IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2020.Doi Number

Efficient Dynamic S-Box Generation Using Linear Trigonometric Transformation for Security Applications

AMJAD HUSSAIN ZAHID[1], LO'AI TAWALBEH[2] (Senior Member, IEEE), MUSHEER AHMAD[3], AHMED ALKHAYYAT[4], MALIK TAHIR HASSAN[1], ATIF MANZOOR[1], AND ALAA KADHIM FARHAN[5]

[1]School of Systems and Technology, University of Management and Technology, Lahore 54700, Pakistan.
[2]Department of Computing and Cyber Security, Texas A&M University, San Antonio, TX 78224, USA.
[3]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India.
[4]Department of Computer Technical Engineering, College of Technical Engineering, The Islamic University, Najaf 54001, Iraq
[5]Department of Computer Sciences, University of Technology, Baghdad 10066, Iraq

Corresponding author: Lo'ai Tawalbeh (ltawalbeh@tamusa.edu), Musheer Ahmad (musheer.cse@gmail.com)

This work was supported by the Chancellor Research Initiative (CRI) grant awarded to Texas A&M University-San Antonio, TX, USA

ABSTRACT Protection of data transmitted over the network from illegal access is one of the major challenges being posed by exponential growth of data in online digital communication. Modern cryptosystems assist in data sanctuary by utilizing substitution-boxes (S-boxes). This paper presents a modest and novel technique to erect dynamic and key dependent S-boxes with the help of a novel linear trigonometric transformation. A new optimization plan is also suggested to improvise the nonlinearity characteristic of the preliminary S-box generated through trigonometric transformation. The proposed technique has the competence to create significant quantity of cryptographic strong S-boxes with the help of projected scheme. A specimen S-box is procreated, and standard performance criteria is applied to appraise the cryptographic strength of the resultant S-box and other known S-boxes available in the literature. Comparative performance analyses validate the noteworthy contribution of the proposed scheme for the generation of dynamic and secure S-boxes. An image privacy preserving scheme based on the proposed S-box is also suggested to validate the fact that it holds strong candidature for modern cryptosystems to protect multimedia data.

INDEX TERMS Substitution-box, Linear Trigonometric Transformation, Security, Cryptosystems.

I. INTRODUCTION

Data communication plays a vigorous role in modern digital era where rapid and innovative developments in communication technology have become daily routines. Along with it, technological advancements bring many challenges and issues too. Security of data transmitted through insecure communication channels is one of the most inevitable issues. Number of network users is growing day-by-day and nature of their diversified usage of the internet has led to an increase in the number of attacks on transmitted data [1]. Data and information are the most important assets of any organization and their protection from the intruders has become a necessity of today's life as the attackers may use captured data for malicious activities. That's why; data and information are transformed into a useless form before communication through insecure media to prevent the intruders to perform such malevolent doings. Investigators and scholars develop different approaches to safeguard the transmitted data [2]. Cryptography is the most applied realm that assists in this data transformation by employing different ciphers to provide the protection of data from attackers. Two main categories of these ciphers are referred as block and stream ciphers [3, 4]. Stream ciphers generally transform one bit or byte at one time and are slower than the block ciphers. These ciphers are used where the systems are deficient in computational resources and efficiency is not a major concern. Block ciphers accomplish the data transformation by operating on a block of bits of predefined length. Due to the easiness in implementation and simplicity in deployment, block ciphers

are commonly espoused for information security applications [5]. Block ciphers confer protection of data with the support of two main operations known as permutation and substitution which transform plaintext into a puzzling arrangement for the attackers. A permutation operation shuffles the data bits or bytes. On the other hand, a substitution operation substitutes plaintext bits or bytes with other bits or bytes which are not part of the plaintext [6]. Most eminent block ciphers employ one or more substitution boxes (S-boxes) that provide assistance in the substitution or replacement process [7-9]. An S-box is a substantial component of contemporary block ciphers and contributes much in the cohort of meaninglessness in the original data (plaintext). An S-box plays an imperative role in producing a non-linear connection among plaintext and ciphertext by inciting added muddle for the attackers of captured data from insecure communication channels. It is the solitary non-linear constituent of a block cipher and has the capability to engender more jumbles in the resultant ciphertext for the invaders as compared to other constituents of the respective block cipher that work linearly and contribute less in the protection. Consequently, the protection of plaintext provided by a block cipher that employs S-box in its structure against attacks is directly reliant on the cryptographic forte of the respective S-box [10, 11].

S-boxes employed in the working of a cipher are referred as static and dynamic one. An S-box having a constant place for each random value always is known as a static S-box. A cipher utilizing static S-box in its operations does not provide enough protection to the data as the attackers have the chance to get knowledge of such S-boxes by some means and may generate plaintext ultimately [12, 13]. Ciphers like Data Encryption Standard (DES) and Advanced Encryption Standard (AES) employed static S-boxes and invaders attempted attacks on such ciphers by taking advantage of the feebleness inherent in the corresponding S-boxes. To diminish the deficiencies and fragilities of static S-boxes, present-day block ciphers adopt the usage of dynamic S-boxes in their working to benefit from the cryptographic strengths linked with these S-boxes [14]. Dynamic S-boxes are generated with the help of a cipher key. A cautiously designed dynamic S-box has the very much capability for the intensification in the cryptographic forte engendered by the respective cipher. Subsequently, researchers have investigated different techniques to construct dynamic S-boxes which offer good cryptographic strength by using values from the respective cipher key. These methods engage diverse mathematical edifices like elliptic curves, finite field, chaotic systems, etc. to project S-boxes. A chaotic dynamical system has the competence to generate strong S-boxes due to their random-like comportment, extreme initial conditions' sensitivity, and non-periodicity [15, 16]. Consequently, many authors [15-19] have taken advantage of chaotic systems to engender vigorous S-boxes by employing diverse techniques. Hyperchaotic edifices own the potential to harvest sturdier S-boxes as compared to the simple chaotic systems. Authors like [20-24] have provoked robust dynamic S-boxes by utilizing hyperchaotic methods.

Many investigators have explored other knowledge domains for the cohort of S-boxes like cellular automata [25], elliptic curve [24, 26], DNA computing [27], graph theory [28, 29], optimization techniques [30-33], etc. Another prime method to generate robust and dynamic S-boxes is the application of linear fractional transformation (LFT) as adopted by researchers [34-36]. These LFT based S-boxes are generated using Galois Field (GF) arithmetic. AES cipher used a GF-based static S-box in its operation. As a static S-box has much dimness associated with it, many researchers [37-40] proposed plentiful enrichments to the AES S-box and the resultant S-boxes showed good cryptographic characteristics. Zahid, *et al* [41-43] presented S-box erection techniques by projecting novel and modest transformations which are simpler than the LFTs.

This research work presents a modest and innovative scheme to erect dynamic and key dependent S-boxes. This technique proposes a very simple and innovative linear trigonometric transformation (LTT). The proposed LTT is dynamic in its working and helps in the erection of a preliminary 8×8 S-box. The preliminary S-box outcomes are further improved by engaging a novel scheme of improving the security strength of S-boxes. Being dynamic in nature, both transformation and the performance improvisation plan use different parameters/variables in the construction and cipher key employs the values to the respective parameters. A change in the cipher key brings changes in the parameters' values and each time a new S-box is spawned. Major contributions of our work are as follows:

- A simple, innovative, and dynamic linear trigonometric transformation (LTT) is put forward to erect a preliminary S-box. As the transformation is dynamic in nature, it has the capability to produce a huge number of sturdy S-boxes when slight changes are made in the parameters' values.
- A novel and dynamic performance improvisation plan is projected to improvise the nonlinearity of the preliminary S-box generated by the innovative LTT. Eventual S-box produced using this heuristic plan is capable to produce further jumble in the ciphertext for the attackers.
- A standard S-box criterion is applied to evaluate the cryptographic strength of the resultant S-box and other rampant S-boxes available in the literature. Comparative performance analysis indorses the noteworthy contribution of the projected scheme for the erection of dynamic and sturdy S-boxes.

- A fast and efficient image protection scheme having high throughput is also suggested using proposed S-box to demonstrate its suitableness for multimedia data encryption.

This paper comprises of four sections. In section II, scheme for S-box generation is proposed which employs a novel trigonometric transformation and a dynamic performance improvisation plan. In section III, a specimen S-box is presented along with its recital as well as comparative investigation with some recently projected S-boxes. A new image encryption scheme based on proposed S-box is presented and analyzed in section IV. Finally, section V presents the conclusion of the work done.

II. PROPOSED SCHEME FOR S-BOX DESIGN

Investigators project techniques for the construction of S-boxes which are used in block ciphers to provide protection to the data from the attackers. An S-box contributes much to produce meaninglessness in the plaintext before its transmission and thus engenders more jumbles in the resultant ciphertext for the invaders. Therefore, researchers and scholars attempt to discover innovative transformations which assist in the erection of robust S-boxes. Here, we put forward a modest and novel technique by proposing an innovative and dynamic linear trigonometric transformation and a distinctive heuristic evolution plan to erect dynamic and robust S-boxes having a commendable cryptographic strength. A detailed description of proposed methodology for the engendering of the project S-box comprising of the two modest phases of (1) novel linear trigonometric transformation (LTT), and (2) Innovative performance improvisation plan.

A. NOVEL LINEAR TRIGONOMETRIC TRANSFORMATION

An n × n S-box is generated by utilizing a novel and dynamic linear trigonometric transformation (LTT). This novel transformation has a mathematical description in the form of a function given in Eq. (1) as:

$$T(z) = \mathrm{Cos}\,(\,(A + B) * X * z + C\,) \qquad (1)$$

Where,

$0 < X < 1$,

$0 \le z \le (2^n - 1)$, $B \in z$, and

$A, C = \{1, 3, \ldots, 2^n - 1\}$.

Values of variables A, B, C, and X in Eq. (1) are employed by the cipher key. Variable X has data type as double and 15 significant decimal digits have been considered for the generation of S-box using proposed method. The computation using such a variable is a bit slow as compared to float type. But, it gives huge key space to an S-box designer compared float type variable. Dynamic nature of Eq. (1) yields a huge number of key-dependent dynamic S-boxes (S-box space = $128 \times 256 \times 128 \times 10^{15} \sim 10^{21}$) using different values of above-mentioned parameters. For n=8, a preliminary $n \times n$ S-box is erected with the help of Eq. (1), procedure given in algorithm 1, and the flowchart presented in Figure 1. The proposed method involves a large number of parameters which may lead to some enhancement in the cryptographic strength of generated S-box by reducing the possibilities of brute force attacks. But, it causes an increase in the computational time of the proposed method. Variable X is providing such capability with its range to avoid brute force attacks while computational efficiency is not much compromised.

Algorithm 1 : Preliminary 8 × 8 S-box Generation

Input parameters:

```
n = 8   // for n × n S-box
X       // 0 < X < 1
A, C    // A, C ∈ { 1, 3, ..... , 2^n - 1 }
B       // B ∈ { 0, 1, 2, ..... , 2^n - 1 }
```

Output:

```
S       // Preliminary 8 × 8 S-box
```

Initializations:

```
h ← 0
g ← -1
Loc ← 0
while ( h <= 255 ) do
    R ← ( A + B ) * X
    B[ h ] = Cos ( R * h + C )
    if ( X > 0.5 ) then
        X = X * X
    else
        X = X * 1.75
    endif
    h ← h + 1
endwhile
g ← g + 1
while ( g <= 255 ) do
    MIN ← B [ 0 ]
    Loc = 0
    h ← 0
    while ( h <= 255 ) do
        if ( MIN > B[ h ] ) then
            MIN = B[ h ]
            Loc = h
        endif
        h ← h + 1
    endwhile
    S[ g ] = Loc
    B[ Loc ] = 111
    g ← g + 1
endwhile
```

return S

B. PERFORMANCE IMPROVISATION PLAN

This phase assists in shuffling the values of the preliminary S-box erected by the procedure as described in Figure 1. Performance improvisation plan in the proposed method contributes a vigorous role to generate sturdy and strong S-boxes having feature of high nonlinearity. The nonlinearity improvisation plan is portrayed in Figure 2 and described in algorithm 2. Values of variables A, B, C, and X are employed by the cipher key. An example 8×8 S-box erected using the proposed method is shown in Table 1.

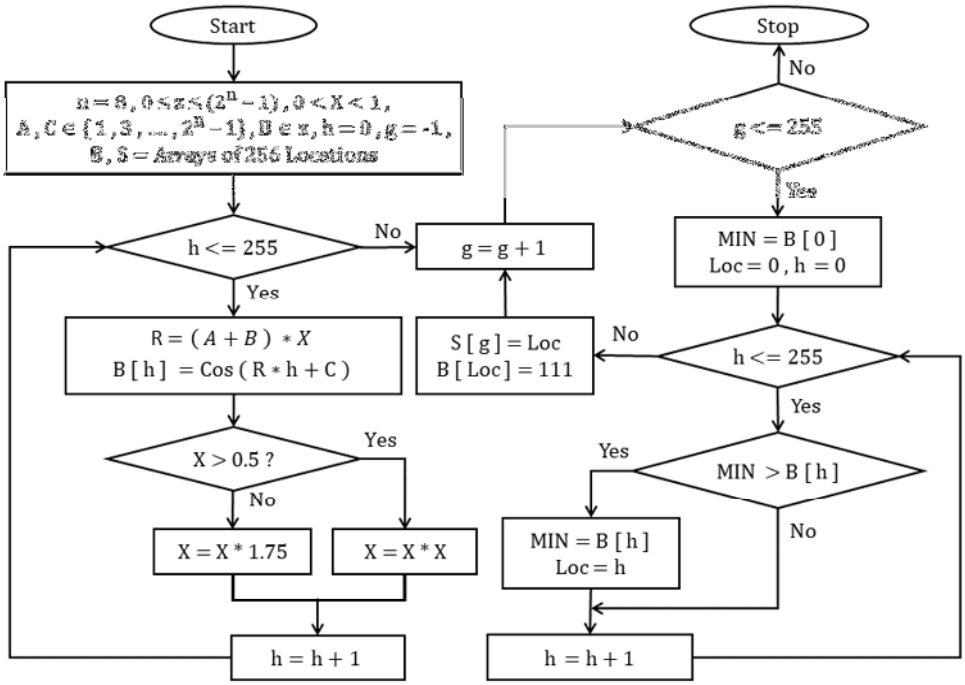


FIGURE 1: **Flowchart for the preliminary S-Box generation**

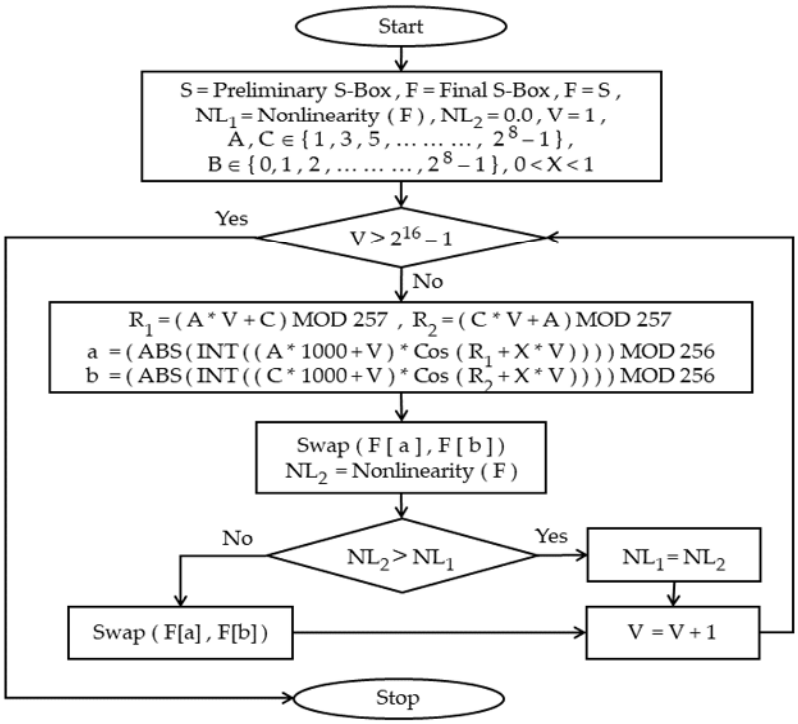


FIGURE 2: **Nonlinearity performance improvisation plan**

Algorithm 2 : Final S-box generation based on nonlinearity improvisation plan

Input parameters:

X // $0 < X < 1$

A, C // $A, C \in \{ 1, 3, \ldots\ldots, 2^n - 1 \}$

B // $B \in \{ 0, 1, 2, \ldots\ldots, 2^n - 1 \}$

S // *Preliminary* 8 × 8 S-box

Output:

F // *Final* 8 × 8 S-box

Initializations:

$V \leftarrow 1$

$F = S$

$NL_1 \leftarrow$ *Nonlinearity (F)*

// Nonlinearity (F) returns nonlinearity of S-box F

$NL_2 \leftarrow 0.0$

while ($V <= 2^{16} - 1$) *do*

$R_1 \leftarrow (A * V + C)$ *MOD* 257

$R_2 \leftarrow (C * V + A)$ *MOD* 257

$R_3 \leftarrow (A * 1000 + V)$

$R_4 \leftarrow (C * 1000 + V)$

$R_5 \leftarrow (R_1 + X * V)$

$R_6 \leftarrow (R_2 + X * V)$

$a \leftarrow ABS (INT (R_3 * Cos (R_5)))$ *MOD* 256

$b \leftarrow ABS (INT (R_4 * Cos (R_6)))$ *MOD* 256

// INT returns an integer from a fractional value

// ABS returns absolute value

// Swap values F[a] and F[b]

Temp $\leftarrow F [a]$

$F [a] \leftarrow F [b]$

$F [b] \leftarrow$ *Temp*

$NL_2 \leftarrow$ *Nonlinearity (F)*

if ($NL_2 > NL_1$) *then*

$NL_1 \leftarrow NL_2$

else

// Swap values F[a] and F[b]

Temp $\leftarrow F [a]$

$F [a] \leftarrow F [b]$

$F [b] \leftarrow$ *Temp*

endif

$V \leftarrow V + 1$

endwhile

return F

III. SECURITY ANALYSIS OF PROJECTED S-BOX

An S-box erected using a particular technique may be a weak S-box and hence an easy target of invaders. A strong S-box has the potential to defy such attempts and provides protection to data. To assess the cryptographic strength of any S-box, different criteria are utilized that must be satisfied by the respective S-box to justify its forte. This segment scrutinizes and quantifies the cryptographic forte of the proposed S-box portrayed in Table 1 by engaging standard evaluation criteria presented in [44]. The performance assessment of proposed S-box and some other recently projected S-boxes is made with respect to the standard criteria. Proposed S-box satisfies all the criteria in a graceful manner. Analyses and performance comparison of such S-boxes are described below.

A. BIJECTIVITY

Bijectivity criterion demands that a unique n-bit input of an n × n S-box should produce a unique output of n-bits. Similarly, for any n-bit output of an n × n S-box, there should be a distinct n-bit input. Proposed n × n S-box for n = 8 portrayed in Table 1 validates this criterion very well as unique inputs harvests unique outputs. Typical bijectivity value of an 8 × 8 S-box is $2^{8-1} = 128$ [26]. It is evident that our proposed S-box has this count as 128 for each of the coordinate Boolean functions. Consequently, bijectivity criterion is validated by proposed S-box in an attired way.

B. NONLINEARITY

An 8×8 S-box offers an association between 8-bit input and 8-bit output. If this association is linear, the cryptographic forte of the respective S-box is feeble and it creates a possibility for the invaders to attack the ciphertext in a successful manner. If an S-box is carefully designed to have this association as nonlinear, it presents more cryptographic strength against the attacks. Application of such S-boxes in the cryptosystems provides a strong shield to resist linear cryptanalytic attacks. This nonlinear mapping (nonlinearity) offered by an n × n S-box is computed using Eq. (2) [44]:

$$NL(B) = [\, 2^n - (W_{max} (B)) \,]\frac{1}{2} \qquad (2)$$

Where, B represents an n-bit Boolean function and $W_{max}(B)$ denotes the value of the Walsh-Hadamard Transformation. If nonlinearity (NL) score of an S-box is high, it offers more resistance to the linear cryptanalytic attempts. Each of the constituent Boolean function of proposed S-box and its respective nonlinearity score is presented in Table 2 and graphically illustrated in Figure 3.

TABLE 1. EXAMPLE S-BOX WITH PARAMETERS A=181, B=185, C=17, AND X =0.58203125

145	28	185	205	30	255	249	1	85	13	158	211	210	239	224	191
138	220	182	97	197	245	90	35	165	130	41	131	104	203	108	228
142	226	93	178	65	12	46	233	81	171	112	63	87	57	175	254

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

TABLE 2. CONSTITUENT BOOLEAN FUNCTIONS AND NL SCORES

Boolean Function	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8
NL(B)	112	112	112	110	112	112	110	112

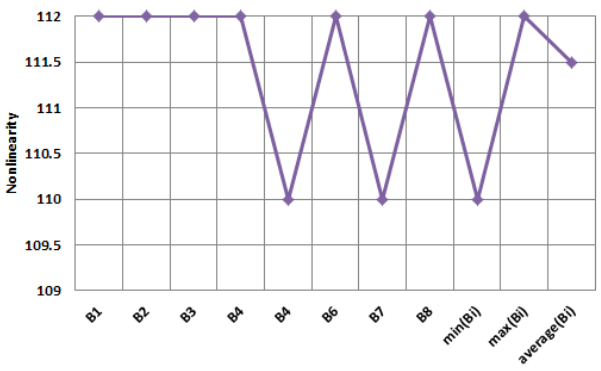


FIGURE 3: **Nonlinearity of component Boolean functions of proposed S-Box**

Both the presentations validate that the proposed S-box has $NL_{Max} = 112$, $NL_{Min} = 110$, and $NL_{Avg} = 111.5$ respectively. A comparison between nonlinearity scores of Boolean functions of proposed S-box and those of rampant S-boxes available in the literature is made in Table 3. It is evident from Table 3 that the average nonlinearity score of proposed S-box is higher than the average NL score of most of the other current S-boxes in literature and nearly at par with other strong S-boxes except few S-boxes.

TABLE 3. NONLINEARITY (NL) SCORES FOR DIFFERENT S-BOXES

S-Box	Publication Year	Nonlinearity Score		
		NL_{Min}	NL_{Max}	NL_{Avg}
Proposed	-	110	112	111.5
Ref. [8]	2021	106	108	106.25
Ref. [23]	2020	112	112	112
Ref. [24]	2021	106	110	106.5
Ref. [35]	2020	112	112	112
Ref. [45]	2021	106	108	107.0
Ref. [46]	2020	106	108	106.5
Ref. [47]	2020	104	110	106.75
Ref. [48]	2020	102	108	105.0
Ref. [49]	2020	100	108	105.0
Ref. [50]	2020	104	108	106.25
Ref. [51]	2011	96	110	104.0
Ref. [52]	2020	106	112	109.5
Ref. [53]	2020	100	108	104.0
Ref. [54]	2020	98	106	103.5
Ref. [55]	2020	106	108	106.5
Ref. [56]	2020	104	110	106.25
Ref. [57]	2021	104	108	105.0
Ref. [58]	2021	106	110	108.5
Ref. [59]	2021	108	110	109.75
Ref. [60]	2021	102	110	106.5
Ref. [61]	2020	112	112	112
Ref. [62]	2020	112	112	112
Ref. [63]	2020	110	112	110.25
Ref. [64]	2021	104	108	105.5
Ref. [65]	2021	104	110	107

C. STRICT AVALANCHE CRITERION (SAC)

This criterion is a vigorous topography of a robust S-box and was presented by Webster et al [66]. According to SAC, if any single input bit is changed, this change should modify half of the output bits. A typical SAC score of approximately

equal to 0.5 is deemed as adequate. Dependency matrix of proposed S-box SAC scores is demonstrated in Table 4.

TABLE 4. DEPENDENCY MATRIX OF PROPOSED S-BOX

0.4688	0.5469	0.5625	0.5000	0.5000	0.4375	0.4688	0.5000
0.5313	0.5000	0.5625	0.5469	0.5625	0.5313	0.4844	0.5156
0.4844	0.4531	0.5469	0.4375	0.4844	0.5000	0.5000	0.5000
0.4844	0.5469	0.5000	0.5469	0.5469	0.4844	0.5000	0.4375
0.5313	0.4844	0.5000	0.4688	0.5000	0.5000	0.5313	0.5313
0.5469	0.4688	0.4844	0.5156	0.5156	0.5000	0.5313	0.5313
0.5313	0.4844	0.5156	0.5156	0.5313	0.4531	0.5000	0.5156
0.5000	0.4844	0.5469	0.5625	0.5313	0.4531	0.5000	0.4375

Average SAC score of our S-box is 0.506 and it substantiates that the proposed S-box justifies SAC decently. A comparison between SAC score of proposed S-box and SAC scores of S-boxes available in the literature is given in Table 6 and it provides evidence that our S-box has consistent performance with other S-boxes.

D. BIT INDEPENDENCE CRITERION (BIC)

This criterion is another vital topography of a strong S-box and was presented by Webster et al [66]. According to BIC, any two output bits should change independently if any single input bit is changed. Table 5 demonstrates the BIC-Nonlinearity values of our S-box.

TABLE 5. BIC-NONLINEARITY SCORES OF PROPOSED S-BOX

-	104	104	104	104	104	102	106
104	-	106	106	104	108	104	104
104	106	-	104	108	98	102	104
104	106	104	-	104	106	102	104
104	104	108	104	-	104	104	104
104	108	98	106	104	-	104	106
102	104	102	102	104	104	-	104
106	104	104	104	104	106	104	-

Average score of BIC-Nonlinearity (BIC-NL) comes out to be 104.2 which indicate that any two output bits have feeble dependence on each other, and proposed S-box justifies BIC in an eminent way. A comparison between BIC-NL score of proposed S-box and BIC-NL scores of S-boxes available in the literature is given in Table 6 and it provides evidence that our S-box has solid performance than many other S-boxes.

TABLE 6. PERFORMANCE ASSESSMENT OF SAC AND BIC-NL SCORES

S-Box Method	SAC	BIC-NL
Proposed	0.506	104.2
Ref. [8]	0.5086	102.37
Ref. [23]	0.496	102.3
Ref. [24]	0.5009	103.93
Ref. [35]	0.498	112
Ref. [45]	0.493	102.3
Ref. [46]	0.499	103.6
Ref. [47]	0.509	106.1
Ref. [48]	0.503	102.9
Ref. [49]	0.500	103.0
Ref. [50]	0.501	103.6
Ref. [51]	0.493	103.0
Ref. [52]	0.507	106.9
Ref. [53]	0.497	102.6
Ref. [54]	0.496	103.5
Ref. [55]	0.501	104.1
Ref. [56]	0.503	103.9
Ref. [57]	0.506	103.5
Ref. [58]	0.500	103.9
Ref. [59]	0.5042	110.6
Ref. [60]	0.4943	103.35
Ref. [61]	0.501	112
Ref. [62]	0.495	112
Ref. [63]	0.495	104.1
Ref. [64]	0.5065	103.57
Ref. [65]	0.4993	103.29

E. DIFFERENTIAL UNIFORMITY (DU)

One of the greatest active attacks a block cipher faces is the differential cryptanalysis. Whenever there is a change in the input, output should change in a uniform way which is known as differential uniformity. Changes in the input should not change respective output in an imbalance way. Attackers capture the ciphertext, make attempt to analyze it, and get input and output differentials or imbalances. If a cautious analysis of these differences is made, an invader gets the opportunity to have the clue of inputs (key or plaintext) [67]. Differential uniformity (DU) helps to calculate the difference of input and output changes. If the difference is less (that is, value of DU is less), an S-box has the potential to defy the differential cryptanalysis. Eq. (3) is used to compute the DU value for an n × n S-box B.

$$DU = \underset{\Delta_c \neq 0,\ \Delta_d}{Maximum} [\#\{c \in P | B(c) \oplus B(c \oplus \Delta_c) = \Delta_d\}] \quad (3)$$

where,

Δ_c = Input differential, Δ_d = Output differential, and
P = {0, … … , 2^n - 1}.

Differential uniformity scores of the proposed S-box are shown in Table 7. It can be observed that the proposed S-box has 10 as the largest value of DU and consequently, 0.039 is the value of differential probability (DP). These lesser scores validate that the proposed S-box is promising enough to dissent differential cryptanalytic attempts. A comparison between DP score of proposed S-box and DP scores of S-boxes available in the literature is given in Table 8. This comparison justifies it rightly that our S-box has the potential to antagonize the differential cryptanalysis.

TABLE 7. VALUES OF DIFFERENTIAL UNIFORMITY OF PROPOSED S-BOX

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

F. LINEAR APPROXIMATION PROBABILITY (LAP)

The main objective behind the design of a good cipher is to generate a nonlinear association between its input and output. This nonlinear association helps in creating a ciphertext that bears more meaninglessness for its invaders. An S-box generated in a thought-provoking way assists in achieving such a nonlinear mapping conveniently. Attackers attempt to exploit the weaker mapping between input and output by linear cryptanalysis. Linear probability helps in measuring the forte of this association using Eq. (4) [68].

$$LAP = \max_{x_t,\ y_t \neq 0} \left| \frac{1}{2^n} (\#\{t \in R |\ t.x_t = F(t).y_t\}) - \frac{1}{2} \right| \quad (4)$$

where,

x_t , y_t = input and output masks
R= {0, 1, 2, …. , 2^n - 1}.

A nonlinear association between input and output gives low value of linear probability and linear cryptanalysis becomes challenging. Our S-box has score of linear probability equal to 0.125 that validates the capability of the proposed S-box to resist linear cryptanalysis. A comparison between LAP score of proposed S-box and LAP scores of S-boxes available in the literature is given in Table 8. This comparison validates that our S-box has the potential to antagonize the linear cryptanalysis.

TABLE 8. RECITAL COMPARISON OF DP, LAP, AND FIXED POINTS OF DIFFERENT S-BOXES

S-Box	DP	LAP	FPs
Proposed	0.039	0.125	0
Ref. [8]	0.047	0.1484	1
Ref. [23]	0.039	0.141	4
Ref. [24]	0.039	0.125	0
Ref. [35]	0.016	0.063	0
Ref. [45]	0.047	0.141	1
Ref. [46]	0.039	0.125	0
Ref. [47]	0.031	0.113	2
Ref. [48]	0.047	0.1484	1
Ref. [49]	0.047	0.125	0
Ref. [50]	0.039	0.139	0
Ref. [51]	0.031	0.125	1
Ref. [52]	0.031	0.1328	0
Ref. [53]	0.039	0.137	0
Ref. [54]	0.055	0.1328	0
Ref. [55]	0.039	0.1328	0
Ref. [56]	0.039	0.1328	1
Ref. [57]	0.039	0.125	2

Ref. [58]	0.039	0.109	1
Ref. [59]	0.023	0.0859	1
Ref. [60]	0.0468	0.1468	1
Ref. [61]	0.016	0.063	4
Ref. [62]	0.016	0.063	1
Ref. [63]	0.039	0.125	1
Ref. [64]	0.039	0.1328	1
Ref. [65]	0.039	0.1328	1

G. FIXED POINTS ANALYSIS (FPA)

An S-box B is said to have a fixed point (FP) in it if $B(v) = v$ for some v. The presence of such fixed point(s) in an S-box offers a weak point to the attackers to get some part of the ciphertext. AES cipher had some FP's in its S-box and its designers overcame this problem with the help of an additive constant (0×63) [42, 49]. An S-box should be designed keeping in view this weakness of fixed points to avoid the attacks [48]. The proposed S-box given in Table 1 is free of any fixed point and thus fulfills FP criterion elegantly. Some prevailing S-boxes as shown in Table 8 have different number of fixed points and offer weakness to the attackers.

H. COMPUTATIONAL EFFICIENCY

Numerous methods have been proposed in literature to produce S-boxes of size 8×8 with nonlinearity greater than or equal to 111. The principal advantage of our projected technique is the competence to produce huge number of such S-boxes. To witness the computational efficiency of the proposed and contemporary methods, we employed Visual C# and run the code on 2.2 GHz Intel Core i7 CPU and 4GB RAM. Final S-box by proposed method is generated with an aim to extemporize the nonlinearity of the preliminary S-box. Computational efficiencies of our proposed scheme and published S-box studies [23, 35, 61, 62] are described in Table 9. Average time (in seconds) over 1000 final S-boxes and average number of iterations were observed for each method with the target nonlinearity greater than or equal to 111.5. It can be observed from Table 9 that our average computational time to construct S-box is quite inspiring as compared to the computational time of [23,35] while nonlinearity values are approximately alike.

TABLE 9. COMPUTATIONAL TIME (SECONDS) OF DIFFERENT S-BOX METHODS

Method	Average Time	Iterations	Nonlinearity
Ref. [23]	403	~ $10^{4.73}$	112
Ref. [35]	367	~ $10^{4.27}$	112
Ref. [61]	213	~ 10^{3}	112
Ref. [62]	293	~ $10^{3.93}$	112
Proposed	283	~ $10^{3.87}$	111.5

Nonlinearity improvisation plan employed is contributing significantly in the proposed technique in the construction of robust and sturdy S-boxes. As the fortification of one's data has the supreme concern and standing, this facet can't be conceded while keeping in view the computational powers of today's CPU. For the projected method, the computation largely emanates from the nonlinearity improvisation plan (phase-2) given in Figure 2. Accordingly, one requires repeating Eq. (1) for 2^n times along with 2^{n+1} iterations to produce a preliminary S-box of size $n \times n$ i.e. about $(2^n + 2^{n+1})$ iterations are needed for phase-1. The computational complexity for preliminary S-boxes is $O(2^n)$. According to the Figure 2, one requires to repeat the operations 2^{2n} times to evolve a final S-box i.e. about 2^{2n} iterations are required to operate leading to a complexity of $O(4^n)$ assuming some constant number of average cycles for cosine and other functions. As a result, time complexity accumulates asymptotically to $O(4^n)$ for the proposed method.

Compared to AES S-box, the proposed method comprises higher computation time because the anticipated method performed computations involving many parameters. The incorporation of parameters creates the dynamism in the proposed method and enormous number of dynamic and key-dependent S-boxes can be generated by altering the initial values of parameters. The computation time (in seconds) of AES S-box is about 0.5 and 0.2 using Extended Euclidean Algorithm (EEA) and Look-Up Table (LUT) methods, respectively. However, the final S-box generation using proposed method takes computation time of about 283 seconds. But, this time is slightly better than few of the optimization-based S-box studies as shown in Table 9. Additionally, one of the merits of the proposed method over AES S-box, which is static, is that has the feature of dynamic S-box generation and around 10^{21} dynamic S-boxes can be constructed using proposed method.

I. COMPARATIVE ANALYSIS

In literature, many studies have been investigated through innovative methods to produce S-boxes having nonlinearity. Many S-box methods are lacking one or more sanctuary canons like static permutation method [35], use of irreducible polynomial of static nature [61, 35], presence of fixed points [23,34,47,51,57-62], high computational cost [23, 35] etc. Our proposed method for the construction of S-box engages simple, pioneering, and linear trigonometric transformation (LTT) along with a novel and dynamic nonlinearity improvisation plan.

The comparison of lineaments of proposed S-box is made in Table 3, 6 and 8 for the standard parameters. We selected the recently investigated S-box studies for the comparison. Each of the S-box studies has already done their performance comparison analysis with earlier S-box methods. Whereas, the comparison of computational

efficiency of proposed method is done in Table 9. Nonlinearity is considered liable for resisting all linear approximation attacks. Therefore, the proposed method involves the nonlinearity improvisation plan as the technique for evolving preliminary S-box for over all nonlinearity feature of the S-box. Table 3 makes it evident that the proposed S-box has considerably higher nonlinearity performance over many recently investigated S-boxes in [8, 24, 46-60, 63-65]. The excellent nonlinearity performance over many existing studies demonstrates that the proposed method is fairly effective in making the high nonlinear transformation of plaintext to ciphertext as compared to other methods.

Table 6 presented the comparison of strict avalanche criterion and bits independence criterion. A strong S-box should be able to alter 50% of output bits whenever a single bit at the input side is flipped. According to Webster and Tavares, a strong S-box should have a SAC value as close to 0.5 as possible. Table 6 indicates that the proposed S-box's SAC score is pretty close to 0.5 and better than many recent S-box methods listed in the Table. Moreover, the pair-wise disjoint Boolean functions comprising the S-box should have as high nonlinearity as possible. We can see that the BIC-nonlinearity score of our S-box is 104.2 which is higher than many S-boxes suggested in [8, 23,24,45,46,48-51,53-5860,63-65] indicating the decent performance of proposed S-box. Hence, the proposed method has the ability to satisfy the SAC and BIC criterions well.

The comparison of abilities of S-boxes to mitigate the differential and linear cryptanalysis is accomplished in Table 8 along with existence of fixed points. Comparison analysis indicates that our S-box has better ability to resist differential cryptanalysis than S-boxes available in [8,45,48,49,54,60] and it is comparable with others. The LAP score of 0.125 is also slightly better than many S-boxes such as [8,23,45,48,50,52-56,60,64,65]. But, S-boxes presented in [35,47,58,59,61,62] show better LAP than our S-boxes. Absence of fixed points is also another significant criterion to assess the security strength of S-boxes. The proposed S-boxes doesn't have any fixed points. But, a number of S-box found to have 1 or more fixed points as in [8,23,45,47,48,51,56-65].

IV. PROPOSED IMAGE SECURITY SCHEME USING S-BOX

The image data has been increasingly becoming the most preferable means of communication. It is always necessary to employ some mechanism which can protect the user's image data from illegal access and illegitimate manipulation [69,70]. The encryption scheme should have the features of simplicity, robustness, low computation, and statistically strong. This section is devoted to the application of proposed S-box given in Table 1 to validate its suitability and appropriateness for digital image encryptions. In comparison to chaos-based image encryption methods, S-box based methods are simpler, faster and hold good encryption quality. Here, a simple and plain-image dependent encryption process is executed which is truly based on the S-box data. The proposed S-box based image encryption procedure involves randomly chosen elements from S-box as the encryption key streams to obtain the encrypted pixel. In order to make the encryption procedure to resist the cryptanalysis, the plain-image dependent hash data is generated by executing the SHA-256 function on the pending plain-image data. The plain-image specific 256-bit hash digest is converted into 32 blocks of 8-bits each. Out of the 32 blocks, one block is selected randomly based on the parameter C0. The parameter C0 is employed to encrypt the pixels of image in cipher block chaining mode of operation so that any illegal change gets dispersed to the all pixels of the encrypted image. Randomly selected 8-bit block is further decomposed into two, lower and upper, nibbles. The obtained nibbles are converted into their corresponding decimal values n_1 and n_2. These two randomly generated decimal values decide the element of the S-box located at (n_1, n_2). This encryption key element from S-box is incorporated to encrypt the current pixel of the plain-image in CBC mode along with parameter C0. The whole process is repeated for every pixel of the image to get the encrypted image C. The steps of the suggested encryption scheme are as follows.

1. Read pending plain-image PP of size M×N to be encrypted.
2. Read the S-box given in Table 1 as SB.
3. Convert image PP into 1-D array as $D = reshape(\text{PP}, 1, \text{M}\times\text{N})$
4. Convert image data D into hex format as $msg = hex\text{-}format(D)$
5. Find 256-bit digest with respect to pending image data msg as $H = SHA256(msg)$
6. Convert the digest H into chunks of 8-bits as:
   $H = H_1, H_2, \ldots, H_{32}$.
7. Take C0
8. Repeat following for each pixels of image PP
   $n = 1 + [\text{C0}] mod(32)$
   $[n_1, n_2] = nibbles(H_n)$
   $K = SB(n_1, n_2)$ // key K is element from S-box SB
   $C(i, j) = PP(i, j) \oplus K \oplus C0$
   $C0 = C(i, j)$
   Where, $i = 1 \sim M, j = 1 \sim N$.
9. Declare C as the encrypted image

The proposed S-box based image encryption procedure is also illustrated using flowchart shown in Figure 4. The S-box based image encryption method is simulated for gray-scale images, but same can be easily scaled to encrypt color images as well. The simulation of suggested encryption method is performed over two widely adopted standard images namely: *Lena* and *Baboon* plain-images of size 256×256. The plain-images and encrypted images from suggested S-box based encryption procedure are shown in Figure 5 along with their corresponding histograms. The security performance analysis of encryption quality offered by the anticipated encryption method is assessed and discussed in the subsequent sections.

A. MAJORITY LOGIC CRITERION

The majority logic criterion (MLC) is one of the widely adopted analyses used to assess the quality of S-box based encryption method [51, 52]. This is set of different parameters that are based on the data obtained from gray-level co-occurrence matrix (GLCM). The set consists of *entropy*, *contrast*, *energy*, *homogeneity*. The descriptions of these parameters of MLC suite are presented in Table 10. These parameters are analyzed for both the plain-images and encrypted-images to get a quantifiable understanding of encryption quality offered by the anticipated encryption method. The computed scores of MLC parameters for Lena and Baboon images are shown in Table 11. The obtained scores for encrypted images demonstrate consistent performance of the suggested S-box based encryption approach.

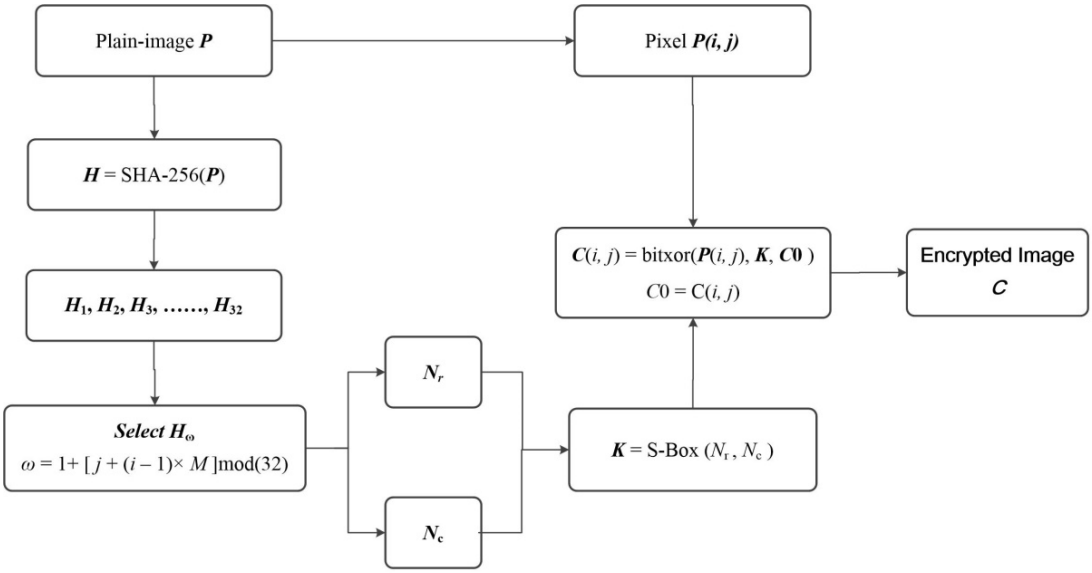
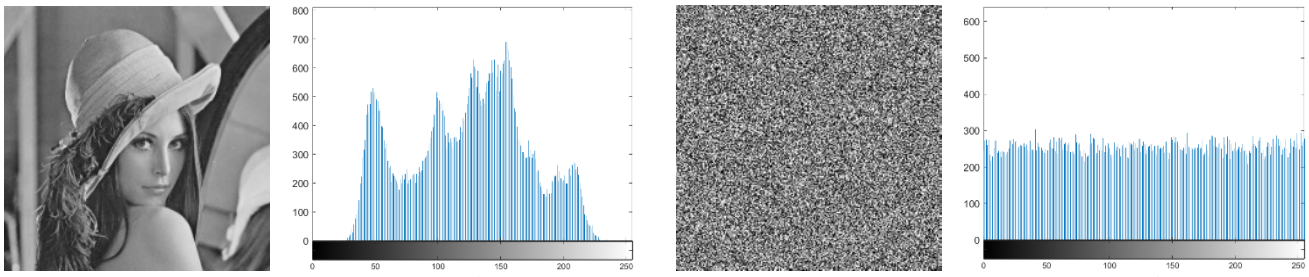
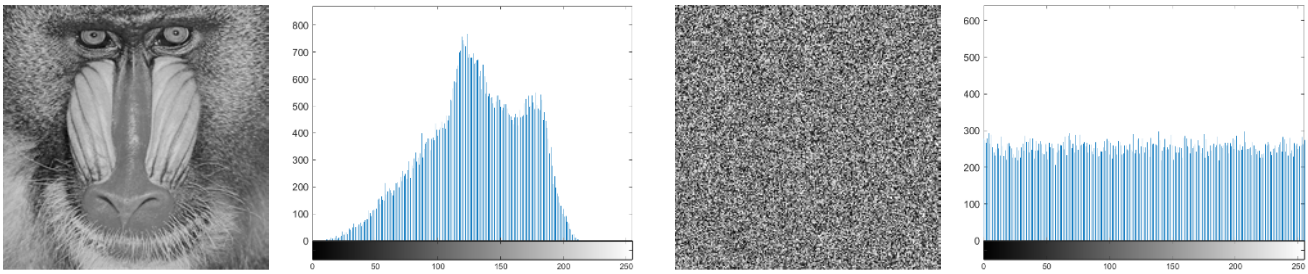


FIGURE 4: **Proposed S-box based image encryption method.**



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



(e) (f) (g) (h)

FIGURE 5: **Visual and pixels distribution plots of test images: Lena image (row-1) (a) plain-image, (b) histogram of plain-image, (c) encrypted image, (d) histogram of encrypted image; Baboon image (row-2)) (e) plain-image, (f) histogram of plain-image, (g) encrypted image, (h) histogram of encrypted image**

TABLE 10. DESCRIPTION OF DIFFERENT PARAMETERS UNDER MLC TEST SUITE

Parameter	Description	Formula
Entropy	Corresponds to the randomness content in an image. A perfect random image has ideal entropy of 8. The encrypted image is expected to have entropy as close to 8 as possible.	$-\sum_{i} p(s_i) log_2(p(s_i))$
Correlation	Measures the resemblance the adjacent pixels in an image have. Pixels of meaningful images have high correlation among its adjacent pixels. Whereas, the encrypted image should have correlation among its adjacent pixels close to 0.	$\sum_{m}\sum_{n}\left[\frac{(m-\mu m)(n-\mu n)}{\sigma_m \sigma_n}\right]$
Contrast	Computes the intensity level of contrast in the vicinity of pixels in an image. A high contrast of encrypted image indicates that the encryption has satisfied the contrast test well.	$\sum_{m}\sum_{n}\lvert m-n\rvert^2 p(m,n)$
Energy	Refers to the rate of change in color or brightness of pixels in the image. It is the sum of squared elements in the GLCM matrix of an image. Encrypted image tends to have low energy compared to plain-image.	$\sum_{m}\sum_{n} p(m,n)^2$
Homogeneity	Meaningful images have dispersed and distributed pixels values and have various peaks in its histograms. Homogeneity determines the closeness of distributed values of Gray Level Co-occurrence Matrix to GLCM diagonal.	$\sum_{m}\sum_{n}\frac{p(m,n)}{1+\lvert m-n\rvert}$

Table 11. MLC RESULTS OF ENTROPY, CORRELATION, CONTRAST, ENERGY, HOMOGENEITY FROM PROPOSED S-BOX BASED ENCRYPTION

Image / Parameters	Plain-image		Encrypted-image	
	Lena	Baboon	Lena	Baboon
Entropy	7.44392	7.26493	7.99689	7.99674
Correlation	0.9026	0.75256	0.010142	0.005698
Contrast	0.29636	0.77625	10.4323	10.4178
Energy	0.12660	0.08984	0.01564	0.01563
Homogeneity	0.89488	0.764468	0.39102	0.39157

The MLC results from our proposed scheme are compared in Table 12 with results of S-box based encryption schemes investigated in [47, 71, 72]. The entropy values from our scheme are quite better, correlation scores are better than scores available in [47, 72], contrast results are again better than all three schemes, energy and homogeneity values for encrypted content are slightly better than values obtained in Ref. [47]. Thus, our proposed scheme offers good encryption effect and satisfies all MLC criterions well.

Table 12. COMPARISON OF MLC RESULTS FOR S-BOX BASED IMAGE ENCRYPTION SCHEMES

Parameters	Proposed		Ref. [71]		Ref.[72]	Ref. [47]
	Lena	Baboon	Lena	Baboon	Baboon	Lena
Entropy	7.9968	7.9964	7.9564	7.9553	7.3583	7.9353
Correlation	0.01014	0.00568	0.00088	0.0087	0.0343	0.0487
Contrast	10.433	10.418	10.2301	10.346	9.8414	9.9764
Energy	0.01564	0.01563	0.0157	0.0157	0.0161	0.0161
Homogeneity	0.391	0.3915	0.3917	0.3895	0.4084	0.4131

B. DIFFERENTIAL ATTACK ANALYSIS

The main goal of the attacker is to get partial or full knowledge of secret data which has been legally encrypted by the sender for its genuine user at the receiver side. The normal practice of attackers is to make some changes in the

plain-images and get the corresponding encrypted images and analyze the pairs to achieve their target. One of the methods to make this approach of attackers none and void is to make the encryption process highly plain-image dependent so that an entirely different encrypted data gets obtained as output of encryption machine even if plain-image is minutely different. Any encryption scheme able to hold this feature will be deemed able to mitigate such differential attacks for illegitimate access of secret data [48, 56]. Our proposed S-box encryption scheme holds this feature of overcoming the differential analysis of attackers. In order show and quantify this feature, there exists performance metrics for differential analysis namely: number of pixels change rate (NPCR) and unified average changing intensity (UACI). NPCR provides the rate of changed pixels that have been altered in the encrypted data when slight alteration is done in the plain-text data. Whereas, UACI gives the averaged intensity of difference between plain-text and encrypted images. Their computation procedure involves two plain-images PP_1 and PP_2 which have difference of merely of one pixel only. Let their corresponding encrypted images be C_1 and C_2. The mathematical expression for NPCR and UACI are the following.

$$NPCR = \frac{\sum E(i,j)}{Total\ number\ of\ pixels} \times 100\%$$

$$UACI = \frac{1}{255}\left[\frac{\sum abs\big(C_1(i,j) - C_2(i,j)\big)}{Total\ number\ of\ pixels}\right] \times 100\%$$

$$E(i,j) = \begin{cases} 1 & C_1(i,j) \neq C_2(i,j) \\ 0 & C_1(i,j) = C_2(i,j) \end{cases}$$

The results of NPCR and UACI obtained for the proposed S-box based image encryption scheme are presented in Table 13. It is evident that the obtained score for NPCR is more than 99.6% and that of UACI is 33.4% which are consistent with the expected values reported in the literature for strong encryption schemes. The comparison of results with available encryption algorithms validates its consistency, robustness, and efficacy in mitigating the differential attacks.

Table 13. PLAIN-IMAGE SENSITIVITY ANALYSIS: NPCR AND UACI SCORES

Encryption scheme	NPCR	UACI
Proposed (Lena)	99.693	33.61
Proposed (Baboon)	99.684	33.43
Ref. [48] (Lena)	99.56	33.48
Ref. [50] (Lena)	99.61	33.43
Ref. [56] (Lena)	99.62	33.58
Ref. [71] (Lena)	99.61	27.83
Ref. [71] (Baboon)	99.57	26.81
Ref. [72] (Lena)	99.667	33.46
Ref. [72] (Baboon)	99.605	33.55

C. ENCRYPTION SPEED ANALYSIS

In order to meet the expectations of today's fast communication, an encryption scheme should be capable to generate the encrypted content at a rapid rate with high throughput. It enables the option of its usage for real-time encryption application. Therefore, in addition to strong statistical and robustness performance, an image encryption is considered for practical application if it takes less time. We implemented our proposed S-box based image encryption scheme on Windows 8 with Intel corei7 operating at 2.2GHz speed and has 4GB RAM. The proposed scheme encrypts a 256×256 image in just 0.08632 seconds time which provides a decent throughput of 5.9313 Mbps. We also compared the encryption time and throughput results with other image encryption schemes outcomes in Table 14. It is evident that our S-box based encryption scheme has the ability to offer strong encryption with an encryption time which is sufficiently shorter than many contemporary schemes investigated in [50, 56, 73-76]. Thus, the suggested S-box based encryption scheme takes less time and faster which confirms its possibility for practical usage.

Table 14. TIME AND THROUGHPUT OF SOME ENCRYPTION SCHEMES

Encryption scheme	Enc Time (sec)	Throughput (Mbps)
Proposed	0.08632	5.9313
Ref. [50]	2.54329	0.2013
Ref. [56]	0.382	1.3403
Ref. [73]	1.1204	0.4569
Ref. [74]	0.631	0.8114
Ref. [75]	0.506	1.0118
Ref. [76]	1.7	0.30117

V. CONCLUSION

This research work presented a modest and novel technique for the erection of dynamic and key dependent S-boxes with the help of an innovative linear trigonometric transformation. A new dynamic performance improvisation plan is proposed that boost the nonlinearity score of preliminary S-box generated through novel trigonometric transformation. Being dynamic in nature, both transformation and the nonlinearity improvisation plan use different parameters in the construction and cipher key employs the values to the respective parameters. A change in the cipher key brings changes in the parameters' values and each time a new nonlinear S-box is spawned. Comparative performance analyses indorse the noteworthy contribution of the projected scheme for the erection of

dynamic and sturdy S-boxes. Moreover, a new image encryption scheme based on proposed S-box is suggested which is capable to offer high encryption effect, high robustness to differential attacks, high throughput value. Thereby confirms the effectiveness of proposed S-box and anticipated method for the application of multimedia image cryptosystems design to protect data.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their constructive comments and suggestions which have significantly improved the article.

REFERENCES

[1] X. Yan, S. Wang, A. A. A. El-Latif, and X. Niu, "Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery," Multimedia Tools and Applications, vol. 74, no. 9, pp. 3231–3252, 2013.

[2] M. Tanveer, G. Abbas, Z. H. Abbas, M. Waqas, F. Muhammad, and S. Kim, "S6AE: Securing 6LoWPAN Using Authenticated Encryption Scheme," Sensors, vol. 20, no. 9, p. 2707, 2020.

[3] L. R. Knudsen and M. J. B. Robshaw, The Block Cipher Companion. Berlin, Germany: Springer-Verlag, 2011.

[4] A. A. A. El-Latif, X. Niu, and M. Amin, "A new image cipher in time and frequency domains," Optics Communications, vol. 285, no. 21-22, pp. 4241–4251, 2012.

[5] M. M. Lauridsen, C. Rechberger, and L. R. Knudsen, "Design and Analysis of Symmetric Primitive," Tech. Univ. Denmark, Kgs. Lyngby, Denmark, Tech. Rep. 382, 2016.

[6] L. Li, B. Abd-El-Atty, A. A. El-Latif, and A. Ghoneim, "Quantum color image encryption based on multiple discrete chaotic systems," Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, 2017.

[7] A. K. Farhan, R. S. Ali, H. R. Yassein, N. M. G. Al-Saidi, and G. H. Abdul-Majeed, "A new approach to generate multi sboxes based on RNA computing," International Journal of Innovative Computing, Information and Control, vol. 16, pp. 331–348, 2020.

[8] Hayat, U., Azam, N. A., Gallegos-Ruiz, H. R., Naz, S., & Batool, L. (2021). A Truly Dynamic Substitution Box Generator for Block Ciphers Based on Elliptic Curves Over Finite Rings. Arabian Journal for Science and Engineering, 1-13.

[9] Azam, N. A., Hayat, U., & Ayub, M. (2021). A Substitution Box Generator, its Analysis, and Applications in Image Encryption. Signal Processing, 108144.(doi: https://doi.org/10.1016/j.sigpro.2021.108144)

[10] 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.

[11] M. Ahmad, E. Al-Solami, A. M. Alghamdi and M. A. Yousaf, "Bijective S-Boxes Method Using Improved Chaotic Map-Based Heuristic Search and Algebraic Group Structures," IEEE Access, vol. 8, pp. 110397-110411, 2020.

[12] K. Mohamed, M. Nazran, M. Pauzi, F. Hani, H. M. Ali, S. Ariffin, N. Huda, and N. Zulkipli, "Study of S-Box Properties in Block Cipher," in Proc. Int. Conf. Comp. Comm. Control Tech., Langkawi Island, Kedah, Malaysia, Sep. 2014, pp. 2-4.

[13] A. Alabaichi, and A. I. Salih, "Enhance Security of Advance Encryption Standard Algorithm Based on Key-dependent S-Box," in Proc. 5th Int. Conf. Digit. Inf. Process. Commun., Sierre, Switzerland, Oct. 2015, pp. 7-9.

[14] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, ``Secure data encryption based on quantum walks for 5G Internet of Things scenario," IEEE Trans. Netw. Service Manage, vol. 17, no. 1, Mar. 2020, Art. no. 118131.

[15] A. A. Alzaidi, M. Ahmad, M. N. Doja, E. A. Solami, and M. M. S. Beg, "A New 1D Chaotic Map and beta-Hill Climbing for Generating Substitution-boxes," IEEE Access, vol. 6, pp. 55405–55418, 2018

[16] D. Lambic, "A novel method of S-box design based on chaotic map and composition method," Chaos, Solitons Fractals, vol. 58, pp. 16-21, Jan. 2014.

[17] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," Neural Comput. Appl., vol. 31, no. 8, pp. 3317-3326, 2019.

[18] M. Ahmad, H. Haleem, and P. M. Khan, "A New Chaotic Substitution Box Design for Block Ciphers," in Pro. Int. Conf. Sig. Processing Integrated Net, Delhi, India, February 2014.

[19] Belazi, A., El-Latif, A.A.A., "A simple yet efficient s-box method based on chaotic sine map," Optik, vol. 130, pp. 1438–1444, 2017.

[20] J. Peng, S. Jin, L. Lei, and R. Jia, "A Novel Method for Designing Dynamical Key-Dependent S-boxes based on Hyperchaotic System," Int. J. Adv. Comput. Technol., vol. 4, pp. 282–289, 2016.

[21] E. A. Solami, M. Ahmad, C. Volos, M. N. Doja, and M. M. S. Beg, "A New Hyperchaotic System-Based Design for Efficient Bijective Substitution-boxes," Entropy, vol. 20, pp. 525, 2018.

[22] Wang, X., Akgul, A., Cavusoglu, U., Pham, V.-T., Vo Hoang, D., Nguyen, X., "A chaotic system with infinite equilibria and its s-box constructing application," Appl. Sci., vol. 8, pp. 2132, 2018.

[23] S. Ibrahim and A. M. Abbas, "A Novel Optimization Method for Constructing Cryptographically Strong Dynamic S-Boxes", IEEE Access, vol. 8, pp. 225004-225017, 2020.

[24] S. Ibrahim and A. M. Abbas, "Efficient key-dependent dynamic S-boxes based on permutated elliptic curves", Inf. Sci., vol. 558, pp. 246-264, May 2021.

[25] B. R. Gangadari, and S. R. Ahamed, "Design of Cryptographically Secure AES like S-Box using Second-Order Reversible Cellular Automata for Wireless Body Area Network Applications," Healthcare Technology Letters, vol. 3, pp. 177–183, 2016.

[26] U. Hayat, N. A. Azam, and M. Asif, "A Method of Generating 8 x 8 Substitution Boxes Based on Elliptic Curves," Wireless Personal Comm., vol. 101, no. 1, pp. 439–451, 2018.

[27] A. Kadhim, and G. H. A. Majeed, "Proposal New S-Box Depending on DNA computing and Mathematical Operations," in Proc. Int. Conf. Multidisciplinary IT Comm. Sc. Appl. Baghdad, Iraq, May 2016.

[28] A. Razaq, H. Alolaiyan, M. Ahmad, M. A. Yousaf, U. Shuaib, W. Aslam, and M. Alawida, "A Novel Method for Generation of Strong Substitution-Boxes Based on Coset Graphs and Symmetric Groups," IEEE Access, vol. 8, pp. 75473–75490, 2020.

[29] B. N. Tran, T. D. Nguyen, and T. D. Tran, "A New S-Box Structure Based on Graph Isomorphism," in Proc. Int. Conf. Comp. Intelligence and Sec., Beijing, China, December 2009.

[30] T. Farah, R. Rhouma, and S. Belghith, "A novel method for designing S-box based on chaotic map and Teaching–Learning-Based Optimization," Nonlinear Dynamics, vol. 88, no. 2, pp. 1059–1074, 2017.

[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, Feb. 2018.

[32] Y. Wang, K. W. Wong, C. Li, and Y. Li, "A novel method to design S-box based on chaotic map and genetic algorithm," Physics Letters A, vol. 376, no. 6-7, pp. 827–833, 2012.

[33] M. M. Dimitrov, "On the design of chaos-based S-Boxes", IEEE Access, vol. 8, pp. 117173-117181, 2020.

[34] A. Altaleb, M. S. Saeed, I. Hussain, and M. Aslam, "An Algorithm for the Construction of Substitution Box for Block Ciphers based on Projective General Linear Group," AIP Adv. vol. 7, no. 035116, 2017.

[35] Chew, L. C. N., & Ismail, E. S. (2020). S-box construction based on linear fractional transformation and permutation function. Symmetry, 12(5), 826.

[36] Belazi, A., Abd El-Latif, A. A., Diaconu, A. V., Rhouma, R., & Belghith, S. (2017). Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Optics and Lasers in Engineering, 88, 37-50.

[37] P. Agarwal, A. Singh, and A. Kilicman, "Development of Key-Dependent Dynamic S-Boxes with Dynamic Irreducible Polynomial

and Affine Constant," Adv. Mech. Eng., vol. 10, no. 7, pp. 1–18, 2018.

[38] E. M. Mahmoud, A. A. E. Hafez, T. A. Elgarf, and A. Zekry, "Dynamic AES-128 with Key-Dependent S-Box," Int. J. Engg. Res. Appl., vol. 3, no. 1, pp.1662–1670, 2013.

[39] S. Sahmoud, W. Elmasry, and S. Abudalfa, "Enhancement the Security of AES Against Modern Attacks by Using Variable Key Block Cipher," Int. Arab J. e-Tech., vol. 3, pp. 17-26, 2013.

[40] J. Cui, L. Huang, H. Zhong, C. Chang, and W. Yang, "An Improved AES S-Box and its Performance Analysis," Int. J. Inno. Comp., Info. Cont., vol. 7, pp. 2291-2302, 2011.

[41] A. H. Zahid, M. J. Arshad, and M. Ahmad, "A Novel Construction of Efficient Substitution-Boxes using Cubic Fractional Transformation," Entropy, vol. 21, no. 3, pp. 245, 2019

[42] A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach-based substitution-box design for image encryption," IEEE Access, vol. 8, pp. 150326-150340, 2020.

[43] A. H. Zahid, and M. J. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," Symmetry, vol. 11, no. 3, pp. 437, 2019.

[44] T. W. Cusick and P. Stanica, "Cryptographic Boolean Functions and Applications," Amsterdam: Elsevier, 2009.

[45] Alshammari, B.M., Guesmi, R., Guesmi, T., Alsaif, H., and Alzamil, A., "Implementing a Symmetric Lightweight Cryptosystem in Highly Constrained IoT Devices by Using a Chaotic S-Box," Symmetry, vol.13, no. 129, pp. 1-20, 2021.

[46] W. Gao, B. Idrees, S. Zafar, and T. Rashid, "Construction of nonlinear component of block cipher by action of modular group PSL(2, Z) on projective line PL(GF(2^8))," IEEE Access, vol. 8, pp. 136736-136749, 2020.

[47] S. Hussain, S. S. Jamal, T. Shah, and I. Hussain, "A power associative loop structure for the construction of non-linear components of block cipher," IEEE Access, vol. 8, pp. 123492_123506, 2020.

[48] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," IEEE Access, vol. 8, pp. 54175-54188, 2020.

[49] H. Liu, A. Kadir, and C. Xu, "Cryptanalysis and constructing S-Box based on chaotic map and backtracking," App. Math. Comp., vol. 376, pp. 1-11, 2020.

[50] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," Nonlinear Dyn., vol. 99, no. 4, pp. 3041-3064, 2020.

[51] I. Hussain, T. Shah, M. A. Gondal, and W. A. Khan, " Construction of Cryptographically Strong 8×8 S-boxes," World App. Sc. J., vol. 13, no. 11, pp. 2389-2395, 2011.

[52] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami, and W. Alhakami, "Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications," IEEE Access, vol. 8, pp. 116132_116147, 2020.

[53] Z. B. Faheem, A. Ali, M. A. Khan, M. E. Ul-Haq, and W. Ahmad, "Highly dispersive substitution box (S-box) design using chaos," ETRI Journal, pp. 1-14, 2020.

[54] A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, "Quantum inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," Sci. Rep., vol. 10, no. 1, pp. 116, Dec. 2020.

[55] D. Lambic, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," Nonlinear Dyn., vol. 100, 2020.

[56] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," IEEE Access, vol. 8, pp. 25664-25678, 2020.

[57] Siddiqui, N., Naseer, A. and Ehatisham-ul-Haq, M. A., "Novel Scheme of Substitution-Box Design Based on Modified Pascal's Triangle and Elliptic Curve," Wireless Pers Commun., vol. 116, no. 20, pp. 3015–3030, 2021.

[58] H. S. Alhadawi, M. A. Majid, D. Lambic, and M. Ahmad, "A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm," Multimedia Tools Appl., vol. 80, no. 20, pp. 7333–7350, 2021.

[59] M. Long and L. Wang, "S-Box Design Based on Discrete Chaotic Map and Improved Artificial Bee Colony Algorithm," IEEE Access, vol. 9, pp. 86144–86154, 2021.

[60] R. Soto, B. Crawford, F. G. Molina, and R. Olivares, "Human Behaviour Based Optimization Supported With Self-Organizing Maps for Solving the S-Box Design Problem," IEEE Access, vol. 9, pp. 84605–84618, 2021.

[61] B. Arshad and N. Siddiqui, "Construction of Highly Nonlinear Substitution Boxes (S-Boxes) Based on Connected Regular Graphs," *Int. J. Comp. Sc. Info. Sec.*, vol. 18, no. 4, 2020.

[62] N. Siddiqui, F. Yousaf, F. Murtaza, M. E. Haq, M. U. Ashraf, A. M. Alghamdi, and A. S. Alfakeeh A. S., "A highly nonlinear substitution-box (Sbox) design using action of modular group on a projective line over a finite field," *PLoS ONE,* vol. 15, no. 11, pp. 1-16, 2020.

[63] Y. Wang, Z. Zhang, L. Y. Zhang, J. Feng, J. Gao, and P. Lei, "A genetic algorithm for constructing bijective substitution boxes with high nonlinearity," *Information Sciences*, vol. 523, pp. 152-166, 2020.

[64] W. Yan and Q. Ding, "A Novel S-Box Dynamic Design Based on Nonlinear-Transform of 1D Chaotic Maps," Electronics, vol. 10, no. 11, p. 1313, 2021.

[65] P. Zhou, J. Du, K. Zhou, and S. Wei, "2D mixed pseudo-random coupling PS map lattice and its application in S-box generation," Nonlinear Dynamics, vol. 103, no. 1, pp. 1151–1166, 2021.

[66] A. F. Webster, and S. E. Tavares, "On the Design of S-Boxes," in Proc. Conf. Theory Appl. Crypto. Tech.," Santa Barbara, CA, USA, August 1986.

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

[68] M. Matsui, "Linear cryptanalysis method for DES cipher," in Proc. Adv. Cryptology, Lofthus, Norway, 1994.

[69] A. A. A. El-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things," Optics & Laser Technology, vol. 124, p. 105942, 2020.

[70] A. A. A. El-Latif, X. Yan, L. Li, N. Wang, J.-L. Peng, and X. Niu, "A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption," Optics & Laser Technology, vol. 54, pp. 389–400, 2013.

[71] M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar, and A. Razaq, ``Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes," IEEE Access, vol. 8, pp. 3978139792, 2020.

[72] B. Idrees, S. Zafar, T. Rashid, and W. Gao, "Image encryption algorithm using s-box and dynamic hénon bit level permutation," Multimedia Tools and Applications, 2019, doi: 10.1007/s11042-019-08282-w.

[73] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, ``A new design of cryptosystem based on S-box and chaotic permutation," Multimedia Tools Appl., Mar. 2020.

[74] T. S. Ali and R. Ali, ``A novel medical image signcryption scheme using TLTS and henon chaotic map," IEEE Access, vol. 8, pp. 71974-71992, 2020.

[75] X. Wang and P. Liu, "A new image encryption scheme based on a novel one-dimensional chaotic system", IEEE Access, vol. 8, pp. 174463-174479, 2020.

[76] M. Asgari-Chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, ``A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," Signal Process., vol. 157, pp. 1-13, Apr. 2019.