




Construction of highly non linear component of block cipher based on mclaurin series and mellin transformation with application in image encryption

Abid Mahboob¹ · Imran Siddique²  · Muhammad Asif³ · Muhammad Nadeem⁴ · Aysha Saleem⁴

Received: 25 February 2022 / Revised: 13 March 2023 / Accepted: 29 May 2023 /
Published online: 6 June 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

A substitution box (S-box) in data encryption is a non-linear tool that conducts substitution to assure the overall security of the system. S-box is the most important part of the block cipher. The non-linearity trait is critical for the construction of more reliable substitution boxes in data encryption. As a result, new approaches for generating high non-linear S-boxes are required. Using the Mellin transformation and the McLaurin series, this work suggests an approach for creating Substitution boxes with a high non-linearity value of 112.5. S-box construction consists of three phases. In step 1, we build a sequence from a function's McLaurin series and then apply Mellin transformation to the sequence's terms without substituting limits. In the second phase, we solved all of the coefficients under mod 257, and in the third step, we improved the unpredictability of the initial S-box by using a particular permutation of Symmetric group S_{256} . Furthermore, the algebraic characteristics of S-box are evaluated using various tests, including non-linearity (NL), Bit Independent Criterion (BIC), Strict Avalanche Criterion (SAC), Linear Approximation Probability (LAP), and Differential Uniformity (DU), all of which certify the algebraic properties of the S-box.

Keywords Block Cipher · Substitution box · McLaurin series · Mellin transformation · Symmetric group S_n

1 Introduction

It is now well acknowledged that the usage of the internet is rapidly growing in all walks of life like engineering, medical, military, educational, political, banking, marketing and vice versa. Everyone wants their data and information to be secured over the internet while transmission third party don't have unauthorized access to the communication between two people. In [7], Shannon proposed the concept of block cipher. Block cyphers such as the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are the critical components of multimedia security. DES [32] like cryptosystem

✉ Imran Siddique
imransmsrazi@gmail.com

Extended author information available on the last page of the article

break easily due to its short 56 bit key and more complicated due to 16 Feistel rounds. AES like cryptosystem used 128, 192 and 256-bits keys for 10, 12 and 14 rounds respectively for encryption. In 2001 NIST introduced AES and modern cryptography based on it [10]. AES is a type of block cypher that encrypts and decrypts data with the same key using the substitution permutation network (SP-network). The substitution box is still the most crucial part of block cyphers, including AES (S-box). This is because this ingredient is the sole source of the nonlinearity effect. Furthermore, according to Shannon's pioneering work [36], S-Box is consistent with the influence of confusion, which obscures the statistical relationship between the plain text and the private keys.

S-box is a vectorial Boolean function that is defined mathematically as: $\varphi : \mathbb{Z}_2^u \rightarrow \mathbb{Z}_2^v$ which map u input bit into v output bit. The algebraic and statistical features of the S-box, such as NL, BIC, SAC, DU, LAP, and MLC, are used to assess its validity. Substitution boxes are essential in symmetric key cryptography because they are used to perform substitutions. S-boxes are commonly used in block ciphers to conceal the relation among the cipher text and the key. Because of the usage of algebraically weak S-boxes, cryptosystems are insecure and unstandardized. Similarly, constructing an efficient and safe cryptosystem requires the creation of a robust algebraic S-box. Many methods have been developed as a result of these significant applications to create more reliable S-boxes that will be used for robust block encryption. For these reasons, researchers are currently concentrating on developing new algorithms for constructing more secure and trustworthy S-boxes. Zhang et al. utilized I-Ching operators to create an S-box in [43]. The nature of the created S-Box was assessed using various techniques, with great results showing the scheme's resilience. [21] Introduces a novel approach for constructing key dependent S-boxes. Firdousi et al. [16] created a modified S-box using quantum maps. The recommended S-box is strong enough to meet the needed requirement of secure encryption technique. [26] Presents a powerful image encryption technique based on a newly developed S-box. Shafique et al. [35] created a secure S-box using Cubic-Logistic mapping. With the use of integer multiplication, a safe and efficient chaotic map [23] is created, which is then used to generate a strong S-box. In [44], authors devised an approach using the combination of chaotic systems. In [37], the authors have investigated matrix action on the Galois field and created an S-box with good cryptographic features.

The symmetric group S_n is utilised to enhance the nonlinearity value of S-box. Rows and columns of 8×8 S-boxes are rearranged using permutations of the S_{16} group, whereas cells of S-boxes are rearranged using permutations of the S_{256} symmetric group. A function's Taylor series is used to express a function in the form of the sum of infinite terms of the function's derivative at a point. Taylor's series, which is named after Brook Tayler, extends a function in terms of Polynomial. The McLaurin series is a special form of the Taylor series at $x = 0$ [1]. Mellin transformation is a type of integral transformation that is similar to Laplace and Fourier transformations. Hjalmar Mellin [25], a mathematician, describes this transformation. It is employed in number theory, asymptotic expansion theory, and mathematical statistics. The literature contains various publications on the Mellin transform based cryptography technique [33, 34]. Mellin transformation was utilised by Bhatti et al. in [8] for encryption and decryption, however the building of S-boxes using Mellin transformation has never been mentioned before. In this study, we introduce a unique, efficient, and creative method for building robust S-boxes utilizing the Mellin transformation.

The following is the main contribution of our work in this manuscript:

- A new S-box construction process based on the McLaurin and Mellin transformation.
- Permutation of symmetric group S_{256} are used to generate the recommended S-box which have an average non-linearity of 112.5.

- The recommended S-box is utilized for image encryption, and its validity in image encryption is assessed using various tests.
- Compare the proposed encrypted image with different algorithm, which shows that our S-box gives the best encryption scheme for the security of image data.

The body of this article is structured as follows: Basic definitions are provided in Section 2. In Section 3, a mathematical algorithm is described for the construction of S-box using the McLaurin series and Mellin transformation. Additionally, the nonlinearity of the initial S-box, which has an average nonlinearity of 112.5 and is higher than the AES NL score, is increased using a special permutation of the symmetric group S_{256} . In Section 4, the proposed S-box is examined using several tests, including NL, BIC, DP, and SAC, and it is compared to existing boxes from the literature. In Section 5, the recommended S-box is employed for image encryption, and the encryption strength is assessed using various tests and the proposed algorithm’s conclusion is provided in Section 5.

2 Preliminaries

2.1 Mellin Transformation

It is an integral transformation that was named by the mathematician Hjalmar Mellin. It is defined as,

$$M[g(x);h] = \int_0^\infty g(x)x^{h-1} dx$$

Hjalmar Mellin also define inverse Mellin transformation as:

$$M^{-1}[g(x);h] = \frac{1}{2\lambda i} \int_{c+i\infty}^{c-i\infty} g(x)x^{(-h)} dx$$

which is the line integral in complex plane.

2.2 Taylor series

The formula for Tayler series of a real or complex-valued function is defined as

$$f(a) + \frac{f'(a)}{1!}(x - a) + \frac{f''(a)}{2!}(x - a)^2 + \frac{f'''(a)}{3!}(x - a)^3 + \dots + \frac{f^n(a)}{n!} + \dots$$

In sigma notation;

$$f(a) = \sum_{n=0}^\infty \frac{f^n(a)}{n!}(x - a)^n$$

where $n!$ denotes factorial of n and $a \in R, C$. McLaurin series is the special case of Taylor series for which $a = 0$

3 Algebraic Structure of S-box

Step 1: Let S indicates a Set of integers ranging from 0 to 255.

$$S = \{k|k \in Z \wedge 0 \leq k \leq 255\}$$

A function $f(x) = 1/(1 - x)$ whose McLaurin series is

$$f(x) = \sum_{n=0}^{\infty} x^n$$

Series is the sum of elements of the sequence

$$\{x^n\}n = 0, 1, 2, 3,$$

Write down all of the components of S in ascending order and multiply with the first 256 terms of $\{x^n\}$ such that $k \cdot x^n$ is possible if $k = n$.

The outcomes will be as follows:

$$0, 1x, 2x^2, 3x^3, \dots, 255x^{255}$$

Now we will develop a new sequence, as seen below.

$$\{nx^n\}n = 0, 1, 2, 3, \dots, 255$$

This sequence can be extended by multiplying x^2 with each term of the sequence $\{nx^n\}0 \leq n \leq 255$ as

$$\{nx^{n+2}\}n = 0, 1, 2, 3, \dots, 255.$$

If we apply the Mellin transformation to the n^{th} term of the sequence while neglecting limitations, we get the following formula:

$$M[nx^{n+2}, h] = n \frac{(x)^{n+h+2}}{n + h + 2}n = 0, 1, 2, 3 \dots 255$$

Table 1 Initial S-box 1

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

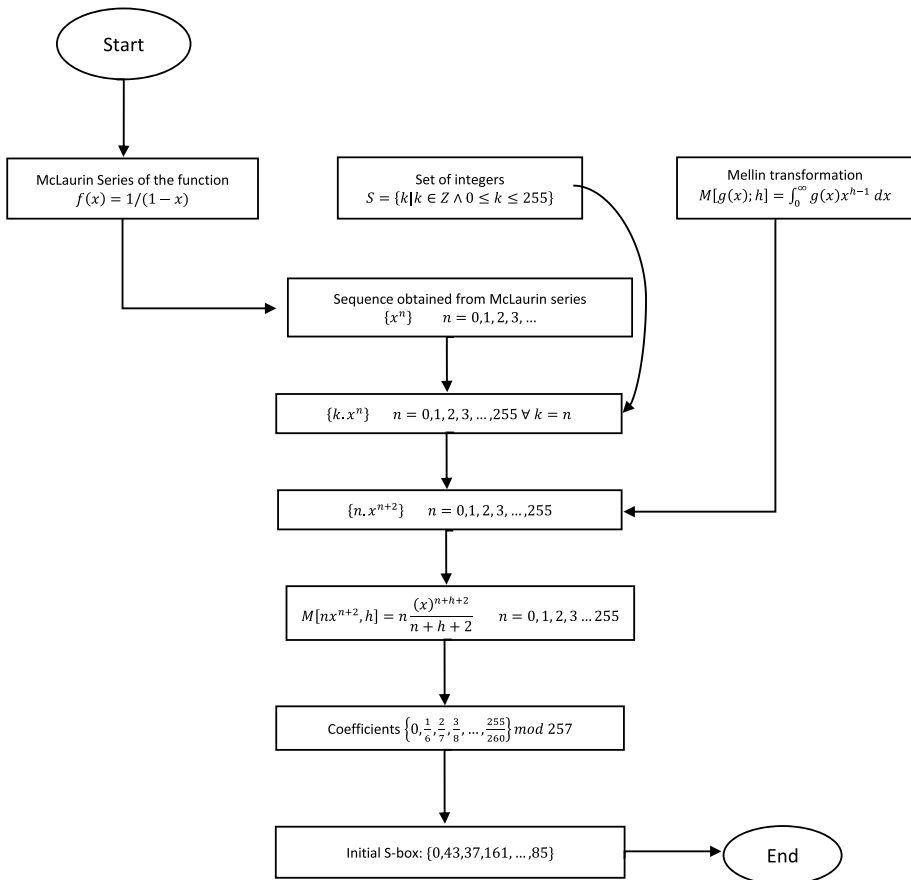
When we apply the above formula to each term in the sequence $\{nx^{n+2}\}$, we get the new sequence shown below

$$\left\{ n \frac{(x)^{n+h+2}}{n+h+2} \right\} n = 0, 1, 2, 3 \dots 255$$

Here we will use $h = 3$ then the sequence will become $\left\{ n \frac{(x)^{n+5}}{n+5} \right\} n = 0, 1, 2, 3 \dots 255$

Step 2: Since an S-box $S : \{0, 1\}^n \rightarrow \{0, 1\}^n$ is basically any rearrangements of the elements of set $S = \{k|k \in Z \wedge 0 \leq k \leq 255\}$. We used $\text{mod } 257$ to solve the coefficients of all sequence terms. As we determined that the 127^{th} coefficient is equal to 256, which does not belong to set S , and the 253^{th} coefficient is equal to ∞ , these coefficients are replaced by 64 and 1 respectively. Put all of these results in the 16×16 table, which is our initial S-box and has an average non-linearity of 102.5. (See Table 1).

A flow chart for the mathematical construction of initial S-box:



Step 3: Since our data is shown in a 16×16 table with 256 cells, we may improve the randomization by swapping the placements of these cells. For this reason, a particular type of permutation from Symmetric group S_{256} , as shown in Table 2, is applied on Table 1, and the new S-box, which is our suggested S-box with an average non-linearity of 112.5, is shown in Table 3.

4 Security analysis

Within this part, a number of tests have been provided to assess the effectiveness of suggested S-box. Non-linearity test (NL), Bit Independent Criterion (BIC), Strict Avalanche Criterion (SAC), Linear Approximation Probability (LAP), and differential Uniformity (DU) of Substitution box are a few examples. Table 9 compares the algebraic characteristics of S-boxes to those of many other S-boxes.

4.1 Non-linearity

In 1988, Pieprzyk and Finkelstein proposed the non-linearity test [31]. It is quite helpful in determining the effectiveness of the S-box. If the correspondence from plain text to cypher is linear, S-box is regarded weak, and attackers may easily perform a linear attack on cypher text. The mathematical formula for determining the non-linearity of S-box is defined as follows:

$$N_f = (2)^{n-1} [1 - (2)^{-n} \max |W_f(a)|] \tag{1}$$

where $W_f(a)$ is the value of Walsh Spectrum

$$W_f(a) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus a \cdot x} \tag{2}$$

and $a \cdot x$ is dot product defined by

Table 2 Permutation of S_{256}

(1	179	245	93	137	4	20	154	95	130	231	178	170	215	193	140
151	134	6	135	88	149	194	248	143	13	84	225	139	21	187	188
102	3	159	112	31	199	16	177	42	77	104	61	169	105	108	70
97	106	12	91	110	22	55	72	128	148	214	208	60	40	87	183
191	52	161	233	203	66	39	64	163	116	51	152	10	213	101	204
107	221	141	111	241	2	100	99	54	197	226	57	67	90	165	220
160	186	59	240	125	239	176	228	47	46	69	216	28	76	23	37
168	86	126	164	210	181	136	156	123	62	33	195	250	89	212	246
205)	(5	247	158	127	254	41	115	118	121	252	19	242	98	36	171
224	129	114	249	219	8	146	65	11	56)	(7	94	167	131	211	44
92	172	222	234	184	79	50	82	30	230	74	32	25	253	175	138
83	24	78	133	201	206	109	49	227	166	15	63	218	209	180	117
38	243	255	81	185	68	122	119	113	124	189	251	75	80	145	29
48	26	198	244	71	232	73	27	157	196	217	236	35	9	14	120
174	207	144	53	256	235	238	17	150	192	142	162	153)	(18	202	155
173	58	237)	(34	45	85	223)	(43	182	132	190	229)	(96	147	103	200)

Table 3 Proposed S-box

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

$$a_1 \cdot x_1 \oplus a_2 \cdot x_2 \oplus \dots \oplus a_n \cdot x_n \tag{3}$$

Table 4 presents the non-linearity values of eight balanced Boolean functions of constructed S-Boxes and Fig. 1 compares the non-linearity values of the proposed S-box to those of several previously developed S-boxes in the literature.

4.2 Bit independent criterion

A Vectorial Boolean $S : \{0, 1\}^n \rightarrow \{0, 1\}^n$ function meets BIC requirements if $\forall i, j, k \in \{1, 2, 3, \dots, n\}$ the inversion of i^{th} input modifies output j^{th} and k^{th} separately [41]. Tables 5 and 6 provide the results of the BIC non-linearity values and the BIC SAC values of the recommended S-box, respectively. Where the relationship is discovered when we modify the i^{th} input and the corresponding change in the j^{th} and k^{th} output bits. Our S-box has a BIC nonlinearity score of 103.79, and a BIC-SAC score of 0.4992, which is quite near to the ideal value of 0.5. As a consequence, our S-box satisfies the BIC’s requirements. Table 9 compares the BIC non-linearity values of the recommended S-boxes to those of numerous other S-boxes.

4.3 Strict avalanche criterion

This is a critical requirement for determining the algebraic characteristics of the S-box [41]. This S-box feature assures that the output bit changes by 50% or 1/2 probability

Table 4 Non- linearity values

Bool Fun	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	Average
S-box 1	100	102	98	104	106	104	104	102	102.5
S-box 2	114	112	112	112	114	112	114	110	112.5

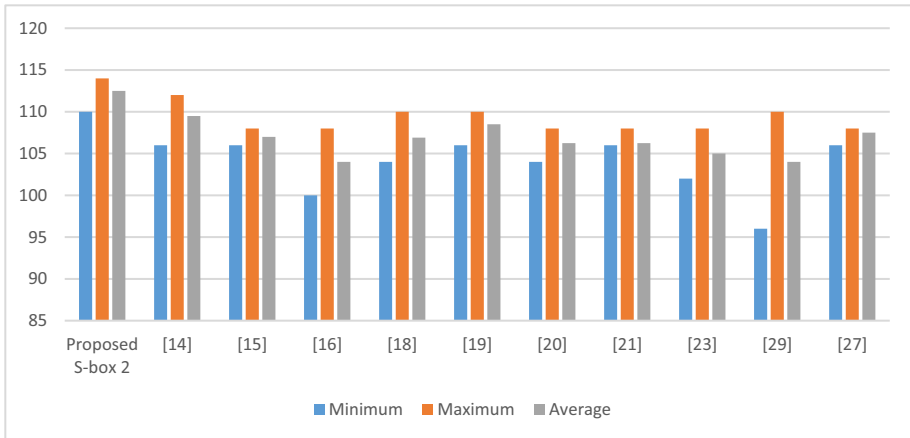


Fig. 1 A comparison between the non-linearity values of suggested S-box and various other S-boxes

after altering a single input bit. This criteria asserts that if a single input bit is changed, each output bit will change with a chance of 1/2. [31, 41] provide a strong approach for calculating SAC of S-boxes using a dependency matrix. The S-Box has an average SAC value of 0.4995, indicating that the recommended S-Box meets the SAC criteria adequately. Table 7 shows the SAC values of the recommended S-box and Table 9 compares them to other S-boxes.

4.4 Differential Uniformity

Biham E and Shamir A [40] proposed this analysis. The differential uniformity of a Boolean function is calculated by requiring that the XOR values of each output have the same probability as the XOR values of each input. The following is the mathematical formula for calculating differential uniformity.

$$DU = \max_{\Delta x \neq 0, \Delta y} (\#\{x \in X | f(x) \oplus f(x \oplus \Delta x) = \Delta y\}) \tag{4}$$

Table 8 shows the differential uniformity values of the recommended S-box, and Table 9 shows a comparison of the differential probability values of the proposed S-box and many other existing S-boxes in the literature. Figure 2 depicts a graphical comparison between DU values of the recommended S-box and several existing S-boxes.

Table 5 BIC Nonlinearity Values of S-box 2

0	104	108	106	106	98	104	104
104	0	106	106	100	108	104	108
108	106	0	104	104	100	106	100
106	106	104	0	106	100	106	102
106	100	104	106	0	104	104	100
98	108	100	100	104	0	102	102
104	104	106	106	104	102	0	104
104	108	100	102	100	102	104	0

Table 6 BIC SAC Values of S-box 2

0	0.5137	0.4688	0.5078	0.5195	0.4961	0.5215	0.4707
0.5137	0	0.4922	0.5117	0.4805	0.4941	0.502	0.5156
0.4688	0.4922	0	0.5078	0.4883	0.498	0.4961	0.5059
0.5078	0.5117	0.5078	0	0.4941	0.4922	0.5234	0.5234
0.5195	0.4805	0.4883	0.4941	0	0.4785	0.5059	0.498
0.4961	0.4941	0.498	0.4922	0.4785	0	0.4805	0.4961
0.5215	0.502	0.4961	0.5234	0.5059	0.4805	0	0.4941
0.4707	0.5156	0.5059	0.5234	0.498	0.4961	0.4941	0

4.5 Linear approximation probability

The present block cypher’s cryptologist seeks to create enough unpredictability and bit diffusion to protect the data from cryptanalytic efforts. An S-box with a low linear probability (LP) denotes a mapping that is more nonlinear and resists linear cryptanalysis. This analysis is performed to determine the event’s greatest value of imbalance. Matsui [28] proposed this approach, and the mathematical formula is as follows,

$$LP = \max_{a_1, a_2 \neq 0} \left| \frac{\#\{x \in X | x.a_1 = f(x).a_2\}}{2^n} - \frac{1}{2} \right| \tag{5}$$

Table 9 illustrates the LP values of the proposed S-box and compares them to other S-boxes.

5 Applications of s-box in image encryption

In this phase, we apply the recommended S-box for image encryption scheme using Advanced Encryption Standard algorithm. MLC specifies a methodology for assessing the findings of various statistical studies, such as energy, homogeneity, contrast, entropy and correlation. This evaluation determined the validity of S-box for image encryption Figs. 3 and 4.

5.1 Contrast

Contrast is the change in color that sorts an image different from other image within the similar field of view. The contrast is high means that disorderness in encrypted image

Table 7 SAC values of recommended S-box

0.5	0.5156	0.4688	0.4688	0.5	0.5312	0.4844	0.5
0.5	0.5312	0.5469	0.4844	0.5	0.5469	0.4531	0.5
0.5312	0.4844	0.4688	0.5156	0.4688	0.4688	0.5625	0.4531
0.5	0.5312	0.4844	0.4844	0.5312	0.5156	0.5	0.4688
0.4844	0.5156	0.5	0.4531	0.4844	0.5	0.5	0.5156
0.4688	0.5156	0.5	0.5156	0.5	0.4688	0.4844	0.4688
0.5	0.5469	0.5	0.4531	0.5	0.4688	0.4688	0.5469
0.5156	0.4844	0.5156	0.4844	0.5625	0.5	0.5	0.5469

Table 8 Input / Output XOR Distribution Table

6	8	6	6	6	6	6	6	6	6	6	6	6	6	4	8
6	6	6	6	8	10	6	10	6	8	6	6	6	12	6	6
6	4	6	6	6	6	8	6	8	8	6	6	6	4	8	8
6	8	8	6	6	6	6	6	8	6	8	6	8	6	10	6
8	6	10	6	6	6	6	6	6	8	6	6	6	6	8	8
8	8	8	6	6	10	6	6	8	8	6	6	10	12	8	6
8	6	6	6	6	8	6	8	6	6	8	8	6	8	8	6
6	6	6	6	6	6	6	6	6	6	8	8	6	8	8	6
6	6	6	8	6	6	6	6	6	6	6	6	10	8	6	6
6	6	6	6	6	6	8	8	6	8	6	6	6	8	6	6
6	6	6	8	6	6	6	6	8	10	6	6	6	6	4	6
8	6	6	6	6	6	6	10	8	8	8	10	6	6	8	6
6	6	6	6	6	6	6	6	6	4	6	6	8	8	6	6
8	8	6	8	8	6	6	6	6	6	6	6	6	6	8	6
6	8	6	6	8	8	8	8	6	8	8	6	8	6	8	6
6	8	6	6	8	8	6	6	6	6	10	8	6	6	8	0

increased. Contrast is related with the amount of confusion which is produced by the s-box to the plan image. The mathematical form of contrast is,

$$Contrast = \sum |k - m|^2 p(k, m)$$

Here k, m denotes the pixels of the image.

Table 9 The comparison between LP, DP, BIL-NL, and SAC values of S-Boxes

S-boxes	LP	DP	BIC-NL	SAC
Recommended S-box	0.125	0.047	103.79	0.4995
[26]	0.1328	0.039	103.9	0.503
[2]	0.1328	0.031	106.9	0.507
[5]	0.141	0.047	102.3	0.493
[12]	0.137	0.039	102.6	0.497
[42]	0.1406	0.039	103.5	0.498
[18]	0.113	0.031	106.1	0.509
[4]	0.109	0.039	103.9	0.500
[13]	0.139	0.039	103.6	0.501
[22]	0.1328	0.039	104.1	0.501
[17]	0.125	0.039	103.6	0.499
[45]	0.1484	0.047	102.9	0.503
[38]	0.125	0.039	103.5	0.506
[14]	0.141	0.047	102.9	0.499
[24]	0.125	0.047	103.0	0.500
[39]	0.1406	0.039	103.1	0.509
[11]	0.1328	0.055	103.5	0.496
[20]	0.125	0.031	103.0	0.493

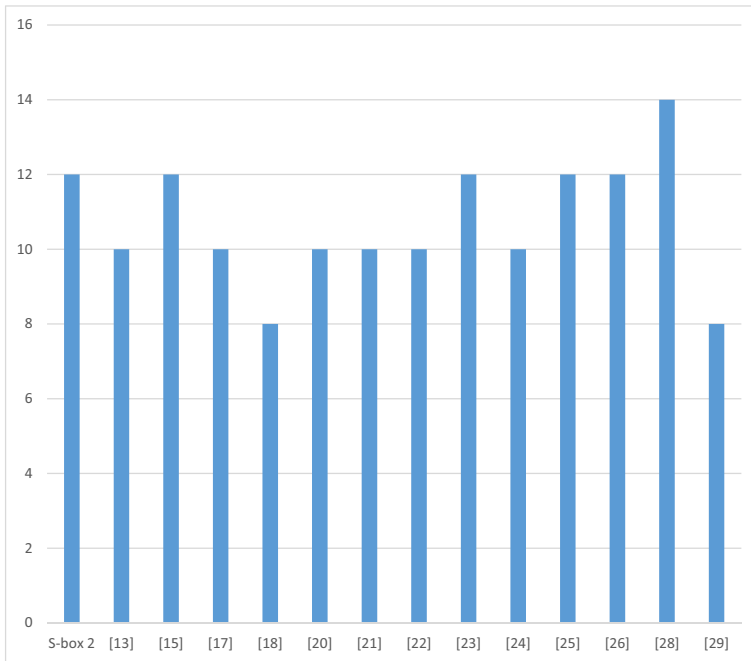


Fig. 2 A comparison between DU scores of different S-boxes

5.2 Correlation

Correlation expands the link among the pixels of the cipher image. This assessment is divided into three categories.

- a. General correlation
- b. Diagonal formats
- c. Vertical and horizontal

If G, H represents two matrices, the correlation is,

$$Correlation = \sqrt{\frac{\sum_m \sum_n (G_{mn} - \bar{G})(H_{mn} - \bar{H})}{\sum_m \sum_n (G_{mn} - \bar{G})^2 \sum_m \sum_n (H_{mn} - \bar{H})^2}}$$

Two distinct images may have similar correlation but dispersal of colors of the pixels may be totally different as shown in Fig. 3.

5.3 Energy

The Grey-level co-occurrence matrix is applied to calculate energy. If energy is nearly equal to zero then encryption scheme is better. The mathematical form of the energy is Fig. 5,

Fig. 3 Original Lena Image

$$Energy = \sum P(k, l)^2$$

5.4 Homogeneity

We put into practice the homogeneity that calculates how closely the scattered components are together. This is called Grey-tone spatial dependency matrix. The homogeneity close to zero ensured that encrypted image is good. The GLCM table radiates the frequency of Grey levels.

The mathematical form of homogeneity is

$$Homogeneity = \sum_{kl} \frac{p(k, l)}{1 + |k - l|}$$

Here grey level co-occurrence matrices in the GLCM is mentioned by $P(k, l)$.

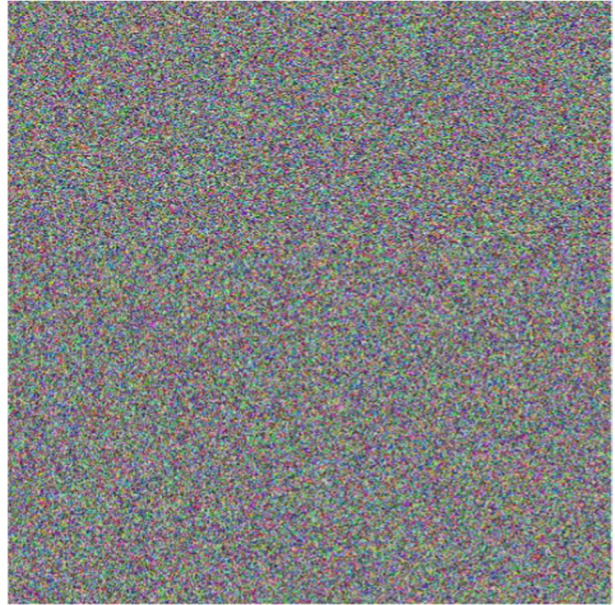
5.5 Entropy

Entropy measures the randomness in the picture. Mathematically its denoted as,

$$Entropy = - \sum_{j=1}^n (p(x_j) \log_b p(x_j))$$

where $p(x_j)$ have the histogram count. Figure 6 shows that assessment of lower and higher entropy. If entropy is close to 8 then encryption quality is better.

Fig. 4 Encrypted Lena Image



Here the Table 10 describes the MLC of s-boxes which fulfill all the conditions up to the mark.

5.6 Complexity analysis

This section explores the computational complexity of the proposed encryption scheme, which involves dividing the image into Most Significant Bits (MSBs) and Least Significant Bits (LSBs). Each pixel in the image is split into two sub-blocks using a constant time complexity of $O(1)$. The initial step requires $O(M \times N)$ bit operations. Next, the scheme maps each element of the image onto proposed S-box in constant time since the image data lies within a fixed range. The preprocessing step requires $O(M \times N)$ bit operations to execute. The substitution module is also performed in linear time. As all

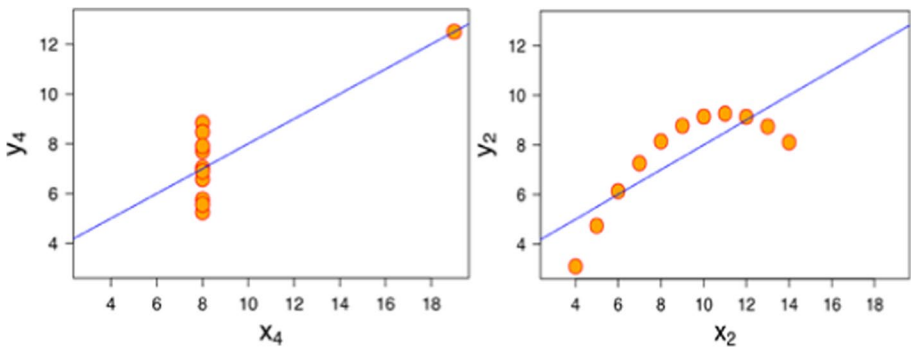


Fig. 5 Encrypted image Correlation

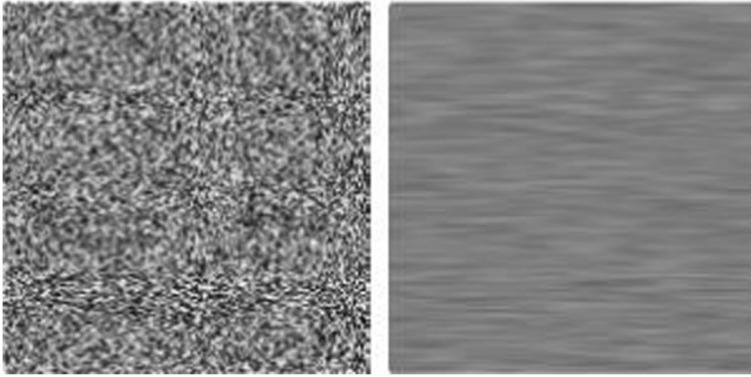


Fig. 6 Lower vs higher entropy

modules of the algorithm operate in linear time, the overall computational complexity of the scheme is $O(M \times N)$, which is linear time. $(M \times N)$ represents the dimension of the plain image. Comparing the computational time complexities of the proposed encryption scheme with those of existing algorithms [30], the computational time complexity for generating the cross-coupled chaotic sequence for one round operation is $O(2 \times M_x)$, where M_x is the maximum value of M_1 and M_2 respectively. The time complexity for the row-column permutation stage is $O(M_1 \times N_1)$, while the computational complexity for the row-column diffusion operation is $8(M_1 + N_1)$. Therefore, the overall total computational time complexity of the encryption algorithm [30] is $O(2Mx + 9(M_1 + N_1))$ which is almost equal to that of the proposed algorithm.

5.7 Pseudocode of encoding of proposed image data

The pseudocode for proposed image encryption scheme is explain in Table 10.

6 Analysis and comparison

In this part, we have applied statistical analysis to proposed encrypted Lena image Fig. 4. We have computed entropy, contrast, correlation, energy, and homogeneity of the ciphered image. Table 10 shows the comparison of recommended S-box encryption scheme with other algorithms. This ensures that our highly non-linear S-box is favorable for the image's encryption reliability (Fig. 5).

Table 11 shows that entropy is nearly equal to 8, contrast is higher. Because if entropy is close to 8 then encryption scheme is good and contrast higher also ensure the quality of the image encryption scheme. The energy and correlation is close to zero and homogeneity is also declines. For better encryption quality energy also nearly equal to zero. From these analysis and comparisons, we can say that proposed S-boxes for image encryption are good.

Table 10 Pseudocode of Proposed Image Encryption Scheme

```

1. Start
2. Input Lena Image = Image name. extension
3. Key = []
4. Output = EncryptedLenaImagedata(.jpg)
5. Compute Numbers from Maclaurin Series
6. Apply Meilin Transformation
7. [m, n] = size(O);
8. Length (m, n)
9. %Sequence generation
10. fork = 1 : Ldo
11.  $f(x) \leftarrow S$ 
12.  $f(x) \leftarrow x^n$ 
13.  $f(x) \leftarrow kx^n$ 
14.  $M[g(x);h] \leftarrow [n, x^{n+2}]$ 
15. End
16. % Binary matrix generation
17. fork = 1 : mdo
18. forl = 1 : ndo
19.  $\beta(k, l) = 1$ 
20. if  $S_{k,l} \geq 0$ 
21. else
22.  $\beta(k, l) = 0$ 
23. FinalS - box = Abs ( $S_1$ )
24. % Data conversion
25. fork = 1 : mdo
26. fork = l : ndo
27. if  $S_{k,l} > 2^{-15}$ 
28.  $S(k, l) = S_{k,l}^{\beta}$ ;
29. else  $S_{k,l} = 2^{-15}$ 
30.  $S(k, l) = S_{k,l} - 1$ ;
31. %Difusionphase
32. fork = 1 : mdo
33. fork = l : ndo
34.  $S(k, l) = S(M[g(x);h], x^{n+2})$ 
35. endend
36. % Generation of S-box
37.  $S_1 \leftarrow [n, x^{n+2}]$ ;
38.  $S_1 \leftarrow M[nx^{n+2}, h]$ 
39.  $S_2 \leftarrow S_{256}[S_1]$ ;
40. % Substitution phase
41.  $M \leftarrow S_1(S_{256})$ 
42.  $M \leftarrow S_1(f(x))$ 
43.  $S \leftarrow S_2(S_1)$ 
44. % Bit-xor operation
45.  $I_1 \leftarrow (f(x) \bmod 257 \oplus S)$ 

```

Table 10 (continued)

```

46.  $I_2 \leftarrow ((f(x) \bmod 257) \oplus S)$ 
47.  $I_3 \leftarrow (M[g(x);h] \bmod 257 \oplus S)$ 
48.  $S(i,j) \leftarrow I_1 \oplus I_2 \oplus I_3$ 
49. % Reverse conversion
50. fork = 1 : mdo
51. fork = l : ndo
52. if  $\beta(k, l) \geq 0$ 
53.  $S_2 \leftarrow S(k, l)$ 
54. else
55.  $S_2 \leftarrow -S(i, j)$ 
56. end;end;end
57. imagewrite('encrypteddata.jpg',  $S_2, F$ )

```

7 Conclusion

In this manuscript, we provided an innovative technique to construct the S-box by using Maclaurin series of logarithmic function and apply Mellin transformation on it to erect the initial S-box. After that, specific permutations of S_{256} utilized to enhance the nonlinearity of preliminary S-box and generate the final S-box. The effectiveness of our suggested S-box is then compared to other famous S-boxes in the literature. We apply statistical and algebraic tests to evaluate the efficiency of our final S-box. NL, SAC, DU, LAP and BIC are all part of the algebraic test. Because our final S-box meet all of the conditions of these analyses, regarded as strong S-box for secure communication. We use the Majority Logic Criterion in the statistical test to evaluate the effectiveness of the final S-box in an image encryption application. In this context, statistical tests such as contrast, energy, homogeneity and entropy are applied. The output result show that S-box consider more secure and effective against invaders attacks. In future, we can construct the S-boxes by using other transformations such as Sumudu and Fourier transformations and further those S-boxes can be utilized in audio, video, and text encryption schemes.

Table 11 Comparison of MLC

S-boxes	Entropy	Contrast	Correlation	Energy	Homogeneity
Original Lena Image	7.5072	0.4996	0.9175	0.0684	0.7108
Proposed Encrypted Lena Image	7.9872	11.3728	-0.0033	0.0147	0.3742
Skipjack [27]	7.684753	6.814102	0.186839	0.035231	0.486187
APA [15]	7.697393	7.745849	0.235826	0.023841	0.497366
Prime [19]	7.669541	6.477377	0.098544	0.037190	0.48858
AES [9]	7.84018	7.423085	0.088914	0.035476	0.389521

Data availability The data used to support the findings of this study are available from the corresponding author upon request.

Declarations

Competing interests The writers affirm that they have no established financial or interpersonal conflicts that would have seemed to have an impact on the research presented in this study.

Conflict of Interest There is no conflict of interest.

References


1. Abramowitz, Milton, Stegun, Irene A (1970) "Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables" New York: Dover's Publications, Ninth printing
2. Ahmad M, Khaja IA, Baz A, Alhakami H, and Alhakami W (2020) Particle swarm optimization based highly nonlinear substitution- boxes generation for security applications. *IEEE Access*, 8, 116132_116147
3. Alanazi AS, Munir N, Khan M, Asif M, Hussain I (2021) Cryptanalysis of Novel Image Encryption Scheme Based on Multiple Chaotic Substitution Boxes. *IEEE Access* 9:93795–93802
4. 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. *Multimedia Tools Appl* 80(20):7333–7350
5. Alshammari BM, Guesmi R, Guesmi T, Alsaif H, Alzamil A (2021) Implementing a Symmetric Lightweight Cryptosystem in Highly Constrained IoT Devices by Using a Chaotic S-Box. *Symmetry* 13(129):1–20
6. Asif M, Shah T (2019) BCH Codes with computational approach and its applications in image encryption. *Journal of Intelligent & Fuzzy Systems* 37(3):3925–3939
7. Bhanot R, Hans R (2015) A review and comparative analysis of various encryption algorithms. *International Journal of Security and Its Applications* 9(4):289–306
8. Bhatti S, Safdar R, Shehzad K, Jawad M, Ahmed H (2020) New Cryptographic Scheme with Mellin Transformation. *Pakistan Journal of Multidisciplinary Research* 1(2):259–272
9. Daemen, Joan, and Vincent Rijmen (1999) "Aes proposal: Rijndael, aes algorithm submission, september 3, 1999." URL http://www.nist.gov/CryptoToolKit:37–38
10. Daemen J, Rijmen V (2002) AES the advanced encryption standard. *The design of Rijndael* 1(1):1–238
11. El-Latif AAA, Abd-El-Atty B, Amin M, Iliyasa AM (Dec.2020) Quantum inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Sci Rep* 10(1):116
12. Faheem ZB, Ali A, Khan MA, Ul-Haq ME, and Ahmad W (2020) Highly dispersive substitution box (S-box) design using chaos. *ETRI Journal*, pp. 1–14
13. Farah MAB, Farah A, Farah T (2020) An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dyn* 99(4):3041–3064
14. Farah MAB, Guesmi R, Kachouri A, Samet M (Mar.2020) A new design of cryptosystem based on S-box and chaotic permutation. *Multimedia Tools Appl* 79(6):19129–19150
15. Feng D, Wu W (2000). Design and analysis of block ciphers
16. Firdousi F, Batool SI, Amin M (2019) A novel construction scheme for nonlinear component based on quantum map. *J Theor Phys* 58(11):3871–3898
17. Gao W, Idrees B, Zafar S, and Rashid T (2020) Construction of nonlinear component of block cipher by action of modular group $PSL(2, Z)$ on projective line $PL(GF(28))$. *IEEE Access*, 8 136736_136749
18. Hussain S, Jamal SS, Shah T, and Hussain I (2020) A power associative loop structure for the construction of non-linear components of block cipher, *IEEE Access*, 8 123492_123506
19. Hussain I, Shah T, Gondal MA, Khan WA, Mahmood H (2013) A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Comput Appl* 23(1):97–104
20. Hussain T, Shah MA, Gondal and Khan WA (2011) Construction of Cryptographically Strong 8×8 S-boxes. *World App. Sc. J.*, 13, 11, 2389-2395
21. Kazlauskas K, Kazlauskas J (2009) Key-dependent S-box generation in AES block cipher system. *Informatica* 20(1):23–34
22. Lambic 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

23. 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
24. Liu H, Kadir A, Xu C (2020) Cryptanalysis and constructing S-box based on chaotic map and backtracking. *App Math Comp* 376:1–11
25. Lokenath debnath, Dambaru Bhatta, (2016) “Integral Transforms and their Applications”. CRC press. ISBN 978–1–4200–1091–6, 19
26. Lu Q, Zhu C, Deng X (2020) An efficient image encryption scheme based on the LSS chaotic map and single S-box. *IEEE Access* 8:25664–25678
27. Mar PP, Latt KM (2008) New analysis methods on strict avalanche criterion of S-boxes. *World Academy of Science, Engineering and Technology* 48(150–154):25
28. Matsui M (1994) “Linear cryptanalysis method for DES cipher”, in *Proc. Adv. Cryptol*, Lofthus, Norway, pp 386–397
29. Muhammad Asif et al (2021) "A Novel Image Encryption Technique Based on Mobius Transformation." Computational Intelligence and Neuroscience 2021
30. Patro KAK, Soni A, Netam PK, Acharya B (2020) Multiple grayscale image encryption using cross-coupled chaotic maps. *Journal of Information Security and Applications* 52:102470
31. Pieprzyk J, Finkelstein G (1988) Towards effective nonlinear cryptosystem design. *IEE Proceedings Part E Computers and Digital Techniques* 135(6):325–335
32. Pub, F. I. P. S. (1999). Data encryption standard (des). FIPS PUB, 46–3
33. Saha M (2017) Application of Laplace-Mellin transform for cryptography. *Rai Journal of Technology Research & Innovation* 5(1):12–17
34. Santana YC (2014) “A Cryptographic Scheme OfMellin Transform,” arXiv preprint arXiv: 1401.1232
35. Shafique A (2020) A new algorithm for the construction of substitution box by using chaotic map. *Eur Phys J Plus* 135(2):1–13
36. Shannon CE (1949) Communication theory of secrecy systems. *TBell Syst. Tech. J* 28(4):656–715
37. Siddiqui N, Khalid H, Murtaza F, Ehatisham-Ul-Haq M, Azam MA (2020) A novel algebraic technique for design of computational substitution-boxes using action of matrices on galois field. *IEEE Access* 8:197630–197643
38. Siddiqui N, Naseer A, Ehatisham-ul-Haq MA (2021) Novel Scheme of Substitution-Box Design Based on Modified Pascal’s Triangle and Elliptic Curve. *Wireless Pers Commun* 116(20):3015–3030
39. Tian Y, Lu Z (Nov.2017) Chaotic S-box: Intertwining logistic map and bacterial foraging optimization. *Math Problems Eng* 2017:1–11
40. Tsafack N, Kengne J, Abd-El-Atty B, Ilyasu AM, Hirota K, El-Latif A (2020) Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. *Inf Sci* 515:191–217
41. Webster A, and Tavares S (1986) “On the design of S-boxes,” in *Advances in Cryptology: Proc. of Crypto’85 Lecture Notes in Computer Science*, 523–534
42. Zahid AH, Al-Solami E, Ahmad M (2020) A novel modular approach based substitution-box design for image encryption. *IEEE Access* 8:150326–150340
43. Zhang T, Chen CP, Chen L, Xu X, Hu B (2018) Design of highly nonlinear substitution boxes based on I-Ching operators. *IEEE Trans Cybern* 48(12):3349–3358
44. Zhu D, Tong X, Zhang M, Wang Z (2020) A new S-box generation method and advanced design based on combined chaotic system. *Symmetry* 12(12):2087
45. Zhang YQ, Hao J-L, and Wang X-Y (2020) “An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map,” *IEEE Access*, 8 54175_54188

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

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Authors and Affiliations

Abid Mahboob¹ · Imran Siddique²  · Muhammad Asif³ · Muhammad Nadeem⁴ · Aysha Saleem⁴

Abid Mahboob
abid.mahboob@ue.edu.pk

Muhammad Asif
muhammad.asif@math.qau.edu.pk

Muhammad Nadeem
muhammadnadeem4464647@gmail.com

Aysha Saleem
ayeshasaleemch@gmail.com

¹ Department of Mathematics, Division of Science and Technology, University of Education, Lahore, Pakistan

² Department of Mathematics, University of Management and Technology, Lahore 54770, Pakistan

³ Department of Mathematics, University of Management and Technology, Sialkot Campus, Pakistan

⁴ Department of Mathematics, University of Education, Vehari Campus, Pakistan