8 S-box. This method exhibited some attractive properties concerning to robustness and resistance to cryptanalysis. This method is again improved by the use of a continuous-time chaotic Lorenz system[19].

In order to obtain discrete data from the chaotic system, the system trajectory values are converted to digital numbers for selected time steps and a linear functional algorithm[12] is applied to these coded discrete outputs. This method exhibits cryptographically strong properties as compared to other algorithms, which synthesize S-boxes based on chaotic methods. In this paper, we mainly relate our chaotic system with linear functional transformation in order to generate a strong S-box. Strength of an S-box lies in the unique combinations of the values present in the S-Box. AES uses a technique referred as affine-power-affine structure which creates 40320 unique instances[18].

Chaotic ciphers are prone to attacks like denial of service and inability of resisting the privileged insider attack. These problems were formed as objective in their paper[5] and provided a security mechanism to fight against those attacks. But to fight against attacks, a large order of keys with novel approach to construct those keys is required[6]. It's not only the key who plays the vital role against cryptanalysis but strong substitution box is also recommended[7]. Different criteria's can be used for the evaluation of the Substitution boxes like Strict Avalanche Criterion, Bit Independent Criterion, nonlinear criterion etc. Further the constituted S-box from this principle can be used in AES and with other techniques to find its optimized allocation[8]. With these criteria's, one can calculate the algebraic and statistical encryption strength cum weakness of the S-box.

2. Lorenz System of Equations

The Lorenz system was initially used to design atmospheric model[19] in 1950 and is the first numerical study of chaos. It is a set of three differential equations with three variables. The system dynamics are represented by the equations shown below.

$$\frac{dx}{dt} = \alpha(y - x), \frac{dy}{dt} = (\beta x - y - xz), \frac{dz}{dt} = (xy - yz)$$

Equation 1: Lorenz system of equations.

Where the values of the parameters are $\alpha = 10$, $\beta = 28$ and $\gamma = 8/3$. The intervals used in the states of the system are $-40 \le x \le 40$, $-40 \le y \le 40$ and $-40 \le z \le 40$. The system exhibits chaotic behavior for the selected parameters and intervals[1].

Initial work depicts a new way to synthesize S-boxes based on chaotic system. The synthesis process is divided into a few different stages. The numerical methods are used to generate and solve the given chaotic system. The process continues by converting the results from the first step into integer values. The range of these values is from 0 and 255. In the last step, the proposed algorithm extracts only distinct values generated by this chaotic system. The refined results are then utilized in the construction of S-boxes used in the block ciphers, which exhibit strong encryption properties.

3. Proposed Algorithm

- First of all obtain x, y, z trajectories by solving the above set of equations with selected set of inputs and chaotic parameters in Matlab software. The plots of the x, y and z trajectories are shown in Figure 1, 2 and 3.
- Take any one trajectory from above mentioned trajectories of x, y and z and then code it at every step starting from 0 to 255.
- After removing all repeated values, 256 distinct values are obtained which is distributed randomly.

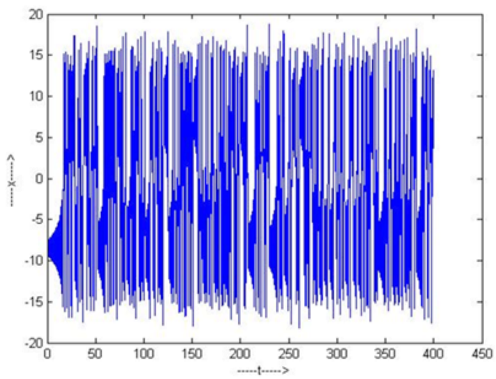

Figure 1. Plot of Lorenz systems for x along t–axis.

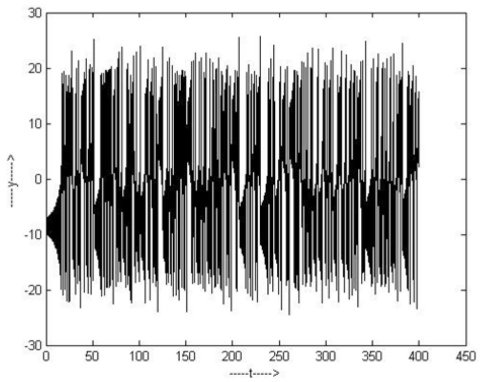

Figure 2. Plot of Lorenz systems for y along t–axis.

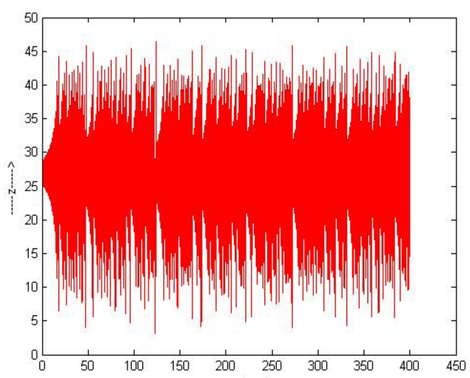

Figure 3. Plot of Lorenz systems for z along t–axis.

- Now make 16 different 4 x 4 matrices say M1, M2… M16 from the array such that first value goes to M1, second value goes to M2 and so on.
- Now reshape these 16 (4 x 4) matrices to form one 16 x 16 matrix which is the resultant S-box. Table 1 shows the resultant matrix prepared using the proposed algorithm.

4. Analysis of the Proposed S-box

For the purpose of the evaluating the cryptographic strength of S-box, SPSS tool is used where Paired Sample T Test is applied to compare the strength of existing S-box with the proposed S-box. Comparison is done on the following parameters:

4.1 Standard Deviation

It is a method used to measure the amount of variation of a set of data values. A standard deviation value which is close to 0 means that the data points tend to be very close to the mean (or the expected value) of the set, while a high value of standard deviation states that the data points are spread out over a much wider range of values.

4.2 Correlation

The more positive the correlation between two data sets more they are similar and more negative the value of correlation less is the similarity between data sets or more is dissimilarity in data sets.

So to get better results one's S-box must possess higher randomness or standard deviation and more negative value of the correlation.

5. Results

The comparison of the strong encryption capabilities shows that the performance of the new proposed S-box is better than some S-boxes used in past in the era of cryptography. The nonlinearity analysis done by comparing standard deviations depicts that the properties are comparable to the S-boxes use as a touchstone in this work. Table 2 presents a list of results of nonlinearity analysis based on standard deviation. It can be understood graphically as well through Figure 4. As per discussion, that more negative the value of correlation less is the similarity between data sets or more is dissimilarity in data sets. The result of correlation is - 0.161 (refer Table 3) and it means that new S-box is stronger and so it assures the acceptability of this S-box to encryption application. Figure 5 clearly demonstrates the essence of correlation in the proposed S-box is more negative as compared to conventional one, hence providing more security and reliability.

Table 1. Construction of S-box in the form of 16 by 16 matrix

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

Table 2. Comparison of two algorithms based on Standard Deviation

S-Box	Standard Deviation
Proposed	112.84
Majid[1]	104.92

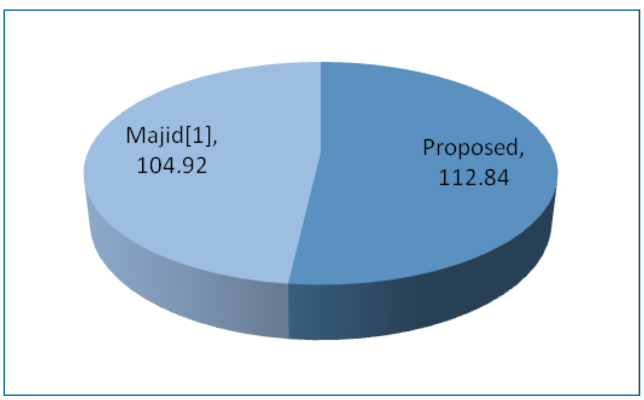

Figure 4. Comparison of two algorithms based on Standard Deviation.

Table 3. Comparison of two algorithms based on Correlation

S-Box	Correlation
Proposed	–0.161
Majid[1]	–0.04

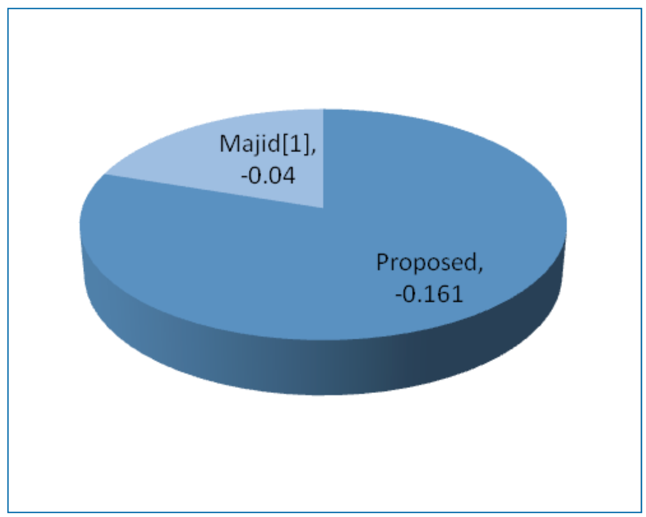

Figure 5. Comparison of two algorithms based on Correlation.

6. Conclusions

In this paper, a new method is presented to construct an S-box with the application of a set of specific differential equations called Lorenz system of equations. This set of equations shows chaotic behavior in given intervals with specific initial parameters. In order to evaluate the performance of the new proposed S-box, a comparison is presented by the application of standard deviation and correlation. The results yield that the new S-box have desirable properties which give more strength to cryptography techniques and is suitable for encryption applications used for secure communications.

7. References

1. Khan M, Shah T, Mahmood H, Gondal MA, Hussain I. A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. Nonlinear Dynamics. 2012; 70(3):2303–11.
2. Chen G, Chen Y, Liao X. An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. Chaos, Solitons and Fractals. 2007; 31(3):571–7.
3. Detombe J, Tavares S. Advances in Cryptology. Proceedings of CRYPTO. Lecture Notes in Computer Science. 1992; 92:165–81.
4. Guoping T, Xiaofeng L, Yong C. A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons and Fractals. 2005; 23(2):413–9.
5. He D, Chen Y, Chen J. Cryptanalysis and improvement of an extended chaotic maps based key agreement protocol. Nonlinear Dynamics. 2012; 69:1149–57.
6. Hussain I, Shah T, Gondal MA, Mahmood H. A new algorithm to construct secure keys for AES. International Journal of Contemporary Mathematical Sciences. 2010; 5(26):1263–70.
7. Hussain I, Shah T, Mahmood H, Afzal M. Comparative analysis of S-boxes based on graphical SAC. Int J Comput Appl. 2010; 2(4):5–8.
8. Hussain I, Shah T, Gondal MA, Khan WA. Construction of new S-box using a linear fractional transformation. World Appl Sci J. 2011; 14(12):1779–85.
9. Hussain I, Shah T, Gondal MA, Mahmood H. Some analysis of S-box based on residue of Prime Number. Proceedings of the Pakistan Academy of Sciences. 2011; 48(2):111–5.
10. Hussain I, Shah T, Gondal MA, Wang Y. Analyses of SKIPJACK S-box. World Appl Sci J. 2011; 13(11):2385–8.
11. Hussain I, Shah T, Gondal MA. An efficient image encryption algorithm based on S_8 S-box transformation and NCA map. Optic Comm. 2012; 285(24):4887–90.
12. Hussain I, Shah T, Gondal MA, Mahmood H. A projective general linear group based algorithm for the construction of substitution box for block ciphers. Neural Comput Appl. 2012; 22(6):1085–93.
13. Hussain I, Shah T, Gondal MA, Mahmood H. Analysis of S-box in image encryption using root mean square error method. Z Naturforsch. 2012; 67:327–32.
14. Hussain I, Shah T, Gondal MA, Mahmood H. Generalized majority logic criterion to analyze the statistical strength of S-boxes. Z Naturforsch. 2012; 67:282–8.
15. Hussain I, Shah T, Gondal MA, Mahmood H. Construction of S_8 Liu J S-boxes and their applications. Comput Math Appl. 2012; 64(8):2450–8.
16. Hussain I, Shah T, Mahmood H, Gondal MA. A projective general linear group based algorithm for the construction of substitution box for block ciphers. Neural Comput Appl. 2012; 22(6):1085–93.
17. Hussain I, Shah T, Mahmood H, Gondal MA. A group theoretic approach to construct cryptographically strong substitution boxes. Neural Comput Appl. 2013; 23(1):97–104.
18. Hussain I, Shah T, Mahmood H, Gondal MA. S8 affine power affine S-boxes and their application. Neural Comput Appl. 2012; 21(1):377–83.
19. Ozkaynak F, Ozer AB. A method for designing strong S boxes based on chaotic Lorenz system. Phys Lett A. 2010; 374:3733–8.
20. Webster AF, Tavares S. In: Advances in cryptology. Proceedings of CRYPTO. Lecture Notes in Computer Science. 1986; 85:523–34.
21. Swapna BS, Sivanandam N. A survey on cryptography using optimization algorithms in WSN’s. Indian Journal of Science and Technology. 2015; 8(3):216–21.
22. Vincent PMDR, Iqbal SA, Bhagat K, Kushwaha KK. Cryptography: A mathematical approach. Indian Journal of Science and Technology. 2013; 6(12):5607–11.
23. Jose JJR, Raj EGDP. PACMATS: An adaptive Symmetric block cipher for parallel computing environments. Indian Journal of Science and Technology. 2014; 7(S4):99–105.
24. Adams C, Tavares S. Advances in Cryptology. Proceedings of CRYPTO, Lecture Notes in Computer Science. 1989; 89:612–5.