IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 6, 2020, accepted February 19, 2020, date of publication February 24, 2020, date of current version March 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2975880

Comparison of Pre and Post-Action of a Finite Abelian Group Over Certain Nonlinear Schemes

MUHAMMAD AWAIS YOUSAF[1], HANAN ALOLAIYAN[2], MUSHEER AHMAD[3], MUHAMMAD DILBAR[1], AND ABDUL RAZAQ[4]

[1]Department of Mathematics, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan
[2]Department of Mathematics, King Saud University, Riyadh 11362, Saudi Arabia
[3]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[4]Department of Mathematics, Division of Science and Technology, University of Education, Lahore 54000, Pakistan

Corresponding author: Muhammad Awais Yousaf (awais.yousaf@iub.edu.pk)

This work was supported by a grant from the Research Center of the Center for Female Scientific and Medical Colleges, Deanship of Scientific Research, King Saud University.

ABSTRACT This paper proposes to present a novel group theoretic approach of improvising the cryptographic features of substitution-boxes. The approach employs a proposed finite Abelian group of order 3720 with three generators and six relations. The pre and post-action of the new Abelian group on some nonlinear schemes is analyzed and investigated. It has been found that post-action is competent to construct substitution-boxes whose cryptographic strengths are quite better compared to them before the group action. The S-box strength improvisation has been perceived on multiple performance parameters including nonlinearity, differential uniformity, bits independent criteria, linear approximation probability, and auto-correlation functions along with the satisfaction of strict avalanche criteria. The suitability of proposed improved S-box is tested for image encryption applications under the majority logic criterions and differential analyses. The conducted statistical investigations demonstrated the proficiency of anticipated group action approach and its suitability for cryptographic usages.

INDEX TERMS Substitution-box, group action, Abelian group, image encryption.

I. INTRODUCTION

Nowadays, the mankind has been eased to communicate through insecure channels owing to the progress in communication technology. The secretiveness of information is momentous in such scenarios. It necessitates to have high level protection for trustworthy end-to-end communication. This problem of security assurance can be resolved by using cryptography, steganography and watermarking. Cryptography is an art of transforming the hidden information into a pretend form of data so that it can do attain its terminus securely without leakage of information. In 1949, modern cryptography was founded by Claude Shannon, by depicting the concept of substitution box [1]. A well-studied block cipher Data Encryption Standard (DES) was proposed in 1977 [2] which lead to the start of development and refinement of block cryptosystem. A number of different block cryptosystems similar to DES have been proposed such as LOKI [3], FEAL [4], KHUFU and KHAFRE [5], REDOC [6], etc.

In 1997, a search was started by NIST when it announced that the successor algorithm is needed for DES, which has gone susceptible to different attacks. NIST established the AES which is a specification for encryption of electronic data. In 2001, NIST announced the AES as the U.S. federal information processing standard. Primarily, Belgian cryptographers developed AES, which is a subset of Rijndael block ciphers, by whom a proposal to NIST was submitted during the selection process of AES. It contains flexibility of having options for different block and key sizes. For AES, NIST selects Rijndael family, each with block size 128 bits and three different key lengths 128, 192, and 256. AES is a symmetric block cipher which can protect the classified information and be implemented in both hardware and software.

The associate editor coordinating the review of this manuscript and approving it for publication was Mohammad Ayoub Khan.

The modern cryptography has two broad categories such as asymmetric and symmetric key cryptography. The block ciphers are related to symmetric key cryptography. Substitution-boxes are nonlinear part and parcel of symmetric key cryptosystems including block ciphers, steam ciphers, hash standards, etc. The S-boxes have the ability to bring confusion in the plain-text during the encryption process. Majorly, the effectiveness of the block ciphers is predominantly dependent on the cryptographic strengths of utilized S-boxes. Therefore, the researchers are interested to develop strong and improved S-boxes compared to existing ones. Since, S-boxes are inherently the vectorial Boolean functions. The performance and quality parameters of Boolean functions are also applicable to assess the security strength of S-boxes. Hence, a number of performance criterions and metrics are available to judge the capableness of S-boxes [7]–[11]. An S-box is said to be a cryptographically strong S-box if it satisfies a number of performance criterions simultaneously and most optimally. Accordingly, the researchers are focusing to develop some simple and effective approaches which can generate to form strong S-boxes for the development of a secure cryptosystems [12]–[15], [46], [52], [56]. To inspect the algebraic and statistical structure of substitution boxes, the different metrics are nonlinearity, strict avalanche criteria (SAC), bits independence criteria (BIC), linear approximation probability and auto-correlation function. The suitability of substitution-boxes for cryptographic applications like image encryption is examined under the histogram analysis, a set of criteria collectively known as majority logic criterion, differential analysis involving NPCR and UACI.

In this paper, the techniques of S-box construction and its performance improvisations are investigated which is based on group theoretic approach. The proposed improved S-boxes have been tested by using combinatorial analyses, majority logic criterion, differential analyses and histogram analysis as mentioned above.

II. ALGRBRAIC STRUCTURE OF PROPOSED SUBSTITUTION-BOXES

A. NONLINEAR SCHEMES FOR Ω

We considered the following four nonlinear schemes applied to generate the ordered sets Ω_i; $i = 1, 2, 3, 4$ which form the basis for getting substitution-boxes for the action of proposed Abelian group.

Scheme.1: Discrete log to the base $b \in GF(2^8)$ under mod 257.

Discrete logarithm is a direct analog in a finite group of the usual log in the field of real numbers. In general, the discrete logarithm of $x \in G$ to the base $b \in G$ is defined to be $y \in G$ such that $b^y = x$ in a finite multiplicative group G, if such $y \in G$ exists. In cryptography, logarithms are considered only in cyclic groups and a generator of G is assumed for the base b. Only a positive integer can be the exponent, and $x, b \neq 0$.

Scheme.2: Pure cubic equation $ax^3 + b$, for all $a, b \in GF(2^8)$ under mod 256.

An equation of the form $ax^3 + b = 0$ is said to be a pure cubic equation in which sum of the roots is 0, while their product is $-\frac{b}{a}$, and sum of their products taken two roots at a time is 0.

Scheme.3: Linear fractional transformation $\frac{ax+b}{cx+d}$ for random $a, b, c, d \in GF(2^8)$ under mod 256.

A linear fractional transformation $f : PGL(2, GF\left(2^8\right) \times GF\left(2^8\right)) \rightarrow GF(2^8)$ is a mapping from $GF(2^8)$ to $GF(2^8)$ of the form $\frac{ax+b}{cx+d}$ where $a, b, c, d \in GF(2^8)$ is obtained by action of $PGL(2, F\left(2^8\right))$ on $GF(2^8)$. f is not bijective usually but can made by replacing repeated values.

Scheme.4: 3D shuffling algorithm for 16×16 matrix.

In this 3D shuffling algorithm, the decimal entries of matrix $\Omega_{16\times16}$ are changed into binary form so that all entries are in $GF(2^8)$. Eight 2-D matrices are prepared for each bit. A 3D matrix $A_{16\times16\times8}$ is made whose ith layer is the 2D matrix of $(9 - i)th$ bit. To construct $B_{16\times8\times16}$, we remove even columns of ith layer and place it to $(8 + i)$ th layer and change it into decimal form so that a matrix $C_{16\times1\times16}$ is formed. Then place ith layer at the ith column to make $D_{16\times16}$ matrix. Find the missing entries, arrange them in order and flip them. Then rearrange each eight-element group using the permutation (1 5 7 6 4 2 3 8) and remaining less than eight entries keep at the same positions. Finally, replace repeated values with arranged missing values.

We tested all the four mentioned schemes on the elements of Galois Field $GF(2^8)$ for high nonlinearity on Ω, the set of members of $GF(2^8)$ and satisfaction of strict avalanche criteria. The input parameters for four nonlinear schemes which satisfy the two properties most optimally are chosen as (1) $b = 94$ as the base of discrete log in *Scheme*1, (2) $a = 114, b = 16$ as the coefficients of cubic equation in *Scheme*2, and $a = 114, b = 1, c = 98, d = 195$ as random parameters of linear fractional transformation in *Scheme* 3. Let $\Omega_i; i = 1, 2, 3, 4$ be an ordered set obtained by applying i^{th} scheme on $GF(2^8)$. The proposed group-theoretic approach involves the following three simple steps.

B. STEP 1

Remove the repeated term 257 in order set Ω_1 and substitute the missing values in Ω_i; $i = 1, 2, 3, 4$.

C. STEP 2

Consider a finite Abelian group $G =< x, y, z; x^{248} = y^5 = z^3 = xyx^{-1}y^{-1} = xzx^{-1}z^{-1} = yzy^{-1}z^{-1} = e >$, consists three generators, six relations and order of 3720.

D. STEP 3

The proposed group G acts naturally on the Index set I_{Ω_i} of Ω_i as $\mu : G \times I_{\Omega_i} \rightarrow I_{\Omega_i}$ defined as, for fixed $g \in G$, $\mu\,(g, \omega) = (\omega)\,\varrho_g, \omega \in \Omega_i$.

Hence, finally through bijection from I_{Ω_i} to Ω_i, we get cryptographically better substitution box Ω_i on post-action of proposed group.

TABLE 1. S-box of Scheme 1 before action of G on I_{Ω_i}.

00	C0	B0	25	A0	73	15	49	90	8A	63	14	05	92	39	D8
80	58	B9	12	85	94	E3	0A	10	C9	95	F3	20	A5	30	40
F0	BA	48	56	A9	6F	02	A6	75	4C	84	2E	D3	91	FA	98
65	51	3C	BD	74	EB	1E	BF	C3	77	81	A7	EA	7C	88	F9
E0	93	AA	B2	38	CE	46	F6	99	47	5F	5D	F2	FD	96	52
B3	EE	67	1D	71	0B	97	9C	DA	8F	6C	B1	78	B4	E9	C5
55	44	41	1F	2C	9B	AD	7E	64	BB	DB	4B	0E	2B	AF	D4
89	0C	37	07	4F	7B	4D	E1	E2	8D	ED	D7	86	5E	42	23
D0	35	83	59	9A	24	A2	E8	28	21	BE	DC	36	FF	E6	4A
CA	66	7F	B6	5C	3E	A1	A8	68	22	A4	1A	D9	03	B5	50
A3	C2	DE	06	57	6D	0D	62	61	CD	FB	CF	87	B7	8C	09
54	2F	AB	8E	CB	5B	3B	E4	FE	2D	1B	AC	9F	C1	C4	D5
45	69	34	F8	31	EC	0F	5A	1C	17	8B	F1	9D	E7	6E	33
D2	16	7D	72	DD	DF	C7	19	76	C6	4E	B8	32	2A	13	60
79	08	FC	6A	27	01	F7	43	3F	9E	6B	F4	3D	BC	D1	E5
18	7A	11	53	AE	04	CC	F5	26	82	EF	29	D6	C8	3A	70

TABLE 2. Proposed S-box after action of G on I_{Ω_i}.

7E	96	35	9B	00	A3	DD	A9	B0	92	DB	D0	2D	04	B3	FC
BA	7C	05	6E	80	A1	5B	0F	AF	20	AA	FF	34	2A	ED	79
02	C1	F7	BD	1E	A8	BF	DF	7B	A0	1C	74	27	83	49	D1
EA	A2	2F	37	54	11	32	0B	57	15	48	8F	B2	33	0C	D6
E3	85	3D	65	6D	A4	C6	76	71	4A	7A	89	EE	90	52	03
55	81	53	39	19	58	51	0D	3F	2C	62	E0	82	7F	94	CE
4B	3B	9D	72	38	8D	21	BC	14	DA	FB	E1	5A	95	68	B9
E4	9C	73	F9	45	3E	56	B4	1B	93	1A	7D	6C	70	CA	4E
3C	C2	60	DE	D3	84	F8	09	13	FA	BB	F2	28	06	18	16
EC	D4	9E	E2	67	CF	D5	98	5E	C5	10	B6	D2	59	1D	E9
5C	8A	86	AB	36	8C	12	26	CC	29	B5	69	44	91	F0	42
F6	C8	75	4F	23	D9	DC	50	31	C4	A7	F1	C0	F3	63	6B
0E	5D	5F	E8	99	9A	F5	0A	A6	78	88	4C	C3	BE	AC	B1
08	43	8E	22	07	40	8B	CB	2E	9F	E5	47	41	30	3A	6A
CD	64	AD	4D	2B	6F	46	FD	25	A5	61	B8	EF	66	D8	77
C7	24	17	01	E7	87	B7	F4	1F	FE	E6	EB	D7	AE	C9	97

The generation of final S-box using scheme 1 and action of proposed group is illustrated as: Consider the entries of Galois field $GF(2^8)$ and arrange its 256 elements in 16 columns, such that, the entries (in hex format) of very first row are (00h, 10h, 20h, 30h, 40h, 50h, 60h, 70h, 80h, 90h, A0h, B0h, C0h, D0h, E0h, F0h). In scheme 1, we assume discrete log of 0 to the base 94 as 0, because log of 0 is not possible. Taking discrete log to the base 94 of remaining entries (like $94^{192} = 16 \ mod 257$, $94^{176} = 32 \ mod 257$), we get (00h, C0h, B0h, 25h, A0h, 73h, 15h, 49h, 90h, 8Ah, 63h, 14h, 05h, 92h, 39h, D8h). These obtained values form the elements of first row initial S-box from Scheme 1 which is shown in Table 1. Now, the action of proposed Abelian group G is to be performed on the indexed set of the S-box in Table 1.

The obtaining of proposed final S-box as follows: through the action of generator x at 1^{st} entry of the Table 1 mapped at 5^{th} place in Table 2, ; 5^{th} is placed at 42^{th}; 42^{th} is placed at 204^{th}, and 204^{th} is placed at 188^{th} (because of permutations offered by generator x of group G). Through the action of Abelian group with three generators x, y, z on S-box in Table 1, the proposed S-box which is in Table 2 is gotten. The S-box from Scheme 1 is shown in Table 1 and the post-action of group on this S-box resulted into the S-box given in Table 2. Similarly, the same group action is performed over the S-boxes generated by other three schemes to get three more S-boxes as the result of action.

The combinatorial S-box analyses of four suggested nonlinear schemes before and after the action of proposed Abelian group are given in Table 3 and Table 4. The group causes features improvement in all four S-boxes. The improvement is achieved on multiple parameters. Specifically, the pre-action nonlinearities of 104.25, 101.75, 92.5, 58 goes post-action as high as 112, 106.5, 105.5, 102.75, respectively. The differential uniformities get better from 128, 28, 40, 114 to as low as 4, 12, 12, 10 respectively. Linear approximation probabilities go excelled from 0.1797 to 0.0625, from 0.1562 to 0.1406, from 0.2109 to 0.1406, and from 0.4609 to 0.1328. Similarly, the autocorrelation function also gets improved from 184 to 32, from 136 to 108, from 184 to 96, and from 248 to 88. Hence, a remarkable performance improvisation has been achieved with post action of proposed group over initial S-boxes from four schemes. The plots for nonlinearity, strict avalanche criterion, differential uniformity, BIC, linear probability and ACF for four suggested schemes before and after the action of our finite group are shown in Figure 1 and Figure 2.

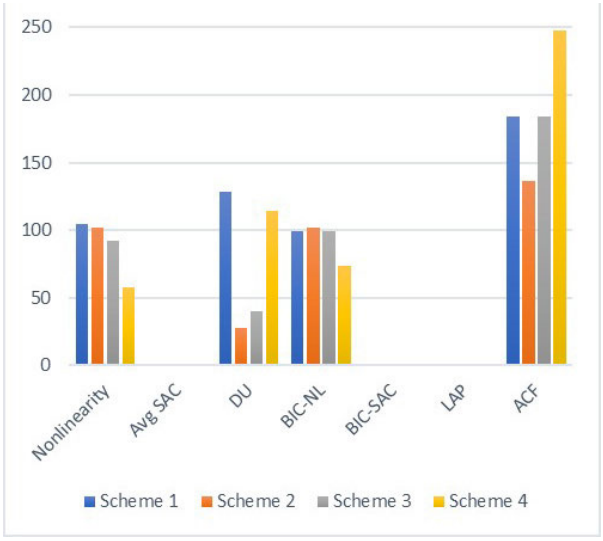

FIGURE 1. Analyses of suggested schemes before group action.

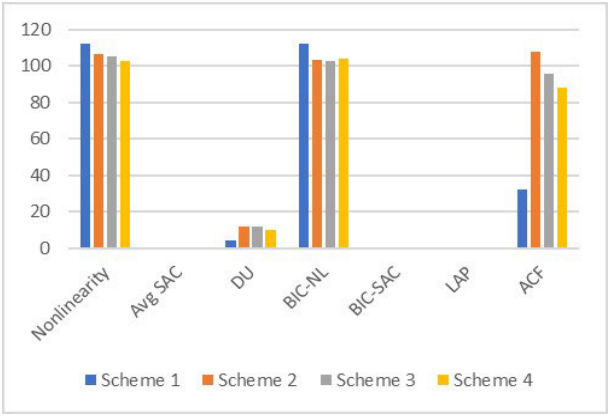

FIGURE 2. Analyses of suggested schemes after proposed group action.

III. ANALYSES OF PROPOSED S-BOX

The different statistical tests have been implemented in MATLAB to determine the security performance of substitution-boxes to judge their cryptographic strengths. The S-box performance metrics and tests such as nonlinearity, strict avalanche criteria (SAC), bits independence criteria (BIC), linear approximation probability and auto-correlation function are applied to estimate the cryptographic competency of S-boxes. Moreover, the suggested substitution-box finds its application in the field of image encryption approaches. The performance outcomes of the suggested substitution-box are compared with some recent substitution-boxes.

A. NONLINEARITY

It is the fundamental tool introduced in 1988 by Pieprzyk and Finkelstein [16] to measure the strength of substitution-box. The Walsh spectrum manifests the nonlinearity of a Boolean function $f(x)$ as

$$N_f = 2^{n-1}(1 - 2^{-n} \max_{\omega \in GF(2^n)} \left|S_{<f>}(\omega)\right|)$$

TABLE 3. S-box analyses before action of G on I_{Ω_i}.

Scheme	1	2	3	4
Nonlinearity	104.25	101.75	92.5	58
Avg. SAC	0.5009	0.5046	0.4619	0.3120
DU	128	28	40	114
BIC-NL	99.64	102.28	99.21	73.57
BIC-SAC	0.5015	0.5025	0.4882	0.4180
LAP	0.1797	0.1562	0.2109	0.4609
ACF	184	136	184	248

TABLE 4. S-box analyses after action of G on I_{Ω_i}.

Scheme	1	2	3	4
Nonlinearity	112	106.5	105.5	102.75
Avg. SAC	0.5051	0.5064	0.5034	0.5002
DU	4	12	12	10
BIC-NL	112	103.71	102.5	103.78
BIC-SAC	0.5044	0.5004	0.5085	0.5019
LAP	0.0625	0.1406	0.1406	0.1328
ACF	32	108	96	88

The following equation defines the Walsh spectrum $S_{<f>}(\omega)$ of $f(x)$

$$S_{<f>}(\omega) = \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus x.\omega}$$

where $\omega \in GF(2^8)$ and $x.\omega$ is the dot product. Concerning the security against linear cryptanalysis, S-box with maximum nonlinearity always shows greater cryptographic resistance to linear attacks. For a bijective S-box $S(x) = (f_1(x), f_2(x), \ldots, f_n(x))$ the benchmarking index includes the highest and lowest nonlinearity and the mean value of all nonlinearity values. The nonlinearity AES S-box considered as the best-known nonlinearity for any 8×8 S-box. The non-linearity of proposed S-box is found as 112 which is same as that of AES S-box and better as compared to many known available S-boxes in literature as shown in Table 5. It shows that our proposed S-box has the ability to offer high nonlinearity the security system and can offer high resistance to linear attacks.

B. STRICT AVALANCHE CRITERION

The strict avalanche criterion was described by Tavares and Webster, which gets its base on the completeness effect's notion and the avalanche [34]. This criterion measures that by making a single change in input bits, how much output bits get altered. The SAC assumed as satisfied when all the output bits are changed with a probability of 0.5, whenever only one input bit is flipped. Table 6 displays the dependency matrix as an outcome of SAC analysis. The outcomes show that proposed S-box satisfies the strict avalanche criterion quite well as it has an average value of 0.5051 which is quite

TABLE 5. The results of nonlinearity of various S-boxes.

S-box	N0	N1	N2	N3	N4	N5	N6	N7	Mean
Proposed	112	112	112	112	112	112	112	112	112
Chaotic S-box [17]	108	110	106	108	108	106	110	106	107.75
AES [18]	112	112	112	112	112	112	112	112	112
Chen [19]	100	102	103	104	106	106	106	108	104.3
Prime [20]	94	100	104	104	102	100	98	94	99.5
Khan [21]	102	108	106	102	106	106	106	98	104.25
Coset Diagram [22]	108	106	108	108	108	104	106	106	106.75
Skipjack [23]	104	108	108	108	108	104	104	106	106.75
Xyi [24]	106	104	106	106	104	106	104	106	105
S-p-box [25]	112	112	112	112	112	112	112	112	112
Arun [26]	108	106	104	98	102	102	98	74	99
Belazi [27]	106	106	106	104	108	102	106	104	105.25
Tang [28]	100	103	104	104	105	105	106	109	104.5
S_8 AES [29]	112	112	112	112	112	112	112	112	112
Gray [30]	112	112	112	112	112	112	112	112	112
Alkhadi [31]	108	104	106	106	102	98	104	108	104
Alzaidi [32]	110	110	110	110	110	108	110	108	109.5
Solami [33]	108	110	108	108	106	110	108	110	108.5
Lu [52]	108	106	104	104	104	106	108	110	106.3
Zhang [34]	108	110	108	110	108	108	110	108	108.75

TABLE 6. SAC of proposed S-box.

0.4688	0.4844	0.4531	0.5313	0.5000	0.4844	0.5625	0.5000
0.5156	0.5156	0.4844	0.5000	0.5625	0.4531	0.4531	0.4531
0.5313	0.5313	0.5313	0.5469	0.4531	0.5000	0.4688	0.5000
0.5156	0.5156	0.5000	0.5000	0.4688	0.5625	0.5000	0.5313
0.4531	0.5156	0.5469	0.5313	0.4688	0.4688	0.5156	0.5313
0.4688	0.5000	0.5156	0.4688	0.4688	0.5469	0.4844	0.5156
0.5156	0.5625	0.5313	0.5156	0.5313	0.4844	0.5156	0.4844
0.5000	0.5469	0.4688	0.4688	0.5156	0.5625	0.5313	0.5156

TABLE 7. Average SAC of various S-boxes.

S-box	Proposed	AES	Gray	Prime	[17]	[25]	[34]
Min value	0.4531	0.4530	0.4210	0.3430	0.3906	0.4370	0.4530
Max value	0.5625	0.5260	0.5250	0.6710	0.5781	0.5260	0.5250
Average	0.5051	0.5040	0.4760	0.5160	0.4976	0.4870	0.5100

close to ideal value of 0.5. The SAC comparison of various S-boxes is made in Table 7. It can be seen that the proposed S-box has comparable performance like other S-boxes when satisfying the SAC criteria.

C. BIT INDEPENDENCE CRITERION

The input bits which remain unchanged are explored under bits independence criterion. The revamping of independent performance of pairwise variables of avalanche vectors and unaltered input bits are the assets of this measure. It is an effective criterion in symmetric cryptosystem, because by augmenting independence between bits, the recognition and prediction of patterns of the system is not possible. The BIC outcomes for nonlinearity are provided in Table 8. We compared the lowest and average values of BIC-nonlinearity and square deviation of suggested S-box with various well-known S-boxes in Table 9. The BIC analysis of suggested S-box has standard deviation = 0, average value = 112 and minimum value = 112. The results are remarkably excellent as compared to many other S-boxes given in Table 9.

TABLE 8. BIC of proposed S-box.

-	112	112	112	112	112	112	112
112	-	112	112	112	112	112	112
112	112	-	112	112	112	112	112
112	112	112	-	112	112	112	112
112	112	112	112	-	112	112	112
112	112	112	112	112	-	112	112
112	112	112	112	112	112	-	112
112	112	112	112	112	112	112	-

D. LINEAR APPROXIMATION PROBABILITY

The method of linear approximation probability (LAP) is helpful in calculating the imbalance of an incident. The maximum value of imbalance of an event is measured with the help of the analysis introduced by Matsui in [35]. There must

TABLE 9. Comparison of BIC of various S-boxes.

S-box	Min value	Average	Square deviation
Proposed	112	112	0
AES [18]	112	112	0
Prime [20]	94	101.71	3.53
Skipjack [23]	102	104.14	1.767
Xyi [24]	98	103.78	2.743
S-p-box [25]	112	112	0
Arun [26]	92	103	3.5225
S_8 AES [29]	112	112	0
Gray [30]	112	112	0

TABLE 10. Linear approximation probability of various S-boxes.

S-box	Proposed	AES	Gray	Prime	Skipjack	[25]	[26]	[29]
Value	144	144	144	162	156	144	164	144
LP	0.0625	0.0625	0.0625	0.132	0.109	0.0625	0.2109	0.062

be no difference between output and input bits uniformity. Each of the input bits with its results in output bits is examined individually. If all the input elements are 2^n, the class of all possible inputs is d and the masks applied on the equality of output and input bits are respectively χ_y and χ_x, then maximum linear approximation is the maximum number of same results and calculated as:

$$LP = \max_{\chi_x,\chi_y\neq 0}\left|\frac{\#\{d|d\cdot\chi_x = S(d)\cdot\chi_y\}}{2^n} - \frac{1}{2}\right|$$

A lower value of this probability indicates that S-box is more capable to fight against linear cryptanalysis attack. The outcomes of this crucial analysis acquired for suggested S-box and various available S-boxes which are mentioned in Table 10. These LAP measures show that our S-box can deal with various linear attacks effectively like AES in better way compared many other S-boxes.

E. DIFFERENTIAL UNIFORMITY

To withstand the famous differential cryptanalysis introduced by Biham and Shamir [36], S-box must have the differential uniformity as low as possible. By ensuring a uniform mapping probability for each $\boldsymbol{J}$, an output differential $\boldsymbol{\Delta y_j}$ must be uniquely mapped with an input differential $\boldsymbol{\Delta x_j}$. For an almost perfect nonlinear $\boldsymbol{n} \times \boldsymbol{m}$ S-box lower band of differential uniformity is $\mathbf{2^{n-m\mathcal{C}1}}$. For $\boldsymbol{n} \in \boldsymbol{E}$, there is no almost perfect nonlinear S-box in $\boldsymbol{GF(2^n)}$. Thus, the DU of 8 × 8 AES S-box is considered as the minimum optimum value which is 4. Table 11 shows differential uniformity of proposed S-box and comparison with others is given in Table 12. The proposed S-box is also found to be a differentially 4-uniform like AES S-box. Therefore, it can oppose differential cryptanalysis quite diligently and comfortably.

TABLE 11. Differential uniformity of suggested S-box.

4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

TABLE 12. Differential uniformity of various S-boxes.

S-box	Proposed	AES	Gray	Skipjack	[19]	[21]	[28]	[29]
DU	4	4	4	12	12	16	10	4

F. AUTOCORRELATION FUNCTION

For two Boolean functions $f(x)$ and $g(x)$, their cross-correlation function $\hat{c}_{fg}(y)$ is defined as

$$\hat{c}_{fg}(y) = 2^{-n}\sum_x (-1)^{f(x)\oplus g(x\oplus y)}$$

The auto-correlation function of a binary Boolean function f is $\hat{c}_{ff}$. It shows that the squares of members of spectrum of f are the members of spectrum of ACF. We denote autocorrelation function of the function f from $GF(2^m)$ to $GF(2^n)$ by $\hat{r}_f(y)$ and mathematically it is defined as

$$\hat{r}_f(y) = 2^{-n}\sum_x (-1)^{f(x)\oplus f(x\oplus y)}$$

The autocorrelation function score for proposed S-box comes out be 32 only.

G. BIJECTIVE PROPERTY

Most of the block ciphers employ the bijective S-boxes during substitution-phase. Hence, it is compulsory for the S-box to be reversible and bijective for correct data decryption in substitution-permutation networks (SPN). The bijective property is fulfilled for $m = n$ if

$$wt\left(\sum_{j=1}^{n} a_j f_j\right) = 2^{n-1}$$

where $\boldsymbol{wt(\cdot)}$ is Hamming weight, $(\boldsymbol{a_1, a_2, a_3, \ldots, a_n}) \neq (0, 0, 0, \ldots, 0)$, $\boldsymbol{a_j} \in \{\mathbf{0, 1}\}$ and $\boldsymbol{f_j}$ represents Boolean function. $\boldsymbol{f}$ is bijective and each $\boldsymbol{f_j}$ should be $\mathbf{0/1}$ balanced.

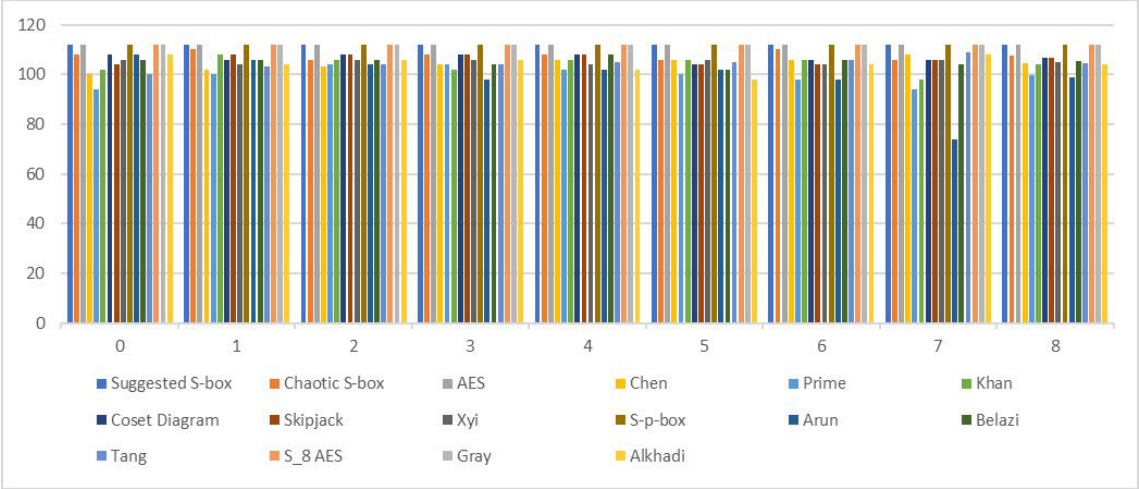

FIGURE 3. Comparison of nonlinearity scores.

We have verified that our all four improvised S-boxes satisfy the bijective property.

IV. MAJORITY LOGIC CRITERION

Through majority logic criterion, the strength and suitability of substitution-boxes are examined and investigated for use in image encryptions. It is momentous to examine the statistical characteristics because by encryption a distortion is created in image. The MLC is set of criterions such as *Correlation*, *Entropy*, *Energy*, *Homogeneity* and *Contrast*. The proposed substitution-box is applied to encrypt digital images to show that it can be used for multimedia security and image encryption [37]. To conduct MLC analysis, we used three standard gray images *Lena*, *Peppers*, *Baboon* each of size 256×256. The encryption procedure involves substitution by proposed S-box in two rounds. In first round, the substitution is carried out in forward direction (from first pixel of image to the last pixel) followed by substitution in reversed direction (from last pixel of image to first pixel). All the experiments and simulations are performed using MATLAB tool. The original and encrypted images with proposed S-box are shown in Figure 4. The encrypted images are extremely distinct and indistinguishable compared to their respective plain-images. The visual distortion is fairly high as the images don't consist of any patterns that may leak even the slight information of plain-image data.

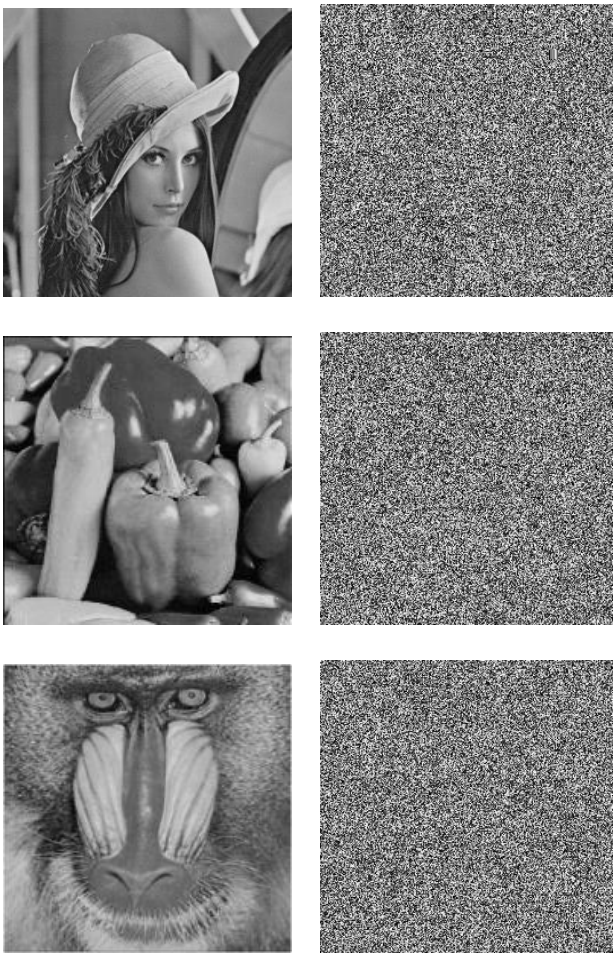

FIGURE 4. Original and encrypted images.

A. CORRELATION

The correlation coefficient measures the closeness of pixel values to its neighboring pixels. It unfolds an existing linear relationship between two pixels values of the image. It can be calculated in horizontal, vertical and diagonal formats. Its range belongs to $[-1, +1]$. If the neighboring pixels of image are negatively correlated, the value of correlation is -1, else $+1$ if they are positively correlated [38]. In general, the plain-images have strong correlation among neighboring pixels. The correlation between pixel values can be soften by encryption. The encrypted images with highly uncorrelated neighboring pixels deem robust for insecure channel.

TABLE 13. Vertical and horizontal correlation matrices.

Image		Lena	Peppers	Baboon
Vertical	Org	0.9374	0.8225	0.9124
	Enc	0.0170	-0.0032	-0.0056
Horizontal	Org	0.9700	0.9541	0.9324
	Enc	0.0035	-0.0035	-0.0152

Mathematically, the correlation analysis is obatined as:

$$Corr = \sum_{j,k} \frac{(j-\mu_j)(k-\mu_k)p(j,k)}{\sigma_j \sigma_k}$$

where μ is the variance, σ is mean of the gray level co-occurrence matrix, and $p(j,k)$ is the pixel value at j^{th} row and k^{th} column. The computed correlation coefficients for images in Figure 4 are given in Table 13. It can be observed from Table that the coefficient values in randomly selected vertical and horizontal adjacent pixels in encrypted images are very less (near to zero) than the corresponding values obtained for plain-images. This shows that proposed S-box is consistent to diminish the existing high correlation in images and make them robust. The correlation plots for vertically and horizontally neighboring pixels in plain-images and encrypted images are shown in Figure 5. The Lena, Papers and Baboon cipher image correlation coefficients encrypted with Khan's algorithm [54], Wang's algorithm [53], and Zhu algorithm [55]. The experimental results indicate that, among the three algorithms, our proposed algorithm has the closest absolute values of the correlation coefficient, having the strongest scrambling effect.

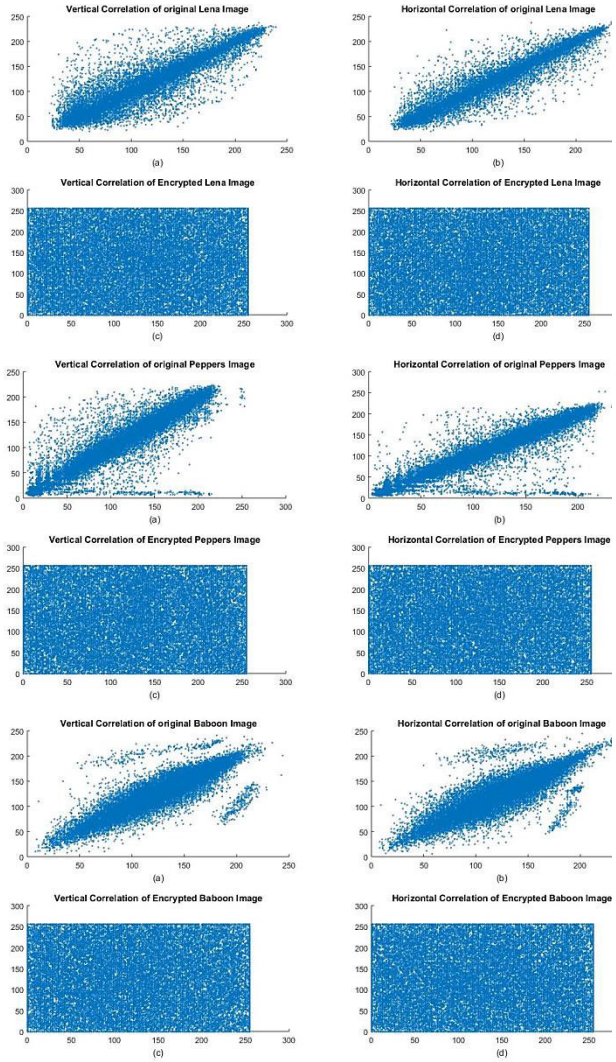

FIGURE 5. Pixel correlation plots.

B. ENTROPY

The value of randomness of encrypted image is measured by entropy analysis. The entropy is mathematically formulated as [39].

$$H(S) = -\sum_{j=0}^{m-1} p(t_j) \log_2 p(t_j)$$

where $\boldsymbol{p(t_j)}$ is the probability of symbol $\boldsymbol{t_j}$ of source S. The entropy is 8, if source emits 256 symbols with equal probabilities; this corresponds to the ideal value for source and represents a real random source. Entropy is greater, if the distribution of gray value is more uniform. There would be a chance of predictability if the entropy of encrypted image is significantly less than 8, and it threatens security of image. The entropy values of original and encrypted images are given in Table 14. It shows that, in our image encryption using proposed S-box, the information leakage is insignificant as the entropy for encrypted images are quite high.

C. ENERGY

The sum of squared members of gray level co-occurrence is calculated in energy analysis [40]. In gray level co-occurrence matrix high valued pixels are found in some places of plain image, therefore the energy value is high. As compared to the original image energy of the encrypted image is smaller because in encrypted image energy values are distributed. The energy analysis under MLC is expressed as:

$$E = \sum_{j,k} p(j,k)^2$$

The energy values of three plain and encrypted images are given in Table 14. The obtained considerably small values of energy for encrypted images shows good encryption effect as compared to plain-images.

D. HOMOGENEITY

The intimacy of the distribution of elements of diagonal gray level co-occurrence and gray level co-occurrence is

TABLE 14. Majority Logic Criterion of proposed S-box.

Criteria	Lena		Peppers		Baboon	
	Org.	Enc.	Org.	Enc.	Org.	Enc.
Correlation	0.9220	-8.81e-4	0.9243	-0.0075	0.8621	-0.0087
Entropy	7.4467	7.9564	7.5553	7.9566	7.2636	7.9553
Energy	0.1227	0.0157	0.1012	0.0157	0.1208	0.0157
Homogeneity	0.8817	0.3917	0.8659	0.3899	0.8403	0.3895
Contrast	0.3563	10.2301	0.4359	10.3042	0.4089	10.3466

calculated in Homogeneity [41]. Its range belongs to [0, 1]. Mainly, its value is dependent on the components presents on the diagonal of the gray level co-occurrence matrix. The small value of homogeneity in encryption reveals the strength of the encryption algorithm. Homogeneity in digital image content is computed as follows:

$$H = \sum_{j,k} \frac{p(j,k)}{1+|j-k|}$$

The computed scores of homogeneity for all three plain and encrypted images are listed in Table 14. Again, the low values of homogeneity for encrypted image as compared to original image indicate that the encryption effect is strong.

E. CONTRAST

For easy viewing contrast and brightness of the image are properly adjusted during image processing. Contrast is related to the difference in the brightness of object. In encryption process, due to the nonlinear substitution by the S-box, the contrast is directly proportional to the randomness of image [42]. A constant plain-image has a contrast value of zero. In general, the contrast measure for an image is obtained as:

$$C = \sum_{j,k}^{m-1,n-1} |j-k|^2 p(j,k)$$

where the position of pixels in gray level co-occurrence matrices is represented by $p(j, k)$. The contrast values of three set of images are given in Table 14. The high contrast scores for encrypted images, compared to original image, show that information leakage is negligible in proposed encryption process.

The MLC results are also depicted graphically in Figure 6 to show high divergence of MLC measures for encrypted images as compared to outcomes for plain-images. The MLC analyses demonstrate that proposed S-box is capable to offer excellent encryption effect which is proven by the evaluated different statistical measures.

V. DIFFERENTIAL ANALYSES

In this analysis, a minor change is incorporated in the original image in order to hide each statistical correspondence between output and input which results in large alteration of

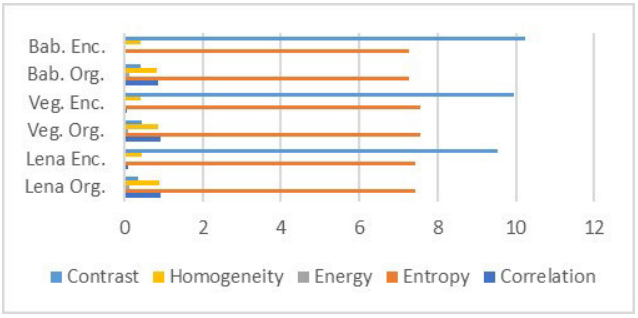

FIGURE 6. Majority logic criteria results for original and encrypted images.

TABLE 15. NPCR, UACI and BACI results.

Image	NPCR	UACI	BACI
Lena	99.61 %	27.85 %	21.25 %
Peppers	99.59 %	29.26 %	19.88 %
Baboon	99.57 %	26.81 %	22.15 %

encrypted image content. This feature is directly related to the confusion and diffusion of the followed encryption system. The following statistical measures are used in practice to gauge the different analysis.

A. NPCR AND UACI

Two most common criteria, number of pixel change rate (NPCR) and unified average changing intensity (UACI) are used to quantitatively measure the influence of one pixel change on the encrypted image [43]. Between the two encrypted images, the percentage of different pixel numbers is measured by NPCR and the average intensity of differences is measured by UACI [44]. Let the difference in pixel of two original images is only one and their corresponding encrypted images are denoted by E_1 and E_2. Then NPCR is determined as:

$$NPCR = \frac{\sum_{j,k} D(j,k)}{X \times Y} \times 100\%$$

where two-dimensional array D with same size as E_1 and E_2 is defined as:

$$D(j,k) = \begin{cases} 1 & if\ E_1(j,k) \neq E_2(j,k) \\ 0 & if\ E_1(j,k) = E_2(j,k) \end{cases}$$

While UACI is defined as:

$$UACI = \frac{1}{X \times Y} \left[\sum_{j,k} \frac{|E_1(j,k) - E_2(j,k)|}{255} \right] \times 100\%$$

where X and Y are the height and width of encrypted image. It is concluded that the high values of NPCR and UACI are required as shown in Table 15.

B. BLOCKED AVERAGE CHANGING INTENSITY (BACI)

In Ref. [45], Zhang highlighted some problems in NPCR and UACI measures for differential analysis. Zhang demonstrated

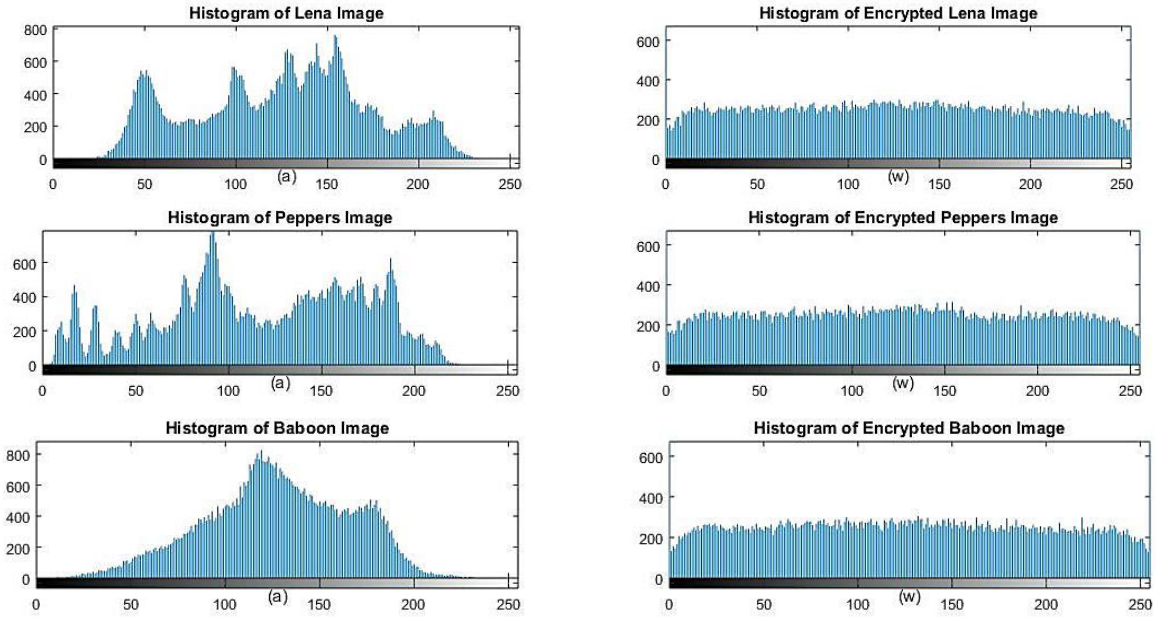

FIGURE 7. Histogram analysis.

that the two different (differ by pixel values) plain-images that are visually similar up to much extent may have the scores of NPCR close to its theoretical value of 100% and UACI close to expected value. Hence, the NPCR and UACI measures are not suitable to describe and account the visual difference between images as shown in [45]. To overcome the existing problems of NPCR and UACI, Zhang suggested an index termed as blocked average changing intensity (BACI). According to BACI index, the difference image $D = abs(E_1 - E_2)$ is divided into blocks of pixels each of size 2×2. A value (say M_i) is computed for each block D_i and BACI is defined as follows:

$$D_i = \begin{bmatrix} d1 & d2 \\ d3 & d4 \end{bmatrix}$$

$$M_i = (|d1 - d2| + |d1 - d3|) + |d1 - d4| + |d2 - d3| + |d2 - d4| + |d3 - d4|)/6$$

$$BACI = \frac{1}{(X-1)(Y-1)} \sum_{i=1}^{(X-1)(Y-1)} \frac{M_i}{255} \times 100\%$$

The expected score of BACI measure is calculated as 26.77% [45]. Following this procedure, we also computed the BACI measure for our encryption algorithm using proposed S-box, the obtained values of BACI are also shown in Table 15. It is evident that our encryption algorithm shows quite satisfactory BACI scores as they are somewhat close to expected value.

Hence, in addition to NPCR and UACI, BACI scores show the encryption algorithm using proposed S-box brings adequate visual difference between two encrypted images whose plain-images have minor change in pixel value.

VI. HISTOGRAM ANALYSIS

The distribution of pixels gray level intensities in an image is represented by histogram. If a non-uniform behavior is presented by distribution, cryptanalyst may use this information to mount histogram attacks. However, the algorithm is deliberated robust against histogram attack and the information is unpredictable if the histogram is flat and uniform [42]. Between ciphered and non-ciphered image, the difference among the intensities of colors is found using it. We have tested the histograms of original and encrypted images. The histogram distribution of the encrypted image with the proposed S-box presents a significant difference from the original image's histogram and is quite uniform as shown in Figure 7. The result denotes that it is extremely difficult to leverage the statistical characteristics of the substituted image to reacquire the original image.

VII. CONCLUSION

In this paper, we constructed four initial S-boxes by applying different nonlinear schemes. Then, a group theory-based approach is proposed to improve the features of generated S-boxes. To achieve features improvisation, a novel finite Abelian group with three generators having an order of 3720 is constructed. The proposed approach analyzes and compares the pre and post action of suggested Abelian group over the nonlinear S-box schemes. The simulation analysis shows that the improvisation of all four S-boxes on multiple performance parameters is achieved. The most optimal proposed S-box among all four is exclusively investigated in detail. In addition, the same proposed S-box is applied for cryptographic image application. It has been found that our encryption algorithm using proposed S-box offers excellent

encryption effect and performance as evident by MLC criterions, differential analyses including NPCR, UACI and BACI measures, and histogram analysis. Hence, the proposed approach is trustful for use in secure communication systems.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Jul. 2013.

[2] *Data Encryption Standard*, Nat. Bureau Standards, U.S. Dept. Commerce, FIPS Pub., Jan. 1977, vol. 46.

[3] J. S. L. Brown and J. Pieprzyk, "LOKI—A cryptographic primitive for authentication and secrecy application," in *Advances in Cryptology—AUSCRYPT* (Lecture Notes in Computer Science), vol. 453. Berlin, Germany: Springer, 1990, pp. 229–236.

[4] A. Shimizu and S. Miyaguchi, "Fast data encryption algorithm FEAL," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 304. Berlin, Germany: Springer, 1987, pp. 267–278.

[5] R. Merkl, "Fast software encryption functions," in *Advances in Cryptology-CRYPTO* (Lecture Notes in Computer Science), vol. 526. Berlin, Germany: Springer, 1990, pp. 476–501.

[6] W. W. T. Xusick, "The REDOC-cryptosystem," in *Proc. Adv. Cryptol. CRYPTO*, in Lecture Notes in Computer Science, vol. 526, 1990, pp. 545–563.

[7] M. Ahmad, M. N. Doja, and M. M. S. Beg, "ABC optimization based construction of strong substitution-boxes," *Wireless Pers. Commun.*, vol. 101, no. 3, pp. 1715–1729, May 2018.

[8] L. Yi, X. Tong, Z. Wang, M. Zhang, H. Zhu, and J. Liu, "A novel block encryption algorithm based on chaotic S-box for wireless sensor network," *IEEE Access*, vol. 7, pp. 53079–53090, 2019.

[9] M. S. Acikkapi, F. Ozkaynak, and A. B. Ozer, "Side-channel analysis of chaos-based substitution box structures," *IEEE Access*, vol. 7, pp. 79030–79043, 2019.

[10] H. A. Ahmed, M. F. Zolkipli, and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7201–7210, May 2018.

[11] E. Tanyildizi and F. Ozkaynak, "A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps," *IEEE Access*, vol. 7, pp. 117829–117838, 2019.

[12] A. A. Alzaidi, M. Ahmad, M. N. Doja, E. A. Solami, and M. M. S. Beg, "A new 1D chaotic map and β-hill climbing for generating substitution-boxes," *IEEE Access*, vol. 6, pp. 55405–55418, 2018.

[13] S. Bukhari, A. Yousaf, S. Niazi, and M. Anjum, "A novel technique for the generation and application of substitution boxes (s-box) for the image encryption," *Nucleus*, vol. 55, no. 4, pp. 219–225, 2019.

[14] A. Razaq, H. A. Al-Olayan, A. Ullah, A. Riaz, and A. Waheed, "A novel technique for the construction of safe substitution boxes based on cyclic and symmetric groups," *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, Oct. 2018.

[15] A. Zahid, M. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Entropy*, vol. 21, no. 3, p. 245, Mar. 2019.

[16] J. Pieprzyk and G. Finkelstein, "Towards effective nonlinear cryptosystem design," *IEE Proc. E, Comput. Digit. Techn.*, vol. 135, no. 6, pp. 325–335, 1988.

[17] J. Daemen and V. Rijmen, *The Design of Rijndael-AES: The Advance Encryption Standard*. Berlin, Germany: Springer, 2002.

[18] G. Chen, Y. Chen, and X. Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic baker maps," *Chaos, Solitons Fractals*, vol. 31, no. 3, pp. 571–579, Feb. 2007.

[19] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal, and U. Y. Bhatti, "Some analysis of S-box based on residue of prime number," *Proc. Pak Acad. Sci.*, vol. 48, no. 2, pp. 111–115, 2011.

[20] M. Khan, T. Shah, and M. A. Gondal, "An efficient technique for the construction of substitution box with chaotic partial differential equation," *Nonlinear Dyn.*, vol. 73, no. 3, pp. 1795–1801, Apr. 2013.

[21] A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah, and A. Waheed, "A novel construction of substitution box involving coset diagram and a bijective map," *Secur. Commun. Netw.*, vol. 2017, pp. 1–16, 2017.

[22] N. Skipjack. (1998). *Kea Algorithm Specifications*. [Online]. Available: http://csrc.nist.org/encryption/skipjack/skipjack.pdf

[23] X. Yi, S. X. Cheng, X. H. You, and K. Y. Lam, "A method for obtaining cryptographically strong 8 × 8 S-boxes," in *Proc. IEEE Global Telecommun. Conf. Conf. Rec. (GLOBECOM)*, vol. 2, Nov. 1997, pp. 689–693.

[24] Y. Naseer, T. Shah, D. Shah, and S. Hussain, "A novel algorithm of constructing highly nonlinear S-p-boxes," *Cryptography*, vol. 3, no. 1, p. 6, Jan. 2019.

[25] A. Gautam, G. S. Gaba, R. Miglani, and R. Pasricha, "Application of chaotic functions for construction of strong substitution boxes," *Indian J. Sci. Technol.*, vol. 8, no. 28, pp. 1–5, Oct. 2015.

[26] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, Aug. 2016.

[27] G. Tang, X. Liao, and Y. Chen, "A novel method for designing S-boxes based on chaotic maps," *Chaos, Solitons Fractals*, vol. 23, no. 2, pp. 413–419, Jan. 2005.

[28] I. Hussain, T. Shah, and H. Mahmood, "A new algorithm to construct secure keys for AES," *Int. J. Contemp. Math. Sci.*, vol. 5, no. 26, pp. 1263–1270, 2010.

[29] M. T. Tran, D. K. Bui, and A. D. Duong, "Gray S-box for advanced encryption standard," in *Proc. Int. Conf. Comput. Intell. Secur.*, Dec. 2008, pp. 253–258.

[30] A. Hussain Alkhaldi, I. Hussain, and M. A. Gondal, "A novel design for the construction of safe S-boxes based on TDERC sequence," *Alexandria Eng. J.*, vol. 54, no. 1, pp. 65–69, Mar. 2015.

[31] A. A. Alzaidi, M. Ahmad, H. S. Ahmed, and E. A. Solami, "Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map," *Complexity*, vol. 2018, pp. 1–16, Dec. 2018.

[32] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyper-chaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, Jul. 2018.

[33] T. Zhang, C. L. P. Chen, L. Chen, X. Xu, and B. Hu, "Design of highly nonlinear substitution boxes based on I-Ching operators," *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3349–3358, Dec. 2018.

[34] A. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1985, pp. 523–534

[35] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1993, pp. 386–397.

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

[37] A. Ullah, S. S. Jamal, and T. Shah, "A novel scheme for image encryption using substitution box and chaotic system," *Nonlinear Dyn.*, vol. 91, no. 1, pp. 359–370, Oct. 2017.

[38] M. Ahmad and T. Ahmad, "Securing multimedia colour imagery using multiple high dimensional chaos-based hybrid keys," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 12, no. 1, pp. 113–128, 2014.

[39] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011.

[40] R. Forrié, "The strict avalanche criterion: Spectral properties of Boolean functions and an extended definition," in *Proc. Conf. Theory Appl. Cryptogr.* New York, NY, USA: Springer, 1988, pp. 450–468.

[41] S. K. Abd-El-Hafiz, A. G. Radwan, M. L. Barakat, and S. H. A. Haleem, "A fractal-based image encryption system," *IET Image Process.*, vol. 8, no. 12, pp. 742–752, Dec. 2014.

[42] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Process.*, vol. 160, pp. 45–58, Jul. 2019.

[43] X. Wang, S. Gao, L. Yu, Y. Sun, and H. Sun, "Chaotic image encryption algorithm based on bit-combination scrambling in decimal system and dynamic diffusion," *IEEE Access*, vol. 7, pp. 103662–103677, 2019.

[44] O. P. Verma, M. Nizam, and M. Ahmad, "Modified multi-chaotic systems that are based on pixel shuffle for image encryption," *J. Inf. Process. Syst.*, vol. 9, no. 2, pp. 271–286, Jun. 2013.

[45] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-Box," *Inf. Sci.*, vol. 450, pp. 361–377, Jun. 2018.

[46] K. M. Ali and M. Khan, "Application based construction and optimization of substitution boxes over 2D mixed chaotic maps," *Int. J. Theor. Phys.*, vol. 58, no. 9, pp. 3091–3117, Jul. 2019.

[47] A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map," *Eur. Phys. J. Plus*, vol. 135, no. 2, Feb. 2020.

[48] M. Khan, F. Masood, and A. Alghafis, "Secure image encryption scheme based on fractals key with fibonacci series and discrete dynamical system," *Neural Comput. Appl.*, Dec. 2019.
[49] D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlinear Dyn.*, pp. 1–13, Jan. 2020.
[50] A. Alghafis, H. M. Waseem, and M. Khan, "A hybrid cryptosystem for digital contents confidentiality based on rotation of quantum spin states," *Phys. A, Stat. Mech. Appl.*, Dec. 2019, Art. no. 123908.
[51] A. Javeed, T. Shah, and A. Ullah, "Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group," *Wireless Pers. Commun.*, Jan. 2020.
[52] Lu, Zhu, and Wang, "A novel S-box design algorithm based on a new compound chaotic system," *Entropy*, vol. 21, no. 10, p. 1004, Oct. 2019.
[53] X. Wang, Ü. Çavuşoğlu, S. Kacar, A. Akgul, V.-T. Pham, S. Jafari, F. Alsaadi, and X. Nguyen, "S-box based image encryption application using a chaotic system without equilibrium," *Appl. Sci.*, vol. 9, no. 4, p. 781, Feb. 2019.
[54] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 26203–26222, Jun. 2019.
[55] Zhu, Wang, and Zhu, "A secure and fast image encryption scheme based on double chaotic S-Boxes," *Entropy*, vol. 21, no. 8, p. 790, Aug. 2019.
[56] U. Arshad, M. Khan, S. Shaukat, M. Amin, and T. Shah, "An efficient image privacy scheme based on nonlinear chaotic system and linear canonical transformation," *Phys. A, Stat. Mech. Appl.*, Nov. 2019.

MUHAMMAD AWAIS YOUSAF received the Ph.D. degree in combinatorial group theory from the Department of Mathematics, Quaid-i-Azam University, Islamabad, in 2015. He is currently working as an Assistant Professor with The Islamia University of Bahawalpur. His main research interests are theory of group graphs, chemical graph theory, algebraic cryptography, homomorphic public-key cryptosystems over groups, and algorithms development over Galois fields.

HANAN ALOLAIYAN received the Ph.D. degree in mathematics from King Saud University, Saudi Arabia. She is currently working as an Assistant Professor with the Department of Mathematics, King Saud University, Saudi Arabia. She has published several research articles in reputable journals. Her area of research interests are algebra, analysis, and cryptography.

MUSHEER AHMAD received the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively. He is currently with the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India, as an Assistant Professor. He has published about 60 research articles in refereed journals and conference proceedings of international repute. His areas of research interest include multimedia security, chaos-based cryptography, and cryptanalysis and image processing.

MUHAMMAD DILBAR received the B.S. degree in mathematics from the Government Sadiq Egerton College Bahawalpur, Pakistan, in 2017. He is currently pursuing the M.Phil. degree with the Department of Mathematics, The Islamia University of Bahawalpur, Pakistan. His research interests include cryptography, communication security, group theory, graph theory, algebra, geometry, combinatorics, and algebraic geometry.

ABDUL RAZAQ received the Ph.D. degree from the Department of Mathematics, Quaid-i-Azam University, Islamabad, in 2015. He is currently working as an Assistant Professor with the University of Education, Lahore, Jauharabad Campus. His main research interests include combinatorial group theory, analysis, and cryptography.