



Innovative image encryption approach based on bitwise XOR high nonlinear S-boxes and random permutation

Firat Artuğer¹

Accepted: 26 January 2025 / Published online: 28 April 2025
© The Author(s) 2025

Abstract

With today's developing technologies, the need for new image encryption algorithms to encrypt images is inevitable. In this study, an innovative image encryption algorithm is proposed. The proposed algorithm first XORs each layer of the image with a unique and strong new key. Each layer is then subjected to a random permutation process. Each of the encrypted layers obtained here is finally passed through a new s-box structure with a high nonlinearity value. After these processes, all layers are combined to obtain an encrypted image. Thus, XOR and s-box confusion meet the criteria, while random permutation meets the diffusion criteria. In this study, both key and s-box structures were originally obtained with a chaotic Gaussian map. The outputs of the chaotic map were converted into bit sequences and five different sequences with a length of 1 million were obtained. All these arrays have successfully passed all NIST SP 800-22 tests. On the other hand, the proposed s-box structures surpassed many studies with nonlinearity values of 108, 108.5, and 108.75. The images were successfully encrypted with the proposed algorithm, and the encrypted images successfully completed tests such as NPCR-UACI, information entropy, histogram analysis, and correlation analysis. It is thought that this study will make many contributions to the fields of s-box development, random number generation, and image encryption.

Keywords Security · Image encryption · Bitwise XOR · S-box · Random permutation

1 Introduction

With the rapid advancement of technology, the number of images is increasing day by day. As new structures emerge, such as the way images are obtained, their formats, and sizes, the processing of these images becomes more complex. At this point, new image encryption algorithms are needed to ensure the security of these images (Gao et al. 2022a; Muhammad and Özkaynak 2021). Because we live in the information age, people use data all the time. Many security problems occur during this use. In recent years, the use of images has become widespread, especially on the internet. For images to be transmitted securely over insecure networks, they must be encrypted with a strong algorithm (Artuğer and Özkaynak 2021). Especially with the rapid development of chaotic dynamics, progress in this

field has accelerated. Because chaotic dynamics are one of the indispensable building blocks of the cryptography field due to their randomness. Encryption philosophies are generally examined under two headings. These are symmetric and asymmetric algorithms. Asymmetric encryption algorithms are not generally used in the encryption process because they are inherently slow. They are mostly used for key exchange. Symmetric encryption algorithms are the philosophy often used for encryption. This philosophy is divided into two. These are stream and block ciphers. In stream encryption, bits are encrypted one by one. Therefore, it is difficult to implement in some cases. Especially as the data increases, its application becomes more difficult. Because it is necessary to generate a key as long as the data size. The other and most used structure for encryption is the block encryption philosophy. These algorithms divide the data into blocks and encrypt each block within itself. Then, these encrypted blocks are combined to obtain encrypted data. Many block cipher algorithms have been developed from the past to the present. The most well-known of these and today's data encryption standard is the

✉ Firat Artuğer
firatartuger@munzur.edu.tr

¹ Department of Computer Engineering, Munzur University, 62200 Tunceli, Turkey

AES (Daemen and Rijmen 1998) algorithm. AES is a secure algorithm with a very flexible structure. However, new algorithms are also needed for various applications.

Image encryption is a very popular topic. Two criteria must be met in the encryption process. The first of these is the process called diffusion. Diffusion means that data must be spread effectively. In this way, the attackers' job will become even more difficult. In encryption algorithms, this criterion is usually met by permutation operations. In this study, this process is achieved by randomly obtained permutations. The other and most important criterion is the criterion called confusion. This criterion must be met in an encryption algorithm. Confusion means that data must be mixed effectively. The more effectively data is scrambled, the harder it will be for attackers to decipher. That's why the confusion criterion is vital in an encryption algorithm. When looking at the literature, XOR operation and s-box structures are generally used in the confusion process. The XOR process has a perfect structure for the mixing process, as 50% of the results are 1 and 50% are 0. In this way, it is a structure that makes it very difficult for attackers to make inferences. XOR operation was also used in this study. Another confusion tool is s-box structures, and this structure is generally used. Since S-box is a non-linear transformation, it converts the data into another format. That is, the strength of encryption algorithms generally depends on the strength of the s-box structure. Developing an S-box is a very popular topic today. However, developing strong s-box structures is a very difficult problem. From past to present, to develop strong s-box structures to be used in encryption algorithms, chaos (Lambić 2020; Artuğer and Özkaynak 2020, 2023a; Belazi and Abd El-Latif 2017; Khan et al. 2012, 2013; Alshekly et al. 2022; Ye and Zhimao 2018; Liu 2017; Özkaynak 2020), mathematical transformations (Hussain 2020; Razaq et al. 2022, 2021; Siddiqui et al. 2020; Anees and Chen 2020; Ahmad and Al-Solami 2020a; Khan and Shah 2014; Arshad et al. 2022; Malik et al. 2020), optimization techniques (Behera and Gangopadhyay 2023; Artuğer and Özkaynak 2022, 2023b; Wang et al. 2012, 2020; Zamli 2021; Zamli et al. 2021, 2023; Kuznetsov et al. 2023; Khan et al. 2021, 2023; Artuğer 2023a; Alhadawi et al. 2020, 2021; Ahmad and Al-Solami 2020b; Ahmad et al. 2015, 2020; Hematpour and Ahadpour 2021; Alzaidi et al. 2018; Ahmed et al. 2019; Chen 2008; Farah et al. 2017; Tian and Lu 2017), cellular automata (Szaban and Seredynski 2008; Alexan et al. 2022; Gangadari and Ahamed 2018; Aboites-González et al. 2018; Haque et al. 2022; Mariot et al. 2019), DNA-RNA chains. Many algorithms have been developed, especially (Artuğer 2023b; Al-Wattar et al. 2015a, b; Basha et al. 2022; Kadhim et al. 2016; Farhan et al. 2020; Mohamed et al. 2021). In this study, three different strong chaos-

based s-box structures were used in the confusion process. These s-box structures were obtained uniquely.

Especially in recent years, many image encryption algorithms have been developed. Some of these are briefly mentioned here. Gao et al. They propose a fast image encryption algorithm using propagation, a chaotic system, and shuffling (Gao et al. 2022a). Elkandoz et al. They first shuffled the pixels of the image to meet the mixing and spreading criteria. Then, they effectively encrypted the image by XORing the key value with this mixed data (Elkandoz and Alexan 2022). Alexan et al. They proposed a new image encryption scheme based on the fusion of multiple chaotic maps. The key value was also obtained with the chaotic map (Alexan et al. 2023a). Lai et al. They first proposed a new chaotic map for effective encryption of images. They claimed that this map gave better results compared to other maps. In the proposed encryption method, pixels are based on the philosophy of spreading randomly. As a result, it was observed because of the analysis that the study worked effectively (Lai et al. 2023). Chai et al. They presented a hybrid approach by using the Hessenberg decomposition-block compression detection-particle swarm optimization algorithm together to develop an effective image encryption scheme. As a result of the analysis, it was shown that the algorithm works effectively (Chai et al. 2022). Gao et al. They developed a new image encryption mechanism using a three-dimensional cube and a hyperchaotic map. Later, they made the algorithm more effective by using the DNA coding structure. Analysis has shown that this algorithm is safe (Gao et al. 2022b). Erkan et al. To develop a powerful image encryption algorithm, they first developed a new two-dimensional hyperchaotic map. Analyzes have shown that this map has strong random properties and can be used for image encryption (Erkan et al. 2023). Muhammad et al. They developed a hybrid scheme for image encryption by using optimization algorithms, chaotic systems, and PUF structures together. Effective results were obtained by using these structures together (Muhammad and Özkaynak 2021). Alexan et al. They developed a new image encryption scheme based on hyperchaotic maps and a neuron model. In this study, XOR operation was also performed with key structures, and each stage was passed through the s-box structure (Alexan et al. 2023b). Gupta et al. They worked on a new image encryption algorithm that combines encryption methods and watermarking technique. This proposed method uses DWT-based watermarking, chaotic map, and crossover operations. With this study, images were effectively encrypted (Gupta et al. 2023). Zhu et al. They developed a new chaotic image encryption scheme using DNA coding and a fish shoal optimization algorithm, specifically to prevent differential attacks. Additionally, large keys were used in this study. This has made the algorithm more

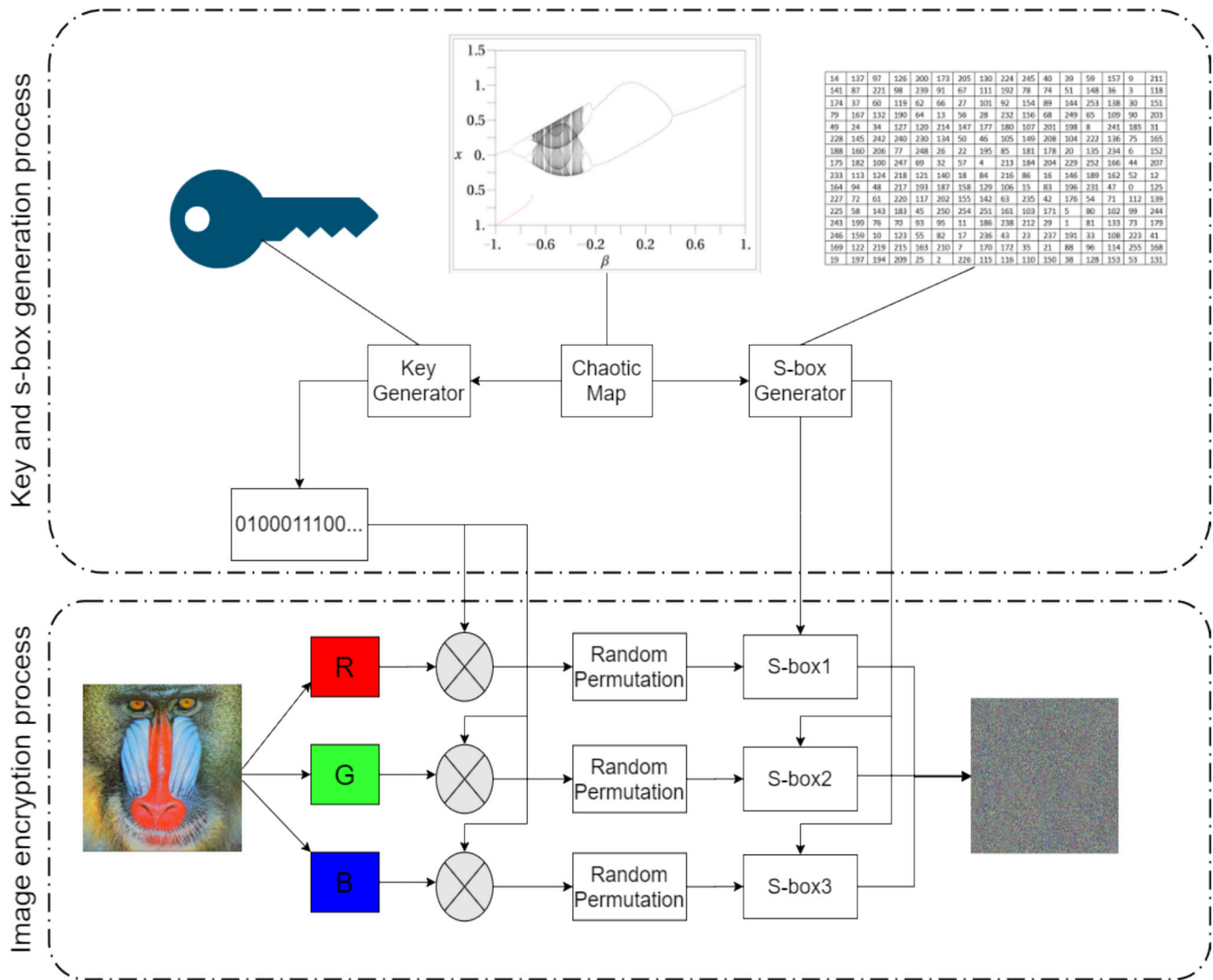


Fig. 1 System model of the proposed image encryption algorithm

powerful, especially against differential attacks (Zhu et al. 2023). Huang et al. To develop a more effective image encryption structure, they used a different approach and hid the image to be encrypted within another image (Huang et al. 2023a). Masood et al. proposed a new image encryption scheme using chaos-based strong s-box and DNA coding together (Masood et al. 2021). Luo et al. proposed a new image encryption scheme using hyper-chaotic system and particle swarm optimization (PSO) (Luo et al. 2022). Huang et al. developed a new image encryption scheme with discrete wavelet transform and compressed sensing techniques (Huang et al. 2023b). Wang et al. They developed a new image encryption algorithm using chaos, XOR, and Josephus problem (Wang et al. 2023).

The proposed algorithm makes many contributions to the literature compared to the existing works mentioned above. A new image encryption approach is proposed by

using various cryptographic units together. The strong s-box structures used in this encryption algorithm are obtained uniquely. The 3 different s-box structures used here make the algorithm much more complex and powerful. With the s-box generation approach proposed in this study, more s-box structures can be generated and used in different encryption algorithms. This is one of the aspects that distinguish this work from other works. On the other hand, this study also presents a unique method for obtaining the key values to be used in the XOR operation. Thanks to this method, a different random bit sequence is used as a key for each layer of an image. This makes the encryption algorithm stronger. In addition, with the key generator method proposed here, keys can be easily generated for other encryption algorithms. Because the method used here has a very effective and simple structure. It is observed that the bit sequences obtained because of the analyses proved this by passing the NIST tests. It is shown

Table 1 Proposed key generator algorithm

```

KeyGeneration()
begin
  for i in range(0,n):
     $a = 7.43551515115$ 
     $\beta = 0.14516166512$ 
     $y = \text{random.random}()$ 
     $y = (\text{math.exp}(-a * y * y) + \beta)$ 
     $\text{random\_number} = (\text{int})(10000000000 * y) \% 256$ 
  end for
end

```

that images can be encrypted effectively by using this s-box and key generation approaches together. Thus, significant contributions have been made to image encryption, s-box generation, and random number generator literature. Considering this point, it is hoped that this study will inspire researchers to combine different cryptographic structures and use them in different ways. In the remainder of the study, the image encryption approach proposed in the second chapter is given together with the system model and pseudocodes. In the third chapter, the key generator was first analyzed with NIST testing under subheadings to better understand the chapter. Subsequently, the proposed s-box structures were evaluated according to the most used s-box evaluation criteria in the literature and the results were compared with other studies. Finally, in this section, images encrypted with the proposed algorithm are analyzed in detail. In the fourth section, the results are discussed.

2 Proposed image encryption algorithm

The proposed image encryption algorithm is based on a strong key, XOR, random permutations, and strong s-box structures. First of all, a color image is separated into layers of red, green, and blue. These pixel values are then converted into an array. Each of these layers is XORed separately with the key value. The XOR operation is one of the structures that meet an important requirement called confusion in encryption algorithms. In addition, encryption and decryption operations are quite simple with the XOR operation. After the layers are XORed with the key, they are individually subjected to a random permutation process. The purpose of the permutation here is to meet the requirement called diffusion. In encryption algorithms, this process is usually carried out by permutation operations. After the permutation process, each layer is passed through

Table 2 Proposed s-box generator algorithm

```

SboxGeneration()
begin
 $a = 7.43551515115$ 
 $c = 0.14516166512$ 
  Sbox = []
  i = 0
  while (i < 256)
     $y = \text{random.random}()$ 
     $y = (\text{math.exp}(-a * y * y) + c)$ 
     $\text{random\_number} = (\text{int})(10000000000 * y) \% 256$ 
    if ( !include (Sbox, random_number) )
      Sbox[i] = random_number
      i++
    end if
  end while
  SboxNew = []
  LastNon = Nonlinearity value of Sbox
  j = 0
  while (i < max_iteration)
    first = First location selected with Gauss map
    second = Second location selected with Gaussian map
    Exchange (Sbox[first], Sbox[second])
    NewNon = Nonlinearity value of SboxNew
    if (NewNon > LastNon)
      update Sbox
    end if
    else
      Sbox = SboxNew
    end else
    j++
  end while
end

```

a separate s-box structure. The aim here is to mix the data thoroughly and increase confusion. So, s-box is another important component that provides confusion like the XOR operation. A highly nonlinear s-box structure makes the algorithm extremely powerful. In the proposed algorithm, passing each layer through a different s-box structure is also one of the unique aspects of the study. In this way, a more effective confusion process is achieved. After the layers are passed through the s-box structures, the layers are combined, and the encrypted image is obtained. The basic system model of the proposed algorithm is given in Fig. 1. Decrypting the image in the proposed algorithm is quite simple. The password can be easily decrypted when the steps are applied in reverse. The layers of the encrypted image are passed through inverted s-box structures respectively. Each layer is then put into the inverse permutation process. Finally, when the decoded layers are XORed with the key value and the layers are combined, the original image is obtained.

Table 3 NIST SP 800-22 test results of bit sequences obtained with the proposed generator algorithm

No	Test	Sequence-1	Sequence -2	Sequence -3	Sequence -4	Sequence -5
		p-value	p-value	p-value	p-value	p-value
1	Frequency Test (Monobit)	0. 24686	0. 65126	0. 55787	0. 85244	0. 71287
2	Frequency Test within a Block	0. 37012	0. 05774	0. 57872	0. 35480	0. 27592
3	Run Test	0. 70791	0. 73099	0. 05827	0. 16575	0. 97777
4	Longest Run of Ones in a Block	0. 48223	0. 64009	0. 38959	0. 50462	0. 55772
5	Binary Matrix Rank Test	0. 67139	0. 71240	0. 88466	0. 83327	0. 78242
6	Discrete Fourier Transform (Spectral) Test	0. 46286	0. 04162	0. 60092	0. 09489	0. 01580
7	Non-Overlapping Template Matching Test	0. 56527	0. 68612	0. 15440	0. 97943	0. 47391
8	Overlapping Template Matching Test	0. 26842	0. 89019	0. 94393	0. 14960	0. 93587
9	Maurer's Universal Statistical test	0. 34688	0. 47593	0. 68097	0. 64742	0. 06277
10	Linear Complexity Test	0. 55937	0. 26910	0. 27563	0. 93186	0. 31309
11	Serial test	0. 93152	0. 97817	0. 67232	0. 68900	0. 19029
12	Approximate Entropy Test	0. 92781	0. 21694	0. 10701	0. 89706	0. 58955
13	Cumulative Sums (Forward) Test	0. 13690	0. 75798	0. 84704	0. 99370	0. 66150
14	Cumulative Sums (Reverse) Test	0. 31059	0. 87979	0. 41646	0. 94367	0. 71392
15	Random Excursions Test(state:+4)	0. 88341	0. 65654	0. 40062	0. 85609	0. 36823

One of the most important points of this study is that both the key value and the s-box structures are obtained in a unique way using a chaotic map. For this purpose, the Gauss map was used in this study. Different maps can also be used. This is one of the rich points of the study. The mathematical structure of the Gauss map is given in Eq. (1).

$$x_{n+1} = \exp(-ax_n^2) + \beta, a \in [4.7, 17], \beta \in [-1, 1] \quad (1)$$

A very simple and fast generator algorithm has been designed for the key generator. This generator can also be used as a random number generator in different applications. The pseudocode of the proposed generator algorithm is given in Table 1. In this algorithm, first, the initial parameters of the chaotic map are defined by the system. The values taken here were chosen randomly in the ranges where the chaotic map shows random features. It is thought that more effective results can be obtained if these values are selected with methods such as optimization in future studies. After the input parameters are defined, a random number is generated, and the chaotic map is initialized with this value. Since the images were encrypted in this study, key values were generated up to the maximum value that the pixel values could take. Therefore, the value obtained from the output of the chaotic map was first converted to an integer by multiplying it by a large number. Then, the mod256 operation was applied to the obtained value and the key value was obtained with random numbers in the range [0–256]. In this way, random number sequences of desired lengths can be generated according to the value of

n. In addition, since there is no seed value in the proposed generator algorithm, a different sequence will be obtained each time it runs. In this way, it will be difficult to reproduce the series. Thus, the proposed generator is an algorithm that can be used in cryptographic applications.

S-box structures were also obtained with a similar philosophy. The pseudocode of the proposed s-box generator algorithm is given in Table 2. The s-box structures to be used here are similar to the s-box structures used in the AES algorithm. In other words, it contains 8-bit long values. Therefore, they consist of 256 values in the range [0–256]. In the proposed algorithm, the initial parameters of the chaotic map are defined as in the key generator. In this study, the initial values used to produce s-box were also chosen randomly. Selecting and analyzing the values here using different methods is one of the future studies. Choosing these initial values optimally is a hot topic that will whet the appetite of researchers. After the initial values are given, the chaotic map is initialized with a random value. When the next value is produced, this value must be multiplied by a larger number to turn it into an integer. Then, mod256 operation is applied to ensure that these values are in the [0–256] range. If this obtained value is not available in the s-box, this value is added. If this value exists in the table, it is not added, and this process continues until the table is full. In this way, a starting s-box can be easily obtained. However, the s-box structures obtained in this way show bad cryptographic properties. To improve these features, in the proposed algorithm, two values are selected with a chaotic map, and the places of these values

Table 4 Proposed s-box1

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

Table 5 Proposed s-box2

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

are changed. If the nonlinearity value increases, the s-box is updated. In this way, the s-box can easily become cryptographically stronger. Here, the elements to be displaced are selected with a chaotic Gauss map. There are quite a few chaotic maps available here. The effects of other maps on the study are also one of the issues that need to be investigated for future studies.

3 Analysis results

In this study, the analysis results were examined separately in three subsections for a better understanding. In the first part, the key generator, in the second part, the s-box, and in the third part, the image encryption analysis results are given in detail.

3.1 Key generator analysis

In this study, the NIST SP 800-22 test suite was used to test whether the proposed key generator algorithm truly generates random numbers. This package consists of 15 tests in total. A p value is calculated in each of these tests. This p value is expected to be in the range [0.01–1]. As this value approaches 1, it means that the quality of the random number generator increases. For NIST SP 800-22 testing, bit sequences of approximately 1 million bits are generally used in the literature. In this study, 5 different random bit strings with a length of 1 million bits were obtained and tested. These test results are given in Table 3. As can be seen in this table, all bit sequences produced have successfully completed all test results.

Table 6 Proposed s-box3

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

Table 7 Performance comparison of proposed s-box structures with other methods

S-BOX	BIC		XOR	SAC	Avg. non
	Non	SAC			
S-box1	102.29	0.4963	10	0.5032	108
S-box2	103.36	0.4997	10	0.5046	108.5
S-box3	103.71	0.501	12	0.5095	108.75
Arshad et al. (2022)	107	–	6	0.501	107.25
Ye and Zhimao (2018)	103.5	0.504	10	0.4976	106.7
Belazi and Abd El-Latif (2017)	104.3	0.4988	12	0.5010	105.5
Lambić (2020)	100	0.5288	10	0.501	106.2
Özkaynak (2020)	103.3	0.4972	10	0.5034	104.7
Alhadawi et al. (2020)	104.6	0.4974	10	0.496	107
Khan and Shah (2014)	105.7	0.4994	32	0.4926	105.5
Tian and Lu (2017)	103.7	0.5025	10	0.5093	107.5
Alhadawi et al. (2021)	103.85	0.5011	10	0.4995	108.5
Ahmed et al. (2019)	104.3	0.5001	10	0.4944	107.5
Wang et al. (2012)	90	0.4950	10	0.5068	108
Chen (2008)	103.2	0.4971	10	0.4980	104
Farah et al. (2017)	105.2	0.4984	10	0.5120	106.5
Ahmad et al. (2015)	105.5	0.5010	10	0.5015	107
Hematpour and Ahadpour (2021)	105.85	0.4995	10	0.5036	106.5

The average nonlinearity values are given in bold

Table 8 Entropy and NPCR-UACI values of encrypted images

Test image	Information entropy value			NPCR	UACI
	R	G	B		
Lenna (512 × 512)	7.99857	7.99871	7.99661	0.99615	0.30402
Baboon (512 × 512)	7.99833	7.99765	7.99884	0.99611	0.29756
Barbara (256 × 256)	7.99646	7.99608	7.99706	0.99600	0.29855
Pepper (256 × 256)	7.99595	7.99639	7.99670	0.99605	0.32027

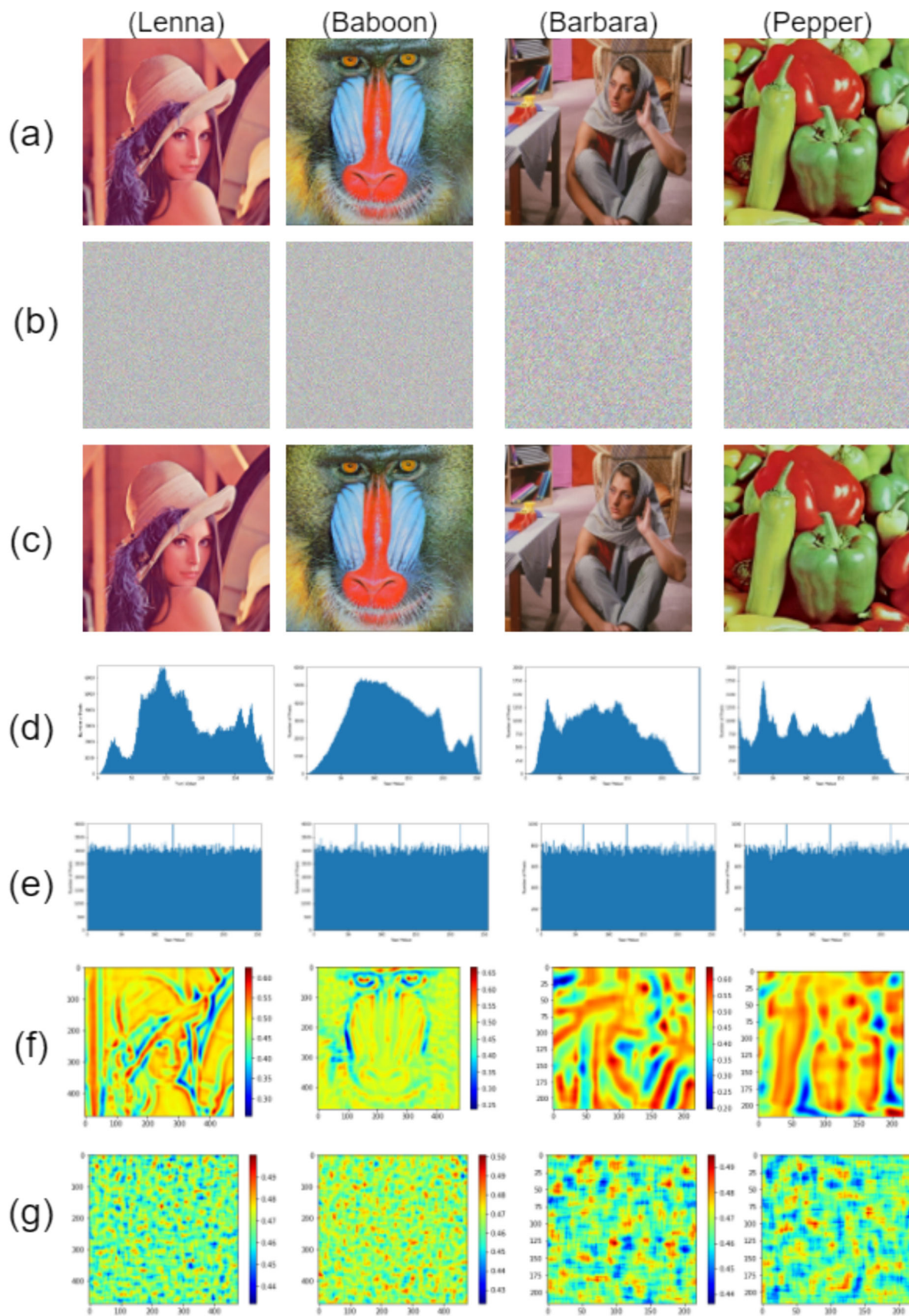


Fig. 2 Analysis results of test images (**a** original images, **b** encrypted images, **c** decrypted images, **d** histogram graphs of original images, **e** histogram graphs of encrypted images, **f** correlation graphs of original images, **g** correlation graphs of encrypted images graphics)

3.2 S-box analysis results

Using the proposed s-box generator algorithm, 3 different s-boxes were obtained after 5000 iterations. These s-box structures are given in Tables 4, 5, and 6. Various metrics are used in the literature to evaluate the performance of an 8-bit s-box structure used in this study. The first of these is the property of bijectivity. This feature states that each value should be used only once. In this way, a more effective mixing process is achieved. Three different s-box structures obtained in this study also meet this criterion. So the suggested s-boxes are bijective. Another important criterion is SAC. This metric briefly states that; A change in the input should change almost half of the bits in the output. Therefore, this value should be 0.5 or very close to it. The averages of these values in the s-box structures proposed in this study are 0.5032, 0.5046, and 0.5095, respectively. These values show that the proposed s-boxes meet this criterion perfectly. Another and most important metric is the nonlinearity metric. Since an s-box is a non-linear transformation, this value is expected to be high. In AES, this value is 112. In the recommended s-box structures, these values are 108, 108.5, and 108.75, respectively. These values are values that can be considered high. Another metric is BIC. Here, nonlinearity and SAC values

are calculated in different ways. For this criterion, the maximum nonlinearity value is 112 and the SAC value is required to be 0.5. Recommended s-box structures where the SAC value is 0.4963, 0.4997, 0.501 respectively. Nonlinearity values are 102.29, 103.36, 103.71. SAC values are provided in the BIC criterion. However, nonlinearity values here can be increased in future studies. Finally, input–output XOR distributions are calculated. This criterion says that changes in the input must independently affect the output. It is desired that this value below. In AES, this value is highest at 4. In the s-box structures in this study, these values are 10, 10, and 12, respectively. These values are a problem in many studies and are another point that needs to be improved. In most studies, this value is calculated as 10. Therefore, these values are acceptable.

The proposed s-box structures are compared with some other studies in the literature. The comparison results are given in Table 7. The comparison is based on BIC, SAC, max XOR, and nonlinearity metrics. When the literature and Table 7 are analyzed; it is seen that the SAC value is obtained very close to 0.5 in most studies. Similarly, it is seen that the BIC-SAC value used to calculate the BIC value in these studies is close to 0.5 and the BIC-Non values are generally close to each other. In most of these studies, the max XOR value, which is the third criterion, is usually 10. This value is 4 for the s-box structure used in the AES algorithm. In other words, a value of 4 must be reached. This is one of the most prominent shortcomings of the literature. Finally, the metric focused on both in this study and most other studies is the nonlinearity value. Because an s-box structure should not have a linear structure. Therefore, researchers have been working for many years to produce s-box structures with high nonlinearity values. The main purpose of the s-box structures used in this study is to ensure that the nonlinearity value is as high as possible. Looking at Table 7, the proposed s-box structures have surpassed many studies in terms of nonlinearity values. This is one of the most important contributions of the proposed work.

Table 9 Comparison of information entropy values for Lenna image

Method	Information entropy value		
	R	G	B
Proposed	7.9985	7.9987	7.9966
Yang et al. (2019)	7.9948	7.9958	7.9950
Khan and Masood (2019)	7.9973	7.9972	7.9975
Liu and Wang (2011)	7.9791	7.9802	7.9827
Elkandoz and Alexan (2022)	7.9970	7.9973	7.9961

Table 10 Comparison of NPCR and UACI values for different images

Test image	NPCR			UACI		
	Proposed	Elkandoz and Alexan (2022)	Alexan et al. (2023b)	Proposed	Elkandoz and Alexan (2022)	Alexan et al. (2023b)
Lenna	0.99615	0.99624	0.99611	0.30402	0.30568	0.30356
Baboon	0.99611	0.99604	0.99604	0.29756	0.29604	0.29542
Pepper	0.99605	0.99605	0.99626	0.32027	0.32226	0.32163

3.3 Analysis results of encrypted images

In this study, two images of 512×512 and 256×256 were encrypted and subjected to various tests. Looking at the literature, various metrics are used to analyze encrypted images. Some of these are NPCR-UACI, information entropy calculation, histogram analyses, and correlation analyses. These four criteria were examined in this study. NPCR calculates the amount of change in pixels for an encrypted image. This value is expected to be high. This value is usually expressed as a percentage. The higher this percentage, the more independent the pixels are from each other. This value is generally expected to be above 99. UACI, on the other hand, calculates the intensity of change in an encrypted image. A high UACI value indicates that most of the pixels have changed from the original image to the encrypted image. Another criterion, information entropy, calculates the distribution of the content of the image. It is calculated separately for R, G, and B channels. A higher value indicates that the image consists of more information. In a strong encryption algorithm, pixels will be distributed randomly and there will be no repetition between patterns. This value should generally be close to 8. Another criterion, histogram analysis, graphically expresses the color distribution for an image. This analysis can provide a lot of information about the image. Therefore, it is an important analysis method. Finally, correlation analysis refers to the similarity of one side of an image to the pixels on the other side. Here the result is again expressed with a graph. If this graph results in high correlation, it means there is similarity between pixels. A low correlation means that the pixels are not like each other. Histogram and correlation analysis of an encrypted image should show a uniform distribution. In this way, attackers cannot make any inferences. NPCR-UACI and information entropy values of four different images encrypted with the proposed encryption algorithm are given in Table 8. Looking at these values, the proposed method performs an effective encryption process.

The original images and their histogram-correlation graphs, their encrypted and decrypted versions, and the histogram-correlation graphs of their encrypted versions are all given in Fig. 2. When looking at this graph, it is seen that there is no relationship between the original images and the encrypted images. Especially when looking at the histogram and correlation graphs, the encrypted images have a uniform distribution. On the other hand, when looking at the histogram and correlation graphs of the original images, it seems that the images are understood. The images encrypted with the proposed method are

compared with similar studies and the comparison of information entropy values for the Lenna image is given in Table 9. When we look at this table, the information entropy values are very close to the value of 8 with a value of 7.99, so it is considered successful. The comparison of NPCR and UACI values for lenna, baboon, and pepper images is given in Table 10. Looking at this table, it is seen that the NPCR value is 99% successful. Similarly, the UACI value around 0.3 is acceptable.

4 Conclusions

In this study, an innovative image encryption algorithm was designed. In the first step, the proposed algorithm XORs each layer of the image with a unique and strong new key. Then, a random permutation process is applied to each layer. Each of the encrypted layers obtained here is finally passed through a new s-box structure with a high nonlinearity value. After these processes, all layers are combined to obtain an encrypted image. Thus, XOR and s-box confusion meet the criteria, while random permutation meets the diffusion criteria. In this study, both key and s-box structures were obtained with a unique chaotic Gaussian map. The outputs of the chaotic map were converted into bit sequences and 5 different sequences with a length of 1 million were obtained. All of these arrays have successfully passed all NIST SP 800-22 tests. On the other hand, the proposed s-box structures surpassed many studies with nonlinearity values of 108, 108.5, and 108.75. With the proposed algorithm, 4 different images were successfully encrypted and the encrypted images successfully completed tests such as NPCR-UACI, information entropy, histogram analysis, and correlation analysis. As a result, it is thought that this study will make many contributions to the literature on s-box development, random number generation, and image encryption. Another important contribution of the study is to show how the important gains obtained in these fields can be used in an image encryption algorithm. At this point, both key and s-box structures can be developed with different methods. This is a promising research question and a source of motivation for the future.

Author contributions FA was involved in the conceptualization, data curation, formal analysis, investigation, methodology and software, supervision visualization, original draft, writing—review and editing, funding acquisition, project administration and resources.

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK).

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Aboytes-González JA, Murguía JS, Mejía-Carlos M, González-Aguilar H, Ramírez-Torres MT (2018) Design of a strong S-box based on a matrix approach. *Nonlinear Dyn* 94(3):2003–2012
- Ahmad M, Al-Solami E (2020a) Improved 2D discrete hyperchaos mapping with complex behaviour and algebraic structure for strong S-boxes generation. *Complexity* 2020:1–16
- Ahmad M, Al-Solami E (2020b) Evolving dynamic S-boxes using fractional-order hopfield neural network based scheme. *Entropy* 22(7):717
- Ahmad M, Bhatia D, Hassan Y (2015) A novel ant colony optimization based scheme for substitution box design. *Procedia Comput Sci* 57:572–580
- Ahmad M, Khaja IA, Baz A, Alhakami H, Alhakami W (2020) Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications. *IEEE Access* 8:116132–116147
- Ahmed HA, Zolkipli MF, Ahmad M (2019) A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. *Neural Comput Appl* 31(11):7201–7210
- Alexan W, ElBeltagy M, Aboshousha A (2022) Rgb image encryption through cellular automata, s-box and the lorenz system. *Symmetry* 14(3):443
- Alexan W, Elkandoz M, Mashaly M, Azab E, Aboshousha A (2023a) Color image encryption through chaos and kaa map. *IEEE Access* 11:11541–11554
- Alexan W, Chen YL, Por LY, Gabr M (2023b) Hyperchaotic maps and the single neuron model: a novel framework for chaos-based image encryption. *Symmetry* 15(5):1081
- Alhadawi HS, Lambić D, Zolkipli MF, Ahmad M (2020) Globalized firefly algorithm and chaos for designing substitution box. *J Inf Secur Appl* 55:102671
- Alhadawi HS, Majid MA, Lambić D, Ahmad M (2021) A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm. *Multimed Tools Appl* 80(5):7333–7350
- Alshekly TK, Albahrani EA, Lafta SH (2022) 4d chaotic system as random substitution-box. *Multimed Tools Appl* 81(11):15793–15814
- Al-Wattar AH, Mahmod R, Zukarnain ZA, Udzir NI (2015a) A new DNA-based S-box. *Int J Eng Technol* 15(4):1–9
- Al-Wattar AS, Mahmod R, Zukarnain ZA, Udzir NI (2015b) Generating a new S-Box inspired by biological DNA. *Int J Comput Sci Appl* 4(1):32–42
- Alzaïdi AA, Ahmad M, Ahmed HS, Solami EA (2018) Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map. *Complexity* 2018:9389065
- Anees A, Chen YPP (2020) Designing secure substitution boxes based on permutation of symmetric group. *Neural Comput Appl* 32(11):7045–7056
- Arshad B, Siddiqui N, Hussain Z, Ehatisham-ul-Haq M (2022) A novel scheme for designing secure substitution boxes (S-boxes) based on mobius group and finite field. *Wirel Pers Commun* 124:1–22
- Artuğer F (2023a) A new S-box generator algorithm based on 3D chaotic maps and whale optimization algorithm. *Wirel Pers Commun* 131:1–19
- Artuğer F (2023b) A novel algorithm based on DNA coding for substitution box generation problem. *Neural Comput Appl* 36:1–12
- Artuğer F, Özkaynak F (2020) A novel method for performance improvement of chaos-based substitution boxes. *Symmetry* 12(4):571
- Artuğer F, Özkaynak F (2021) An effective method to improve nonlinearity value of substitution boxes based on random selection. *Inf Sci* 576:577–588
- Artuğer F, Özkaynak F (2022) SBOX-CGA: substitution box generator based on chaos and genetic algorithm. *Neural Comput Appl* 34(22):20203–20211
- Artuğer F, Özkaynak F (2023a) A new post-processing approach for improvement of nonlinearity property in substitution boxes. *Integration* 94:102105
- Artuğer F, Özkaynak F (2023b) A new algorithm to generate aes-like substitution boxes based on sine cosine optimization algorithm. *Multimed Tools Appl* 83:1–16
- Basha HAMA, Mohra ASS, Diab TOM, El Sobky WI (2022) Efficient image encryption based on new substitution box using DNA coding and bent function. *IEEE Access* 10:66409–66429
- Behera PK, Gangopadhyay S (2023) Evolving bijective S-Boxes using hybrid adaptive genetic algorithm with optimal cryptographic properties. *J Ambient Intell Humaniz Comput* 14(3):1713–1730
- Belazi A, Abd El-Latif AA (2017) A simple yet efficient S-box method based on chaotic sine map. *Optik* 130:1438–1444
- Chai X, Fu J, Gan Z, Lu Y, Zhang Y (2022) An image encryption scheme based on multi-objective optimization and block compressed sensing. *Nonlinear Dyn* 108(3):2671–2704
- Chen G (2008) A novel heuristic method for obtaining S-boxes. *Chaos Solitons Fractals* 36(4):1028–1036
- Daemen J, Rijmen V (1998) AES proposal: Rijndael. In: *Proceedings of 1st advanced encryption conference*. CA, USA, pp 1–45
- Elkandoz MT, Alexan W (2022) Image encryption based on a combination of multiple chaotic maps. *Multimed Tools Appl* 81(18):25497–25518
- Erkan U, Toktas A, Lai Q (2023) 2D hyperchaotic system based on Schaffer function for image encryption. *Expert Syst Appl* 213:119076
- 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

- Farhan AK, Ali RS, Yassein HR, Al-Saidi NMG, Abdul-Majeed GH (2020) A new approach to generate multi S-boxes based on RNA computing. *Int J Innov Comput Inf Control* 16(1):331–348
- Gangadari BR, Ahamed SR (2018) Programmable cellular automata-based low-power architecture to S-box: an application to WBAN. *Circuits Syst Signal Process* 37(3):1116–1133
- Gao X, Mou J, Xiong L, Sha Y, Yan H, Cao Y (2022a) A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. *Nonlinear Dyn* 108(1):613–636
- Gao X, Mou J, Banerjee S, Cao Y, Xiong L, Chen X (2022b) An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map. *J King Saud Univ Comput Inf Sci* 34(4):1535–1551
- Gupta M, Singh VP, Gupta KK, Shukla PK (2023) An efficient image encryption technique based on two-level security for internet of things. *Multimed Tools Appl* 82(4):5091–5111
- Haque A, Abdulhussein TA, Ahmad M, Falah MW, Abd El-Latif AA (2022) A strong hybrid s-box scheme based on chaos, 2D cellular automata and algebraic structure. *IEEE Access* 10:116167–116181
- Hematpour N, Ahadpour S (2021) Execution examination of chaotic S-box dependent on improved PSO algorithm. *Neural Comput Appl* 33(10):5111–5133
- Huang X, Dong Y, Ye G, Yap WS, Goi BM (2023a) Visually meaningful image encryption algorithm based on digital signature. *Digit Commun Netw* 9(1):159–165
- Huang X, Dong Y, Ye G, Shi Y (2023b) Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform. *Front Comput Sci* 17(3):173804
- Hussain I (2020) True-chaotic substitution box based on Boolean functions. *Eur Phys J plus* 135(8):1–17
- Kadhim FA, Majeed GHA, Ali RS (2016) Proposal new s-box depending on DNA computing and mathematical operations. In: 2016 Al-Sadeq international conference on multidisciplinary in IT and communication science and applications (AIC-MITCSA). IEEE, pp 1–6
- Khan M, Masood F (2019) A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimed Tools Appl* 78:26203–26222
- Khan M, Shah T (2014) A novel image encryption technique based on Hénon chaotic map and S8 symmetric group. *Neural Comput Appl* 25(7):1717–1722
- Khan M, Shah T, Mahmood H, Gondal MA, Hussain I (2012) A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. *Nonlinear Dyn* 70(3):2303–2311
- Khan M, Shah T, Gondal MA (2013) An efficient technique for the construction of substitution box with chaotic partial differential equation. *Nonlinear Dyn* 73(3):1795–1801
- Khan LS, Hazzazi MM, Khan M, Jamal SS (2021) A novel image encryption based on rossler map diffusion and particle swarm optimization generated highly non-linear substitution boxes. *Chin J Phys* 72:558–574
- Khan H, Hazzazi MM, Jamal SS, Hussain I, Khan M (2023) New color image encryption technique based on three-dimensional logistic map and Grey wolf optimization based generated substitution boxes. *Multimed Tools Appl* 82(5):6943–6964
- Kuznetsov A, Karpinski M, Ziubina R, Kandy S, Frontoni E, Peliukh O, Kozak R (2023) Generation of nonlinear substitutions by simulated annealing algorithm. *Information* 14(5):259
- Lai Q, Hu G, Erkan U, Toktas A (2023) A novel pixel-split image encryption scheme based on 2D Salomon map. *Expert Syst Appl* 213:118845
- Lambić D (2020) A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. *Nonlinear Dyn* 100(1):699–711
- Liu G (2017) Designing S-box based on 4D–4wing hyperchaotic system. *3D Res* 8(1):1–9
- 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
- Luo Y, Ouyang X, Liu J, Cao L, Zou Y (2022) An image encryption scheme based on particle swarm optimization algorithm and hyperchaotic system. *Soft Comput* 26:1–27
- Malik MSM, Ali MA, Khan MA, Ehatisham-Ul-Haq M, Shah SNM, Rehman M, Ahmad W (2020) Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. *IEEE Access* 8:35682–35695
- Mariot L, Picke S, Leporati A, Jakobovic D (2019) Cellular automata based S-boxes. *Cryptogr Commun* 11(1):41–62
- Masood F, Masood J, Zhang L, Jamal SS, Boulila W, Rehman SU, Ahmad J (2021) A new color image encryption technique using DNA computing and Chaos-based substitution box. *Soft Comput* 26:7461–7477. <https://doi.org/10.1007/s00500-021-06459-w>
- Mohamed AG, Korany NO, El-Khamy SE (2021) New DNA coded fuzzy based (DNAFZ) S-boxes: application to robust image encryption using hyper chaotic maps. *IEEE Access* 9:14284–14305
- Muhammad AUS, Özkaynak F (2021) SIEA: secure image encryption algorithm based on chaotic systems optimization algorithms and PUFs. *Symmetry* 13(5):824
- Özkaynak F (2020) An analysis and generation toolbox for chaotic substitution boxes: a case study based on chaotic labyrinth rene thomas system. *Iran J Sci Technol Trans Electr Eng* 44(1):89–98
- Razaq A, Ullah A, Alolaiyan H, Yousaf A (2021) A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers. *Wirel Pers Commun* 116(4):3165–3190
- Razaq A, Ahmad M, Yousaf A, Alawida M, Ullah A, Shuaib U (2022) A group theoretic construction of large number of AES-like substitution-boxes. *Wirel Pers Commun* 122(3):2057–2080
- Siddiqui N, Yousaf F, Murtaza F, Ehatisham-ul-Haq M, Ashraf MU, Alghamdi AM, Alfakeeh AS (2020) A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field. *PLoS One* 15(11):e0241890
- Szaban M, Seredynski F (2008) Application of cellular automata to create S-box functions. In: 2008 IEEE international symposium on parallel and distributed processing. IEEE, pp 1–7
- Tian Y, Lu Z (2017) Chaotic S-box: intertwining logistic map and bacterial foraging optimization. *Math Probl Eng*. <https://doi.org/10.1155/2017/6969312>
- Wang Y, Wong KW, 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
- Wang Y, Zhang Z, Zhang LY, Feng J, Gao J, Lei P (2020) A genetic algorithm for constructing bijective substitution boxes with high nonlinearity. *Inf Sci* 523:152–166
- Wang L, Cao Y, Jahanshahi H, Wang Z, Mou J (2023) Color image encryption algorithm based on Double layer Josephus scramble and laser chaotic system. *Optik* 275:170590
- Yang F, Mou J, Sun K, Cao Y, Jin J (2019) Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit. *IEEE Access* 7:58751–58763
- Ye T, Zhimao L (2018) Chaotic S-box: six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. *Nonlinear Dyn* 94(3):2115–2126
- Zamli KZ (2021) Optimizing S-box generation based on the adaptive agent heroes and cowards algorithm. *Expert Syst Appl* 182:115305

- Zamli KZ, Kader A, Din F, Alhadawi HS (2021) Selective chaotic maps Tiki-Taka algorithm for the S-box generation and optimization. *Neural Comput Appl* 33:1–18
- Zamli KZ, Din F, Alhadawi HS, Khalid S, Alsolai H, Nour MK, Assam M (2023) Exploiting an Elitist barnacles mating optimizer implementation for substitution box optimization. *ICT Express* 9(4):619–627
- Zhu Y, Wang C, Sun J, Yu F (2023) A chaotic image encryption method based on the artificial fish swarms algorithm and the DNA coding. *Mathematics* 11(3):767

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.