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

AMJAD HUSSAIN ZAHID\textsuperscript{1}, LO'AI TAWALBEH\textsuperscript{2}, (Senior Member, IEEE), MUSHEER AHMAD\textsuperscript{3}, AHMED ALKHAYYAT\textsuperscript{4}, MALIK TAHR HASSAN\textsuperscript{1}, ATIF MANZOOR\textsuperscript{1}, AND ALAA KADHIM FARHAN\textsuperscript{5}

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

Corresponding authors: Lo’ai Tawalbeh (ltawalbeh@tamusa.edu) and Musheer Ahmad (musheer.cse@gmail.com)

This work was supported by 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 meaningfulness 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], [42], and Zahid and Arshad [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 $8 \times 8$ 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 suitability 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
A novel transformation has a mathematical description in the dynamic linear trigonometric transformation (LTT). This two modest phases of (1) novel linear trigonometric transformation (LTT), and (2) innovative 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 \( n \times n \) 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:

\[
T(z) = \cos((A + B) \times X \times z + C)
\]

where,

\[
0 < X < 1, \\
0 \leq z \leq (2^n - 1), \ B \in z, \ \text{and} \\
A, \ C = \{1, 3, \ldots, 2^n - 1\}.
\]

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 \( 8 \times 8 \) s-Box Generation

Input parameters:
\[
\begin{align*}
&n = 8 \quad // \text{for } n \times n \text{ S-box} \\
&X \quad // \quad 0 < X < 1 \\
&A, C \quad // \quad A, C \in \{1, 3, \ldots, 2^n - 1\} \\
&B \quad // \quad B \in \{0, 1, 2, \ldots, 2^n - 1\}
\end{align*}
\]

Output:
\[
S \quad // \quad \text{Preliminary } 8 \times 8 \text{ S-box}
\]

Initializations:
\[
\begin{align*}
&h \leftarrow 0 \\
&g \leftarrow -1 \\
&\text{Loc} \leftarrow 0 \\
&\text{while}(h <= 255)\text{ do} \\
&R \leftarrow (A + B) \times X \\
&B[h] = \cos(R \times h + C) \\
&\text{if}(X > 0.5)\text{ then} \\
&\quad X = X \times X \\
&\text{else} \\
&\quad X = X \times 1.75 \\
&\text{endif} \\
&h \leftarrow h + 1 \\
&\text{endwhile} \\
&g \leftarrow g + 1 \\
&\text{while}(g <= 255)\text{ do} \\
&M\text{IN} \leftarrow B[0] \\
&\text{Loc} = 0 \\
&h \leftarrow 0 \\
&\text{while}(h <= 255)\text{ do} \\
&\text{if}(\text{MIN} > B[h])\text{ then} \\
&\quad \text{MIN} = B[h] \\
&\quad \text{Loc} = h \\
&\text{endif} \\
&h \leftarrow h + 1 \\
&\text{endwhile} \\
&S[g] = \text{Loc} \\
&B[\text{Loc}] = 111 \\
&g \leftarrow g + 1 \\
&\text{endwhile} \\
&\text{return } S
\end{align*}
\]

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 \( 8 \times 8 \) 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.

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...
Algorithm 2 Final S-Box Generation Based on Nonlinearity

**Input parameters:**
X // 0 < X < 1
A, C // A, C ∈ {1, 3, ..., 2^n - 1}
B // B ∈ {0, 1, 2, ..., 2^n - 1}
S // Preliminary 8 × 8 S-box

**Output:**
F // Final 8 × 8 S-box

**Initializations:**
V ← 1
F = S
NL1 ← Nonlinearity (F)
// Nonlinearity (F) returns nonlinearity of S-box F
NL2 ← 0.0

while ( V <= 2^{16} - 1 ) do
    R1 ← (A × V + C) MOD 257
    R2 ← (C × V + A) MOD 257
    R3 ← (A × 1000 + V)
    R4 ← (C × 1000 + V)
    R5 ← (R1 + X × V)
    R6 ← (R3 + X × V)
    a ← ABS ( INT ( R3 × Cos (R5)) ) MOD 256
    b ← ABS ( INT ( R4 × Cos (R6)) ) MOD 256
    // INT returns an integer from a fractional value
    // ABS returns absolute value
    // Swap values F[a] and F[b]
    Temp ← F[a]
    F[a] ← F[b]
    F[b] ← Temp
    NL2 ← Nonlinearity (F)
    if (NL2 > NL1) then
        NL1 ← NL2
    else
    // Swap values F[a] and F[b]
    Temp ← F[a]
    F[a] ← F[b]
    F[b] ← Temp
    endif
    V ← V + 1
endwhile
return F

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**

Bijection 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 feebly 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]:

\[
NL (B) = \left[ 2^n - (W_{max}(B)) \right] \frac{1}{2}
\]

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.

Both the presentations validate that the proposed S-box has NL_{max} = 121, 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 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 | 192| 200 | 184 | 154| 232 | 52  | 227| 14 | 18 | 241 | 140 | 53  | 209| 207 |
| 144 | 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   | 110   | 112   | 112   |

C. STRICT AVALANCHE CRITERION (SAC)

This criterion is a vigorous topography of a robust S-box and was presented by Webster and Tavares [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.

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 and Tavares [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.

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.

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 $n \times n$ S-box $B$.

$$DU = \text{Maximum} \left[ \# \{ c \in P \mid B(c) + B(c + \Delta_c) = \Delta_d \} \right] \quad (3)$$

where,

- $\Delta_c =$ Input differential,
- $\Delta_d =$ Output differential, and
- $P = \{0, \ldots, 2^n - 1\}$.

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 3. Nonlinearity (NL) scores for different S-boxes.

| S-Box      | Publication Year | Nonlinearity Score | NLMin | NLMax | NLAvg |
|------------|------------------|--------------------|-------|-------|-------|
| 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   |

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

### TABLE 5. BIC-nonlinearity scores of proposed S-box.

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

### 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 |
TABLE 7. Values of differential uniformity of proposed S-box.

| 8  | 8  | 6  | 6  | 8  | 10 | 6  | 6  | 6  | 6  | 8  | 6  | 6  | 6  | 6  | 8  | 6  | 6  | 6  | 8  | 6  | 6  | 6  | 6  | 8  | 6  | 6  | 8  | 6  | 6  | 8  | 6  |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|

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].

\[
LAP = \max_{x_t, y_t \neq 0} \left| \frac{1}{2^n} \left( \# \{ t \in R \mid t \cdot x_t = F(t) \cdot y_t \} \right) - \frac{1}{2} \right|
\]  

where,

\[ x_t, y_t = \text{input and output mask} \]

\[ R = \{0, 1, 2, \ldots, 2^n - 1\} \]

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.

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 \((0 \times 63)\) [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 \( 8 \times 8 \) 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.

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

### 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   |

### TABLE 9. Computational time (seconds) of different S-box methods.

| Method  | Average Time | Iterations | Nonlinearity |
|---------|--------------|------------|--------------|
| Ref. [23] | 403          | $\sim 10^{473}$ | 112          |
| Ref. [35] | 367          | $\sim 10^{477}$ | 112          |
| Ref. [61] | 213          | $\sim 10^{4}$   | 112          |
| Ref. [62] | 293          | $\sim 10^{493}$ | 112          |
| Proposed | 283          | $\sim 10^{487}$ | 111.5        |
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]–[58], [60], [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 \(M \times N\) to be encrypted.
2. Read the S-box given in Table 1 as \(SB\).
3. Convert image \(PP\) into 1-D array as \(D = \text{reshape}(PP, 1, M \times N)\)
4. Convert image data \(D\) into hex format as \(msg = \text{hexformat}(D)\)
5. Find 256-bit digest with respect to pending image data \(msg\) as \(H = \text{SHA256}(msg)\)
6. Convert the digest \(H\) into chunks of 8-bits as: \(H = H_1, H_2, \ldots, H_{32}\).
7. Take \(C_0\)
8. Repeat following for each pixel of image \(PP\)
   \[n = 1 + [C_0 \bmod 32]\]
   \[\{n_1, n_2\} = \text{nibble}(H_i)\]
   \[K = SB(n_1, n_2) // key K\text{ is element from S-box }SB\]
   \[C(i, j) = PP(i, j) \oplus K \oplus C_0\]
   \[C_0 = C(i, j)\]
   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 \(256 \times 256\). 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 \(\text{entropy, contrast, energy, homogeneity}\). 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.

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.

**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...
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. | \( \sum_{m,n} \left( \frac{(m-\mu_m)(n-\mu_n)}{\sigma_m \sigma_n} \right) \) |
| 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. | \( \sum_{m,n} |m-n|^5 p(m,n) \) |
| 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. | \( \sum_{m,n} p(m,n)^3 \) |
| 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. | \( \sum_{m,n} \frac{p(m,n)}{1+|m-n|} \)

TABLE 11. MLC results of entropy, correlation, contrast, energy, homogeneity from proposed S-box based encryption.

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

TABLE 12. Comparison of MLC results for S-box based image encryption schemes.

| Parameters | Proposed | Ref. [71] | Ref. [72] | Ref. [47] |
|------------|----------|-----------|-----------|-----------|
| Entropy    | Lena     | 7.9968    | 7.9964    | 7.9553    |
|            | Baboon   | 7.9564    | 7.9553    | 7.3583    |
| Correlation| Lena     | 0.01014   | 0.00568   | 0.0087    |
|            | Baboon   | 0.00988   | 0.0087    | 0.0343    |
| Contrast   | Lena     | 10.433    | 10.2301   | 10.346    |
|            | Baboon   | 9.8414    | 9.9764    | 9.9764    |
| Energy     | Lena     | 0.01564   | 0.01563   | 0.0157    |
|            | Baboon   | 0.0157    | 0.0157    | 0.0161    |
| Homogeneity| Lena     | 0.3915    | 0.3917    | 0.3895    |
|            | Baboon   | 0.4084    | 0.4131    | 0.4131    |

A. H. Zahid et al.: Efficient Dynamic S-Box Generation Using Linear Trigonometric Transformation

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 one pixel only. Let their corresponding encrypted images be \( C_1 \) and \( C_2 \). The mathematical expression for NPCR and UACI are the following.

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

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

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

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.

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 encryption scheme based on proposed S-box is noteworthy contribution of the projected scheme for the is spawned. Comparative performance analyses indorse the parameters' values and each time a new nonlinear S-box parameters. A change in the cipher key brings changes in improvisation plan use different parameters in the construction and the nonlinearity generated through novel trigonometric transformation. Being that boost the nonlinearity score of preliminary S-box.

A new dynamic performance improvisation plan is proposed for the erection of dynamic and key dependent S-boxes with this research work presented a modest and novel technique which confirms its possibility for practical usage. This research work investigated in [50], [56], [73]–[76]. Thus, the suggested 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.

| 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 |

**TABLE 13.** Plain-image sensitivity analysis: NPCR and UACI scores.

| 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           |

**TABLE 14.** Time and throughput of some encryption schemes.

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.

**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 Appl., vol. 74, no. 9, pp. 3231–3252, May 2015.
[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, May 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,” Opt. Commun., vol. 285, nos. 21–22, pp. 4241–4251, Oct. 2012.
[5] M. M. Lauridsen, C. Rechberger, and L. R. Knudsen, “Design and analysis of symmetric primitive,” Tech. Univ. Denmark, 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,” in *Proc. Federated Conf. Comput. Sci. Inf. Syst.*, Sep. 2017, pp. 555–559.
[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 S-boxes based on RNA computing,” Int. J. Innov. Comput., Inf. Control, vol. 16, pp. 331–348, Oct. 2020.
[8] U. Hayat, N. A. Azam, H. R. Gallegos-Ruiz, S. Naz, and L. Batool, “A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings,” Arabian J. Sci. Eng., pp. 1–13, May 2021, doi: 10.1007/s13369-021-05666-9.
[9] N. A. Azam, U. Hayat, and M. Ayub, “A substitution box generator, its analysis, and applications in image encryption,” Signal Process., vol. 187, Oct. 2021, Art. no. 108144, doi: 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. Zaidi, “Study of S-box properties in block cipher,” in *Proc. Int. Conf. Comput. Commun. Control Technol.*, Langkawi, Malaysia, Sep. 2014, pp. 2–4.
[13] A. Asabaichi 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. (ICDIPC)*, Sierre, Switzerland, Oct. 2015, pp. 7–9.
[14] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazureczyk, 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, pp. 118–131, Mar. 2020.
[15] 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.
[16] D. Lambić, “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. Ozkaynak, “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 *Proc. Int. Conf. Signal Process. Integ. Netw. (SPIN)*, Delhi, India, Feb. 2014, pp. 255–258.
A. Hazid et al.: Efficient Dynamic S-Box Generation Using Linear Trigonometric Transformation

IEEE Access, Vol. 9, 2021

[19] A. Belazi and A. A. A. El-Latif, “A simple yet efficient S-box method based on chaotic sine map,” Optik, vol. 130, pp. 1438–1444, Feb. 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. Advancements Comput. Technol., vol. 4, no. 18, pp. 282–289, Oct. 2012.

[21] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, “A new hyperchaotic system-based design for efficient bijective substitution-boxes,” Entropy, vol. 20, no. 7, p. 525, 2018.

[22] X. Wang, A. Akgul, U. Cavusoglu, T. V. Pham, V. H. Duy, and Q. N. Xuan, “A chaotic system with infinite equilibria and its S-box constructing application,” Appl. Sci., vol. 8, no. 11, p. 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 perturmed 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 Technol. Lett., vol. 3, no. 3, pp. 177–183, 2016.

[26] U. Hayat, N. A. Azam, and M. Asif, “A method of generating 8 × 8 substitution boxes based on elliptic curve,” Wireless Pers. Commun., vol. 101, no. 1, pp. 439–451, Jul. 2018.

[27] F. A. Kadhim, G. H. A. Majeed, and R. S. Ali, “Proposal new S-box depending on DNA computing and mathematical operations,” in Proc. AlSadeq Int. Conf. Multidisciplinary IT Commun. Sci. Appl. (ICMITCSA), Baghdad, Iraq, May 2016, pp. 1–6.

[28] A. Razaq, H. Alolaiyan, M. Ahmad, M. A. Yousaf, U. Shuaib, W. Aslam, and M. Alawida, “A novel method for generation for strong substitution-boxes based on cost 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. Comput. Intell. Secur., Beijing, China, Dec. 2009, pp. 463–467.

[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 Dyn., 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, Dec. 2018.

[32] Y. Wang, K.-W. Wong, C. Li, and L. Yang, “A novel method to design S-box based on chaotic map and genetic algorithm,” Phys. Lett. A, vol. 376, nos. 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. Hassan, 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. 3, Mar. 2017, Art. no. 035116.

[35] L. C. N. Chew and E. S. Ismail, “S-box construction based on linear fractional transformation and permutation function,” Symmetry, vol. 12, no. 5, p. 826, May 2020.

[36] A. Belazi, A. A. A. El-Latif, A.-V. Diaconu, R. Rhouma, and S. Belghith, “Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms,” Opt. Lasers Eng., vol. 88, pp. 37–50, Jan. 2017.

[37] P. Agarwal, A. Singh, and A. Kiliçman, “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. Abd, T. A. E. El Hafez, and T. A. El Hafez, “Dynamıc AES-128 with key-dependent S-box,” Int. J. Eng. Res. Appl., vol. 3, no. 1, pp. 1662–1670, Jan./Feb. 2013.

[39] S. Sahnoun, W. Elmasry, and S. Abudalafa, “Enhancement the security of AES against modern attacks by using variable key block cipher,” Int. Arab J. E.-Tech., vol. 3, pp. 17–26, Jan. 2013.

[40] J. Cui, L. Huang, H. Zhong, C. Chang, and W. Yang, “An improved AES S-box and its performance analysis,” Int. J. Innov. Comput., Inf. Control, vol. 7, no. 5, pp. 2291–2302, 2011.

[41] A. H. Hazid, M. J. Arshad, and M. Ahmad, “A novel construction of efficient substitution-boxes using cubic fractional transformation,” Entropy, vol. 21, no. 3, p. 245, May 2019.
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 Dyn.*, vol. 103, no. 1, pp. 1151–1166, Jan. 2021.

A. F. Webster and S. E. Tavares, “On the design of S-boxes,” in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, Santa Barbara, CA, USA, Aug. 1986, pp. 253–254.

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

M. Matsui, “Linear cryptanalysis method for DES cipher,” in *Advances in Cryptology*. Lofthius, Norway: Springer, 1994.

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,” *Opt. Laser Technol.*, vol. 124, Apr. 2020, Art. no. 105942.

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,” *Opt. Laser Technol.*, vol. 54, pp. 389–400, Dec. 2013.

M. A. Yousef, H. A. Hayyan, 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, 2020, Art. no. 3978139792.

B. Idrees, S. Zafar, T. Rashid, and W. Gao, “Image encryption algorithm using S-box and dynamic Hénon bit level permutation,” *Multimedia Tools Appl.*, vol. 79, nos. 9–10, pp. 6135–6162, Mar. 2020, doi: 10.1007/s11042-019-08282-w.

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.*, vol. 79, nos. 27–28, pp. 19129–19150, Mar. 2020.

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.

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.

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.

AMJAD HUSSAIN ZAHID received the Ph.D. degree in computer science (information security) from the University of Engineering and Technology, Lahore, Pakistan. He has been an Active Member with the Faculty Board of Studies, Punjab University College of Information Technology (PUCIT), Virtual University of Pakistan. He is currently working as an Assistant Professor with the University of Management and Technology (UMT), Lahore. He is also the Program Advisor for B.S. (IT) Program and a member of many academic bodies. He has more than 23 years of qualitative experience in teaching. He possesses quality monitoring and maintaining capabilities along with the strong interpersonal, leadership, and team management skills. He is vigorous in academic research and his research interests include information security, programming languages, algorithm design, enterprise architecture, technology management, IT infrastructure, and blockchain. He has been an Active Member of the Higher Education Commission (HEC) National Curriculum Revision Committee (NCRC), Pakistan. He is serving as an efficient and effective reviewer in several reputed international research journals of high impact factor in the domain of information security.

AHMED ALKHAYYAT received the B.Sc. degree in electrical engineering from Al-Kufa University, Najaf, Iraq, in 2007, the M.Sc. degree from the Dehradun Institute of Technology, Dehradun, India, in 2010, and the Ph.D. degree from Cankaya University, Ankara, Turkey, in 2015. He is currently the Dean of international relationship and a Manager of the word ranking with Islamic University, Najaf. His research interests include the IoT in the health-care systems, SDN, network coding, cognitive radio, efficient-energy routing algorithms and efficient-energy MAC protocol in cooperative wireless networks, wireless body area networks, and cross-layer design for self-organized networks. He contributed in organizing a several IEEE conferences, workshop, and special sessions. To serve his community, he acted as a reviewer for several journals and conferences.

LO‘AI TAWALBEH (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees (Hons.) in computer engineering from Oregon State University (OSU), Corvallis, OR, USA, in 2002 and 2004, respectively. From 2005 to 2012, he worked as an Adjunct Professor to teach in the master’s programs with the New York Institute of Technology (NYIT), DePaul University, and Princess Sumaya University for Technology (PSUT). He is currently an Associate Professor with the Department of Computing and Cybersecurity, Texas A&M University-San Antonio, San Antonio, TX, USA. He is the Founder and the Director of the Cryptographic Hardware and Information Security (CHIS) Lab, JUST. He won many research grants and awards. He has more than 90 research publications in many refereed international journals and conferences. His research interests include information security, cryptographic applications, cryptosystems hardware implementations, and mobile cloud security. He is chairing many international conferences and workshops in mobile cloud security, blockchain, and related cybersecurity areas. He is a reviewer and an associate editor of many international journals.

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, and the Ph.D. degree in chaos-based cryptography from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India. From 2007 to 2010, he worked with the Department of Computer Engineering, Aligarh Muslim University. Since 2011, he has been working as an Assistant Professor with the Department of Computer Engineering, Jamia Millia Islamia. He has published over 85 research articles in international reputed refereed journals and conference proceedings of the IEEE/Springer/Elsevier. He has more than 1500 citations of his research works with an H-index of 22. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, machine learning for security, image processing, and optimization techniques. He has served as a technical program committee member and a reviewer for many international conferences. He has served as a Referee for some renowned journals, such as Information Sciences, Signal Processing, *Journal of Information Security and Applications*, *IEEE Journal on Selected Areas in Communications*, *IEEE Transactions on Circuits and Systems for Video Technology*, *IEEE Transactions on Industrial Informatics*, *IEEE Transactions on Neural Networks and Learning Systems*, *IEEE Transactions on Nanobioscience*, *IEEE Access*, *Wireless Personal Communications*, *Neural Computing and Applications*, *International Journal of Bifurcation and Chaos*, *Chaos, Solitons & Fractals*, *Physica A: Statistical Mechanics and its Applications*, *Signal Processing: Image Communication*, *Neurocomputing*, *IET Information Security*, *IET Image Processing, Security and Communication Networks*, *Optik, Optics and Laser Technology*, *Complexity, Computers in Biology and Medicine*, *Computational and Applied Mathematics*, and *Concurrency and Computation: Practice and Experience*.

IEEE Access
MALIK TAHIR HASSAN received the M.Sc. degree in computer science from Quaid-e-Azam University, Islamabad, Pakistan, in 2001, and the M.S. and Ph.D. degrees from the Lahore University of Management Sciences, Pakistan, in 2007 and 2013, respectively. He has held research and teaching positions with the University of Management and Technology, Lahore, and the Gwangju Institute of Science and Technology, South Korea. He is currently working as an Assistant Professor and the Head of the Software Engineering Department, UMT, Lahore. His research interests include data mining, information security, and machine learning algorithms and applications with recent focus on educational data mining.

ATIF MANZOOR received the M.S. degree in computer science from the University of Management and Technology (UMT), Lahore, Pakistan, where he is currently pursuing the Ph.D. degree in computer science. He is currently working as the Deputy Director IT with the Local Government and Community Development Department, Government of Punjab, Lahore. He has more than 15 years of qualitative experience in government and private sectors. He has multiple international certifications of Cisco, EC-Council, and Juniper, which includes CCNA, CCNP, CCIE, CEH, Juniper, and Data Center Design (ATD) training from uptime institute London, U.K. He has distinction of designing, implementation, and successfully delivering the first state-of-the-art Tier-III Data Center for Government of Punjab, in 2016. He is energetic in research and his research interests include information security, data center design, network security, it infrastructure, smart city design, ethical hacking, and cyber-security. He is working on First Smart City Project for Government of Punjab.

ALAA KADHIM FARHAN received the bachelor’s degree in computer science and the M.Sc. and Ph.D. degrees in information security from the Department of Computer Sciences, University of Technology, Baghdad, Iraq, in 2003, 2005, and 2009, respectively. In 2005, he joined the Department of Computer Sciences, University of Technology, as an Academic Staff Member. He is currently a Professor with the Department of Computer Sciences, University of Technology. Since 2008, he has been authoring numerous technical articles. His research interests include cryptography, programming languages, chaos theory, and cloud computing.

***