Design of Chaotic Neural Network Based Method for Cryptographic Substitution Box

Musheer Ahmad
Department of Computer Engineering,
Jamia Millia Islamia, New Delhi 110025, INDIA
musheer.cse@gmail.com

Manish Malik
Department of Computer Engineering,
Jamia Millia Islamia, New Delhi 110025, INDIA
manishmalikkvs@gmail.com

***Abstract*—The cryptographic substitution boxes are the substantive constituent of most modern day block cryptosystems. Here, we proposed a novel method to generate cryptographically potent S-boxes by exploring the blended strength of chaos and neural network in its design. The designed chaos-based neural network, engaged to yield S-boxes, consists of four layers each of which have eight, four, two and one neuron(s), respectively. The excogitation and cognitive operation of chaotic neural network is couched to sample the random elements which eventually render infrangible configuration of S-box. By utilizing the features of chaos and neural network efficiently, we explicate cryptographically strong S-boxes that have the desired potentiality and practicability. The statistical scrutiny of proposed method against widely accepted performance measures suggest that the method is amicable to contrive dynamical S-boxes for strong block cryptosystem with respectable cryptographic features.**

Keywords—Substitution box; neural network; chaotic maps; block cryptosystem; security.

I. INTRODUCTION

Information security plays an indispensable role to realize secure and trustworthy communication over the open networks. The modern effective block cryptographic methods have been designed and employed to cater end-to-end security. In modern block cryptosystems such as the Blowfish, the Data Encryption Standard (DES), the Advanced Encryption Standard (AES), the Twofish, etc., the substitution boxes are the most substantive nonlinear components. In most block cryptosystems, S-boxes are typically meant to conceal the relationship among the cipher-text and the secret key as described by the Claude E. Shannon [1]. Mathematically, an n×m S-box is a nonlinear one to one mapping $S:\{0,1\}^n \rightarrow \{0,1\}^m$, which can also be represented by $S(x)=[a_{m-1}(x)a_{m-2}(x)...a_0(x)]$, where the $a_i(0 \le i \le m-1)$ is a Boolean function $\forall i, a_i:\{0,1\}^n \rightarrow \{0,1\}$. An strong S-box with respectable statistical features ascertains the strength of cryptosystems. Thus, the construction of strong S-boxes is an extremely significant part of cryptosystem designs. A strong S-box should have bijectiveness, high nonlinearity scores to withstand linear approximation attack, low differential probability to thwart differential cryptanalysis, and low transparency order to resist side channel attack. Realizing the grandness of efficient S-boxes, researchers have been focusing on the design of cryptographically strong S-boxes that can be employed to develop secure systems. As a result, a number of methods utilizing different approaches and techniques have been published in the past decade [2-6]. There has been a trend of constructing random S-boxes by utilizing the features of chaotic systems. The broad investigations of chaotic maps dynamics have uncovered the fascinating relationship in the middle of chaos and cryptography. In chaos hypothesis, the chaos maps are the dynamical systems whose future motion advances with time. They exhibits attributes of ergodicity, pseudorandom conduct, blending properties, and significantly their high affectability to initial conditions/parameters, that are quite virtuous for the construction of strong cryptosystem [7]. The chaotic systems are panoptically incorporated to design cryptographic primitives like image encryption, hash function, authentication, S-box, data hiding, etc., and hence popularize the field of chaos-based cryptography [7-13].

The complex interconnected nonlinear nature of neurons in neural networks introduces complexity in the system. Due to the presence of multiple layers in which the neuron outputs from one layer are mixed to the neuron(s) of next layer. The clubbing of chaos with neural network system makes the network nonlinear and touchy to the plaintext and produces an apparently random output. This property of chaotic neural systems makes them suitable for producing cryptographic keys and the inputs at different points. Besides, the structure of the chaotic neural system viz. the weights, biases and neural's transfer function parameters are produced utilizing chaotic maps to ad lib the randomness of the entire framework. In this paper, the properties of both chaotic maps and neural systems are coalesced to invent an efficient substitution box. The performance analyses of the proposed S-box against standard quality parameters as bijectivity, nonlinearity, strict avalanche characteristics, differential approximation probability and transparency order, verifies the effectiveness of the proposed method.

The remaining part of this paper is prepared as follows. The proposed method of designing chaotic neural network and procedure for generating S-box is presented in next section. In Section 3, the world-wide accepted quality measures for assessing effectiveness of an S-box are summarized which is followed by the performance analyses of proposed S-box in Section 4. Finally, the conclusion of the work is delineated in Section 5.

978-1-4673-9939-5/16/$31.00 ©2016 IEEE

II. Proposed Design And Method

A. Design of Chaotic Neural Network

In proposed method, a neural network is designed to generate S-box, depicted in Figure1, contains four layers: the input layer (which contains eight neurons), the 1st hidden layer (which contains four neurons), the 2nd hidden layer (contains 2 neurons) and the output layer (has a single neuron). The proposed neural network is chaotic in the sense that the all initial inputs, internal weights and biases are chaotic values that are extracted from well studied PWLCM chaotic map. The same chaotic map is explored to serve as the transfer function for each neuron of the network. The input to the designed network is a key P of size 64-bit which is segmented into eight parts each of 8-bit as $P=[P_0P_1....P_7]$. The result of input layer C_i takes the key segment P_i (where $0 \le i \le 7$) and evaluated as:

$$C_i = F^{N_0}(\sum W_0 P_i + B_0, Q_0) \tag{1}$$

Where N_0 $(20 \le N_0 \le 100)$ is a value produced by the key -generator and function is transfer function of each neuron in proposed neural network. The PWLCM map is amongst the most studied chaotic systems and its system equation can be defined as [14]:

$$F(y(k),r) = y(k+1) = \begin{cases} \dfrac{y(k)}{r} & 0 < y(k) \le r \\ \dfrac{1-y(k)}{1-r} & r < y(k) < 1 \end{cases} \tag{2}$$

Where $y(k)$ is variable of map and r is the control parameter and $0 < y(k) < 1$, $0 < r < 1$. The PWLCM exhibits excellent chaotic behaviour because it has highest rate of separation of two minutely closed trajectories when $r = 5$. Here, the input weight matrix $W_0 = [w_{0,0}, w_{0,1}, ... w_{7,7}]$ of size 8×8, the bias matrix $B_0 = [b_0, b_1, ... b_7]$ is of size 8×1, and the control parameter matrix $Q_0 = [q_0, q_1, ... q_7]$ is of size 8×1. To obtain output C of the input layer, first input P is multiplied by respective weights W_0 and added the respective biases B_0 of neurons. The value $\Sigma W_0 P + B_0$ is used as current state x, and generated Q_0 control parameter r to repeat the PWLCM map for N_0 times, as described in Eq. (1). Following the similar procedure, the matrices outputs of subsequent layers i.e. D, E and Op are enumerated as given in Eqn 3, 4 and 5. Where matrix W_1 is of size 4×8, W_2 of 2×4, W_3 of 1×2, B_1 of 4×1, B_2 of 2×1, B_3 of 1×1, Q_1 of 4×1, Q_2 of 2×1, Q_3 of 1×1. Initially, the matrices W_0, B_0, Q_0, W_1, B_1, Q_1, W_2, B_2, Q_2, W_3, B_3, Q_3 receives a value generated by the key generator. Like N_0, the random numbers N_1, N_2 and N_3 are generated randomly $(20 \le N_1, N_2, N_3 \le 100)$ and defines the iterations number of transfer function for every layer. The random iterations of transfer functions ameliorate the randomness in the relation of inputs and outputs of neurons in network layer.

$$D = F^{N_1}(\sum W_1 C + B_1, Q_1) \tag{3}$$

$$E = F^{N_2}(\sum W_2 D + B_2, Q_2) \tag{4}$$

$$Op = F^{N_3}(\sum W_3 E + B_3, Q_3) \tag{5}$$

After one operation of CNN network, the output Op where $(0 < Op < 1)$ is annealed as:

$$w = (Op \times 10^{10}) \bmod (256) \tag{6}$$

Which is now stored in the S-box vector, provided w is not in the vector already. This ensures that the S-box produced by this method remain bijective. If w is already in the vector than the same process is repeated with different randomly generated values of N_0, N_1, N_2 and N_3.

B. Key Generator

The key generator that is used in our method is 1D chaotic map and accepts a key of size 64-bit as $K = K_0 K_1 K_2 K_3$, where K_i is 16-bit part of K. To fix the initial values of cubic map in (8), the following transformation is applied:

$$x(0) = \left(\sum_{i=0}^{3} \left(\frac{K_i}{2^{16}} \right) \right) \bmod (1) \tag{7}$$

$$x(n+1) = \lambda \times x(n) - \lambda \times x(n)^3 \tag{8}$$

Where $\lambda = 2.59$ is map's control parameter and the x is state variable which satisfies $0 \le x(n) \le 1$, the cubic map returns the chaotic values $x(n)$ on applying iterations. The *mod*(1) is an operate which returns a floating-point value between 0 and 1.

C. Method for Substitution-box Synthesis

The steps of proposed method for chaotic neural network based substitution box synthesis are as follows.

1. Initialize the input 64-bit secret key K, and an empty array S of size 1×256.
2. Supply K to key generator and iterate for 50 times.
3. Further iterate key generator to initialize N_0, N_1, N_2 and N_3
4. Further iterate key generator to initialize W_0, W_1, W_2, W_3, B_0, B_1, B_2, B_3, Q_0, Q_1, Q_2, and Q_3 with chaotic values.
5. Operate the neural network, as discussed in section 2.1, to get output Op.
6. Anneal the Op according to Eq. (6).

7. Store the value *w* in array *S* if it is absent, else ignore.
8. Repeat the step 2 to 8 unless the *S* is filled with all unique entries.
9. Reshape *S* to 16×16 table and declare as final S-box.

The suggested CNN network, depicted in Figure 1., is aimed to construct cryptographically potent substitution boxes.

III. Performance Evalauation

The substitution box provided in Table III is retrieved with proposed method. The following cryptographic measures are widely accepted among researchers and cryptographers worldwide [3, 6, 15-19] for evaluating the strengths and potency of generated substitution boxes.

A. Bijectiveness

The bijectiveness of an $n \times n$ S-box can be easily verified by following the procedure given in Ref. [2]. A Boolean function g_i $(1 \le i \le n)$ of an S-box is said to be bijective when it satisfies the condition that hamming weight of $Sum(\alpha_i g_i)$ is 2^{n-1}, where $\alpha_i \in \{0,1\}$ $((\alpha_1, \alpha_2, ..., \alpha_n) \neq (0,0,...,0))$. The proposed S-box has all distinct elements in the range [0, $2^8 - 1$] and the hamming weight of $Sum(\alpha_i g_i)$ is 128, this verifies that the S-box satisfies the bijectiveness.

B. Nonlinearity

Nonlinearity is an important property, which can decide the usability of an S-box as nonlinear component in block ciphers. In terms of the Walsh spectrum, it is defined as [15,16,19]:

$$N_g = 2^{n-1}\left(1 - 2^{-n} \max_{\omega \in GF(2^n)} \left| s_{\langle g \rangle}(\omega) \right| \right) \tag{9}$$

Where N_g is the nonlinearity of the Boolean function g and the Walsh spectrum of *g(x)* is described as:

$$S_{\langle g \rangle}(\omega) = \sum_{x \in GF(2^n)} (-1)^{g(x) \oplus x \bullet \omega} \tag{10}$$

Where ω belongs to $GF(2^8)$ and $x.\omega$ denotes the scalar product of x and ω. Following the mathematics for proposed 8×8 S-box, the nonlinearity of eight Boolean function g_i $(1 \le g_i \le 8)$ involved come out as 108, 106, 108, 106, 104, 106, 104, 106, respectively, providing an amazing average value of 106. The performance of the S-box is tested against some recent chaos-based S-boxes in Table I and II. The honorable performance outcomes of proposed S-box are evident from comparisons made in same Table. Comparatively, the proposed S-box has better statistical results in terms of minimum, maximum and average nonlinearity score. High nonlinearity scores of all eight Boolean functions in S-boxes are requisite since it diminishes the input-output correlation.

TABLE I. Comparison of Nonlinearity Scores of Some 8×8 Chaotic S-boxes

S-Box	Nonlinearity							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Proposed	108	106	108	106	104	106	104	106
In [15]	98	100	100	104	104	106	106	108
In [16]	104	100	106	102	104	102	104	104
In [17]	108	102	100	104	104	102	98	106
In [18]	100	108	106	104	102	102	106	108
In [19]	98	100	106	104	106	100	106	104

TABLE II. Comparison of Min, Max, Mean Nonlinearity of Some 8×8 Chaotic S-boxes

S-Box	Nonlinearity		
	Min	**Max**	**Mean**
Proposed	104	108	106
In [15]	98	108	103.25
In [16]	100	104	103.25
In [17]	98	108	103
In [18]	100	108	104.5
In [19]	98	106	103

C. Differential Probability

A poor S-box design is easily vulnerable to the differential cryptanalysis. To avoid such scenarios, S-boxes should ideally have low differential probability. To ensure a uniform mapping probability, an input differential δx_j should map uniquely to an output differential δy_j for each *j*. The differential approximation probability, for an S-box, is a measure of differential probability [5] which is defined as:

$$DP(\delta x \to \delta y) = \left(\frac{\#\{x \in X \mid f(x) \oplus f(x \oplus \delta x) = \delta y\}}{2^n} \right) \tag{11}$$

Here, X is the set of all input values and 2^n are number of S-box elements. The maximum differential probability, listed in Table 4, for the proposed S-box is 10/256, which is quite better than the maximum DP of S-boxes investigated by Jakimoski, Khan, Khan and Gondal *et al.* in [15,17,18,19], where it is 12/256.

D. Strict Avalanche Criteria (SAC)

The strict avalanche criterion (SAC) was initially presented by Webster and Tavares [4] in 1986. If a Boolean function satisfies SAC, then when an input bit is changed then each of its output bits should have a change with a probability of 0.5. There is an efficient procedure, called dependence matrix, introduced by Webster and Tavares in Ref. [4] are commonly used to test the SAC of an S-box. The SAC of our S-box is evaluated as 0.4987 with a SAC difference of 0.0013 from its ideal score of 0.5. In Table IV, the SAC score shows

that the our S-box slightly outperforms than the S-boxes investigated in [15,16,18,19].

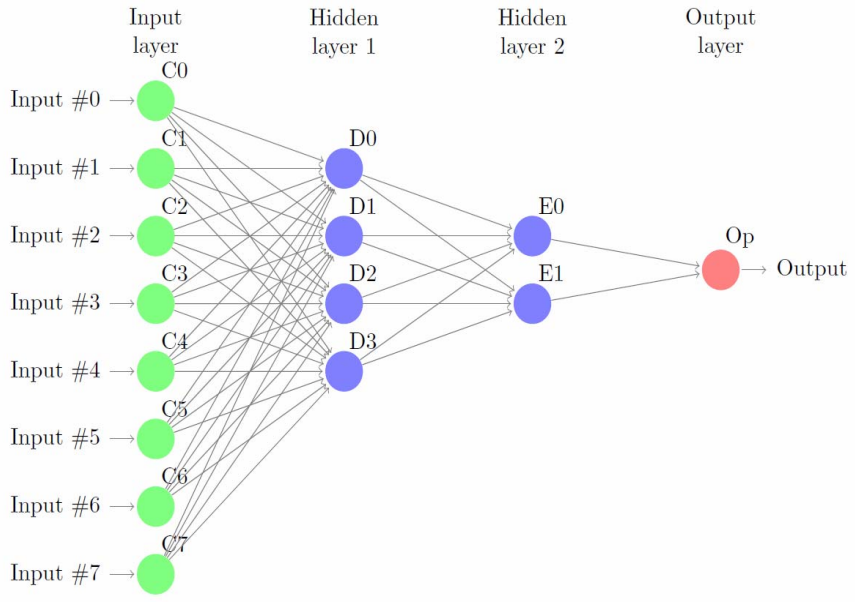

Fig. 1. Synoptic of proposed four-layer chaotic neural network

TABLE III. PROPOSED CHAOTIC SUBSTITUTION BOX

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

E. Transparency Order

The resistivity of an S-box towards algebraic attack or side channel attack (SCA) is equally significant. But, it has been marked that the SCA is more practical than algebraic attack. Since, the vast majority of digital gadgets are not flawlessly carefully designed; one can get sensitive data from side channels, for example, power consumption or the timing of operations or the software implementation. The differential power analysis (DPA) is said to be a standout amongst the most capable strategy against block ciphers to execute SCA

assault. Rijindael S-box included in the AES is generally focused by cryptanalysts as oracles giving the output corresponding to a given information [21]. The procedures are accounted to check the resistivity against SCA assault. To evaluate the resistance of S-boxes towards DPA assaults, transparency order (TO) measure is suggested by the cryptographers [21]. If an S-box show lower TO score, then the S-box tends to exhibit more resistant against DPA attack, i.e. the count of power traces to identify the correct key will be higher. According to the Ref. [21], the transparency order of S-box is defined as:

$$TO(F) = \max_{\beta \in F_2^m} \left(\left| m - 2H(\beta) \right| - \frac{1}{2^{2n} - 2^n} \sum_{a \in F_2^n} \left| \sum_{i=1}^{m} (-1)^{\beta_i} \mathrm{A}_{F_i}(a) \right| \right)$$

The transparency order of proposed S-box is obtained as 7.8, which is slightly better than value 7.86 for the well-known Rijindael AES S-box. This clearly depicts that the proposed S-box has better DPA attacks resistivity than AES S-box.

TABLE IV. SAC AND MAX DP OF SOME CHAOS BASED 8×8 S-BOXES

S-Box	SAC	Max DP
Proposed	0.4987	10/256
In [15]	0.4972	12/256
In [16]	0.5048	10/256
In [17]	0.5012	12/256
In [18]	0.4978	12/256
In [19]	NR	12/256

IV. CONCLUSION

In this paper, we suggested a method to blend the features of chaos and neural network for the synthesis of cryptographically strong 8×8 substitution boxes. The chaotic maps offer sensitiveness to key, while the neural network caters one-way property. The anticipated method is framed to derive inviolable configuration of the generated S-box. The effectiveness of the anticipated method is justified by the honourable statistical scores of SAC, nonlinearity, differential probability, transparency order obtained for generated S-box. Hence, the statistical performance of proposed method against widely accepted measures signal that the method is amicable to contrive dynamical S-boxes for strong block cryptosystem with respectable cryptographic features.

References

[1] C. E. Shannon, "Communication theory of secrecy systems", Bell Systems Technical Journal, vol. 28, pp. 656-715, 1949.

[2] C. Adams, S. Tavares, "Good S-boxes are easy to find", Advances in cryptology: CRYPTO'1989 Proceedings, Lecture notes in computer science, vol. 435, p. 612–5, 1989.

[3] J. Detombe, S. Tavares, "Constructing large cryptographically strong S-boxes", Advances in cryptology: AUSCRYPT'1992 Proceedings, Lecture notes in computer science, vol. 718, pp. 165-181, 1992.

[4] A. F. Webster and S. E. Tavares, "On the design of S-boxes", Advances in Cryptology-CRYPTO'1885 Proceedings, Lecture Notes in Computer Science, vol. 218, pp 523-534, 1986.

[5] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", Journal of Cryptology, vol 4, no. 1, pp. 3-72, 1991.

[6] M. Ahmad, S. Alam, "A Novel Approach for Efficient S-Box Design Using Multiple High-Dimensional Chaos." International Conference on Advanced Computing & Communication Technologies, pp. 95-99, 2014.

[7] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos based cryptosystems", International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151, 2006.

[8] N. Masuda, K. Alihara, "Cryptosystems with discretized chaotic maps", IEEE Transaction on Circuits and Systems-I, vol. 49, no. 1, pp. 28-40, 2002.

[9] M. Ahmad, H. Chugh, A. Goel, P. Singla, "A chaos based method for efficient cryptographic S-box design", International Symposium on Security in Computing and Communications, CCIS, vol. 377, pp. 130-137, 2013.

[10] M. Ahmad, P. M. Khan, M. Z. Ansari, "A simple and efficient keydependent S-box design using Fisher-Yates shuffle technique", International Conference on Security in Networks and Distributed Systems, CCIS, vol. 420, pp. 540-550, 2014.

[11] M. Ahmad, H. Haleem, P.M. Khan, "A new chaotic substitution box design for block ciphers." International Conference on Signal Processing and Integrated Networks, pp. 255-258, 2014.

[12] M. Ahmad, F. Ahmad, Z. Nasim, Z. Bano, S. Zafar, "Designing chaos based strong substitution box." International Conference on Contemporary Computing, pp. 97-100, 2015.

[13] M. Ahmad, D. Bhatia, Y. Hassan, "A Novel Ant Colony Optimization Based Scheme for Substitution Box Design." Procedia Computer Science 57, pp. 572-580, 2015.

[14] S. Li, G. Chen and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps", International Journal of Bifurcation and Chaos, vol. 15, no. 10, pp. 3119–3151, 2005.

[15] G. Jakimoski, and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps", IEEE Transaction on Circuits Systems, vol. 48, no. 2, pp. 163-169, 2001.

[16] F. Özkaynak and A. B. Özer, "A method for designing strong S-boxes based on chaotic Lorenz system", Physics Letters A, vol. 374,no. 36, pp. 3733–3738, 2010.

[17] M. Khan, T. Shah, H. Mahmood and M. A. Gondal, "An efficient method for the construction of block cipher with multi-chaotic systems", Nonlinear Dynamics, vol. 71, no. 3, pp. 489-492, 2013

[18] M. Khan and T. Shah, "An efficient construction of substitution box with fractional chaotic system", Signal, Image and Video Processing, vol. , no. , pp. , November 2013. doi 10.1007/s11760-013-0577-4.

[19] M. A. Gondal, A. Raheem, I. Hussain, "A Scheme for Obtaining Secure S-Boxes Based on Chaotic Baker's Map", 3D Research, pp. 5-17, 2014. doi: 10.1007/s13319-014-0017-4

[20] M. Matsui, "Linear Cryptanalysis Method of DES Cipher", Advances in Cryptology: EuroCrypt'1993 Proceedings, Lecture Notes in Computer Science, vol. 765, pp. 386-397, 1994.

[21] E. Prou, "DPA Attacks and S-Boxes", Proceedings of FSE'2005, Lecture Notes in Computer Science, vol. 3557, pp 424-441, 2005.

[22] M. Ahmad, D.R. Rizvi, Z. Ahmad, "PWLCM-Based Random Search for Strong Substitution-Box Design", Second International Conference on Computer and Communication Technologies, pp. 471-478. Springer, 2016.