Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 5, 2026

THE HIDING OF IMAGE DATA USING S-BOXES BASED ON LINEAR FRACTIONAL TRANSFORMATION

[1]Muhammad Asif
[1]Department of Mathematics, University of Management and Technology, Sialkot Campus, Pakistan
[1]muhammad.asif@math.qau.edu.pk

DOI:-

Keywords
Substitution Box, Mobius transformation, Galois Field, MATLAB

Article History
Received: 12 March 2026
Accepted: 11 April 2026
Published: 12 May2026

Corresponding Author: *

Abstract
Digital image divulgence is being practiced as an indispensable approach to information channeling across the board. The credibility of images in the course of conveyance has now become a crucial assignment to work upon. Thereupon, significantly more surveillance has been devoted to contriving the non-linear component acknowledged as the substitution box (S-box), which possesses the caliber to outlast against unauthorized intrusion. The suggested piece of work comprises two portions; the first part proposes a technique to generate a secured non-linear component of block cipher (S-box) underpinning both the Galois field and the Mobius transformation. Besides, the elements of (28) created via fastidious kinds of primitive irreducible elements are practiced for the realization of Mobius transformation. In the other portion, applications of the S-box are applied to digital image encryption centered on the Advanced Encryption Standard (AES) in MATLAB. Ultimately, the competence of the designed S-box is scrutinized through bringing into efficacious action of multiple procedures from literature to wit, strict avalanche criterion, nonlinearity, linear approximation probability, Histogram analysis, bit independence criterion, and differential approximation probability."

1. Introduction

Multifold novel options for the purport and presentation crystallized as digital data are delivered owing to the blistering raise in international networking. Digital data comprising audio, video, images, electronic libraries, electronic advertising, web designing, and digital repositories necessitates maximum security inasmuch as a smooth approach to the data. Secure communication can further be categorized into three main categories, which include cryptography, watermarking, and steganography [1]. Through the exercise of non-identical methods, the two methods fixate at length on the basic purpose, which is to arcane the actual data.

Cryptology dole out special traditions of using encryption capabilities to provide security of information. Joan Daemen and Vincent, the Belgium cryptographers' proposed encryption standard (AES) algorithm [2]. As Advanced encryption standard reserve the power of puissant capability to stand against attacks [3]. Likewise, in many algorithms, S-box depict individual nonlinear component in AES to establish confusion in the data and ultimately play a dynamic purpose in their security. S-box plays a primary role to produce confusion in the course of encryption to dispense more security of confidential information [4- 5]. The strength of the cipher is directly proportional to the level of confusion produced in the cipher text. As a result, the cryptographic strength of a block cipher using an S-Box is dependent on the cryptographic strength of that S-Box [6]. The chief utilization of image processing is pioneered in military communication, forensic, robotics, intelligent systems, etc. Different encryption techniques [13-27] are applied to secure the text and image data. Here, we will administer the modified AES algorithm on an image encryption with the help of MATLAB software.

The inspired work comprises five parts. The first section reviews the principles of the AES algorithm, whilst the second portion describes the construction of a substitution box using Mobius transformation. In the third part, comparison between the potency of generated substitution boxes and well-known S-boxes will take place through cryptographic analysis. The fourth section is to practice the applications of S-box generated through Mobius transformation in image encryption. Lastly, the conclusion of the paper is discussed in portion five.

2. AES Algorithm Principles

Advanced Encryption Standard, also known as Rijndael algorithm [7], was issued by the National Institute of Standards and Technology (NIST) in 2000. It is one of the block cipher encryption algorithms. The advanced encryption standard (AES) specifies a Federal Information Processing Standards publication (FIPS) approved cryptographic algorithm that can be utilized to secure electronic data [8].

The AES encryption system is symmetric in group, counting on the key length, sorted into three kinds: 128-bits, 196-bits and 256-bits.

This categorization is done on the basic of key practices for encryption and decryption in AES. The security degree is umpired via key size, as the size of key increases the level of protection is amplified. In the three key lengths of the AES algorithm, a 128-bits key length is preferred. The AES algorithm is round oriented, and under the key length of 128-bits, 10 iterative computations (rounds) in the internal algorithm transpire. AES permit data length of 128 bits, which can be divided into four blocks of the main process. These blocks works on a set of data units and are organized in a matrix of 4 × 4 [9].

For the sake of encryption process, each iterative round comprises four steps:

- Substitute byte / Substitution Box
- Shift rows
- Mix column
- Add round-key

In the inspired work, modifications in AES iterative steps take place. The key to be utilized in the image processing is distinctive in comparison to the standard AES key. Besides, ten different s-boxes are used for ten iterative rounds

through which we can obtain maximum data security. While the decryption process is the reverse process of the encryption,

There are number of rounds present of for keys and blocks in the algorithm. The number of rounds depends on the length of key use for Encryption and Decryption.

Table 1: ***Key Block – Round Combinations***

#	Key length	Block size (Nb words)	Number of Round
128-bits	4	4	10
196-bits	6	4	12
256-bits	8	4	14

Pertaining such type of design thought, the data to be encrypted is revealed in AES algorithm while the key dwell to vary. The key length and block size determine the counts of iteration rounds to take place during the process. AES encryption and decryption is illustrated through Fig 1.

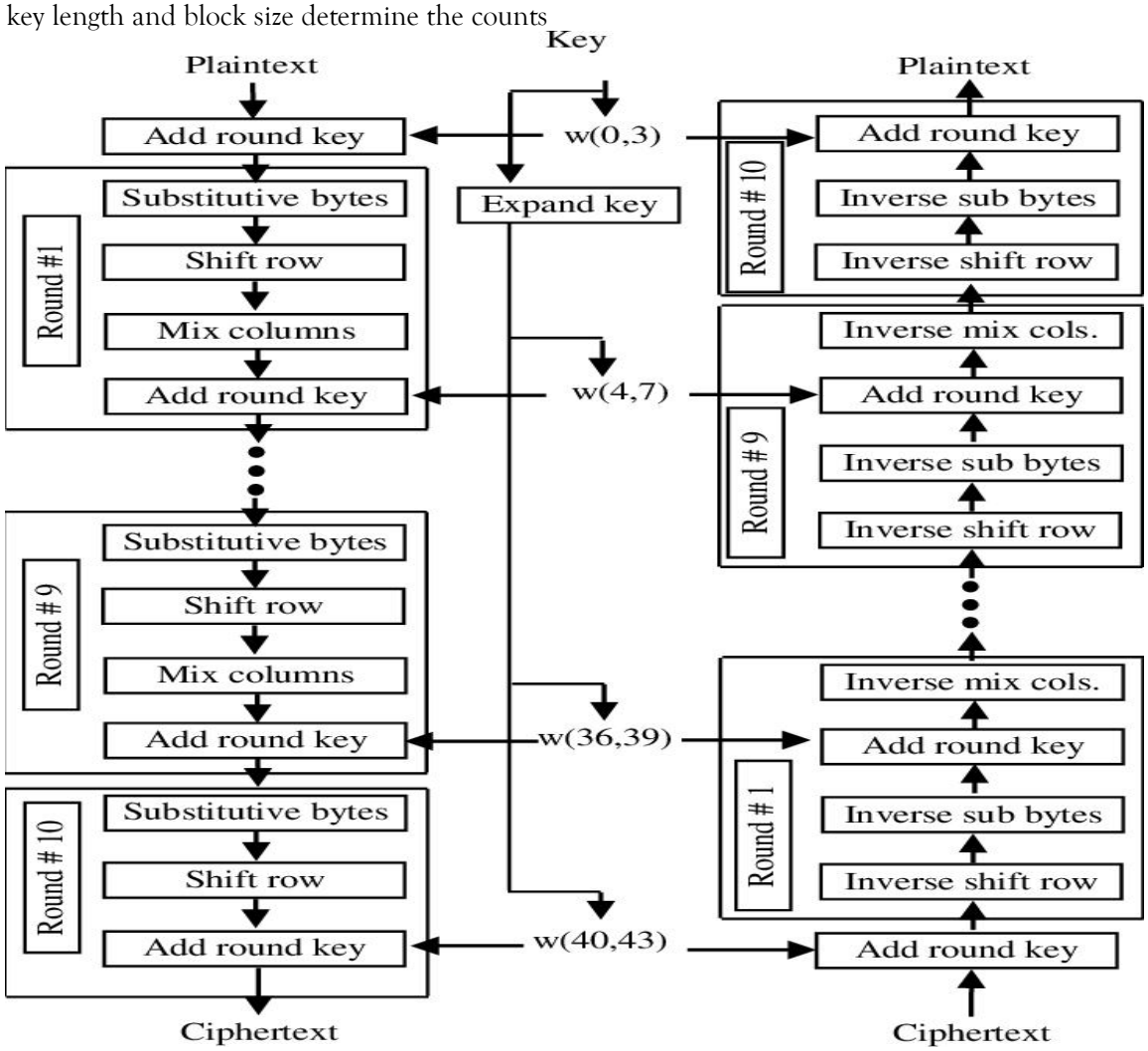


Fig 1: Process of encryption and decryption in AES

3. Algorithm for construction of S-box on Galois Field

The building of an s-box is commenced using action of $PGL\ (2, GF(2^8))$on $GF(2^8)$, where latter is a field of order 256. An exceptional set up of Mobius transformation (LFT) is employed and its applications on preferred Galois field. The algebraic structure of Mobius Transformation is given below,

$$T:\ PGL\ (2, GF(2^8))\ \times GF(2^8)\ \rightarrow GF(2^8)$$

$$T(t) = \frac{(a(t)+b)}{(c(t)+d)}$$

$$where\ a.d - b.c \neq 0\ and\ t, a, b, c, d \in GF(2^8).$$

The output secured from $T(t)$ are segments of Galois field to constitute the s-box.

The functioning on Galois field of order 256 will transpire through calculating elements of our Galois field. In order to evaluate the values of ( ) , its denominator and numerator must be managed discretely after utilizing values from 0 to 255 of t, a, b, c, d into binary form. To make the procedure fewer knotty, the binary form is represented into polynomial form. In view of Table 2, the values obtained from $a(t) + b$ and $c(t) + d$ the numerator and denominator respectively are altered with corresponding binary values which are displayed as the power of m' .

Referring $'m'$ is the primitive root or primitive element of the particular primitive irreducible polynomial written below.

$$p(x) = x^8 + x^4 + x^3 + x^2 + 1 \quad \ldots (1.1)$$

$$p(m) = m^8 + m^4 + m^3 + m^2 + 1 = 0 \ldots (1.2)$$

The peculiar polynomial $P(m)$ is employed to calculate multiple segments of $GF(2^8)$.

The substitution box can be generated by following the steps given below,

STEP I: Consider the Galois Field $GF(2^8)$.

STEP II: Calculate the elements of Galois Field by making use of primitive irreducible polynomial.

STEP III: Convert the elements into both binary form and decimal form.

STEP IV: Make use of the Mobius transformation

$$T(t) = \frac{a(t)+b}{c(t)+d}$$

by selecting different values of 't' and a, b, c, d from 0 -255.

STEP V: Generate elements of S-box by utilizing the converted decimals.

Below is explained the procedure through a table to generate elements of Galois field in *table* 2 and to calculate entries of substitution box in *table* 3

Table 2: *Elements of Galois Extension Field of order 256*

$GF(2^8)$	*Polynomials* $P(x)$	*Binary form*	*Decimal form*
0	0	00000000	0
m	m	00000010	02
m^2	m^2	00000100	04
m^3	m^3	00001000	08
m^4	m^4	00010000	16
m^5	m^5	00100000	32
m^6	m^6	01000000	64
m^7	m^7	10000000	128

m^8	$m^4 + m^3 + m^2 + 1$	00011101	29
m^9	$m^5 + m^4 + m^3 + m$	00111010	58
m^{10}	$m^6 + m^5 + m^4 + m^2$	01110100	116
m^{11}	$m^7 + m^6 + m^5 + m^3$	11101000	232
m^{12}	$m^7 + m^6 + m^3 + m^2 + 1$	11001101	205
m^{13}	$m^7 + m^2 + m + 1$	10000111	135
m^{14}	$m^4 + m + 1$	00010011	19
m^{254}	$m^7 + m^3 + m^2 + m$	10001110	142
m^{255}	1	00000001	01

Table: 3: *Construction Of Transformed Substitution Box*

GF( ): (0-255)	Decimal Form	$T(t) = \frac{199(t)+67}{83(t)+243}$	Utilizing Table	Segments of S-box
00000000	0	67/243	$m^{98}/m^{233} = m^{120}$	59
00000001	1	133/163	$m^{128}/m^{91} = m^{37}$	74
00000010	2	209/153	$m^{161}/m^{68} = m^{182}$	182
00000011	3	166/123	$m^{207}/m^{172} = m^{35}$	156
00000100	4	95/63	$m^{64}/m^{166} = m^{153}$	146
00000101	5	19/73	$m^{14}/m^{152} = m^{117}$	237
00000110	6	97/57	$m^{66}/m^{154} = m^{167}$	126
00000111	7	109/206	$m^{133}/m^{111} = m^{22}$	234
00001000	8	123/139	$m^{172}/m^{237} = m^{190}$	174

11111110	254	63/27	$m^{42}/m^{145} = m^{152}$	73
11111111	255	218/188	$m^{115}/m^{55} = m^{60}$	185

Hereunder, Substitution box is evaluated and inscribed ensuing the homogeneous procedure.

Table4: ***Substitution-Box 1***

0	1	2	3	4	5	6	7	8	9	10	A	B	C	D	E	F
1	134	63	113	62	37	153	244	55	236	126	138	59	19	151	231	184
2	10	170	226	172	89	98	96	189	161	146	69	226	201	117	75	108
3	45	209	139	110	18	127	41	221	163	185	193	11	214	24	31	13
4	206	89	204	12	115	25	40	106	241	0	113	170	124	205	179	77
5	80	87	85	189	41	19	162	92	48	69	98	194	03	239	115	07
6	19	115	163	105	198	223	68	117	148	105	89	172	186	47	116	57
7	211	217	15	82	212	117	207	132	57	184	248	63	27	26	13	164
8	85	224	88	147	206	47	27	106	229	192	255	22	52	67	180	36
9	165	169	121	151	110	71	204	251	68	107	210	167	170	240	31	45
10	152	156	154	60	167	207	51	51	180	105	10	87	173	97	140	251
A	60	23	32	63	175	252	234	39	54	171	167	183	213	131	28	61
B	238	95	184	98	58	142	255	241	39	215	203	86	116	107	169	129
C	249	37	50	83	83	60	168	120	34	137	198	100	35	154	238	254
D	199	241	125	22	135	251	08	234	200	126	163	50	215	178	209	90
E	112	148	107	58	25	72	198	173	124	112	180	67	214	48	91	9
F	165	115	04	177	209	37	95	230	160	89	24	135	202	49	92	210

Table5: ***Substitution-Box 2***

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**A**	**B**	**C**	**D**	**E**	**F**
1	130	217	141	247	202	24	181	246	162	100	215	240	68	249	187	254
2	197	47	59	140	171	155	210	221	205	69	34	156	63	253	129	118
3	172	01	154	198	206	251	185	20	220	01	153	143	200	117	57	91
4	143	208	212	240	238	116	43	186	99	246	53	204	168	230	174	231

5	127	117	198	08	13	193	64	221	24	199	39	50	112	21	101	250
6	05	228	103	02	24	27	131	143	51	243	99	42	155	28	78	172
7	144	155	47	116	137	109	90	14	254	40	231	105	170	115	10	237
8	31	23	123	76	105	252	23	202	140	210	68	189	64	35	127	40
9	221	151	45	217	42	133	127	211	69	53	44	155	240	112	141	197
10	168	124	63	232	237	174	143	66	07	154	151	126	120	84	252	217
A	208	175	17	253	192	71	255	114	115	82	48	223	189	154	111	18
B	96	183	107	86	07	139	245	150	156	36	30	236	89	105	10	232
C	51	236	162	241	139	217	235	176	144	246	183	138	22	87	212	27
D	47	123	251	03	16	201	88	73	133	120	67	200	224	205	151	202
E	238	150	109	222	12	65	58	223	24	52	163	238	249	64	55	226
F	38	18	212	125	68	71	165	73	11	38	00	122	111	134	54	09

Table 6: *Substitution-Box 3*

0	1	2	3	4	5	6	7	8	9	10	A	B	C	D	E	F
1	244	42	222	112	244	71	84	244	54	244	101	244	04	90	91	59
2	101	33	138	81	09	237	197	33	221	120	198	59	94	192	77	191
3	152	72	198	33	143	28	77	98	240	206	106	168	132	117	17	246
4	180	29	128	67	233	165	22	23	68	255	244	104	244	34	241	35
5	221	134	22	162	244	229	58	50	243	154	118	232	199	158	80	147
6	20	233	80	238	60	236	241	108	248	42	175	03	132	185	227	80
7	240	180	73	60	138	65	33	208	178	67	18	189	131	182	70	186
8	227	42	203	98	40	245	05	180	122	10	71	107	140	226	100	00
9	61	51	243	64	168	252	158	185	31	255	46	231	121	43	65	34
10	123	130	249	99	58	64	61	07	248	137	187	22	122	132	179	80
A	154	128	35	119	114	46	75	163	45	218	130	57	106	249	151	63
B	175	149	241	230	249	144	127	135	240	129	82	121	33	42	40	148

C	105	201	99	180	184	100	38	174	219	127	218	218	55	251	21	13
D	181	111	176	239	77	163	83	50	13	108	182	69	150	118	120	57
E	109	202	166	46	207	116	95	147	255	16	86	183	251	30	141	33
F	241	101	134	184	126	01	239	25	189	115	05	222	50	04	79	197

Table 7: *Substitution-Box 4*

0	1	2	3	4	5	6	7	8	9	10	A	B	C	D	E	F
1	56	116	197	40	184	232	181	14	97	67	207	64	144	120	57	223
2	201	169	188	155	218	42	143	252	74	36	90	159	234	93	144	28
3	63	219	202	151	189	29	165	70	74	129	229	212	198	162	251	83
4	22	26	41	85	240	103	202	126	25	171	105	253	185	226	220	146
5	225	243	188	191	139	184	42	255	183	218	230	185	179	83	236	63
6	66	39	14	45	75	80	107	199	183	31	47	172	194	194	42	243
7	148	50	26	208	116	216	106	141	162	168	246	81	85	246	160	203
8	04	202	254	170	82	127	44	126	170	151	94	148	73	61	217	133
9	70	112	140	47	175	254	36	215	161	187	212	135	86	30	133	00
10	48	188	43	189	158	249	58	09	122	152	73	176	25	24	229	11
A	255	174	236	162	117	248	101	209	51	56	54	166	67	41	167	242
B	140	54	173	180	153	199	27	77	159	101	175	60	209	141	166	242
C	206	190	04	71	36	29	05	218	81	86	108	41	68	219	60	182
D	89	156	238	38	195	109	181	231	170	60	180	46	38	22	114	110
E	225	75	106	98	109	73	54	18	50	130	48	71	72	123	210	187
F	196	254	87	238	183	233	126	63	190	235	32	158	228	02	220	241

Table 8: *Substitution-Box 5*

0	1	2	3	4	5	6	7	8	9	10	A	B	C	D	E	F
1	244	252	227	87	42	36	137	82	05	134	195	238	209	223	220	52
2	134	249	147	36	79	74	228	01	09	43	106	96	239	181	167	01
3	07	107	68	173	66	167	228	07	35	29	81	247	14	156	07	194

4	249	114	180	165	183	51	47	235	60	207	121	33	19	74	83	160
5	71	231	139	29	18	216	81	136	05	200	162	243	101	22	114	97
6	03	133	52	77	175	154	07	158	48	67	227	169	124	23	64	07
7	239	155	255	196	156	190	145	177	75	147	206	121	102	146	150	23
8	86	236	21	174	221	04	95	37	174	50	12	128	185	207	117	226
9	171	135	201	116	194	82	235	13	214	218	129	82	179	79	109	35
10	252	187	99	78	143	45	71	00	140	226	34	12	220	06	200	81
A	64	219	91	92	243	227	73	32	17	78	50	96	57	86	174	172
B	30	211	209	236	32	117	118	138	178	95	74	37	119	24	204	84
C	93	156	159	21	179	78	127	196	46	38	53	90	197	73	86	63
D	11	191	186	82	180	154	220	217	253	11	230	58	194	125	237	194
E	10	244	139	128	145	150	69	174	31	167	57	244	112	244	176	33
F	194	74	24	09	189	73	96	59	77	249	112	72	166	33	18	64

Table 9: *Substitution-Box 6*

0	1	2	3	4	5	6	7	8	9	10	A	B	C	D	E	F
1	59	151	217	204	189	11	191	208	186	78	58	25	236	94	238	119
2	74	208	94	05	35	128	03	150	105	188	03	145	25	86	139	191
3	182	252	204	207	89	49	78	134	38	82	18	196	16	168	180	29
4	156	105	222	170	117	58	241	194	39	153	25	50	232	226	187	139
5	146	55	59	52	25	89	206	74	196	227	140	165	249	243	173	132
6	237	31	153	180	205	12	81	57	11	17	162	86	194	107	189	63
7	126	215	159	166	95	52	41	212	111	180	234	109	139	158	245	56
8	234	199	117	111	164	136	213	253	122	33	115	229	73	10	193	134
9	174	73	129	125	200	64	94	185	216	86	182	155	68	22	142	154
10	136	205	176	138	147	238	128	45	173	100	168	89	248	75	38	51
A	181	154	253	145	12	76	98	231	125	141	242	230	105	173	88	153

B	09	88	60	81	51	00	105	191	20	150	225	152	30	43	181	42
C	162	01	31	72	190	01	81	123	100	101	137	48	212	01	124	187
D	196	91	41	109	80	164	10	121	63	213	19	118	175	40	113	03
E	70	220	34	123	200	152	163	12	208	197	101	78	43	106	242	73
F	40	99	67	35	27	229	36	99	200	150	48	197	203	48	253	185

Table 10: *Substitution Box 7*

0	1	2	3	4	5	6	7	8	9	10	A	B	C	D	E	F
1	03	134	16	152	210	133	104	50	144	181	28	38	53	146	51	130
2	78	20	131	228	218	74	56	02	187	229	126	116	114	24	190	237
3	244	60	234	193	26	64	139	173	95	210	244	20	244	222	161	77
4	59	28	108	151	104	66	38	12	80	163	87	10	121	96	186	213
5	75	201	125	214	235	29	77	223	126	96	227	09	174	107	190	188
6	105	139	236	87	234	234	108	00	209	37	21	157	18	158	82	104
7	210	234	155	236	165	57	138	89	130	86	25	200	78	205	220	162
8	246	223	138	76	250	209	138	199	199	10	204	33	89	237	129	109
9	52	03	208	99	168	46	124	185	248	104	23	37	70	100	76	67
10	222	129	133	35	116	148	126	13	52	219	225	68	97	160	41	72
A	68	176	149	43	142	172	190	197	23	211	105	196	109	111	90	164
B	146	93	170	99	216	138	161	237	92	09	164	32	201	73	155	41
C	46	104	131	88	149	41	123	166	100	109	176	104	168	40	137	94
D	142	214	48	107	28	227	103	139	28	210	86	113	207	51	209	138
E	102	62	30	88	80	229	162	14	84	183	92	171	52	112	222	246
F	228	150	167	56	151	95	254	141	64	67	93	192	182	234	101	111

Table 11: *Substitution Box 8*

0	1	2	3	4	5	6	7	8	9	10	A	B	C	D	E	F
1	253	82	26	41	71	00	201	43	02	114	186	153	111	192	215	82
2	125	252	145	215	149	06	101	221	148	167	115	122	46	83	160	42

3	44	189	108	59	205	223	208	45	31	80	90	123	236	170	47	129
4	190	40	240	52	83	198	51	238	146	10	210	140	115	104	141	89
5	03	120	35	225	153	177	171	99	08	63	70	154	229	104	29	205
6	225	09	195	161	221	50	04	192	240	156	109	137	215	35	74	110
7	33	238	119	126	198	35	135	236	153	127	187	215	165	68	255	154
8	41	91	118	166	253	56	146	239	110	166	58	106	139	52	223	248
9	107	226	216	79	229	165	200	135	151	25	162	228	41	122	29	197
10	87	237	103	215	03	193	162	08	159	108	44	193	17	43	86	134
A	33	193	41	59	85	247	07	163	151	181	167	143	247	153	119	251
B	24	215	125	197	91	187	60	223	64	173	196	128	184	155	209	218
C	10	01	156	53	89	173	62	169	145	159	244	141	210	243	183	225
D	46	72	207	192	168	69	207	24	104	128	254	111	59	247	216	66
E	04	105	25	217	62	20	01	205	102	82	78	218	41	95	128	215
F	11	96	224	181	185	13	152	164	112	147	109	35	74	238	87	94

Table 12: *Substitution Box 9*

0	1	2	3	4	5	6	7	8	9	10	A	B	C	D	E	F
1	42	22	11	155	89	80	59	17	230	00	148	51	89	80	59	34
2	25	00	148	51	154	24	33	74	194	180	225	67	154	24	33	74
3	194	180	225	67	156	66	233	17	163	109	253	35	156	66	233	17
4	223	109	253	35	37	237	169	20	107	183	59	50	37	237	156	20
5	81	06	59	50	172	12	31	97	162	250	136	169	172	12	31	97
6	162	250	136	169	197	147	172	186	188	71	118	248	170	147	172	186
7	238	71	118	248	11	132	70	199	214	72	222	187	11	132	70	199
8	162	72	222	39	14	140	116	72	98	59	153	237	14	140	116	83
9	149	185	153	153	159	146	69	103	120	44	234	153	159	208	09	103
10	120	44	106	13	04	247	250	140	214	162	140	101	04	184	250	140
A	67	163	140	17	186	177	72	222	252	97	91	09	186	177	94	222

B	181	97	91	48	177	90	202	190	226	114	163	48	177	90	202	190
C	226	01	163	200	242	232	32	157	93	104	156	200	249	232	32	157
D	105	104	156	129	151	91	90	55	223	245	211	129	151	91	90	55
E	223	245	211	16	189	118	123	119	24	112	78	16	189	118	123	119
F	24	247	78	94	91	241	140	42	22	11	155	94	91	241	140	03

Table 13: *Substitution Box 10*

0	1	2	3	4	5	6	7	8	9	10	A	B	C	D	E	F
1	104	96	28	117	51	89	50	79	136	183	214	236	247	121	124	104
2	206	99	56	195	57	252	173	107	216	245	55	32	38	174	49	22
3	111	06	164	30	179	119	203	38	180	07	143	12	33	84	158	42
4	249	253	08	183	60	173	243	159	32	19	124	107	106	47	176	93
5	91	192	250	104	66	141	161	123	144	102	05	105	88	05	47	165
6	25	252	251	84	254	82	106	209	71	87	54	172	31	142	166	178
7	78	177	128	62	92	35	82	132	37	141	39	168	161	32	81	243
8	25	202	199	66	09	109	21	151	102	51	11	19	41	234	13	83
9	209	224	146	04	39	60	54	15	178	130	237	145	28	50	197	180
10	68	131	143	45	206	181	155	04	05	75	153	38	14	187	115	191
A	213	230	209	193	06	172	212	245	80	64	177	128	67	71	93	09
B	78	70	189	253	157	168	225	149	02	78	19	22	95	128	154	190
C	223	228	235	00	226	202	203	182	168	28	132	20	132	250	15	25
D	67	224	190	235	248	239	188	144	29	222	179	61	133	176	164	177
E	124	225	94	15	254	119	228	34	238	130	32	230	02	219	196	135
F	177	75	35	105	91	65	250	132	43	13	131	76	141	109	32	140

Above are the ten s-boxes that will be used in the encryption process. Ten iterative rounds will practice ten respective s-boxes.

4. ANALYSIS OF S-BOXES AND ITS COMPARISON

Aforementioned substitution box algorithm will be scrutinized by implementing non-linearity, strict avalanche criterion, Bit independent criterion, linear approximation probability and differential approximation. The quality of as of late created S-boxes is analyzed through different tests. Compare our S-boxes with famous S-boxes counting APA, Skipjack [10], Liu J, Hussain [11] and Residue Prime [12] S-boxes.

Non-linearity:

Non-linearity is the number of bits which must be altered in the truth table of a Boolean function to outstretch at close quarters a¢ ne function. The distance in the middle of the function and all the a¢ ne function is crowned as the nonlinearity of a Boolean function. In order to calculate non-linearity when accounting for the substitution box in Galois Field of order 256 (I: e $GF(2^n)$ where $n = 8$). The non- linearity must hold the condition,

$$N_f = \frac{2^n - 2^{\frac{n}{2}}}{2} = 120$$

From Table 14, it can be seen that the minimum non-linearity of our s-boxes is 101 which is better and impressive than the s-box in [12], Having minimum non-linearity 98.

Table 14: ***Non-Linearity of the S- boxes***

S-Boxes	Non-Linearity
SB 1	104.125
SB 2	105
SB 3	104.25
SB 4	104.125
SB 5	102.375
SB 6	103.125
SB 7	103.625
SB 8	105
SB 9	101
SB 10	102.625

Strict Avalanche Criteria (SAC):

Another kind of criterion for s-box to gauge the potency. While altering the input bits in any cryptographic structure, the commission of the output bits is inspected by this criterion. A refashion in a sole input bit must effectuate changes in half of the output bits. Viz, the function:

$$F: F^n \rightarrow F^n$$

Is uttered to convince SAC if for a change in an input bit $i \in \{1,2,3,\ldots,n\}$the possibility of modification I the output bit $i \in \{1,2,3,\ldots,n\}$is [1].

Looking at the table below, a very clear outcome can be observed. The results of SAC is better as compared to Prime residue [12], skipjack [10] and Liu, also is~ 0.5.

Table 15: ***SAC comparison of the S-boxes***

S-Boxes	SAC/Max value
SB 1	0.617188
SB 2	0.517188

SB 3	0.640625
SB 4	0.609375
SB 5	0.578125
SB 6	0.585938
SB 7	0.601563
SB 8	0.601563
SB 9	0.564063
SB 10	0.59375

Bit Independent Criterion (BIC):

Another kind of basis of s-box to gauge the strength which we depict as yield bits' y and z must be changed individually every time by sole input bit x is given$\forall x, y, z$. Bits autonomous basis is befitting property for cryptographic conspire which was displayed by Webster and Tavares. For the Boolean capacities $f_y; f_z(y \neq z)$ of two particular yield bits of S-box, in the event that the substitution box assemblage bits' independence model,

$f_y \oplus f_z(y \neq z, 1 \leq y, z \leq n)$

must be notably non-linear and come close at hand as possible to satisfy the SAC [18]. The bit's independence can be authenticated by appraising the non-linearity and SAC of $f_y \oplus f_z$.

Analysis BIC from Table 16 represents that the average value from one of our S-boxes is good to the Skipjack [10] , Liu J, Hussain[11] and Residue Prime[12] S-boxes.

Table 16: ***Results for the BIC non-linearity of S-boxes***

S-Boxes	BIC (Max nonlinearity)
SB 1	104.464
SB 2	104.143
SB 3	103.357
SB 4	104.321
SB 5	103.536
SB 6	103.607
SB 7	103.464
SB 8	102.5
SB 9	101.75
SB 10	104.393

Linear Approximation Probability (LP):

Direct guess likelihood is sketched out as the extravagant esteem of difference of an occasion. The coordination of the input bits and yield bits must be equivalent. The Linear Approximation Probability of a substitution box is communicated as,

$$LP = \max_{\phi(x)\phi(y)\neq 0} \left| \frac{Number of x \in X / x.\phi(x) = S(x).\phi(y)}{2^{m}} - \frac{1}{2} \right|$$

where 2 points the quantity of rudiments appertains the created substitution box. As well $\phi(x)$ and $\phi(y)$ represents the input/output masks correspondingly.

at that point we compare the LP of our proposed s-boxes with a few renowned S-boxes. Investigation comparison shows that behavior of S-boxes against direct assaults is superior when comparison to Buildup Prime S-box, to Hussain S-box, APA, Skipjack and Liu J.

Table 17: ***Results of LP***

S-box	SB 1	SB 2	SB 3	SB 4	SB 5	SB 6	SB 7	SB 8	SB 9	SB 10
LP	0.039062	0.0390625	0.0390625	0.0390625	0.0390625	0.0390625	0.0390625	0.0390625	0.0390625	0.0390625

Differential Approximation Probability (DP):

The non-linear constituent amidst encryption of classified data is referred to as the substitution box. This very substitution box bespeaks of differential correspondence.

Δx is weighed as differential for input and Δy differential for output. In order to fashion the surety of differential consistency, at the input level require to distinctive map to an output . To calculate differential consistency, the DP of a demonstrated substitution box can be communicated as:

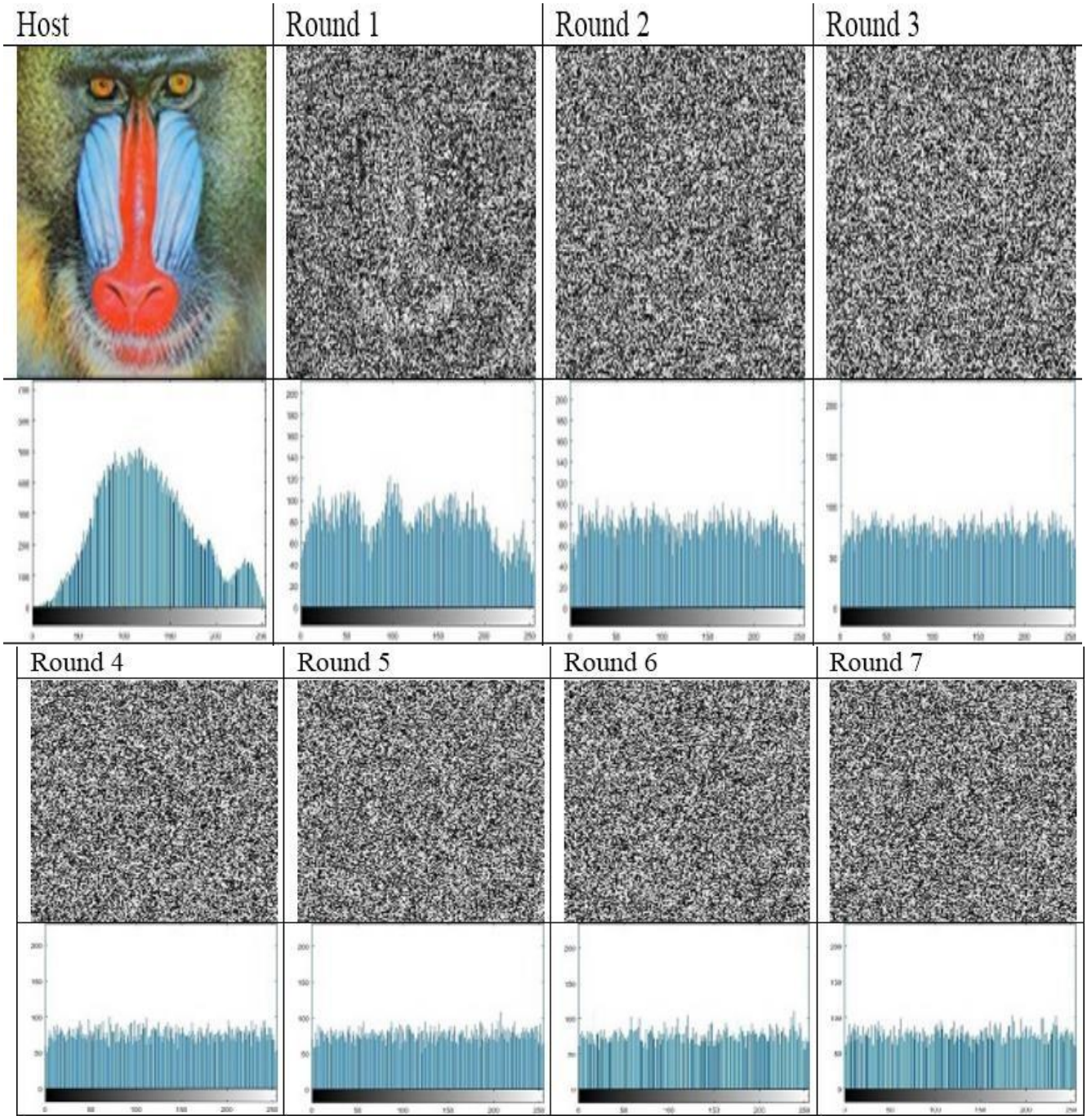
$$DP_{\Delta x \to \Delta y} = \left[\frac{Number of \{x \in S(x) \oplus S(x \oplus \Delta(x) = \Delta y\}}{} \right]$$

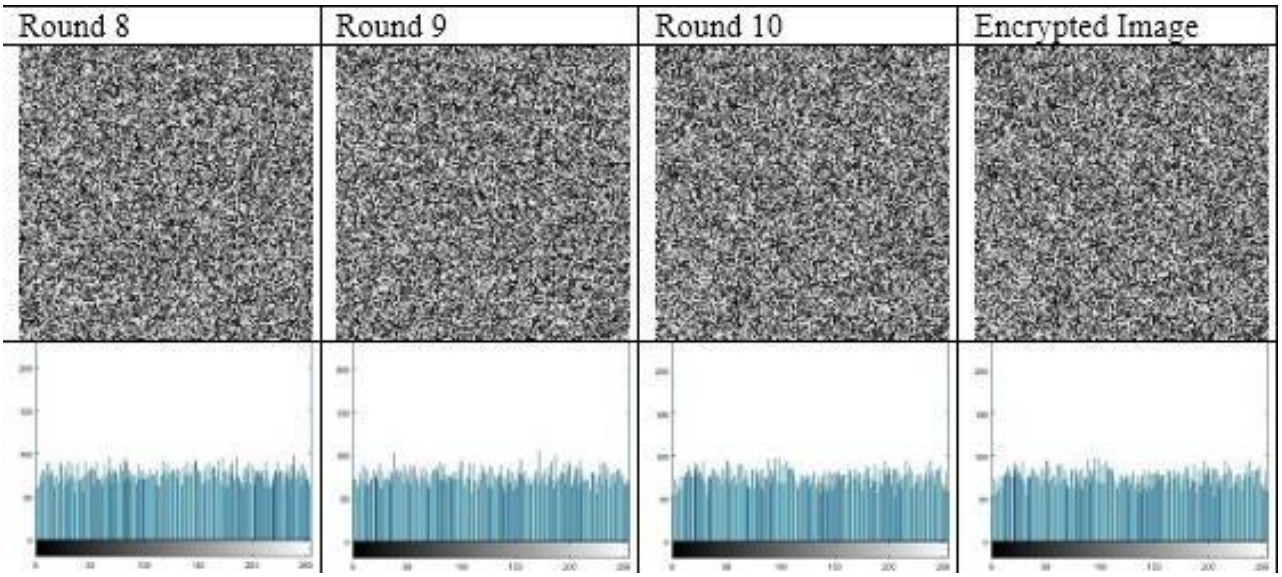
Table 18: ***Differential Approximation Probability***

S-Boxes	DP
SB 1	0.132813
SB 2	0.144531
SB 3	0.132813
SB 4	0.132813
SB 5	0.152344
SB 6	0.128906
SB 7	0.144531
SB 8	0.132813
SB 9	0.160156
SB 10	0.125

5. Applications of S-boxes in Image Encryption

Basically, whereas scrambling the advanced picture based on the AES calculation, we interpret an advanced picture into a double network. The fragments of the network in lines and columns are the facilitates of the point that the picture has appeared on the screen. Ready to cope with the computerized picture based on AES encryption calculation on MATLAB. The original picture and the encrypted image are shown as:





We can definitely see that we were unable to decipher any information from the original image once the image encryption was finished. This allows us to comply with the fact that picture encryption can be achieved using the AES encryption technique. The gray histogram of the image, which shows the frequency of various pixel values, can be used to characterize the overall aspect of the image. The histogram is narrow and concentrated in the middle of the grayscale for a low contrast photograph. Switch between the original image histogram and the encrypted image histogram. The admeasurement of pixels and the pixels themselves have undergone numerous changes. It is clear from the data that picture encryption is significantly impacted by the AES calculation. Additionally, it suggests that this computation had superior security.

Table 19: ***Encryption Analysis***

Correlation		Contrast	Homogeneity	Energy	Entropy
Host image	0.9075	0.4896	0.8009	0.0785	7.6062
Encryption	0.00013	11.2067	0.3849	0.0159	7.8878

6. CONCLUSION

A method has been presented for the development of strong S-box and is established through the utilizing the action of $PGL(G, GF(28\ ))$on the Field $GF(2^8)$. These creatively constructed S-box relates to a special form of Mobius transformation (230 + 33) = (93 + 204). Besides, the advantage of the calculation is that an expansive number of substitution boxes can be delivered through the utilization of distinctive components of Galois field $GF(2^8)$.The fundamental inquiry shows that the representation tool of the modified S-box is straightforward and easy to use for a computer program and equipment application. The modified S-box also incorporates all of the nonlinearity test, bit independence, and tight avalanche criteria, which are more important characteristics for robust substitution boxes to increase perplexity inside the encryption method, in order to investigate the encryption capacity of the modified substitution box. Following the successful development of the S-box, its use will be linked to AES-based image encryption. The foundation of the AES calculation uses the network as the basic unit, and MATLAB offers efficient numerical calculation operations, especially for cluster and matrix computations. Therefore, it is easy to implement the AES-based image encryption in the MATLAB environment. Following the analysis, we further

compared the possibilities for straight estimation, differential estimation and other analyses, and it seems that the constructed S-box is capable of withstanding both straight and differential attacks.

References

[1] Jamal, S. S., Anees, A., Ahmad, M., Khan, M. F., & Hussain, I. (2019). Construction of cryptographic S-Boxes based on mobius transformation and chaotic tent-sine system. *IEEE Access*, *7*, 173273-173285.

[2] Daemen, J., & Rijmen, V. (2002). *The design of Rijndael* (Vol. 2). New York: Springer-verlag.

[3] Zhang, Q., & Ding, Q. (2015, September). Digital image encryption based on advanced encryption standard (aes). In *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)* (pp. 1218-1221). IEEE.

[4] Coppersmith, D. (1994). The Data Encryption Standard (DES) and its strength against attacks. *IBM journal of research and development*, *38*(3), 243-250.

[5] Joan, D., & Vincent, R. Springer Science & Business Media; 2013. *The Design of Rijndael: AES-The Advanced Encryption Standard.[Google Scholar]*.

[7] Li, Y., Wu, W., & Zhang, L. (2011, August). Improved integral attacks on reduced-round CLEFIA block cipher. In *International Workshop on Information Security Applications* (pp. 28-39). Springer, Berlin, Heidelberg.

[8] Deshmukh, P. (2016). An image encryption and decryption using AES algorithm. *International Journal of Scientific & Engineering Research*, *7*(2), 210-213.

[9] AlRababah, A. (2017). Digital Image Encryption Implementations Based on AES Algorithm. *VAWKUM Transactions on Computer Sciences*, *13*(1), 1-9.

[10] Sarfraz, M., Hussain, I., & Ali, F. (2016). Construction of S-Box based on Mobius transformation and increasing its confusion creating ability through invertible function. *International Journal of Computer Science and Information Security*, *14*(2), 187.

[11] Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., & Mahmood, H. (2013). A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*, *23*(1), 97-104.

[12] Hussain, I., Shah, T., Mahmood, H., Gondal, M. A., & Bhatti, U. Y. (2011). Some analysis of S-box based on residue of prime number. *Proc Pak Acad Sci*, *48*(2), 111-115.

[13] Asif, M., Wajiha, S., Askar, S., & Ahmad, H. (2024). A novel scheme for construction of S-box using action of power associative loop and Its applications in text encryption. IEEE Access, 12, 90853-90861.

[14] Bahaddad, A., Asif, M., Ashraf, U. M., Asiri, Y., & Alkhalaf, S. (2024). The security of text data based on cyclic codes over algebraic structure. Thermal Science, 28(6 Part B), 5205-5215.

[15] Mahboob, A., Siddique, I., Asif, M., Nadeem, M., & Saleem, A. (2024). Construction of highly non linear component of block cipher based on mclaurin series and mellin transformation with application in image encryption. Multimedia Tools and Applications, 83(3), 7159-7177.

[16] Mahboob, A., Asif, M., Zulqarnain, R. M., Saddique, I., Ahmad, H., & Askar, S. (2023). A Mathematical Approach for Generating a Highly Non-Linear Substitution Box Using Quadratic Fractional Transformation. Computers, Materials & Continua, 77(2).

[17] Mahboob, A., Asif, M., Zulqarnain, R. M., Siddique, I., Ahmad, H., Askar, S. S., & Pau, G. (2023). An Innovative Technique for Constructing Highly Non-Linear Components of Block Cipher for Data Security against Cyber Attacks. Comput. Syst. Sci. Eng., 47(2), 2547-2562.

[18] Hussain, S., Asif, M., Shah, T., Mahboob, A., & Eldin, S. M. (2023). Redesigning the serpent algorithm by PA-Loop and its image encryption application. IEEE Access, 11, 29698-29710.

[19] Khalid, I., Shah, T., Eldin, S. M., Shah, D., Asif, M., & Saddique, I. (2022). An integrated image encryption

scheme based on elliptic curve. IEEE Access, 11, 5483-5501.

[20] Mahboob, A., Asif, M., Nadeem, M., Saleem, A., Eldin, S. M., & Siddique, I. (2022). A cryptographic scheme for construction of substitution boxes using quantic fractional transformation. IEEE Access, 10, 132908-132916.

[21] Khalid, I., Shah, T., Almarhabi, K. A., Shah, D., Asif, M., & Ashraf, M. U. (2022). The SPN network for digital audio data based on elliptic curve over a finite field. IEEE Access, 10, 127939-127955.

[22] Mahboob, A., Asif, M., Siddique, I., Saleem, A., Nadeem, M., Grzelczyk, D., & Awrejcewicz, J. (2022). A novel construction of substitution box based on polynomial mapped and finite field with image encryption application. IEEE Access, 10, 119244-119258.

[23] Asif, M., Asamoah, J. K. K., Hazzazi, M. M., Alharbi, A. R., Ashraf, M. U., & Alghamdi, A. M. (2022). A novel image encryption technique based on cyclic codes over Galois field. Computational Intelligence and Neuroscience, 2022(1), 1912603.

[24] Khan, M., Jamal, S. S., Hazzazi, M. M., Ali, K. M., Hussain, I., & Asif, M. (2021). An efficient image encryption scheme based on double affine substitution box and chaotic system. Integration, 81, 108-122.

[25] Alanazi, A. S., 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.

[26] Asif, M., Mairaj, S., Saeed, Z., Ashraf, M. U., Jambi, K., & Zulqarnain, R. M. (2021). A novel image encryption technique based on Mobius transformation. Computational intelligence and neuroscience, 2021(1), 1912859.

[27] 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.