Computers, Materials & Continua
DOI:10.32604/cmc.2021.014442
Article

Tech Science Press

Non-Associative Algebra Redesigning Block Cipher with Color Image Encryption

Nazli Sanam[1,*], Asif Ali[1], Tariq Shah[1] and Ghazanfar Farooq[2]

[1]Department of Mathematics, Quaid-i-Azam University, Islamabad, 44000, Pakistan
[2]Department of Computer Science, Quaid-i-Azam University, Islamabad, 44000, Pakistan
[*]Corresponding Author: Nazli Sanam. Email: nazli.sanam@ iiu.edu.pk
Received: 21 September 2020; Accepted: 23 October 2020

Abstract: The substitution box (S-box) is a fundamentally important component of symmetric key cryptosystem. An S-box is a primary source of non-linearity in modern block ciphers, and it resists the linear attack. Various approaches have been adopted to construct S-boxes. S-boxes are commonly constructed over commutative and associative algebraic structures including Galois fields, unitary commutative rings and cyclic and non-cyclic finite groups. In this paper, first a non-associative ring of order 512 is obtained by using computational techniques, and then by this ring a triplet of 8×8 S-boxes is designed. The motivation behind the designing of these S-boxes is to upsurge the robustness and broaden the key space due to non-associative and non-commutative behavior of the algebraic structure under consideration. A novel color image encryption application is anticipated in which initially these 3 S-boxes are being used to produce confusion in three layers of a standard RGB image. However, for the sake of diffusion 3D Arnold chaotic map is used in the proposed encryption scheme. A comparison with some of existing chaos and S-box dependent color image encryption schemes specs the performance results of the anticipated RGB image encryption and observed as approaching the standard prime level.

Keywords: Block cipher; s-box; nonlinearity; color image encryption; 3D chaotic map

1 Introduction

Cryptology is the science dealing with storage and data communication in secure and typically secret form. There are two further subdivisions of cryptology viz; cryptography and cryptanalysis. Cryptography is the method of keeping the information confidentiality using mathematical tools. Cryptanalysis is the art of cracking encrypted information by the means of mathematical and computational devices. It is powerful enough to breach the cryptographic security systems, without accessing the cryptographic key, and it obtains permissions to the content of encrypted communications. Although, both cryptography and cryptanalysis aim at the same target, however the methods and techniques for cryptanalysis have been modified radically throughout the history

of cryptography. Among several the Differential cryptanalysis is frequently used for block ciphers. It is based on the analysis of the concern of specific difference in plaintext pairs on the difference of the consequent cipher text pairs. These differences are used to allocate probabilities to the practicable keys and to find the virtually all possible keys [1].

A repetitive arrangement from the concept of single output Boolean function is the extension of that idea to multiple output Boolean functions, along with denoted as a substitution box (S-box) [2]. The linking between the input and output bits in standings of dimension and exclusivity gives upsurge to several S-boxes. A $k \times l$ S-box is a mapping $\varphi: F_2^k \to F_2^l$ from k input to l output binary bits, whereas, there are 2^k and 2^l number of inputs and outputs, respectively. Formerly, an S-box is just a set of m single output Boolean functions combined in a static order. The dimension of an S-box has an outcome on the exclusiveness of the output and the input, which might disturb the characteristics of S-box. If there is an S-box with dimension $k \times l$, $l < k$ such that the number of input bits is greater than output bits, then certain entries in the S-box unquestionably be repeated; where, an $k \times k$ S-box might whichever contain different entries, where each input is mapped to dissimilar output, or replication of several entries of the S-box. Bijective S-boxes are the ones which are both injective and surjective and they are reversible [3,4]. S-box is the backbone of almost all the cryptosystems, which makes the system nonlinear. In the improvement of symmetric cryptosystems, which are constructed as substitution-permutation networks (DES and AES-like systems), most of the nonlinearity is found in the S-boxes portion of the algorithm. Modest softness in the S-boxes might hence lead to cryptosystems, which are just cracked. S-boxes are used as an exasperating scheme to allow the strength of cryptographic algorithms. So, the design of S-boxes must be cryptographically sound in order to acquire secure cryptosystems [2,3,5]. In contemporary cryptography, the S-boxes are commonly constructed over finite Galois fields ($GF(2^n)$ *for* $2 \leq n \leq 8$). For instance S-boxes; AES, Residue Prime [6], Gray [7], APA [8], S8 AES, Skipjack [9], and Xyi [10].

It is concluded from the literature review that differential attack is the only attack which applies on such S-boxes that are constructed by finite Galois field extension of binary field $\mathbb{Z}_2$. The S-boxes are typically constructed over Galois field and some other commutative and associative structures. In [11], a novel design of S-boxes is introduced over the elements of inverse property loop and the attractive features of the structure are; it is non-associativity and the existence of the inverse of zero elements. These properties increase the availability of the number of structures of IP-Loops. This motivated us to initiate this study to size 8×8 S-boxes through a non-commutative and non-associative ring of order 512. The purpose of these S-boxes is to increase the robustness due to non-associative and non-commutative behavior of the ring structure under consideration and increase 65,536 times the key space. Thus, the obtained S-boxes having significant level of resistance against existing crypt analyses attack.

In last two decades, the notion of chaos has found several applications in various scientific. In Cryptography 8×8 S-boxes are also been produced by using chaotic maps [12,13]. Because of its low non-linearity, they do not get much significance like S-boxes constructed through algebraic structures. Cryptography, which might be supposed to be a branch of arithmetic and technology, has clutched a tremendous deal of consideration and an oversize variety of analysis work, is devoted to the experience of chaos-based cryptologic algorithms [13,14]. The qualities of chaotic maps stand after their use within the smartness of such algorithms. These main options comprise highly sensitive dependence on initial conditions and controlling parameter, ergodicity, randomness, mixing, etc., that are alike the confusion and diffusion properties of Claude Shannon [15]. Precisely, the random-like behavior of the outputs of chaotic maps brands them suitable bases to

be used in cryptographs. A lot of image encryption algorithms are built on chaotic systems, for instance [16–18]. Whereas Liu et al. [19], anticipated a chaos-based color image block encryption scheme using S-box. A novel color image encryption application is foreseen in which primarily newly obtained 3 S-boxes are being castoff to crop confusion in three layers of a standard RGB image. Though, for diffusion 3D Arnold chaotic map is used in the proposed encryption scheme. A comparison with some of current chaos and S-box reliant color image encryption schemes spectacles the performance results of the estimated RGB image encryption and pragmatic as approaching the standard principal level.

2 Fundamentals on Order 512 Non-Associative Algebraic Structure

A left almost semigroup (LA-semigroup) (or AG-groupoid) is a groupoid S satisfying the left invertive law; $(ab)c = (cb)a$ for all, a, b, c in S [20]. It is a structure mid-way amongst a groupoid and a semigroup and it is a generalization of a commutative semigroup. The extended notion of LA-semigroup to LA-group or AG-group is given in [21]. An LA-group is an LA-semigroup with a left identity e in S, such that $ea = a$, for all a in S; and for each a in S, its inverse exists, i.e., there exists a^{-1} such that $aa^{-1} = a^{-1}a = e$. In case of an additive LA-group the left identity would be called left zero element. Accordingly, the notion of a non-associative structure with respect to the two binary operations '+' of LA-group and '·' of LA-semigroup was the natural consequence. Therefore, an LA-ring is a non-empty set R with at least two elements such that $(R, +)$ is an LA-group and $(R, \cdot)$ is an LA-semigroup and both left, and right distributive laws hold. Fundamental properties are given in [22], while in [23] the existence of non-associative LA-rings is documented and a special case of LA-ring is launched.

Using a special LA-ring R_n of order n, a set $R = \sum_{k=0}^{m} u^k R_n$ can be constructed where m is a positive integer and $u^{m+1} = 0$. There are n^{m+1} elements in R of the form $\sum_{k=0}^{m} a_k u^k$, where all a^k belong to R_n. R is a special LA-ring. The operations in R follow from the operations in R_n are defined as: $\sum_{k=0}^{m} a_k u^k + \sum_{k=0}^{m} b_k u^k = \sum_{k=0}^{m} (a_k + b_k) u^k$ and $\sum_{k=0}^{m} a_k u^k \sum_{k=0}^{m} b_k u^k = \sum_{k=0}^{m} c_k u^k$. In R, $\sum_{k=0}^{m} a_k u^k$, $\sum_{k=0}^{m} b_k u^k$, $c_k = \sum_{i+j=k} a_i b_j$. $\sum_{k=0}^{m} a_k u^k$ is a unit in R if and only if a_0 is unit in R_n.

3 For S-Boxes Pairs Generating Algorithm

Take LA-ring $R_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ with identity. Addition and multiplication are defined in Tab. 1.

Table 1: Operations on R_8

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	6	5	0	2	7	4	3	1	0	4	0	2	1	3	7	6	5
1	5	6	1	7	2	3	4	0	1	3	4	2	0	1	5	6	7
2	0	1	2	3	4	5	6	7	2	2	2	2	2	2	2	2	2
3	2	7	3	6	5	1	0	4	3	1	3	2	4	0	7	6	5
4	7	2	4	5	6	0	1	3	4	0	1	2	3	4	5	6	7
5	4	3	5	1	0	2	7	6	5	5	7	2	5	7	6	2	6
6	3	4	6	0	1	7	2	5	6	6	6	2	6	6	2	2	2
7	1	0	7	4	3	6	5	2	7	7	5	2	7	5	6	2	6

Here the element 0 is 2 and the left identity element is 4. Units in R_8 are: $0, 1, 3$, and 4. The set $R = R_8 + uR_8 + u^2R_8$ (with $u^3 = 0$) is a special LA-ring with 512 elements. The left identity element in R is 422. An element $a + bu + cu^2$ is a unit in $R = R_8 + uR_8 + u^2R_8$ if and only if a is a unit in R_8. So, there are 256 units in $R = R_8 + uR_8 + u^2R_8$. The scheme of the S-boxes triplets is based on two substructures of the special LA-ring R. One of the substructures is the sub LA-module $M = \{200, 201, \ldots, 277, 500, 501, \ldots, 577, 600, 601, \ldots, 677, 700, 701, \ldots, 777\}$ of LA-ring R, which is decimal equivalent to $\{128, 129, \ldots, 191, 320, 321, \ldots, 511\}$ and the second is the multiplicative group $U(R) = \{000, 001, \ldots, 077, 100, 101, \ldots, 177, 300, 301, \ldots, 377, 400, 401, \ldots, 477\}$ of unit elements of the ring R which is decimal equivalent to $\{0, 1, \ldots, 127, 192, 193, \ldots, 319\}$. The first one has two operations; addition and scalar multiplication, the last one holds only multiplication. Actions of group $PGL(2, GF(2^8))$ to the Galois field $GF(2^8)$ yield the ultimate S-boxes.

3.1 Case I: Generating S-Boxes Over Sub LA-Module of R-LA-Module R

As M is R-sub LA-module of R-module R, we can define an affine mapping $\theta: M \to M$, $\theta(s) = rs + m$, where $r = 342$ and $m = 653$ are fixed elements in $U(R)$ and M respectively. As the elements of M are 9 binary bits representation, so we define a bijection $\sigma : M \to GF\left(2^8\right)$ by

$$\sigma(x) = \begin{cases} x + 64, & \text{if } 128 \le x \le 191; \\ x - 320, & \text{if } 320 \le x \le 511. \end{cases}$$

Finally, the linear fractional transformation is given as; $\psi: PGL(2, GF(28)) \times GF(28) \to GF(28)$ defined as: $\psi(x) = \frac{ax+b}{cx+d}$, where $a = 158$, $b = 54$, $c = 20$, $d = 92$ in $GF(2^8)$ such that $ad - bc \neq 0$. For the construction of this S-box, the algorithm begins with the sub LA-module M of a special LA-ring R and use of GF(2^8). Eventually, the function. purposes the S-box with the action of $PGL(2, GF(2^8)$ on $GF(2^8)$. The newly constructed S-box, using the suggested algorithm is given in Tab. 2. This is a 16×16 look up table and it can be used to process eight binary bits of data.

Table 2: S-Box 1 designed over LA-sub-module of LA-ring R

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

3.2 Case II: Generating S-Boxes over $U(R)$

We define the inverse and affine linear mappings φ', θ': $U(R) \to U(R)$ by $\varphi'(t) = t - 1$ and $\theta'(t) = r't + m'$, where $r' = 436$ and $m' = 275$ are fixed elements in $U(R)$ and MM respectively. Accordingly, the composition $\theta' \circ \varphi'$: $U(R) \to U(R)$ of mappings is defined by $\theta' \circ \varphi'(t) = (r't + m') - 1$. As the elements of $U(R)$ are 9 binary bits representation, so we define a bijection σ': $U(R) \to GF(2^8)$ by

$$\sigma'(z) = \begin{cases} z, & \text{if } 0 \le z \le 255; \\ R_m + 128, & \text{if } 320 \le z \le 511 \end{cases},$$

R_m is the remainder when divided by 256. So, in the end, the linear fractional transformation is given as; ψ': $PGL(2, GF(2^8)) \times GF(2^8) \to GF(2^8)$, $\psi'(z) = a'z + b'/c'z + d'$, where $a' = 210$, $b' = 17$, $c' = 84$, $d' = 60$ in $GF(2^8)$ such that $a'd' - b'c' \neq 0$. For the construction of this S-box, the algorithm activates with the LA-group $U(R)$ of unit elements in the special LA-ring R and use of Galois field $GF(2^8)$. Ultimately, the function τ' designs the S-box with the action of $PGL(2, GF(2^8))$ on $GF(2^8)$. Tab. 3 shows the new S-box constructed through the proposed algorithm, a 16×16 look up table that can be used to process eight binary bits of data.

Table 3: S-Box 2 designed over LA-group of units in LA-ring R

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

To synthesize another S-box, we take the composition of above generated S-boxes. The S-box obtained by the composition is given by Tab. 4. Fig. 1 illustrates the flow chart for S-boxes pairs generation over the special LA-ring $\boldsymbol{R}$.

4 Key Space Analysis

In case when we consider the special LA-ring $R = R_8 + uR_8 + u^2R_8$, the affine map g: $U(R) \to U(R)$ such that $g(x) = ax + b$ for all x in $U(R)$ results 256 possible choices of the fixed unit element a in $U(R)$ and 256 choices of the element b in M. Hence, we obtained $256 \times 256 = 65{,}536$ possible affine mappings. Accordingly, we get 65,536 number of 9×9 pseudo S-boxes of

dimension 16×16. These 9×9 pseudo S-boxes are transforming into byte based 65,536 vague random sequences by using the bijective maps σ. Thus we are able to get a huge number of 8×8 S-boxes with their diversified strength.

Table 4: S-Box 3 obtained by composition of S-boxes 1,2

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

$$R = \mathbf{M} \cup U(R)$$

$$\Downarrow$$

Define $\theta: \mathbf{M} \to \mathbf{M}$ by $\theta(s) = rs + m$, for fixed $r \in U(R), m \in \mathbf{M}$ and Define $\varphi', \theta': U(R) \to U(R)$ by $\varphi'(s) = s^{-1}$ and $\theta'(s) = rs + m$, for fixed $r \in U(R), m \in \mathbf{M}$

$$\Downarrow$$

Define $\sigma: \theta(\mathbf{M}) = \mathbf{M} \to GF(2^8)$ by

$$\sigma(x) = \begin{cases} x + 64, & if\ 128 \le x \le 191; \\ x - 320, & if\ 320 \le x \le 511 \end{cases}$$

Define $\sigma': \varphi' o \theta'(U(R)) = U(R) \to GF(2^8)$ by $\sigma'^{(x)} = \begin{cases} x, & if\ 0 \le x \le 255; \\ R_m + 128, & if\ 320 \le x \le 511 \end{cases}$

$$\Downarrow$$

Action ψ of $PGL(2, GF(2^8))$ on $Im(\theta) = GF(2^8)$ gives $\psi(z) = \frac{az+b}{cz+d} \in GF(2^8)$

Action ψ' of $PGL(2, GF(2^8))$ on $Im(\varphi' o \theta') = GF(2^8)$ gives $\psi'(z) = \frac{a'z+b'}{c'z+d'} \in GF(2^8)$

$a, b, c, d, a', b', c', d' \in GF(2^8)$ are fixed with $ad - bc \neq 0$ and $a'd' - b'c' \neq 0$

$$\Downarrow$$

End

Figure 1: Flow chart for S-boxes pairs generation over the non-associative ring $\boldsymbol{R}$

The key space is the total number of unlike keys cast-off in the encryption or decryption process. For an efficient cryptosystem, the key space must be sufficiently large to repel brute-force attacks. In the first case of proposed algorithm 256! Number of choices for affine function and from the action of $PGL(2, GF(2^8))$ on $\sigma(U(R)) = GF(2^8)$, we could design 16776960 number of

S-boxes [24]. Though due to step 2 of the algorithm 256 choices for Affine functions could be considered and thus $256 \times (16776960)$ will be the possible choices in computing 8×8 S-boxes. Consequently, combining all possibilities, we have large enough key space to armor contrary to brute force attack.

5 Performance Analyses of S-Boxes

An efficient S-box should satisfy some specific cryptographic criteria; bijectiveness, nonlinearity, outputs bit independence, strict avalanche and linear approximation probability. We device diverse analyses to test their strong suit and standing with respect to few other well-known S-boxes.

5.1 Nonlinearity

The distance between the Boolean function f and the set of all affine linear functions is said to be nonlinearity of f. This means the nonlinearity of a Boolean function f represents the number of bits which changed in the truth table of f to touch the nearby affine function. The upper bound of nonlinearity (NL) is $NL = 2^{n-1} - 2^{\frac{n}{2}-1}$ [10], thus, for $n = 8$, the maximum value of nonlinearity is 120. Followed Tab. 5 that average nonlinearity of S-boxes 1and 2 are 103.25 and 104.75, and better than Prime S-box.

Table 5: Performance Indexes for proposed S-Box

Analysis for S-box 1 and S-box 2	Max.	Min.	Average	Square Deviation	Differential approximation probability (DP)	Linear approximation probability (LP)
Nonlinearity	106	100	**103.25**			
	106	100	**104.75**			
SAC	0.625	0.40625	**0.504883**	**0.0218748**		
	0.59375	0.375	**0.498047**	**0.0216392**		
BIC		98	**103.571**	2.79577		
		96	**102.714**	3.08055		
BIC-SAC	0.476563		**0.500558**	0.0139369		
	0.464844		**0.498535**	0.0155518		
DP			**0.0390625**			
			0.0390625			
LP	164					**0.140625**
	160					**0.132813**

5.2 Strict Avalanche Criteria

The SAC was first familiarized in 1895 by Webster et al. [2]. The SAC constructs on the notions of completeness and avalanche. It is satisfied if, whenever a single bit of input changed, each of the output bits changes with a 0.5 probability that is, while one bit of input is altered, half of its corresponding output bits will change. Tab. 5 shows that the proposed S-box successfully satisfied SAC.

5.3 Bit Independent Criterion

The BIC was also first introduced in [2] which is another required property for any cryptographic methods. Tab. 5 shows the results of BIC analysis of proposed S-box and in the sense of encryption strength; the BIC of the proposed S-box is adequate. Tab. 5 shows that the rank of designed S-box is comparable with S-boxes in literature and its BIC is adequate.

5.4 Linear Approximation Probability

The maximum value of the imbalance of an event is said to be the linear approximation probability. The parity of the input bits selected by the mask G_x is equal to the parity of the output bits selected by the mask G_y. By [25], LP of a given S-box is defined as: $LP = \max_{G_x,G_y\neq 0}\{x \in X|x.G_x = S(x).G_y\}/2^n - \frac{1}{2}, G_x$and G_y is input and output covers, respectively, "X" the set of all possible inputs; and 2^n is the number of elements of X. From Tab. 5, we see that the average value of LP of the proposed S-boxes is 0.132813 and it is appropriate against linear attacks and better from Xyi S-box and S-box on residue of prime numbers.

5.5 Differential Approximation Probability

The differential approximation probability (DP) of S-box is a measure for differential uniformity and is defined as: $DP(\Delta a \rightarrow \Delta b) = \{a \in X|S(a) \oplus S(a \oplus \Delta a) = \Delta b\}/2^m$. This implies, an input differential Δa_i, should uniquely map to an output differentialΔb_i, thus ensuring a uniform mapping probability for each i. The average value of differential approximation probability for proposed S-boxes are 0.140625 and (see Tab. 5), whereas the Tab. 6 shows the comparison of differential approximation probability of new S-box with AES, APA, Gray, S_8 AES, Skipjack, Xyi and residue prime S-boxes and we observed that the results of DP of proposed box are relatively better from skip jack, Xyi, prime and Lui S-boxes. As there are $256 \times (16776960)$ possible S-boxes depending on the choice of defined parameters, so after variety of options one can obtain the best S-boxes having optimal strength against statistical attacks.

Table 6: Comparison of performance indexes of proposed S-Box

S-boxes	Nonlinearity	SAC	BIC–SAC	BIC	DP	LP
AES S-box	112	0.5058	0.504	112.0	0.0156	0.062
APA S-box	112	0.4987	0.499	112.0	0.0156	0.062
Gray S-box	112	0.5058	0.502	112.0	0.0156	0.062
Skipjack S-box	105.7	0.4980	0.499	104.1	0.0468	0.109
Xyi S-box	105	0.5048	0.503	103.7	0.0468	0.156
Residue Prime	99.5	0.5012	0.502	101.7	0.2810	0.132
LuiS-box	105	0.499756	0.500698	104.071	0.0390625	0.128906
Proposed S-box 1	**103.25**	**0.504883**	**0.500558**	**103.571**	**0.0390625**	**0.140625**
Proposed S-box 2	**104.75**	**0.498047**	**0.498535**	**102.714**	**0.0390625**	**0.132813**

6 RGB Image Encryption

The Arnold map is one the most important $2D$ Chaotic map [26,27], specifically in image encryption algorithms. The following equation signifies the $2D$ Arnold cat map. For x_i, y_i in the interval [0,1),

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod 1 \tag{1}$$

The determinant of the matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ is 1. Thus, the map is area preserving. The Eigen values $\lambda_1 = \ln\left(3+\sqrt{5}\right)/2$ and $\lambda_2 = \ln\left(3-\sqrt{5}\right)/2$ of the matrix A represents the two Lyapunov exponents. The positive Lyapunov exponent spectacles the chaotic behavior in Eq. (1) hence its exponential sensitivity to its initial conditions is observed. In [26], the generalized form of Eq. (1) is given as

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod 1 \tag{2}$$

Furthermore, the map of Eq. (2) is transformed to a 3D cat map described as

$$X_{i+1} = \begin{pmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{pmatrix} = A \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix} \bmod 1 \tag{3}$$

where the matrix A is answerable for producing chaotic behavior, here $A = \begin{pmatrix} 3 & 1 & 4 \\ 8 & 3 & 11 \\ 6 & 2 & 9 \end{pmatrix}$.

The general form of matrix A is

$$A = \begin{pmatrix} 1+a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y b_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{pmatrix}$$

In matrix A all a_x, a_y, a_z, b_x, b_y, b_z are considered to be the positive integers. It is trivial to verify that matrix A is area preserving, that is $|A| = 1$. The Eigen values of A are $\lambda_1 = 14.3789, \lambda_2 = 0.4745$ and $\lambda_3 = 0.1466$. As the larger Eigen value is greater than 1, so Eq. (3) shows chaotic behavior and thus holds all the characteristics of chaos. To generate the chaotic sequence X_{i+1}, the initial values used in this work are $x_0 = 0.9557$, $y_0 = 0.3494$ and $z_0 = 0.6789$.

S-boxes are considered as a main part of a block cipher, the only component of a cipher that produces non-linearity and hence surety the resistance against linear and differential attacks. Currently, advancement in techniques of cryptanalysis and in computer technology, which enhances correspondingly support, generating S-boxes of good quality is the subject of core attention. Due to uncertainty in communication and in storage of RGB images, a need for the encryption is preferred. One of the aims of this article is to encrypt RGB images using 3 S-boxes originated by a non-associative structure of LA-ring. For the need of the RGB image encryption each layer is passed through the different 8×8 S-box. In the subsequent step, the $3D$ Arnold cat map is functional not to correlate the adjacent pixel of the image.The image encryption scheme is illustrated below. Following are the steps for encrypting the image: Substitute the S-boxes S_1, S_2 and S_3 in Red, Green and Blue channels of the color image. Thus, instead of a single S-box used for encryption our proposed scheme provides three different S-boxes $S_1, S_2$and S_3. Use the $3D$ Arnold cat map to produce non-correlated behavior between adjacent pixels of the image.

7 Texture Analysis of Image Encryption

Texture is one of the further most significant parameters of a material that enlightens the physical appearance of a material surface except its chromatic character. Texture may be analyzed in diverse approaches but Fourier methodology among these techniques is the most operative. A fascinating analysis, however, is intriguing as it relates to how the human visual system realizes the texture, the first line of the texture, and is extensively used in the segmentation of photograph. Over and done with this method we can calculate 5 diverse characteristics of image which are: Contrast, Homogeneity, Correlation, Energy and Entropy to elucidate texture.

7.1 Energy

Through energy analysis we can measure the energy of an encrypted image which discards the gray-level co-occurrence matrix (GLCM). The energy is defined as the sum of squared components in GLCM and is given as $E = \sum_m \sum_n f^2(m,n)$, where m and n are the image pixels and $p(m,n)$ gives the number of gray-level co-occurrence matrices. Remark that for constant image the energy value is unity.

7.2 Entropy

The entropy is the measure of level of disorder and randomness in a system. The maximal level of randomness makes the image difficult to recognize and the randomness of an image can be amplified by considering its non-linear components which is defined as $H = \sum_{i=0}^{n} f(x_i) \log_b f x_i$, where x_i defines the Histogram calculations.

7.3 Contrast

To differentiate the objects of an image the observer has to contrast it is used. Owed to image encryption process, a robust encryption can be realized from the high level of contrast. This factor is directly linked to the confusion created by the S-box. Mathematically, the contrast is obtained by the formula: $C = \sum_m \sum_n (m-n)^2 f\,(m,n)$.

7.4 Homogeneity

In Homogeneity analysis, the closeness of distributed pixels of Gray Level Co-occurrence Matrix (GLCM) to GLCM is tested. Mathematical equation is $H^* = \sum_m \sum_n f\,(m,n)\,/1 - |m-n|$.

7.5 Correlation

To analyse the adjacent pixel correlation of an image, correlation analysis is performed. Normally, three different types of correlation are performed to ensure the strength of the encrypted image. These are: the horizontal, the vertical, and the diagonal correlation. The following equation shows how to calculate the correlation: $K = (m - \alpha m)(n - \alpha n) f(m,n)/\sigma_m \sigma_n$. For a healthier correlation value we need to achieve the number 1 or -1. Whereas uncorrelated data this figure is round about 0. Tab. 7 realizes that the new encryption algorithm has robust upright cryptographic properties, and succeeds for encryption.

Tab. 8 signifies the entropy of Lena color image. Obviously, the proposed encryption procedure displays opposition to all the well-known attacks. Analyses reveal that the entropy score of our proposed scheme is close to the optimal values. In analogy, the comparison with chaos-based encryption scheme is also provided. Entropy of the proposed scheme is nicer than the rest. In Tab. 9, the result for correlation coefficient of Lena 256×256 color image is presented. Results ensure the potency of the proposed encryption technique. It is apparent from analyses that the

correlation results are up to the mark and can be matched with other chaos-based encryption techniques. Information images transmitting via digital communicating media has great similarity amongst their neighboring pixels. For an incredibly well-connected image the estimated correlation coefficient is ± 1, while for an extra ordinary non-correlated image its values move toward 0. The pixels correlation among original and encrypted Lena image is displayed in Tab. 9. The correlation score shows that the pixels are good non-correlated as its value are more equally 0. Hence, the proposed algorithm gives extra ordinarily de connections the nearby pixels of the encrypted image and meet on hopes of an effective encryption structure.

Table 7: Second order texture analyses for plain and encrypted Lena image

	Plain color components of image			Cipher color components of image		
	Red	Green	Blue	Red	Green	Blue
Contrast	0.445343	0.659896	0.483655	9.96034	10.0962	10.2181
Homogeneity	0.857543	0.831937	0.845328	0.411186	0.404886	0.403524
Entropy	7.27958	7.63153	6.98912	7.99712	7.99725	7.99744
Correlation	0.910667	0.887815	0.804591	0.0516558	0.0379861	0.0239547
Energy	0.135318	0.0838048	0.156122	0.0157684	0.0157087	0.0157107

Table 8: Comparing entropy for Lena (256×256) image

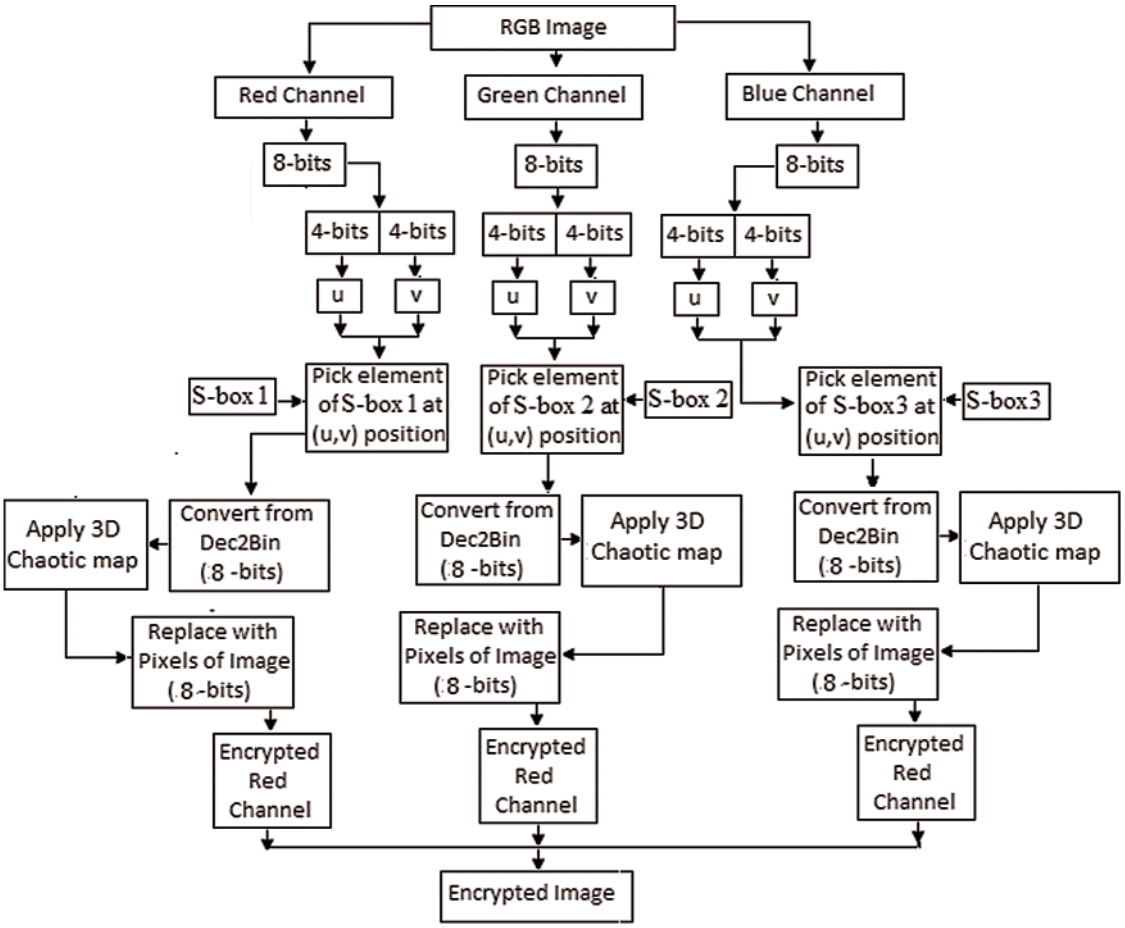
Images	Red	Green	Blue	RGB Image
Proposed	**7.99712**	**7.99725**	**7.99744**	**7.9990**
Ref. [19]	7.9901	7.9898	7.9899	7.9899
Ref. [28]	7.9913	7.9914	7.9916	7.9914
Ref. [29]	7.9808	7.9811	7.9914	7.9844
Ref. [30]	7.9901	7.9912	7.9921	7.9113
Ref. [31]	7.9949	7.9953	7.9942	7.9948

Table 9: Horizontal, vertical and diagonal correlations between different layers of original and encrypted images

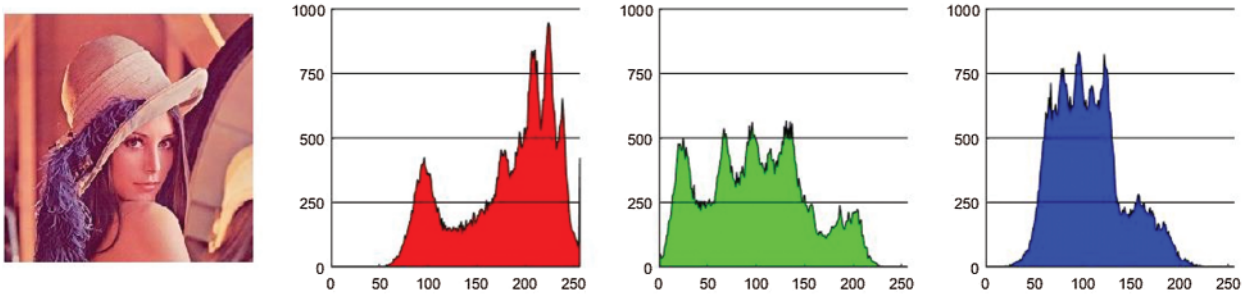
Image	Horizontal			Vertical			Diagonal		
	R	G	B	R	G	B	R	G	B
Plain image	0.9491	0.9175	0.8561	0.9602	0.9528	0.8962	0.9025	0.8984	0.8715
Encrypted image	0.0569	0.0658	−0.0014	0.0036	−0.0180	0.0132	−0.0499	0.0123	−0.0210

Figs. 4–9 show the correlation distribution of horizontally, vertically and diagonally adjacent pixels of a color image. Figs. 4, 6, 8 (a, b, c) signifies the correlation of the adjacent pixels of Lena original image whereas Figs. 5, 7, 9 (a, b, c) looks from the nearby pixels of encrypted image. It is clear from the figure that there is a great dispassion between nearby pixels of the

encrypted image. The approving correlation coefficient is computed for Lena encrypted image and are shown in Tab. 9.



RGB image encryption scheme using S-boxes designed over LA-sub-module of R



(a) (b) (c) (d)

Figure 2: (a) represents Lena original image. (b), (c) and (d) represent the histogram of red(R) green(G) and blue(B) layer of (a)

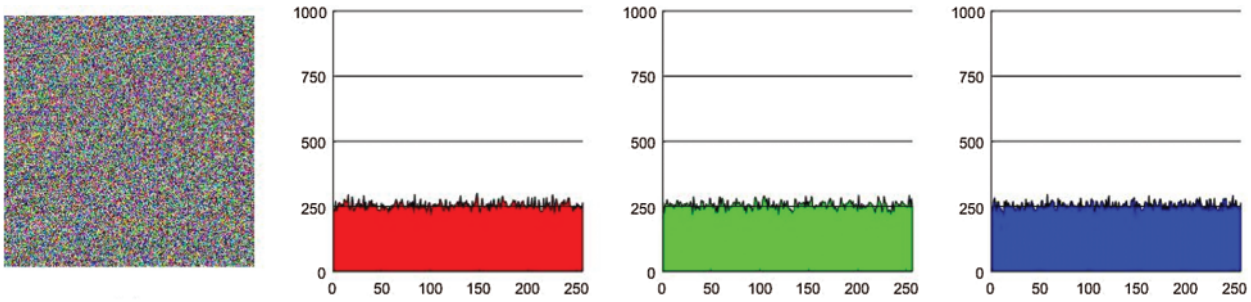


Figure 3: (a) Encrypted Lena image. (b), (c) and (d) show the histogram layers of R, G and B channel of the encrypted image (a)

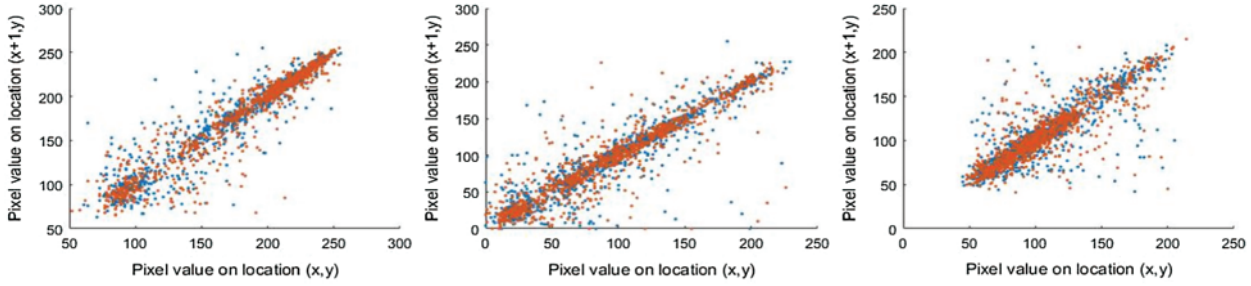


Figure 4: (a–c): represent horizontal correlation pixels for R, G and B layers of original 256×256 Lena image respectively

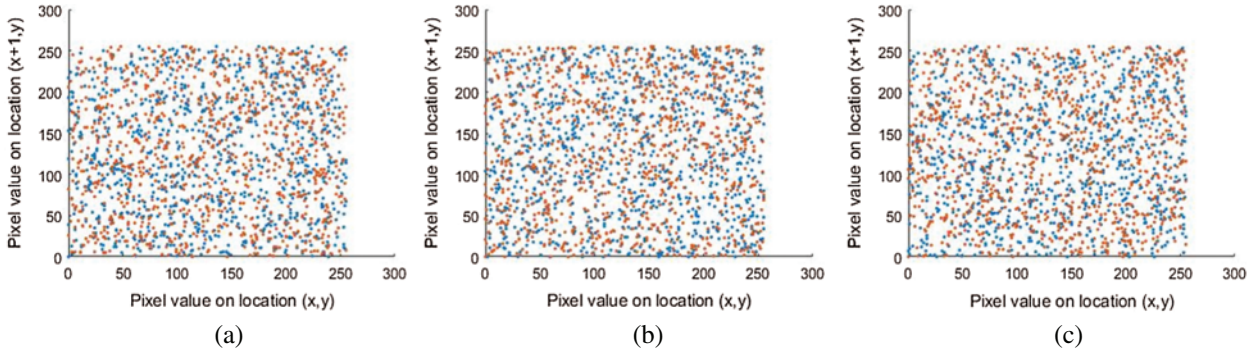


Figure 5: (a–c): Shows the horizontal Correlation pixels for R, G and B channel of encrypted Lena image

8 Analyses of Experimental Work

Experimental analyses of the image encryption technique are given here. A standard Lena image of size $256 \times 256 \times 3$ is chosen for encryption as shown in Fig. 2. Where Fig. 3, represents the encrypted Lena image. Histogram of RGB layers of the original and encrypted image are also

shown in parallel. Tab. 8 enlists the image quality measures of the encrypted and original image using one round encryption by 3 S-boxes and AC 3D map. The performance of the proposed notion is shown in Tab. 9.

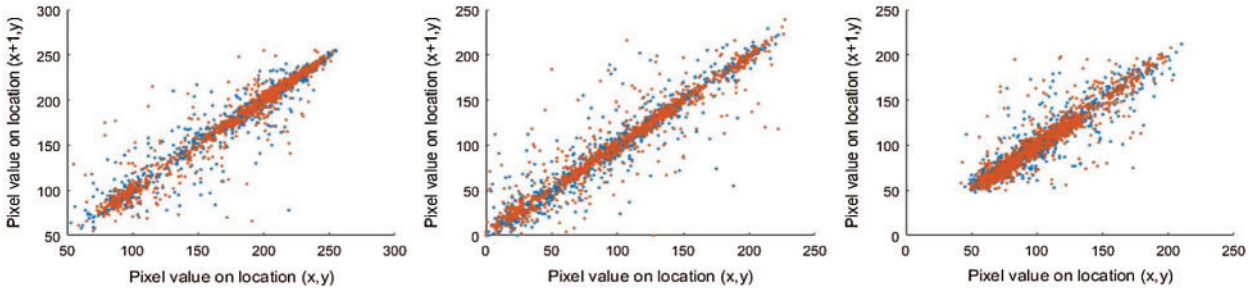


Figure 6: (a–c): represent vertical correlation pixels for R, G and B layers of original 256 × 256 Lena image respectively

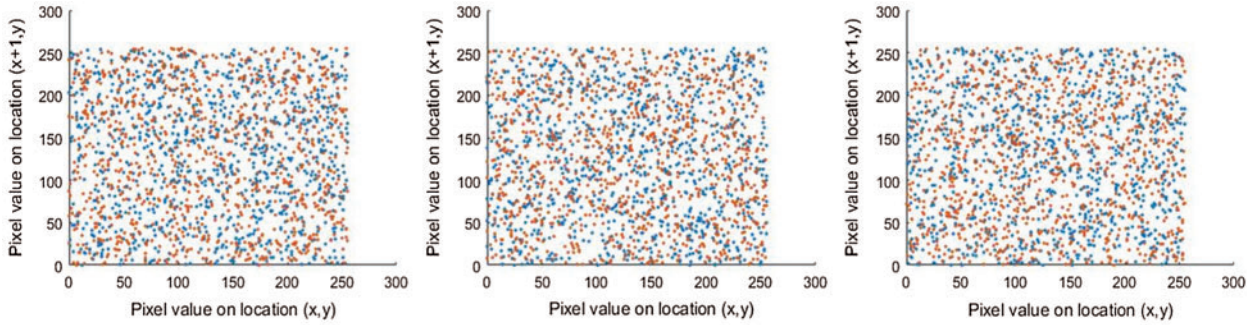


Figure 7: (a–c): shows the vertical correlation pixels for R, G and B channel of encrypted Lena image

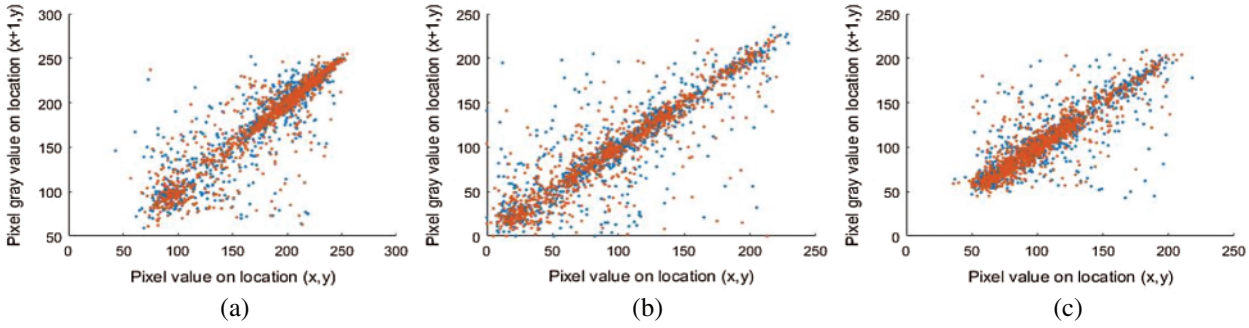
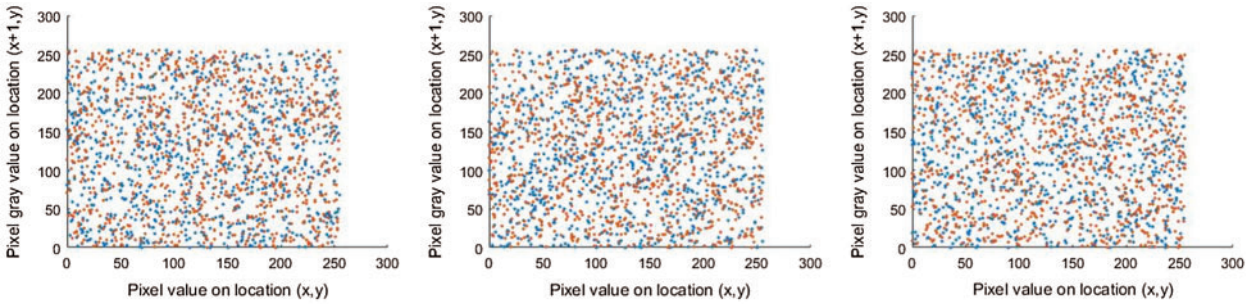


Figure 8: (a–c): represent diagonal correlation pixels for R, G and B layers of original 256 × 256 Lena image respectively



(a) (b) (c)

Figure 9: (a–c): shows the diagonal correlation pixels for R, G and B channel of encrypted Lena image

8.1 Mean Square Error (MSE)

In statistics, the mean square error (MSE) or mean square deviation (MSD) of an image measures the common of the squares of the errors. This means the arithmetic mean square distinction between the calculable values and what's estimated. MSE is a risk function, comparable to the mean of the squared error loss. Followed [26], it judges quality of an encrypted image. It is calculated as $MSE = \sum_{y=1}^{M} \sum_{X=1}^{N} [I(x,y) - C(x,y)]^2 / M \times N$, where $I(x,y)$ is the plain image, $C(x,y)$ is the ciphered version and M, N are the dimensions of the images, respectively. A higher value for MSE can be understood as the better first-rate.

8.2 Peak Signal-To-Noise Ratio (PSNR)

Signal representation dependability may be affected by corrupting noise [32]. Thus the ratio defined amongst the power of a signal and the power of corrupting noise is designated as Peak signal-to-noise ratio (PSNR). It is expressed in terms of the logarithmic decibel gauge due to the diverse dynamic range of signals. Occasionally, the PSNR is used for to evaluate the quality of restoration of the encrypted image. In this study, signal is characterized by plain image and noise is the distortion created by encryption. The PSNR value is directly proportional to the rate of rebuilding of an image. It is defined as $PNSR = 10log_{10}MAX_1^2/\sqrt{MSE}$.

8.3 Normalized Cross-Correlation (NK)

The correlation function also gives the idea that how much two digital images are closed to each other as shown in [33]. The normalized cross-correlation (NK) measures the resemblance amongst two images and is calculated by as: $NK = \sum_{y=1}^{M} \sum_{X=1}^{N} (I(x,y) \times C(x,y)) / \sum_{y=1}^{M} \sum_{X=1}^{N} [I(x,y)]^2$, where $I(x,y)$ is the plain image, $C(x,y)$ is the ciphered version and M, N are respectively the dimensions of the images.

8.4 Average Difference

The difference between reference signal and test image is given the name of Average difference (AD) [32]. AD is calculated by the formula: $AD = \sum_{y=1}^{M} \sum_{X=1}^{N} [I(x,y) - C(x,y)] / M \times N$, where $I(x,y)$ is original, $C(x,y)$ is the encrypted version and M, N are the dimensions of the images.

8.5 Structural Content

One of the correlation based measure is the structural content (SC) [32] and it measures the resemblance among two images. SC is premeditated as $C = \sum_{y=1}^{M} \sum_{X=1}^{N} [I(x,y)]^2 / \sum_{y=1}^{M} \sum_{X=1}^{N} \cdot [C(x,y)]^2$, where $I(x,y)$ is the plain image, $C(x,y)$ is the encrypted version and M, N are respectively the dimensions of the images.

8.6 Maximum Difference (MD)

Scheming maximum of the error signals gives what we call maximum difference (MD) (difference between the test image and reference signal) (see [34]) and it is attained by $MD = \max |I(x,y) - C(x,y)|$, where $I(x,y)$ is the plain image, C(x, y)C (x, y)) is the encrypted version and M, N are respectively the dimensions of the images.

8.7 Normalized Absolute Error

By [31], the Normalized absolute error between the plain and ciphered image is calculated as $NAE = \sum_{y=1}^{M} \sum_{X=1}^{N} |I(x,y) - C(x,y)| / \sum_{y=1}^{M} \sum_{X=1}^{N} |I(x,y)|$, where $I(x,y)$ is the plain image, $C(x,y)$ is the encrypted version and M, N are the dimensions of the images.

8.8 Root Mean Square Error (RMSE)

It is the square root of the mean of the square of all the errors [31]. RMSE is a regularly times used method to measure the variations between original image and the cipher image. $RMSE = \sqrt{(\sum_{y=1}^{M} \sum_{X=1}^{N} [I(x,y) - C(x,y)]^2 / M \times N)}$, where $I(x,y)$ represents the plain image, $C(x,y)$ is the encrypted version and M, N are respectively the dimensions of the images.

8.9 Universal Quality Index (UQI)

According to [35], the UQI breaks the comparison between original and distorted image into three comparisons: Contrast, luminance and structural comparisons. The UQI for original image "O" and encrypted image "E" might be defined as $UQI(O,E) = 4\mu_I \mu_C \mu_{IC} / (\mu_I{}^2 - \mu_C{}^2)(\sigma_I{}^2 - \sigma_C{}^2)$, where μ_I, μ_C represents the mean values of plain and distorted images and σ_I, σ_C denote the standard deviation of plain and distorted images.

8.10 Mutual Information (MI)

To obtain the amount of information from encrypted image for the agreeing plain image is termed as MI given in [35]. The MI of two images "O" and "E" can be defined as $MI(O,E) = \sum_{y \in C} \sum_{y \in I} p(x,y) \, log_2 p(x,y)/p(x)p(y)$, where $p(x,y)$ is the joint probability function of I and C, further $p(x)$ and $p(y)$ are the marginal probability distribution functions of O and E respectively.

8.11 Structural Similarity (SSIM)

By [36], the structural similarity index is an enhanced edition of the universal quality index. Through this technique we determine the similarity between two images. The structural similarity index is calculated on various frames of an image. The measure between two frames X and Y of common size N × N is $SSIM(X,Y) = (2\mu_X \mu_Y + c_1)(2\sigma_X \sigma_Y + c_2) / (\mu_X{}^2 + \mu_Y{}^2 + c_1)(\sigma_X{}^2 + \sigma_Y{}^2 + c_2)$, where average of Y and X is represented by $\mu_Y \mu_Y$ and $\mu_x \mu_X$ the variance of Y and X by σ_Y^2 and σ_X^2 respectively. Whereas σ_{XY} is the covariance of X and Y, $c_1 = (k_1 L)^2$ and

$c_2 = (k_2 L)^2$ are the variables to soothe the division with weak denominator. L Lis the range of the pixel values and $(k_1, k_2) = (0.01, 0.03)$ by default. The SSIM index lies between -1 and 1. For similar images this value is 1. Tab. 10 shows that through our proposed RGB image encryption scheme the optimal values of Image Quality Measures can be achieved.

Table 10: Image quality measures for proposed RGB image encryption of Lena image

No.	Quality measure	Encryption by 3 S-boxes and 3D Arnold chaotic map			Optimal values		
		Red	Green	Blue	Red	Green	Blue
8.1	**MSE**	10626.4	9224.93	7162.78	**10057.2**	**9898.89**	**6948.19**
8.2	**PSNR**	7.86695	8.48117	9.57999	**8.1060**	**8.1749**	**9.7120**
8.3	**NCC**	0.66015	0.993966	1.09709	**0.6725**	**1.0031**	**1.0923**
8.4	**AD**	52.1404	−28.6657	−22.7034	**50.0448**	**−31.4276**	**−19.7989**
8.5	**SC**	1.59967	0.582213	0.562247	**1.5787**	**0.5582**	**0.5711**
8.6	**MD**	250	234	216	**236**	**210**	**210**
8.7	**NAE**	0.467414	0.796259	0.671177	**0.4537**	**0.8310**	**0.6628**
8.8	**RMSE**	103.084	96.0465	84.6332	**100.286**	**99.4932**	**83.3558**
8.9	**UQI**	−0.00013497	−0.000714523	−0.0011433	**−0.0050**	**−0.0077**	**0.0107**
8.10	**MI**	0.491086	0.689748	0.394636	**5.6534**	**7.2283**	**6.0723**
8.11	**SSIM**	0.00982045	0.0084672	0.00937046	**0.0078**	**0.0053**	**0.0187**

9 Security Measurement

9.1 Histograms

A uniform histogram for an image is the calmest and supreme approach to measure the security strength of an encryption procedure against various attacks. Here, we analyze an RGB Lena image of size $256 \times 256 \times 3$. The histogram of the three channels of ciphered image under the proposed scheme is likewise matching though for plain Lena image they are dissimilar. Figs. 2 and 3 show histogram of different layers of plain image and encrypted image. A perfect encrypted image comprises of uniform histogram trickles to sphere the opposing of separating any supportive data from the rocky histogram. Subsequently, no statistical attack can die out this proposed encryption scheme.

9.2 Differential Analyses

To exploit the strong suit of differential analyses on an image encryption arrangement the NPCR (Number of Pixels Change Rate) and UACI (unified average changing intensity) analyses are implemented. It measures the normal power of contrast between the two images, i.e., original and encrypted image. To compare the encrypted images cryptanalysts realize the bond among the plain image and ciphered image. Attack of this kind is famous for differential attack.The NPCR and UACI are the two typically used tests to ensure the strength of the encrypted scheme against differential analysis. For more details, see [35]–[37].

9.2.1 Number of Pixels Change Rate (NPCR)

By [36], the impact of one-pixel change on the whole image ciphered by the suggested scheme has been verified by NPCR. The number of pixels change rate of encrypted image when one pixel of original image is changed is measured by NPCR. Take an encrypted image "Img_1" of dimension $M \times N$, whose corresponding original image "Img_2" has only one-pixel difference. $NPCR = \sum_{I,j} D(I,j) M \times N$, where $D(I,j) = \begin{cases} 0, & \text{if } Img_1(I,j) = Img_2(I,j) \\ 1, & \text{if } Img_1(I,j) \neq Img_2(I,j) \end{cases}$

9.2.2 Unified Average Changing Intensity (UACI)

By [36], the unified average changing intensity of the given two (plain and ciphered) images measures the average intensity of the images. Take two encrypted images Img_1 and Img_2 of dimension $M \times N$. $UACI = \sum_{i,j} \left[\left| Img_1(i,j) - Img_2(i,j) \right| 255 \right] / M \times N$.

Tab. 11 gives the NPCR and UACI measures of different channels of the color Lena encrypted image. The comparison is taken with encryption schemes based on Chaos and S-box. It verifies the strength of the proposed Image encryption scheme *via* S-boxes 1, 2 and 3. Clearly, analyses show that the NPCR and UACI values of our novel encryption technique give optimal values.

Table 11: A comparison of differential analyses 256 × 256 Lena image

Schemes	NPCR			UACI		
	Red	Green	Blue	Red	Blue	Green
Proposed	0.995819	0.9961	0.995926	0.339945	0.338623	0.336869
Ref. [28]	0.9960	99.5895	0.9961	0.3343	0.3350	0.3343
Ref. [32]	0.9964	0.9962	0.9959	0.3353	0.3327	0.3343
Ref. [37]	0.9468	0.9568	0.9868	0.3346	0.3450	0.3549
Ref. [38]	0.9850	0.9850	0.9850	0.3210	0.3210	0.3210
Ref. [19]	0.9960	0.9963	0.9959	0.3343	0.3346	0. 3347

10 Randomness of Test for Cipher

Uniform distribution, Long period and high complexity of the output are the main properties to observe the security strength of a cryptosystem. By a definite end objective to attain these prerequisites, we used NIST SP 800–22 [39] for testing the randomness of digital images. A part of these tests involve copious subclasses. The distorted Lena digital image is cast-off to clasp all NIST tests. The ciphered data is produced by the proposed RGB image encryption scheme of a colored Lena plain image of dimension $256 \times 256 \times 3$ and $3D$ a chaotic map. Tab. 12, shows the outcomes of the tests.

Noticeably our proposed digital image encryption tool proficiently passes the NIST tests. Thus, due to the proficient outcomes, the designed random cryptosystem used for RGB Image Encryption constructed via S-boxes from a non-commutative and non-associative finite ring and $3D$ chaotic map might be professed that are very irregular in its crop.

Table 12: NIST test results for proposed encrypted image

Test		P-values for color encryptions of ciphered image			Results
		Red	Green	Blue	
Frequency		0.32694	0.80028	0.82481	Pass
Block frequency		0.74131	0.54713	0.97235	Pass
Rank		0.29191	0.29191	0.29191	Pass
Runs (M = 10,000)		0.084845	0.09393	0.52759	Pass
Long runs of ones		0.67514	0.7127	0.7127	Pass
Overlapping templates		0.85988	0.85988	0.85988	Pass
No overlapping templates		1	0.9994	0.24017	Pass
Spectral DFT		0.77167	0.56166	0.38399	Pass
Approximate entropy		0.84462	0.85692	0.11867	Pass
Universal		0.99437	0.99976	0.99498	Pass
Serial	p values 1	0.0083409	0.13423	0.34362	Pass
Serial	p values 2	0.12342	0.5943	0.15727	Pass
Cumulative sums forward		0.14445	0.24644	0.24227	Pass
Cumulative sums reverse		0.89099	1.16	0.79042	Pass
Random excursions	$X = -4$	0.79553	0.98021	0.66539	Pass
	$X = -3$	0.37236	0.88823	0.16569	Pass
	$X = -2$	0.57859	0.9465	0.41097	Pass
	$X = -1$	0.22905	0.9464	0.78375	Pass
	$X = 1$	0.48349	0.8282	0.44466	Pass
	$X = 2$	0.13673	0.32154	0.33772	Pass
	$X = 3$	0.6194	0.020103	0.39284	Pass
	$X = 4$	0.70227	0.34143	0.62245	Pass
Random excursions variants	$X = -5$	0.39287	0.0016344	0.46138	Pass
	$X = -4$	0.66407	0.026809	0.59298	Pass
	$X = -3$	0.96847	0.12819	0.52709	Pass
	$X = -2$	0.44399	0.10171	0.91871	Pass
	$X = -1$	0.33092	0.18588	0.92957	Pass
	$X = 1$	0.65853	1	0.25054	Pass
	$X = 2$	0.54029	1	0.30743	Pass
	$X = 3$	0.81252	0.6726	0.40648	Pass
	$X = 4$	0.50404	0.31731	0.59298	Pass
	$X = 5$	1	0.37782	0.76828	Pass

11 Conclusion and Future work

In this paper we constructed S-boxes through non-associative and non-commutative structures of rings having order 512. The main resolution of these S-boxes designing was to produce 256 times more 8×8 S-boxes created through linear fractional transformations having excellent robustness. This study provides $256 \times (16776960)$ choices in constructing 8×8 S-boxes of diverse strength. Thus, combining all possibilities, we have a large enough key space to defend brute force attack. As a futuristic perspective, a successful development in constructing 256 elements LA-field will be more helpful in designing 8×8 S-boxes over it. A new color image encryption usage is

estimated in which firstly these 3 S-boxes were used in producing confusion in each layer of a standard RGB color image. Nevertheless, for the purpose of diffusion 3D Arnold chaotic map is utilized in the newly introduced encryption scheme. A comparison with some of existing chaos and S-box dependent color image encryption schemes were given and the performance outcomes of the estimated RGB image encryption and noted as approaching the standard main level.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[2] A. F. Webster and S. Tavares, "On the design of S-boxes," in *Advanced Cryptology: Proc. CRYPTO-85. Lecture Notes in Computer Science*, Berlin, Heidelberg: Springer, pp. 523–534, 1986.

[3] C. Adams and S. E. Tavares, "Good S-boxes are easy to find," in *Advanced Cryptology: Proc. CRYPTO-89. Lecture Notes in Computer Science*, NY, USA: Springer, pp. 612–615, 1989.

[4] I. Hussain and T. Shah, "Literature survey on nonlinear components and chaotic nonlinear components of block cipher," *Nonlinear Dynamics*, vol. 74, no. 4, pp. 869–904, 2013.

[5] I. Hussain, T. Shah and H. Mahmood, "A group theoretic approach to construct cryptographically strong substitution boxes," *Neural Computing and Applications*, vol. 23, no. 1, pp. 97–104, 2012.

[6] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal and U. Y. Bhatti, "Some analysis of S-box based on residue of prime number," *Proceedings of the Pakistan Academy of Sciences*, vol. 48, no. 2, pp. 111–115, 2011.

[7] M. T. Tran, D. K. Bui and A. D. Doung, "Gray S-box for advanced encryption standard," in *Int. Conf. on Computational Intelligence and Security*, Suzhou, China, pp. 253–256, 2008.

[8] L. Cui and Y. Cao, "A new S-box structure named affine-power-affine," *International Journal of Innovative Computing, Information and Control*, vol. 3, no. 3, pp. 45–53, 2007.

[9] J. Kim and R. C. W. Phan, "Advanced differential-style cryptanalysis of the NSA's skipjack block cipher," *Cryptologia*, vol. 33, no. 3, pp. 246–270, 2009.

[10] X. Yi, S. X. Cheng, X. H. You and K. Y. Lam, "A method for obtaining cryptographically strong 8×8 S-boxes," in *IEEE GLOBECOM 97. Conf. Record*, Phoenix, AZ, USA, pp. 689–693, 1997.

[11] Y. Naseer, T. Shah, S. Hussain and A. Ali, "Steps towards redesigning cryptosystems by a non-associative algebra of IP-loops," *Wireless Personal Communications*, vol. 108, pp. 1–14, 2019.

[12] I. Hussain, T. Shah, M. A. Gondal and H. Mahmood, "An efficient approach for the construction of LFT S-boxes using chaotic logistic map," *Nonlinear Dynamics*, vol. 71, no. 1, pp. 133–140, 2013.

[13] M. Khan, T. Shah, H. Mahmood and M. A. Gondal, "An efficient method for the construction of block cipher with multi-chaotic systems," *Nonlinear Dynamics*, vol. 71, no. 3, pp. 489–492, 2013.

[14] G. Jakimoski and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps," *IEEE Transactions on Circuits and Systems I: Fundament Theory and Applications*, vol. 48, no. 2, pp. 163–169, 2001.

[15] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[16] I. Hussain, T. Shah and M. A. Gondal, "A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm," *Nonlinear Dynamics*, vol. 70, no. 3, pp. 1791–1794, 2012.

[17] X. Wang and Q. Wang, "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos," *Nonlinear Dynamics*, vol. 75, no. 3, pp. 567–576, 2014.

[18] A. K. Farhan, N. M. G. Al-Saidi, A. T. Maolood and F. Nazarimehr, "Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder," *Entropy*, vol. 21, no. 10, pp. 958, 2019.
[19] H. Liu, A. Kadir and Y. Niu, "Chaos-based color image block encryption scheme using S-box," *AEU International Journal of Electronics and Communications*, vol. 68, no. 7, pp. 676–686, 2014.
[20] M. A. Kazim and M. Naseerudin, "On almost semigroups," *Aligarh Bulletin of Mathematics*, vol. 2, pp. 1–7, 1972.
[21] M. S. Kamran, "*Conditions for LA-semigroups to resemble associative structures*," Ph.D. dissertation, Quaid-i-Azam University, Islamabad, Pakistan, 1993.
[22] T. Shah and I. Rehman, "On LA-rings of finitely non-zero functions," *International Journal of Contemporary Mathematical Sciences*, vol. 5, no. 5, pp. 209–222, 2010.
[23] I. Rehman, M. Shah, T. Shah and A. Razzaque, "On existence of non-associative LA-rings," *Analele Universitatii Ovidus Costanta. Seria Matematic*, vol. 21, no. 3, pp. 223–228, 2013.
[24] A. Altaleb, S. M. Saeed, I. Hussain and M. Aslam, "An algorithm for the construction of substitution boxes for block ciphers based on projective general linear group," *AIP Advances*, vol. 7, no. 3, pp. 035116, 2017.
[25] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT'93. Lecture Notes in Computer Science*, T. Helleseth, vol. 765. Berlin, Heidelberg: Springer, pp. 386–397, 1993.
[26] G. Chen, Y. Mao and C. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
[27] G. Chen and X. Dong, "*From chaos to order: Methodologies, perspectives and applications*," Singapore: World Scientific, 1998.
[28] H. Liu, A. Kadir, X. Sun and Y. Li, "Chaos based adaptive double-image encryption scheme using hash function and S-boxes," *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 1391–1407, 2018.
[29] H. Liu, A. Kadir and P. Gong, "A fast color image encryption scheme using one-time s-Boxes based on complex chaotic system and random noise," *Optics Communications*, vol. 338, pp. 340–347, 2015.
[30] J. H. Wu, X. F. Liao and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Processing*, vol. 141, pp. 109–124, 2017.
[31] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez and O. A. Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.
[32] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," *Electronic Letters*, vol. 44, no. 13, pp. 800–801, 2008.
[33] Z. Wang, "A universal image quality index," *IEEE Signal Processing Letters*, vol. 9, no. 3, pp. 81–84, 2002.
[34] M. E. Ahmet and S. F. Paul, "Image quality measures and their performance," *IEEE Transactions on Communications*, vol. 43, no. 12, pp. 2959–2965, 1995.
[35] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.
[36] Y. Wu, J. P. Noonan and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications*, April Edition, pp. 31–38, 2011.
[37] I. Hussain, T. Shah and M. A. Gondal, "Image encryption algorithm based on PGL (2, GF (2^8)) S-boxes and TD-ERCS chaotic sequence," *Nonlinear Dynamics*, vol. 70, no. 1, pp. 181–187, 2012.
[38] I. Hussain and M. A. Gondal, "An extended image encryption using chaotic coupled map and S-box transformation," *Nonlinear Dynamics*, vol. 76, no. 2, pp. 1355–1363, 2014.
[39] F. Pareschi, R. Rovatti and G. Setti, "On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 491–505, 2012.