Neural Comput & Applic
DOI 10.1007/s00521-017-3287-y

ORIGINAL ARTICLE

Construction of robust substitution boxes based on chaotic systems

Fatih Özkaynak[1]

Received: 1 July 2017 / Accepted: 13 November 2017

Abstract The construction of substitution boxes (s-boxes) is an important research area in cryptography. S-box is an important mathematical object. The aim of this study is to construct s-box designs with the best performance criteria for all chaotic system classes. The proposed method achieves the best s-box designs for all chaotic systems classes. The method is independent of the chosen chaotic system. The analyses show that maximum value of non-linearity criterion is 106.75 and minimum value of equiprobable input/output XOR distribution table is 10. The importance of the best generated s-boxes based on chaotic systems is that cryptologic properties of the best generated s-box structures are the upper bound for chaos-based s-box literature.

Keywords Cryptography · S-box · Chaos

1 Introduction

Cryptography algorithms have been used in many applications areas. Today, developments on computer and communication technology have helped transferring important personal data through the long-distance channels. These data must be protected in several ways to provide confidentiality, integrity and authentication. Cryptology is the science which answers all such needs in today's communication systems. There are two basic cryptographic trust models, symmetric (private) and asymmetric (public) key cryptography. Both approaches have various advantages and disadvantages according to their usage areas.

In the literature, many chaos-based encryption algorithms have been proposed since chaotic systems are theoretically ideal candidates for cryptographic applications [1–3]. Although there are examples of successful encryption algorithms [4–13], many chaos-based cryptology studies have several problems [14–16]. The main problem of chaos-based encryption algorithms is that cryptanalysis studies are done using very simple statistical tests such as UACI, NPCR and histogram analysis. The success of these tests does not mean that the encryption algorithm is secure. Many cryptanalysis studies have shown this result both theoretically and practically [17]. Therefore, researchers should be very careful when proposing new encryption algorithms. If a chaos-based cryptographic encryption algorithm is proposed, objectives and test criteria should be clearly defined.

The aim of the study is not to design an encryption algorithm. This study focuses on s-box structure that is part of symmetric encryption algorithms. Because, the evaluation criteria of s-box design are clearly known. This is one of the major advantages of focusing chaos-based s-box designs. Another advantage of study is that generated chaos-based s-box structures can also be used in well-known block cipher algorithms such as AES. In the literature, security features of the AES algorithm have been studied in detail. This guarantees provable security.

1.1 Substitution boxes

One of the main blocks in the design architecture of symmetric encryption algorithms is s-box. These structures are also known as vectorial Boolean functions. It is a

✉ Fatih Özkaynak
ozkaynak@firat.edu.tr

[1] Department of Software Engineering, Faculty of Technology, Fırat University, 23119 Elazig, Turkey

Published online: 20 November 2017

necessity that to construct robust s-boxes with strong cryptographic properties. Since the security of the symmetric encryption algorithms is directly related to these structures [18]. The best example of the importance of s-box structures is the cryptanalysis studies of the DES. One of these cryptanalysis studies was done by Matsui [19]. Matsui showed that nonlinear components (s-boxes) of DES have bad cryptographic properties. This attack technique, known as linear cryptanalysis, examined the nonlinear characteristics of the s-box structures. The attack aims to find a linear approximation to s-boxes. There are eight different s-boxes in the DES architecture. These s-boxes numbered from S_1 to S_8. Linear cryptanalysis of DES showed that some s-boxes have very weak nonlinear characteristics such as the S_5. Starting from this weakness; Matsui analyzed using 2^{43} known plaintext/ciphertext pairs [19]. After linear cryptanalysis, another cryptanalysis study has been carried out by Biham and Shamir [20]. These analyzes reveal that a new construction architecture is needed to resistance differential and linear attacks, and at the end of this process, advanced encryption standard (AES) has been developed [21].

It is very difficult to find methods for constructing robust s-boxes. General methods for constructing s-boxes are power polynomial, inversion mapping and random methods [18]. The first two methods are proposed by Nyberg. Nyberg's inversion mapping method is designed in the best-known cryptographic features. Still not known better. This method has been used in AES design architecture. For example, AES s-box nonlinearity value is 112 [21]. It is resistant to linear and differential attacks due to its cryptographic features. However, recently developed algebraic and side channel analysis studies showed that these type s-box design techniques remained weak [22]. Therefore, many researchers are currently working on new designs will be an alternative to algebraic structures.

Lately, some s-box construction methods based on random method have been proposed as an alternative to the algebraic techniques. Generally chaotic systems have been used as randomness source. A number of s-box structures have been proposed using different chaotic systems in different design architectures. However, the upper bounds of the cryptographic properties of this design approach have not been given.

1.2 Our contribution

This study has been investigated chaos-based s-box structures with the best cryptographic properties. Investigations have been carried out for all chaotic system classes. In the experiments and simulations, more than 20,000 s-box structures have been randomly produced based on discrete- and continuous-time chaotic systems. The well-known discrete- and continuous-time chaotic systems are the logistic map and the Lorenz system, so the examples are based on these two systems. The proposed method is independent of the chosen chaotic system. Different s-box tables can be produced for other chaotic systems. For example, generated s-boxes and performance values for the Henon map and Chen system are included in "Appendix" section. The importance of the best generated s-boxes based on chaotic systems is that cryptologic properties of the best generated s-box structures are the upper bound for chaos-based s-box literature.

The rest of study is organized in following manner. Section 2 is to present a detailed overview on the chaos-based s-box literature. Main s-box design architectures based on chaotic systems are discussed in this section. Nearly all the works covering the SCI journals have been tried to be listed for the last 10 years. Section 3 introduces selection process of the chaotic systems with best randomness properties and design method to be used in experiments and simulations. In Sect. 4, s-box evaluation criteria are explained and the results obtained by experiments and simulations are shown. A detailed comparison table is given in this section. This comparison table gives the most comprehensive comparison in the literature. In the last section, the study has been summarized.

2 Review of chaos based s-box literature

In the design process of cryptographic systems, chaotic systems have been attracting many researchers since they have some special properties [1–3, 23]. These properties are:

- Chaotic systems' long-term behavior is non-periodic.
- System trajectories dependent on the initial conditions and control parameters.
- The equation of system is deterministic. Namely, the reason for the irregular behavior is intrinsic nonlinearities rather than noise.

These features are used to ensure confusion and diffusion properties which are of the cryptographic security requirements [23]. The most common approach used in chaos based s-box designs is to convert chaotic values into integers. In this construction approach, continuous-valued chaotic orbits are digitized in order to generate integer-valued random sequence. Digitized random sequence is entropy source of random s-box.

Several studies were conducted about building s-box generators based on chaos [24–63]. In the first examples of chaos based s-box construction studies, outputs of discrete-time chaotic system have been transformed into s-box cells [24–27]. In Ref. [43, 55, 56, 59, 61], new design proposals have been developed combining the simple mathematical structure of discrete-time chaotic systems with the different design architectures.

The use of continuous-time chaotic systems in the s-box construction process is proposed for the first time in Ref. [29]. Following this work, many good design studies have been proposed using continuous-time chaotic systems [31, 36, 45, 62].

To improve s-box performance criteria, the idea of using chaotic systems with richer dynamic features has become a common approach. Researchers have proposed various s-box construction structures using time delay [35], hyperchaotic [48, 50, 63] and fractional chaotic systems [51, 52, 58, 60].

In order to obtain the best performance measurements, designers have combined chaotic systems with optimization algorithms [28, 30, 49, 57]. Comparing these design works with other designs can lead to misperception. Because the optimization process rather than the entropy source plays a more important role in these design process.

Many good design architectures based on mathematical structures that play a more important role in design than chaotic systems have been proposed by a research group of members Khan, Hussain, Shah, Gondal, Batool and Mahmood [32–34, 37–42, 53, 54].

3 Properties of proposed s-box construction method

The aim of the study is to generate chaos based s-box structure with best performance criteria. One of the best approaches to achieving this aim is the optimization algorithms, which are a branch of artificial intelligence. Optimization is the task of obtaining the best solution for a problem among all the solutions under given conditions. Where the targeted conditions are the highest nonlinearity value and the smallest XOR distribution table. A design logic based on a search algorithm has been established to achieve the best performance values.

The proposed approach is named as random generate and test. In this approach, s-box is constructed with random entries using chaotic systems and tested to satisfy cryptographic metrics. The quality of the randomness source to be used in this approach is of great importance. In the proposed approach, chaotic systems are used as a source of randomness. In the algorithm, the fraction part of the chaotic values is converted to integer values between 0 and 255. AES-like s-box structures have been constructed using these integer values.

It is important to be able to choose the best randomness source (chaotic system) at this stage. Because there are many chaotic system classes such as discrete- and continuous-time chaotic systems. Besides the selection of the chaotic system class, it is necessary to select the appropriate initial conditions and control parameters for these systems.

Reference [64] shows what is the most appropriate initial conditions and control parameters for various chaotic systems. Properties of various discrete- and continuous-time chaotic systems are given in Tables 2 and 3 of Ref. [64]. The initial conditions and control parameters given in this study are values for which chaotic behavior can be observed. These values guarantee a rich entropy source.

The basic steps of the proposed algorithm used to construct the s-box are as follows. In addition, the flowchart diagram of the proposed method is given in Fig. 1.

- Output values (trajectories) of any chaotic systems are calculated.
- The value between digits 3 and 6 of the fraction part of output values is normalized to the range 0–255 by the mode function.
- If there is no table, the calculated value is added to the table. The three digits are normalized to 0–255 range by applying the mod 256. Otherwise, it will continue with a new output value.
- These operations are continued until all the entries of s-box are filled.

The operation of the proposed algorithm is illustrated by an example. The first three cells of the s-box have been produced for simplicity. The first five output values obtained from the chaotic system orbit are as 0.274062652189317; 0.220809856520422; 0.359821010419312; 0.486193899848855; and 0.666470162335694. The value between digits 3 and 6 of the fraction part of first output value is 406. This value is normalized to the range 0–255 by the mode function. Normalized value is 150. So the value of the first cell s-box is 150. The value between digits 3 and 6 of the fraction part of second output value is 080. Normalized value is 80. So the value of the second cell s-box is 80. Third value of s-box is 214 since 982 mod 256 = 214.

4 Experiments and simulations results

Five criteria have been used in the evaluation process, bijective property, nonlinearity, strict avalanche criterion (SAC), outputs bit independence criterion (BIC) and equiprobable input/output XOR distribution. These criteria are widely used in the literature. The proposed algorithm in Sect. 3 guarantees the bijective property [18].

Nonlinearity property measures the degree of linearity of the s-box. This test calculates the similarity between *N*-

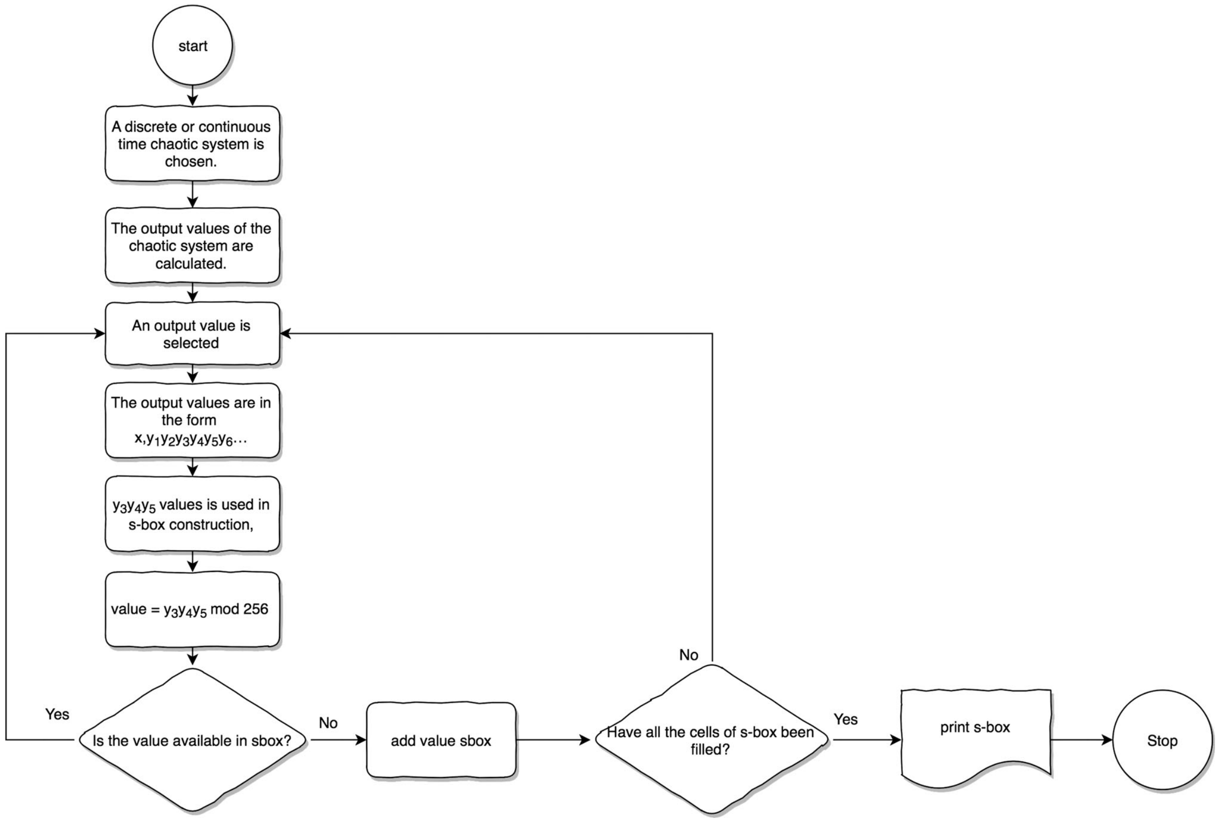

Fig. 1 Flowchart of proposed method

variable Boolean function of s-box and *N*-variable affine functions. In the test of nonlinearity property, affine functions have been used since these functions are cryptographically weak. If hamming distance between *N*-variable Boolean function of s-box and *N*-variable affine function is closer, then s-box is so cryptographically weak. Nonlinearity value can be calculated using Eq. (1). WHT in Eq. (1) represents Walsh Hadamard transform vector [18].

$$NL(f) = \frac{1}{2}\left(2^n - \mathrm{WHT}_{\max}\right). \tag{1}$$

Figure 2 shows the calculated average nonlinearity values for s-box structures based on discrete-time chaotic systems. The worst, best and average values are 99, 106.75 and 103.52, respectively. Figure 3 shows the calculated average nonlinearity values for s-box structures based on continuous-time chaotic systems. The worst, best and average values of s-box structures based on continuous-time chaotic systems are 99.25, 106.75 and 103.55, respectively.

Webster and Tavares proposed another important measure, which known as strict avalanche criterion. This measure calculates how the spreading of the input bits affects uniform distribution in the number of 0 and 1 bits in

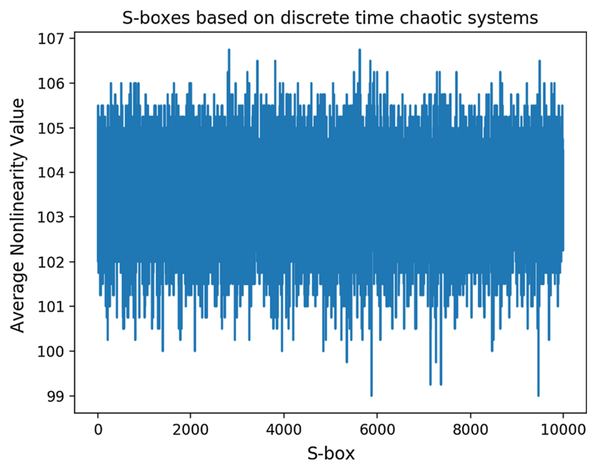

Fig. 2 Calculated average nonlinearity values for s-box structures based on discrete-time chaotic systems

the output. Therefore, derivative of a Boolean function is important for strict avalanche criterion. If $f(x)$ fulfills Eq. (2) for any $a \in GF(p)$ and any $\alpha \in GF(p)^n$ with $wt(\alpha) = 1$, then strict avalanche criterion has been satisfying.

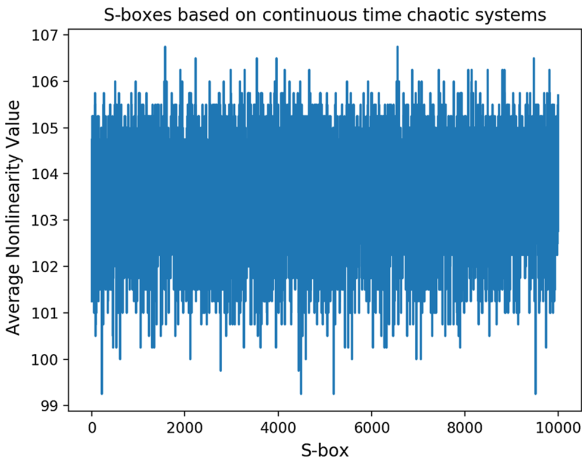

Fig. 3 Calculated average nonlinearity values for s-box structures based on continuous-time chaotic systems

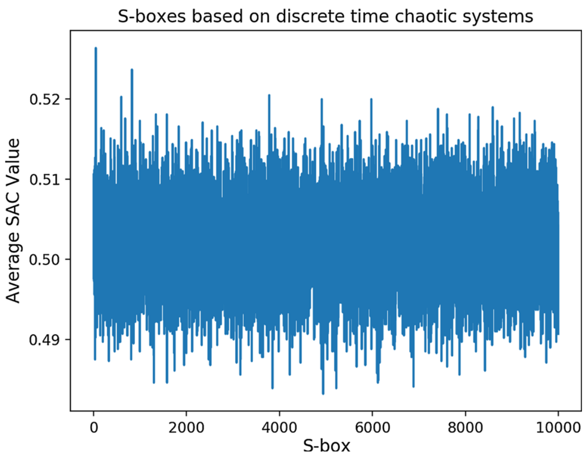

Fig. 4 Calculated average SAC values for s-box structures based on discrete-time chaotic systems

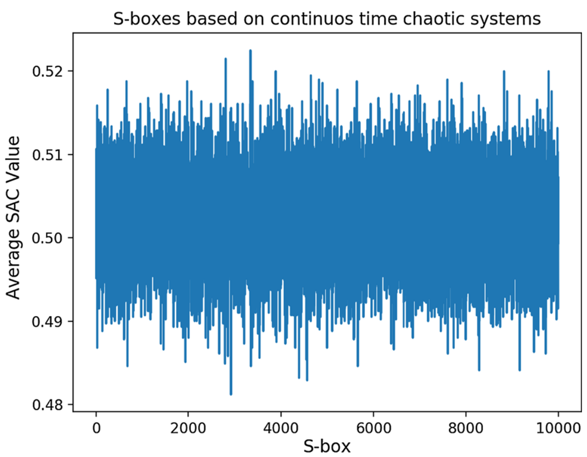

Fig. 5 Calculated average SAC values for s-box structures based on continuous-time chaotic systems

$$\text{prob}(f(x+\alpha) = f(x) + a) = 1/p \tag{2}$$

where wt(α) be the Hamming weight of α, i.e., the number of nonzero components of α, $\alpha \in \text{GF(p)}^n$.

The optimum value of the strict avalanche criterion (SAC) is 0.5. Figure 4 shows the calculated average SAC values for s-box structures based on discrete-time chaotic systems. The worst, best and average values are 0.4832, 0.5264 and 0.5020, respectively. Figure 5 shows the calculated average SAC values for s-box structures based on continuous-time chaotic systems. The worst, best and average values of s-box structures based on continuous-time chaotic systems are 0.4812, 0.5225 and 0.5019, respectively.

The output bits independence criterion is calculated independence of the avalanche vectors sets. These sets are

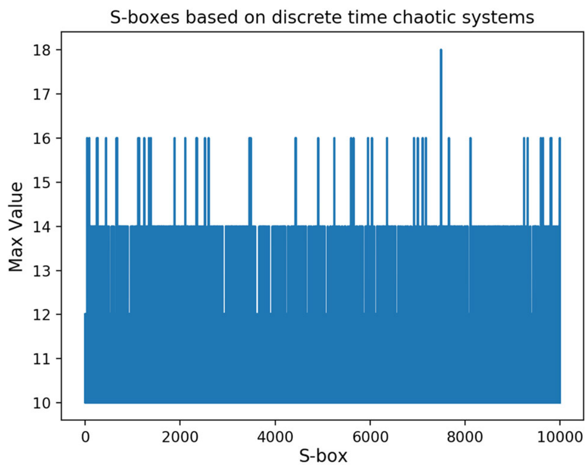

Fig. 6 The maximum value of differential distribution table for discrete-time chaotic systems

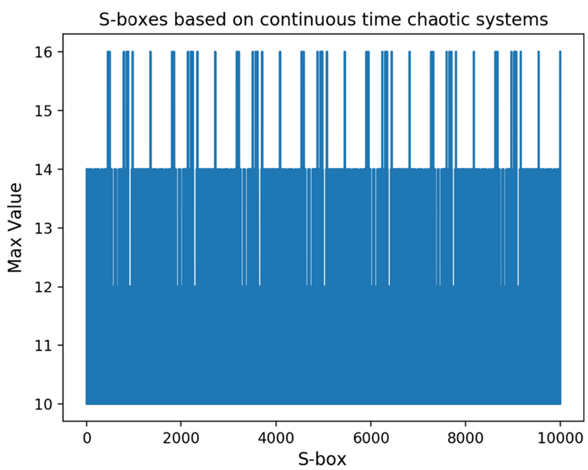

Fig. 7 The maximum value of differential distribution table for continuous-time chaotic systems

Table 1 Performance comparison for chaotic s-boxes

S-box	Maximum I/O XOR	Nonlinearity			BIC-SAC	BIC-nonlinearity	SAC		
		Avg	Min	Max			Avg	Min	Max
Ref. [24]	12	103.2	98	108	0.5031	104.2	0.5058	0.3671	0.5975
Ref. [25]	10	103.3	99	106	0.4995	103.3	0.4987	0.4140	0.6015
Ref. [26]	14	103.8	101	108	0.4958	102.6	0.5058	0.3906	0.5781
Ref. [27]	14	103	100	106	0.5024	103.1	0.5	0.4218	0.6093
Ref. [28]	10	104	102	106	0.4971	103.2	0.4980	0.3750	0.6093
Ref. [29]	10	103.2	100	106	0.5009	103.7	0.5048	0.4218	0.5937
Ref. [30]	10	108	108	108	0.4950	90	0.5068	0.4063	0.5781
Ref. [31]	12	103	96	106	0.5010	100.3	0.5039	0.3906	0.625
Ref. [32]	12	104.8	100	107	0.4890	104.7	0.4990	0.4290	0.5850
Ref. [33]	12	104.7	102	108	0.5021	104.1	0.5056	0.3906	0.5937
Ref. [34]	12	103	98	108	0.4988	104.1	0.5012	0.4062	0.5937
Ref. [35]	10	103.8	101	106	0.5037	103.4	0.5036	0.4140	0.6328
Ref. [36]	12	104	98	108	0.4967	102	0.4954	0.2813	0.6094
Ref. [37]	32	105.5	100	110	0.4983	107	0.5022	0.4063	0.5781
Ref. [38]	32	104.7	100	108	0.4965	105	0.4037	0.3906	0.5938
Ref. [39]	4	112	112	112	0.4992	112	0.5049	0.4531	0.5625
Ref. [40]	4	112	112	112	0.4992	112	0.5049	0.4531	0.5625
Ref. [41]	12	105.2	102	108	0.5013	104.3	0.5059	0.4063	0.5781
Ref. [42]	10	104	100	106	0.4990	102.5	0.4946	0.3750	0.6250
Ref. [43]	32	105.5	98	110	0.4994	105.7	0.4926	0.4062	0.5937
Ref. [44]	8	109	108	112	0.5012	104	0.5012	0.4531	0.5156
Ref. [46]	10	104	102	106	0.5019	103.5	0.5018	0.4825	0.5175
Ref. [47]	12	108	104	110	0.5006	112	0.5007	0.4258	0.5175
Ref. [48]	10	105.7	104	108	0.5032	104	0.4976	0.4219	0.5938
Ref. [49]	10	107	106	110	0.5010	105.5	0.5015	0.4063	0.5625
Ref. [50]	16	100	84	106	0.4962	101.9	0.4812	0.125	0.625
Ref. [51]	12	104.75	100	108	0.5009	103,6	0.4978	0.4218	0.6093
Ref. [52]	14	102.3	98	108	0.4992	100	0.4836	0.3281	0.6016
Ref. [53]	16	100	84	106	0.4962	101.9	0.4812	0.125	0.625
Ref. [54]	12	104	98	108	0.5078	104	0.5039	0.4218	0.6093
Ref. [55]	54	102.5	96	106	0.4026	102.5	0.5178	0.3906	0.6719
Ref. [56]	10	106.7	106	108	0.4951	104	0.5034	0.4219	0.6250
Ref. [57]	10	106.5	104	110	0.4984	105.2	0.5120	0.4375	0.6406
Ref. [58]	10	104.7	100	108	0.4942	103.1	0.4982	0.4218	0.5781
Ref. [59]	12	105.5	102	110	0.4988	104.3	0.5010	0.4063	0.6094
Ref. [60]	8	112	112	112	0.5027	108	0.5115	0.4219	0.5469
Ref. [61]	10	105.3	102	108	0.4971	104	0.5056	0.4375	0.5781
Ref. [62]	10	106.2	104	110	0.5023	102.3	0.5039	0.4219	0.5938
Ref. [63]	10	106	102	108	0.4968	105.4	0.5002	0.4219	0.5938
Proposed 1	10	106.7	106	108	0.4957	103.5	0.4941	0.3909	0.6094
Proposed 2	10	106.7	106	108	0.4994	103.2	0.4063	0.4063	0.4971

generated by changing the inverse of single bits of input [1]. This criterion is not shown graphically for all generated s-boxes since the calculated value is a matrix. Only the calculated values for the best s-box are given in the comparison table.

The equiprobable input/output XOR distribution table is an analysis method which is related differential cryptanalysis. It is desirable that the obtained values as a result of the analysis process are as small as possible. So the evaluations are made according to the calculated maximum value. This criterion is directly related to differential cryptanalysis. The differential table is a $2^n \times 2^m$ table whose entries are defined as Eq. (3) [1].

$$\mathrm{DP}_f = \max_{\Delta x \neq 0, \Delta y} \left(\frac{\#\{x \in X | f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^m} \right) \tag{3}$$

where X is the set of all possible input values and 2^m is the number of its elements.

The variation of the maximum value of differential distribution table for discrete-time chaotic systems is shown in Fig. 6. The best and worst values are 10 and 18, respectively. The variation of the maximum value of differential distribution table for continuous-time chaotic systems is shown in Fig. 7. The best and worst values are 10 and 16, respectively.

4.1 Performance comparison

The chaos-based s-box structures previously proposed in the literature and the comparison of the best examples of the proposed method are given in Table 1. The best s-box designs based on discrete- and continuous-time chaotic systems are given in Tables 2 and 3, respectively. S-boxes

Table 2 The best s-box design based on discrete-time chaotic systems

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

Table 3 The best s-box design based on continuous-time chaotic systems

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

in Tables 2 and 3 have been produced using logistic map and Lorenz system, respectively.

5 Conclusions

The aim of this study is to search for the chaos-based s-box structure with best cryptographic properties. In the study, the best s-box structures have been obtained for both discrete-time and continuous-time chaotic systems. The results obtained in the study can be summarized as follows.

- A comprehensive literature review has been given in Sect. 2. Nearly 50 studies published in SCI journals in the last decade have been reviewed. Performance comparisons of these studies are given in Table 1.
- Upper bound of nonlinearity is 106.75 for chaos-based s-box structures. This value is maximum value for designs based on only chaotic systems.
- In the proposed algorithm, the upper bound of nonlinearity is reached for both discrete-time and continuous-time chaotic systems.
- Maximum nonlinearity value can be improved up to 112 using optimization algorithms or mathematical constructions.
- The largest value of equiprobable input–output XOR distribution table is 10 for chaos-based s-box structures.
- Generated s-box structures are better than previously proposed s-box structures for SAC and BIC criteria.
- Generated s-box structures can be used as masks to prevent side channel attacks of symmetric encryption algorithms.

Acknowledgements F. Özkaynak is deeply grateful to the editors for smooth and fast handling of the manuscript. The author would also like to thank the anonymous referees for their valuable suggestions to improve the quality of this paper.

Appendix

See Tables 4 and 5.

Table 4 Proposed s-box based on chaotic Henon map (nonlinearity value is 106.75)

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

Table 5 Proposed s-box2 based on chaotic Chen system (nonlinearity value is 106.75)

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

References

1. Zhang H, Ma T, Huang G, Wang Z (2010) Robust global exponential synchronization of uncertain chaotic delayed neural networks via dual-stage impulsive control. IEEE Trans Syst Man Cybern Part B Cybern 40(3):831–844
2. Zhang H, Huang W, Wang Z, Chai T (2006) Adaptive synchronization between two different chaotic systems with unknown parameters. Phys Lett A 350(5–6):363–366
3. Zhang H, Liu D, Wang Z (2009) Controlling chaos: suppression, synchronization and chaotification. Springer, London
4. Liu H, Wang X (2010) Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 59(10):3320–3327
5. Liu H, Wang X (2011) Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 284(16–17):3895–3903
6. Liu H, Wang X, Kadir A (2012) Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 12(5):1457–1466
7. Wang X, Yang L, Liu R, Kadir A (2010) A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn 62(3):615–621
8. Wang X, Wang Q (2014) A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. Nonlinear Dyn 75(3):567–576
9. Wang X, Teng L, Qin X (2012) A novel colour image encryption algorithm based on chaos. Sig Process 92(4):1101–1108
10. Zhang Y, Wang X (2014) A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf Sci 273:329–351
11. Zhang Y, Wang X (2015) A new image encryption algorithm based on non-adjacent coupled map lattices. Appl Soft Comput 26:10–20
12. Wang X, Liu L, Zhang Y (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–18
13. Wang X, Zhang Y, Bao X (2015) A novel chaotic image encryption scheme using DNA sequence operations. Opt Lasers Eng 73:53–61
14. Zhang Y, Wang X (2014) Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation. Nonlinear Dyn 77(3):687–698
15. Özkaynak F, Yavuz S (2013) Security problems of pseudorandom sequence generator based on Chen chaotic system. Comput Phys Commun 184(9):2178–2181
16. Özkaynak F, Özer A (2016) Cryptanalysis of a new image encryption algorithm based on chaos. Optik 127:5190–5192
17. Wu Y, Noonan J, Agaian S (2011) NPCR and UACI randomness tests for image encryption. Cyber J Multidiscipl J Sci Technol J Sel Areas Telecommun 2:31–38
18. Cusick T, Stanica P (2009) Cryptographic boolean functions and applications. Elsevier, Amsterdam
19. Matsui M (1994) Linear cryptanalysis method for DES cipher, advances in cryptology—Eurocrypt'93. Lect Notes Comput Sci 765:386–397
20. Biham E, Shamir A (1991) differential cryptanalysis of DES-like cryptosystems. J Cryptol 4:3–72
21. Daemen J, Rijmen V (1998) AES proposal: Rijndael. In: First advanced encryption conference, California
22. Bard G (2009) Algebraic cryptanalysis. Springer, Berlin
23. Kocarev L, Lian S (2011) Chaos based cryptography theory algorithms and applications. Springer, Berlin
24. Jakimoski G, Kocarev L (2011) Chaos and cryptography: block encryption ciphers. IEEE Trans Circ Syst I 48(2):163–169
25. Tang G, Liao X, Chen Y (2005) A novel method for designing S-boxes based on chaotic maps. Chaos Solitons Fractals 23:413–419
26. Tang G, Liao X (2005) A method for designing dynamical S-boxes based on discretized chaotic map. Chaos Solitons Fractals 23(5):1901–1909
27. Chen G, Chen Y, Liao X (2007) An extended method for obtaining S-boxes based on 3-dimensional chaotic baker maps. Chaos Solitons Fractals 31:571–579

28. Chen G (2008) A novel heuristic method for obtaining S-boxes. Chaos Solitons Fractals 36:1028–1036
29. Özkaynak F, Özer A (2010) A method for designing strong S-boxes based on chaotic Lorenz system. Phys Lett A 374:3733–3738
30. Wang Y, Wong K, Li C, Li Y (2012) A novel method to design S-box based on chaotic map and genetic algorithm. Phys Lett A 376(6–7):827–833
31. Khan M, Shah T, Mahmood H, Gondal M, Hussain I (2012) A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. Nonlinear Dyn 70(3):2303–2311
32. Hussain I, Shah T, Mahmood H, Gondal M (2012) Construction of S8 Liu J S-boxes and their applications. Comput Math Appl 64(8):2450–2458
33. Hussain I, Shah T, Gondal M (2012) A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. Nonlinear Dyn 70(3):1791–1794
34. Khan M, Shah T, Mahmood H, Gondal M (2013) An efficient method for the construction of block cipher with multi-chaotic systems. Nonlinear Dyn 71(3):489–492
35. Özkaynak F, Yavuz S (2013) Designing chaotic S-boxes based on time-delay chaotic system. Nonlinear Dyn 74(3):551–557
36. Khan M, Shah T, Gondal M (2013) An efficient technique for the construction of substitution box with chaotic partial differential equation. Nonlinear Dyn 73(3):1795–1801
37. Hussain I, Shah T, Mahmood H, Gondal M (2013) A projective general linear group based algorithm for the construction of substitution box for block ciphers. Neural Comput Appl 22(6):1085–1093
38. Hussain I, Shah T, Gondal M, Khan W, Mahmood H (2013) A group theoretic approach to construct cryptographically strong substitution boxes. Neural Comput Appl 23(1):97–104
39. Hussain I, Shah T, Gondal M, Mahmood H (2013) An efficient approach for the construction of LFT S-boxes using chaotic logistic map. Nonlinear Dyn 71(1):133–140
40. Hussain I, Shah T, Gondal M (2013) Efficient method for designing chaotic S-boxes based on generalized Baker's map and TDERC chaotic sequence. Nonlinear Dyn 74(1):271–275
41. Hussain I, Shah T, Gondal M, Mahmood H (2013) A novel method for designing nonlinear component for block cipher based on TD-ERCS chaotic sequence. Nonlinear Dyn 73(1):633–637
42. Khan M, Shah T (2014) A construction of novel chaos base nonlinear component of block cipher. Nonlinear Dyn 76(1):377–382
43. Khan M, Shah T (2014) A novel image encryption technique based on Hénon chaotic map and S8 symmetric group. Neural Comput Appl 25(7–8):1717–1722
44. Lambić D (2014) A novel method of S-box design based on chaotic map and composition method. Chaos Solitons Fractals 58:16–21
45. Zaibi G, Peyrard F, Kachouri A, Prunaret D, Samet M (2014) Efficient and secure chaotic S-box for wireless sensor network. Secur Commun Netw 7:279–292
46. Liu H, Kadir A, Niu Y (2014) Chaos-based color image block encryption scheme using S-box. AEU Int J Electron Commun 68(7):676–686
47. Zhang X, Zhao Z, Wang J (2014) Chaotic image encryption based on circular substitution box and key stream buffer. Sig Process Image Commun 29(8):902–913
48. Liu G, Yang W, Liu W, Dai Y (2015) Designing S-boxes based on 3-D four-wing autonomous chaotic system. Nonlinear Dyn 82(4):1867–1877
49. Ahmad M, Bhatia D, Hassan Y (2015) A novel ant colony optimization based scheme for substitution box design. Proc Comput Sci 57:572–580
50. Khan M (2015) A novel image encryption scheme based on multiple chaotic S-boxes. Nonlinear Dyn 82(1):527–533
51. Khan M, Shah T (2015) An efficient construction of substitution box with fractional chaotic system. SIViP 9(6):1335–1338
52. Jamal S, Khan M, Shah T (2016) A watermarking technique with chaotic fractional S-box transformation. Wirel Pers Commun 90(4):2033–2049
53. Khan M, Shah T, Batool S (2016) Construction of S-box based on chaotic Boolean functions and its application in image encryption. Neural Comput Appl 27(3):677–685
54. Khan M, Shah T, Batool S (2016) A new implementation of chaotic S-boxes in CAPTCHA. SIViP 10(2):293–300
55. Khan M, Asghar Z (2016) A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation. Neural Comput Appl. https://doi.org/10.1007/s00521-016-2511-5
56. Lambić D (2017) A novel method of S-box design based on discrete chaotic map. Nonlinear Dyn 87(4):2407–2413
57. Farah T, Rhouma R, Belghith S (2017) A novel method for designing S-box based on chaotic map and teaching–learning-based optimization. Nonlinear Dyn 88(2):1059–1074
58. Özkaynak F, Çelik V, Özer A (2017) A new S-box construction method based on the fractional-order chaotic Chen system. SIViP 11(4):659–664
59. Belazi A, Latif A (2017) A simple yet efficient S-box method based on chaotic sine map. Opt Int J Light Electron Opt 130:1438–1444
60. Belazi A, Latif A, Diaconu A, Rhouma R, Belghith S (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt Lasers Eng 88:37–50
61. Belazi A, Khan M, Latif A, Belghith S (2017) Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. Nonlinear Dyn 87(1):337–361
62. Çavuşoğlu Ü, Zengin A, Pehlivan İ, Kaçar S (2017) A novel approach for strong S-box generation algorithm design based on chaotic scaled Zhongtang system. Nonlinear Dyn 87(2):1081–1094
63. Islam F, Liu G (2017) Designing S-box based on 4D-4Wing hyperchaotic system. 3D Res 8:9
64. Özkaynak F (2015) A novel method to improve the performance of chaos based evolutionary algorithms. Opt Int J Light Electron Opt 126(24):5434–5438