Egyptian Informatics Journal 23 (2022) 127–135

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

A method for generation of substitution box based on random selection

Fırat Artuğer [a,*], Fatih Özkaynak [b]

[a] Munzur University, Facult of Engineering, Department of Computer Engineering, 62100, Tunceli, Turkey
[b] Fırat University, Faculty of Technology, Department of Software Engineering, 23119, Elazig, Turkey

ARTICLE INFO

Article history:
Received 3 January 2021
Revised 5 May 2021
Accepted 18 August 2021
Available online 31 August 2021

Keywords:
Block cipher
S-box
Nonlinearity
Image encryption

ABSTRACT

Two basic requirements must be met to encrypt data. These requirements are confusion and diffusion properties. In particular, block cipher algorithms are based on a cryptographic component known as substitution-box to provide the need for confusion. Therefore, attack scenarios generally focus on this cryptographic component. There are alternative design approaches for substitution-box design. It is known that each design approach has several advantages and disadvantages. In this study, an alternative method is proposed to address the problems of the substitution-box design approach based on random selection. The success of the proposed method has been tested in three different scenarios. Analysis results for these three scenarios showed that generated substitution-box provides performance increase for nonlinearity criterion from s-box design criteria. Successful results achieved; It points out that improvement cryptographic components can be used in a variety of practical applications such as block ciphers, masks to prevent side-channel attacks, random number generators, and image encryption algorithms.

1. Introduction

The priorities of individuals, societies, and states have been changed with the digital transformation [1]. As a result of this change, information security is an issue that cannot be neglected for everyone [2]. Although information security is an umbrella concept, one of the topics associated with this concept (perhaps the first one that comes to mind) is cryptology. There are several alternatives for encrypting data. A notable among these alternatives is block encryption algorithms. These cryptographic solutions are widely used in ATM devices, biometric passports, and many IoT applications [3]. Two basic requirements must be met for a block cipher algorithm to be considered secure. These requirements are confusion and diffusion. Block cipher algorithms are based on cryptographic components known as substitution boxes (s-boxes) to provide the need for confusion properties [4]. Therefore, attack scenarios generally focus on this cryptographic component. Especially; linear and differential attack scenarios on s-box structures have been decisive in the transition from the DES (Data Encryption Standard) to AES (Advanced Encryption Standard [5]. Although the AES s-box design is a very successful example mathematically, diverse cryptanalysis scenarios such as application attacks have revealed various problems. A comparison for s-box design approaches is provided in Table 1 [6].

This study focuses on s-box design method based on random selection. Demonstrating that random selection-based s-box structures can be used as a countermeasure to prevent application attacks played an important role in making this selection. However, it is a serious problem that this design approach has low values for the nonlinearity criterion from the s-box design criteria [7]. Optimization algorithms attract attention as a common approach used recently in the literature to solve this problem [8–11]. Computational load in optimization algorithms is another problem that designers have to solve as a disadvantage [12].

The original aspect of this study is that a method has been proposed that can be an alternative to approaches based on both mathematical [13–18] and optimization techniques [8–11]. The aim of this study is to overcome the disadvantages of random selection approaches. In the study, s-box structures similar to AES have been generated to increase practical applicability. Any

* Corresponding author.
E-mail addresses: firatartuger@munzur.edu.tr (F. Artuğer), ozkaynak@firat.edu.tr (F. Özkaynak).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.eij.2021.08.002
1110-8665/

Table 1
Comparison for s-box design approaches.

Design Approach	Advantages	Disadvantages
Mathematical methods	It can best meet design metrics.	There are various weaknesses in application attacks.
Optimization Algorithms	The optimization of s-box design criteria can be chosen as the objective function.	The computational cost required by the optimization algorithm is high.
Random Selection	It has a simple structure and produces fast results. It does not require complex mathematical transformations.	It does not provide the most appropriate design metrics that can be achieved.

random selection approach can be used to generate AES-like s-box structures. For example, chaos-based random selection designs are very popular approaches in this area. The focus of the study is to improve the nonlinearity value of s-box structures generated by random selection from an entropy source. It has been shown that nonlinearity measurement can be improved by applying the proposed post-processing technique.

The rest of the study is organized as follows. In the second section, the working logic of the proposed method is explained. In the third section, analysis results are given over three different scenarios. In the fourth section, a practical application of the obtained outputs is given. In the last section, the results are discussed and possible future studies are given.

2. Proposed method

The working logic of the proposed architecture is presented in Fig. 1. The method consists of two steps. These steps are the generation of s-box based on random selection and then mixing the positions of the s-box with the proposed approach.

In most general terms, s-box structure is a nonlinear function that maps an m-bit length input to an n-bit length output [19]. This nonlinear structure aims to prevent the success of differential attacks in cryptographic designs. The design technique proposed by Nyberg in the AES s-box is aimed to address differential attacks in the best way [20]. Another advantage of the AES s-box structure is that it has an effective software. Since many programming languages work based on bytes, AES s-box structures convert 8-bit length inputs into 8-bit length outputs. To make a fair comparison, therefore, AES-like s-box structures have been generated using a random entropy source in the first step of proposed method. Discrete-time chaotic systems, continuous-time chaotic systems, and classical rand() function can be used as the entropy source. By applying the mode 256 functions to the obtained outputs, random values are transformed between 0 and 255. Ref. [21] can be examined for details of this s-box generator program. As an example, generated s-box structure by using this program is shown in Table 2.

As stated before, the AES s-box structure is designed to be resistant to differential attacks. Since the highest value is calculated in the XOR distribution table, one of the s-box design criteria associated with the success of differential attacks, this value is desired to be as small as possible. Similarly, it is desired to be as high as possible in the nonlinearity criterion, which is another measurement used to show the complexity of the s-box structure. For the s-box designed by Nyberg [22], the XOR value is 4 and the nonlinearity value is 112. However, the deterministic nature of the mathematical method has begun to threaten the security of the encryption system as an open point for application attacks such as side-channel analysis [23]. Although random selection-based methods are more resistant to side-channel analysis [24], the most successful results obtained among studies so far have been calculated as 10 for the XOR value and 106.75 for the nonlinearity value. When these values are compared with the AES s-box, the problem becomes more obvious. This comparison is given in Table 3. One method that can be used for performance improvements of random selection-based designs is optimization algorithms. However, in these designs, the processing load due to optimization algorithms is also a disadvantage.

The method suggested in this study has a simpler and faster structure than optimization algorithms. The method aims to increase the value of the nonlinearity criterion without sacrificing simplicity and speed. To achieve this aim, it is proposed to mix row, column, and both s-box structures. It has recently been shown that performance metrics can be improved by changing the positions of s-box cells [25]. The post-processing technique suggested in this study is to be further improved through DES s-box structures. In the method suggested previously, a new s-box structure is generated from each original s-box structure with the post-processing technique. The advantage of this work over than

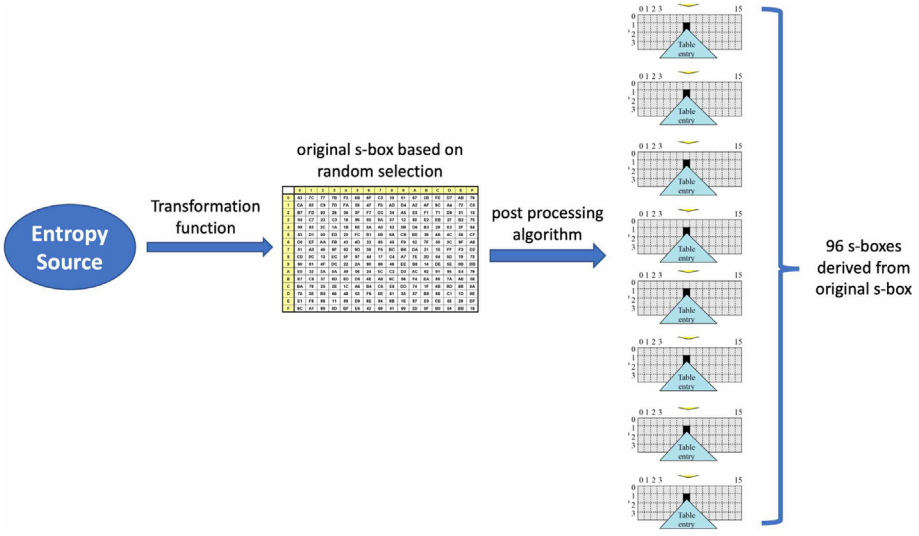

Fig. 1. General overview of proposed architecture.

Table 2
A sample s-box structure based on random selection.

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

Table 3
Performance comparison for AES and random selection s-box.

S-box	Nonlinearity			Bit Independence Criterion		Strict Avalanche Criterion			Maximum I/O XOR
	min	max	avg	Non.	SAC	avg	max	min	
AES s-box	112	112	112	112	0.5	0.5	0.5	0.5	4
Random selection [7]	106	108	106.75	103.2	0.4994	0.4971	0.6094	0.3909	10
s-box in Table 1	98	106	102.75	103.36	0.502	0.4978	0.5938	0.3906	12

previous is that 96 different s-box structures can be obtained from each original s-box. Because DES s-boxes consist of eight tables in 4*16 dimensions. Values between 0 and 15 in each row are mixed with DES s-box designs [5]. A total of 32 different mixing tables are given in Table 4.

For example, by using the first row of Table 4, the rows of the s-box structure given in Table 2 can be shuffled. To be able to express it more clearly, the operation of the method is shown in Fig. 2. Since the first value in the first row of Table 4 is 14, so row14 of the original table has been replaced as row0 in the derived new table. As a result of all these displacements, the new derived s-box structure in Table 5 has been generated.

3. Analysis results

There are five basic criteria for evaluating the success of an s-box structure. Among these criteria, the XOR distribution and nonlinearity criteria have been explained in the second section. Other criteria are known as bijective, SAC, and BIC criteria. For more details on these criteria, Ref. [6,19,22] can be examined. The s-box design criteria for derived 32 s-box structures obtained as a result of mixing the rows of the s-box structure in Table 2 according to the values in Table 4 are given in Table 6.

Similarly, the s-box design criteria for the newly derived 32 s-box structure obtained as a result of the replacement of the columns of the original s-box structure in Table 2 using the values in Table 4 are given in Table 7.

The analysis results for the 32 s-box structure obtained as a result of changing the positions of the rows first and then the columns are given in Table 8.

The values given in Tables 6, 7, and 8 are new s-boxes derived from the original s-box structure in Table 2. To evaluate the success of the proposed method more generally, one hundred random s-box structures have been generated, then 96 different s-boxes were produced from each table for three different approaches and the analysis results were tested. According to the test results, it has been observed that there is an increase of 81.25% of s-boxes in row-based mixing, 91.6% in column mixing, and 75% in row-column mixing according to the test results.

4. A practical application of the proposed method

Billions of digital content are transferred, processed, and stored every day from one point to another with the widespread use of 5G technology [26]. Ensuring the security of this valuable content has become increasingly important with the increasing demand. To meet this demand, many image encryption algorithms have been proposed in recent years [27–29]. In this section, a practical application is tried to be given by showing how the outputs can be used in an image encoding algorithm. However, designing an encryption algorithm is not an easy process [30–34]. It has been observed that many proposals can be easily broken without following specific design guidelines and carrying out comprehensive cryptanalysis. An improved version of the image encryption algorithm in Ref. [35] is proposed in this section. The image encryption algorithm is presented in Ref. [35] uses robust components of modern cryptology. In this way, the provable secure design approach has been used. By using the proposed s-box structures in this study, it has been shown that the keyspace of the encryption algorithm can be increased by using more than one s-box structure instead of just a single s-box structure. The flowchart detailing the operation of the improved image encryption algorithm is given in Fig. 3.

A sample test image and its encrypted version are given in Fig. 4.

Histogram analysis for the original and encrypted image is shown in Fig. 5.

Although all these statistical analyzes indicate that the proposed image encryption algorithm is working successfully, it is

Table 4
DES s-box structures.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
4	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
5	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
6	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
7	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
8	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
9	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
10	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
11	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
12	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
14	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
15	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
16	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
17	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
18	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
19	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
20	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
21	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
22	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
23	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
24	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
25	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
26	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
27	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
28	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
29	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
30	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
31	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

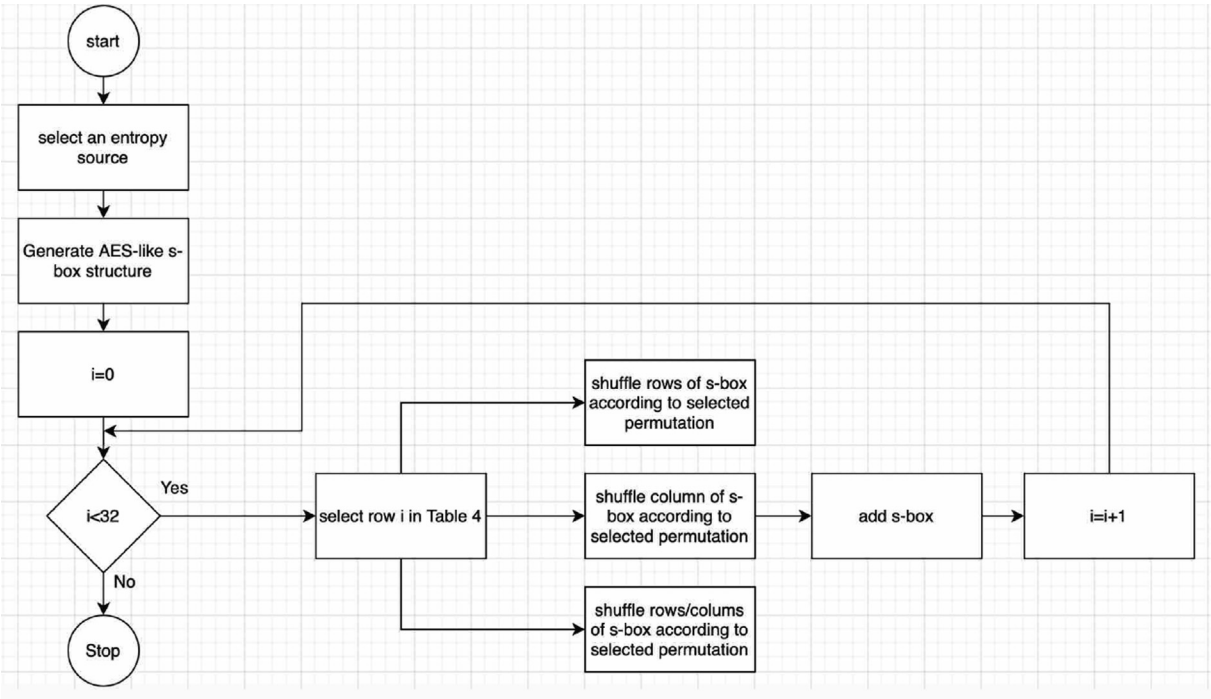

Fig. 2. Operation step of proposed method.

Table 5
New s-box structure derived from s-box in Table 2.

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

Table 6
Performance analysis of s-boxes derived from original s-box using row shuffling.

S-box	Nonlinearity			Bit Independence Criterion		Strict Avalanche Criterion			Maximum I/O XOR
	min	max	avg	Non.	SAC	avg	max	min	
1	100	108	104.75	103.71	0.5054	0.5037	0.625	0.3906	12
2	98	106	103.75	103.43	0.4987	0.501	0.5781	0.3906	12
3	98	108	103.75	103.71	0.5015	0.502	0.5781	0.3906	10
4	100	106	103.5	103.29	0.4994	0.5051	0.6094	0.3906	10
5	96	106	102.75	103.5	0.5002	0.5044	0.625	0.3906	12
6	100	106	103.75	103.79	0.5015	0.5042	0.5938	0.3906	12
7	96	106	101	103.29	0.5037	0.5049	0.5781	0.3906	10
8	98	108	104.75	103.07	0.5029	0.5056	0.6094	0.3594	10
9	102	108	104.25	104	0.4969	0.5024	0.6406	0.3906	12
10	100	106	103.75	104.21	0.4999	0.5002	0.5938	0.3906	10
11	100	108	103.75	103.79	0.4935	0.5029	0.5781	0.3594	10
12	100	106	103.25	103.57	0.5033	0.5042	0.625	0.3594	10
13	100	106	103.5	104.79	0.5004	0.4985	0.5781	0.3906	10
14	100	106	103.25	103.07	0.5001	0.5022	0.6094	0.375	12
15	100	106	103.25	103.07	0.5032	0.502	0.6094	0.3906	12
16	96	108	101.75	103.43	0.4978	0.5024	0.6094	0.3906	12
17	100	108	104.5	103.57	0.4981	0.5015	0.5938	0.3906	10
18	100	106	103	104.21	0.4999	0.5071	0.5938	0.3906	10
19	100	108	104	103.86	0.495	0.5017	0.5781	0.3906	10
20	104	108	106	103.71	0.502	0.5015	0.5938	0.3906	12
21	100	108	103.75	103.93	0.4969	0.5037	0.5781	0.3906	12
22	90	108	101.75	103.14	0.4986	0.5066	0.5938	0.3906	12
23	98	108	103.5	103.86	0.5001	0.501	0.5938	0.3906	12
24	94	108	103.25	103.36	0.5	0.5029	0.5781	0.3906	10
25	102	108	105.5	104.21	0.4964	0.5098	0.6094	0.3906	12
26	100	108	103	103	0.4958	0.5066	0.5938	0.3906	12
27	92	108	103.25	103.29	0.4985	0.5103	0.625	0.3906	12
28	98	108	102.5	102.71	0.5033	0.499	0.5781	0.3906	12
29	98	108	104.5	104.14	0.4978	0.5017	0.6094	0.3906	12
30	94	108	102.5	104.21	0.4987	0.5044	0.6094	0.3906	10
31	98	108	104	104.29	0.5024	0.501	0.5781	0.3906	10
32	102	106	103.5	103.71	0.501	0.5024	0.5781	0.3906	10

not sufficient in terms of a cryptology point of view [36,37]. For details on the provable security analysis of the algorithm, Ref. [35] can be viewed.

5. Conclusion

One of the main reasons behind the widespread use of electronic commerce is undoubtedly the provable security promise of cryptographic algorithms. However, advances in the cryptanalysis branch together with technological developments constantly threaten the security of modern encryption algorithms. Although modern encryption algorithms are mathematically secure, application attacks have revealed that various weaknesses may exist. One of the cryptographic components affected by the application attacks has been s-box structures. The demonstration that s-box structures generated based on

Table 7
Performance analysis of s-boxes derived from original s-box using column shuffling.

S-box	Nonlinearity			Bit Independence Criterion		Strict Avalanche Criterion			Maximum I/O XOR
	min	max	avg	Non.	SAC	avg	max	min	
1	100	106	103.75	103.5	0.5027	0.4998	0.625	0.4062	10
2	100	110	105.5	103.21	0.5013	0.4985	0.5938	0.4062	12
3	100	106	103.75	104.43	0.4988	0.5017	0.6094	0.4062	12
4	100	108	104.5	104.07	0.5	0.499	0.5938	0.4062	10
5	102	108	104.25	103.29	0.4979	0.5002	0.6094	0.4062	12
6	102	108	104.75	103.36	0.5056	0.5034	0.5938	0.4062	10
7	102	108	105.25	103.21	0.4982	0.499	0.5938	0.4062	10
8	98	108	103.5	103.86	0.4998	0.5017	0.5938	0.4062	12
9	102	108	104.75	103.5	0.4987	0.4976	0.5938	0.4062	12
10	102	108	104	102.79	0.4994	0.5012	0.5938	0.4062	10
11	100	108	104.25	103.86	0.4971	0.4966	0.5938	0.4062	10
12	98	108	104.5	103.43	0.4964	0.4993	0.6094	0.4062	12
13	98	106	103.5	103.29	0.4995	0.5027	0.5938	0.4062	12
14	102	110	104.5	102.93	0.4976	0.4944	0.5938	0.4062	12
15	102	110	104.5	102.93	0.504	0.4939	0.5938	0.4062	12
16	100	108	104.75	103.5	0.4996	0.501	0.5938	0.4062	10
17	98	106	102.75	103.5	0.5047	0.4978	0.5938	0.4062	10
18	100	108	104.5	103.64	0.5023	0.5015	0.5938	0.4062	10
19	96	106	103.5	103.5	0.4939	0.5037	0.5938	0.4062	12
20	100	106	104	103.57	0.4937	0.4998	0.6562	0.4062	10
21	96	106	103	102.43	0.4929	0.5002	0.5938	0.4062	10
22	102	106	103.5	102.93	0.5023	0.4954	0.5938	0.4062	12
23	98	110	102.75	104.36	0.4988	0.4995	0.5938	0.4062	10
24	102	106	105.25	103.21	0.499	0.4963	0.5938	0.4062	12
25	98	108	103.75	104	0.493	0.4998	0.5938	0.4062	10
26	100	108	104	103.86	0.5002	0.498	0.5938	0.3906	10
27	100	108	104.75	103.93	0.4956	0.5007	0.6094	0.4062	12
28	102	110	105.75	102.86	0.4986	0.5022	0.6094	0.4062	12
29	98	108	104.5	103.79	0.499	0.4983	0.5938	0.3594	10
30	100	106	102.5	103.43	0.5021	0.5032	0.5938	0.4062	14
31	98	108	103	104.21	0.4991	0.501	0.6094	0.4062	10
32	102	108	104.75	102.93	0.4987	0.5022	0.6094	0.4062	10

Table 8
Performance analysis of s-boxes derived from original s-box using row/column shuffling.

S-box	Nonlinearity			Bit Independence Criterion		Strict Avalanche Criterion			Maximum I/O XOR
	min	max	avg	Non.	SAC	avg	max	min	
1	98	110	103.5	103.36	0.5038	0.5056	0.625	0.4062	10
2	104	106	104.75	103.29	0.5052	0.5017	0.5781	0.3906	12
3	100	106	102.75	103.57	0.5029	0.5059	0.6094	0.4219	14
4	102	108	104.25	104	0.5022	0.5063	0.6094	0.4219	10
5	100	108	102	102.5	0.504	0.5068	0.625	0.4062	12
6	102	106	104	103.5	0.4991	0.5098	0.5938	0.4062	10
7	102	110	105	102.64	0.4978	0.5061	0.5781	0.4062	12
8	94	108	102.5	103.79	0.4971	0.5095	0.6094	0.3594	10
9	94	106	101.75	103.71	0.5032	0.5022	0.6406	0.4062	12
10	100	108	105.5	103.36	0.4976	0.5037	0.5938	0.3906	12
11	96	106	102	103.29	0.491	0.5017	0.5781	0.3594	12
12	98	106	103.5	103.57	0.5023	0.5056	0.625	0.3594	12
13	102	108	104.5	103.57	0.5033	0.5034	0.5781	0.4062	12
14	102	108	104.75	103.43	0.499	0.4988	0.6094	0.375	12
15	102	108	104.75	103.43	0.5024	0.498	0.6094	0.4062	12
16	100	108	104.25	103.64	0.4985	0.5056	0.6094	0.4219	12
17	98	106	102.75	104.43	0.501	0.5015	0.5938	0.3906	12
18	100	108	104.5	103.86	0.5061	0.5107	0.5938	0.3906	12
19	98	108	103.5	103.29	0.5043	0.5076	0.5938	0.4219	12
20	94	106	103	103.36	0.502	0.5034	0.6562	0.4219	10
21	98	106	102.5	103.5	0.4992	0.5061	0.5781	0.4375	12
22	98	106	102.75	103.93	0.4943	0.5042	0.5938	0.4062	12
23	100	108	104.25	104.71	0.5031	0.5027	0.5938	0.3906	12
24	102	108	104.25	103.64	0.4983	0.5015	0.5625	0.4062	12
25	94	106	101.75	103.5	0.4992	0.5117	0.6094	0.4219	10
26	100	106	104	103.5	0.5005	0.5068	0.5938	0.3906	10
27	96	106	103.75	103.5	0.5001	0.5132	0.625	0.4219	12
28	100	108	103.25	101.64	0.5022	0.5034	0.6094	0.4219	12
29	100	108	104	103	0.501	0.5022	0.6094	0.3594	12
30	100	108	103.25	103.21	0.5023	0.5098	0.6094	0.4062	16
31	100	106	103.5	103.86	0.5022	0.5042	0.6094	0.4219	12
32	102	106	104.5	103.86	0.5021	0.5068	0.6094	0.4219	12

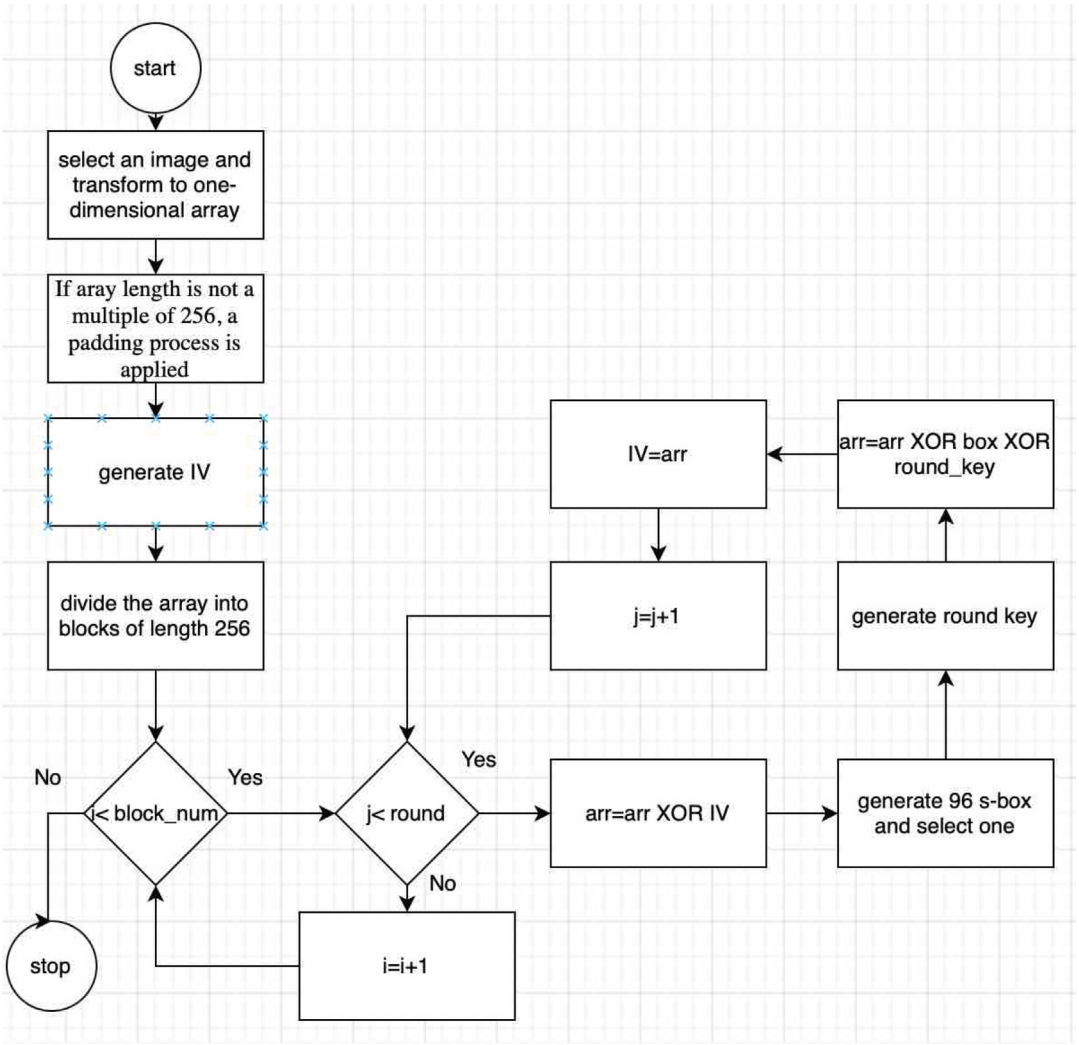

Fig. 3. Improvement version of image encryption algorithm.

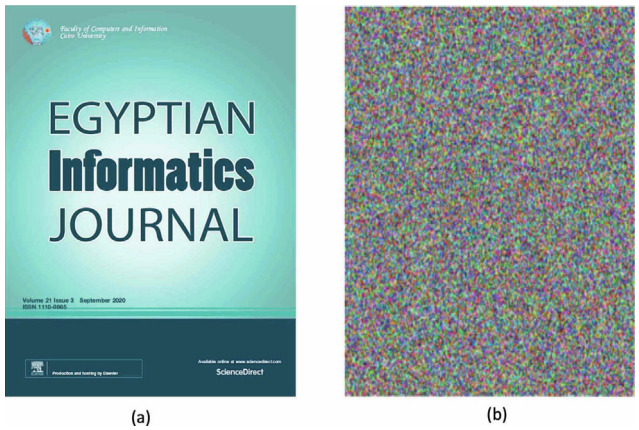

Fig. 4. Outputs of improvement image encryption algorithm.

mathematical techniques are more vulnerable to side-channel attacks compared to random selection-based designs, brings to mind the question of how the design criteria of s-box structures generated based on random selection can be improved. In this study, a method that serves this purpose is proposed.

It has been observed that the proposed method provides significant performance improvements in s-box structures with below-average performance characteristics. It has been shown that derived s-box structures can be obtained from the original s-box structure for three different scenarios. It has been observed that design criteria can be improved by 81.25% in row transformations, 91.6% in column transformations, and 75% in row-column transformations. Considering these results, mixing the columns has been particularly effective. These results indicate that the success of random selection-based approaches can be further improved by using different techniques and methods in future studies.

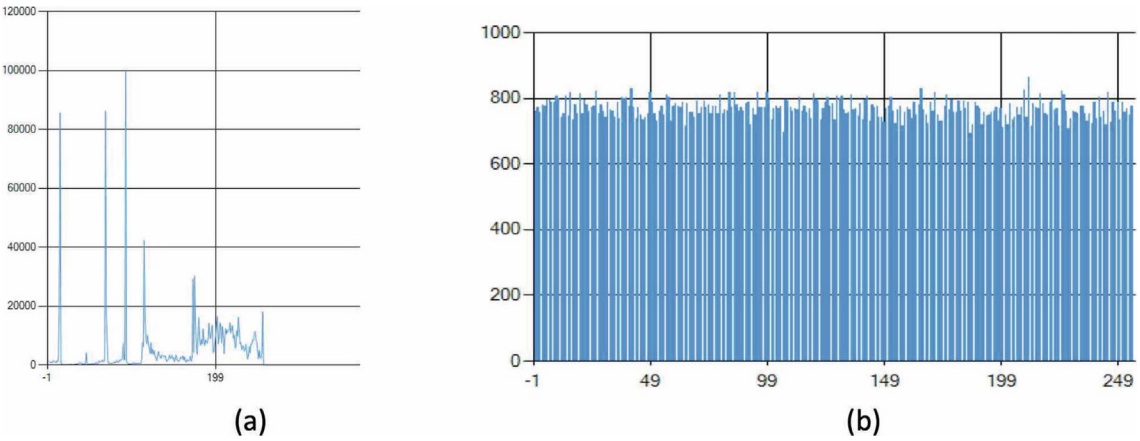

Fig. 5. Histogram analysis of images in Fig. 4.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This study was supported in part by the Firat University Scientific Research Project under Grant TEKF.20.21.

References

[1] Keshta I, Odeh A. Security and privacy of electronic health records: concerns and challenges. Egypt Inform J 2021;22(2):177–83.
[2] Elshabka MA, Hassan HA, Sheta WM, Harb HM. Security-aware dynamic VM consolidation. Egypt Inform J 2021;22(2):277–84.
[3] B. Soewito, Y. Marcellinus, IoT security system with modified Zero Knowledge Proof algorithm for authentication, Egyptian Informatics Journal, 2021;22 (3):269–276.
[4] C. Paar, J. Pelzl, Understanding cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. 10.1007/978-3-642-04101-3.
[5] L. R. Knudsen, M. Robshaw, The block cipher companion, 2011, Springer.
[6] Cusick T, Stanica P. Cryptographic boolean functions and applications. Amsterdam, The Netherlands: Elsevier; 2009.
[7] Özkaynak F. Construction of robust substitution boxes based on chaotic systems. Neural Comput & Applic 2019;31:3317–26. doi: https://doi.org/10.1007/s00521-017-3287-y.
[8] Hematpour N, Ahadpour S. 'Execution examination of chaotic S- box dependent on improved PSO algorithm. Neural Comput Appl. Aug. 2020. doi: https://doi.org/10.1007/s00521-020-05304-9.
[9] Ahmad M, Khaja IA, Baz A, Alhakami H, Alhakami W. Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications. IEEE Access 2020;8:116132–47. doi: https://doi.org/10.1109/ACCESS.2020.3004449.
[10] Tanyildizi E, Ozkaynak F. A new chaotic S-Box generation method using parameter optimization of one dimensional chaotic maps. IEEE Access 2019;7:117829–38. doi: https://doi.org/10.1109/ACCESS.2019.2936447.
[11] Ahmad M, Al-Solami E, Alghamdi AM, Yousaf MA. Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures. IEEE Access 2020;8:110397–411. doi: https://doi.org/10.1109/ACCESS.2020.3001868.
[12] M.Ş. Açıkkapı, F. Özkaynak, A method to determine the most suitable initial conditions of chaotic map in statistical randomness applications in IEEE Access, 10.1109/ACCESS.2020.3046470.
[13] Gao W, Idrees B, Zafar S, Rashid T. 'Construction of nonlinear component of block cipher by action of modular group PSL(2, Z) on projective line PL(GF (28))'. IEEE Access 2020;8:136736–49. doi: https://doi.org/10.1109/ACCESS.2020.3010615.
[14] Razaq A, Ullah A, Alolaiyan H, Yousaf A. 'A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers. Wireless Pers Commun. Oct. 2020. doi: https://doi.org/10.1007/s11277-020-07841-x.
[15] Ahmad M, Al-Solami E. Evolving dynamic S-boxes using fractional-order hopfield neural network based scheme. Entropy Jun. 2020;22(7):717.
[16] Mahmood Malik MS, Ali MA, Khan MA, Ehatisham-Ul-Haq M, Shah SNM, Rehman M, Ahmad W. Generation of highly non- linear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. IEEE Access 2020;8:35682–95. doi: https://doi.org/10.1109/ACCESS.2020.2973679.
[17] Siddiqui N, Khalid H, Murtaza F, Ehatisham-Ul-Haq M, Azam MA. A novel algebraic technique for design of computational substitution-boxes using action of matrices on Galois field. IEEE Access 2020;8:197630–43. doi: https://doi.org/10.1109/ACCESS.2020.3034832.
[18] N. Siddiqui, F. Yousaf, F. Murtaza, M. Ehatisham-Ul-Haq, M.U. Ashraf, A.M. Alghamdi, A.S. Alfakeeh, 'A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field,' PLoS ONE, vol. 15, no. 11, Nov. 2020, Art. no. e0241890, 10.1371/journal.pone.0241890.
[19] Wu C, Feng D. Boolean functions and their applications in cryptography. Berlin, Germany: Springer; 2016.
[20] Daemen J, Rijmen V. The design of rijndael the advanced encryption standard (AES). Springer; 2020.
[21] F.Ozkaynak, An analysis and generation toolboxfor chaotic substitution boxes: A case study based on chaotic labyrinth rene thomas system, Iranian J. Sci. Technol., Trans. Electr. Eng., vol. 44, no. 1, pp. 89–98, Mar. 2020, 10.1007/s40998-019-00230-6.
[22] K. Nyberg, Differentially uniform mappings for cryptography, inProc. Eurocrypt, in Lecture Notes in Computer Science, vol. 765. Berlin, Germany: Springer, 1994, pp. 55–64.
[23] S.B. Ors, B. Preneel, I. Verbauwhede, Side-channel analysis attacks on hardware implementations of cryptographic algorithms, in Wireless Security and Cryptography-Specifications and Implementations. Boca Raton, FL, USA: CRC Press, 2007.
[24] Acikkapi MS, Ozkaynak F, Ozer AB. 'Side-channel analysis of chaos-based substitution box structures'. IEEE Access 2019;7:79030–43. doi: https://doi.org/10.1109/ACCESS.2019.2921708.
[25] F. Artuğer, F. Ozkaynak, A novel method for performance improvement of chaos-based substitution boxes, Symmetry, vol. 12, no. 4, p. 571, Apr. 2020.
[26] Shareef FR. A novel crypto technique based ciphertext shifting. Egypt Inform J 2020;21(2):83–90. doi: https://doi.org/10.1016/j.eij.2019.11.002.
[27] Ge M, Ye R. A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties. Egypt Inform J 2019;20(1):45–54. doi: https://doi.org/10.1016/j.eij.2018.10.001.
[28] Abdul N, Abbas M. Image encryption based on independent component analysis and Arnold's cat map. Egypt Inform J 2016;17(1):139–46. doi: https://doi.org/10.1016/j.eij.2015.10.001.
[29] Khan JS, Boulila W, Ahmad J, Rubaiee S, Rehman AU, Alroobaea R, Buchanan WJ. DNA and plaintext dependent chaotic visual selective image encryption. IEEE Access 2020;8:159732–44. doi: https://doi.org/10.1109/ACCESS.2020.3020917.
[30] Muhammad ZMZ, Özkaynak F. Security problems of chaotic image encryption algorithms based on cryptanalysis driven design technique. IEEE Access 2019;7:99945–53. doi: https://doi.org/10.1109/ACCESS.2019.2930606.
[31] C. Li, When an attacker meets a cipher-image in 2018: A year in review, 2019, arXiv:1903.11764. [Online]. Available: https://arxiv. org/abs/1903.11764.
[32] Xie EY, Li C, Yu S, Lü J. On the cryptanalysis of Fridrich's chaotic image encryption scheme. Signal Process. Mar. 2017;132:150–4.

[33] Zhang LY, Liu Y, Pareschi F, Zhang Y, Wong K-W, Rovatti R, Setti G. On the security of a class of diffusion mechanisms for image encryption. IEEE Trans. Cybern. Apr. 2018;48(4):1163–75.
[34] W. Feng, Y.-G. He, 'Cryptanalysis and improvement of the hyper- chaotic image encryption scheme based on DNA encoding and scram- bling, IEEE Photon. J., vol. 10, no. 6, Dec. 2018, Art. no. 7909215. 10.1109/JPHOT.2018.2880590.
[35] Muhammad ZMZ, Ozkaynak F. An image encryption algo- rithm based on chaotic selection of robust cryptographic primitives. IEEE Access 2020;8:56581–9. doi: https://doi.org/10.1109/ACCESS. 2020.2982827.
[36] Wu Y, Noonan JP, Agaian S. NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology. J Selected Areas Telecommunications (JSAT) 2011:31–8.
[37] F. Özkaynak, Role of NPCR and UACI tests in security problems of chaos based image encryption algorithms and possible solution proposals, 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, 2017, pp. 621-624, 10.1109/UBMK.2017.8093481.