Construction of Cryptographic S-Boxes Based on Mobius Transformation and Chaotic Tent-Sine System

SAJJAD SHAUKAT JAMAL, AMIR ANEES, MUSHEER AHMAD, MUHAMMAD FAHAD KHAN, AND IQTADOR HUSSAIN

1Department of Mathematics, College of Science, King Khalid University, Abha 62529, Saudi Arabia
2Victorian Institute of Technology, Melbourne, VIC 3000, Australia
3Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
4Department of Software Engineering, Foundation University Islamabad, Islamabad 44000, Pakistan
5Department of Mathematics, Statistics, and Physics, Qatar University, Doha 2713, Qatar

Corresponding author: Muhammad Fahad Khan (fahad.khan@fui.edu.pk)

This work was supported by the Deanship of Scientific Research at King Khalid University through the Research Groups Program under Grant R.G.P 2/58/40.

ABSTRACT Over the last few decades, different mediums of secure communication use chaos which is demonstrated by some nonlinear dynamical systems. Chaos shows unpredictable behavior and this characteristic is quite helpful in different encryption techniques and for multimedia security. In this work, the chaotic behavior of the improved Tent-Sine map is conferred and ultimately a new method to construct substitution-boxes is proposed. This new method explores the features of chaos through TSS map and algebraic Mobius transformation to generate strong S-boxes. The S-boxes are assessed using standard tests suit which includes nonlinearity, strict avalanche criterion, bit independence criterion, linear approximation probability and differential uniformity. Moreover, the proposed S-boxes show excellent statistical properties under majority logic criterions such as correlation, homogeneity, energy, entropy, contrast. The statistical encryption results are demonstrate the better performance of the proposed S-boxes when compared with some of state of the art S-boxes including AES, Gray, APA S8 AES, Skipjack and validate the suitability of anticipated method.

INDEX TERMS Substitution-box, block cipher, improved chaotic map, nonlinearity.

I. INTRODUCTION

The rapid increase in international networking provides many new options for the design and presentation in the form of digital data. This easy access and disposal to digital data which includes audio, video, electronic libraries, electronic advertising, web designing, and digital repositories develop the concern of security. The protection while transferring or saving data is indispensably important. For ensuring the security of such digital data and information, a specific field which is named as secure communication plays its vital role to counter this major problem. Secure communication can further be categorized into three main categories which include cryptography, watermarking and steganography. The basic purpose of both steganography and cryptography is similar but the difference lies in applying different methods. In these two methods, the basic purpose is to obscure the original information. Interestingly, the method adopted in both multimedia security techniques, steganography and watermarking is the same but they vary in purposes. Hiding of digital content in images is the goal of steganography whereas watermarking helps in declaring right ownership [1]–[4]. In symmetric-key cryptography, block cipher has a very important role to play in encrypting the information. By keeping the same dimensions, block cipher converts plaintext data into ciphertext data with the assistance of a user-provided an undisclosed key [5], [6], [29]. By following the reverse pattern on ciphertext data, decryption of the whole process is performed provided that secret keys of the process remain unchanged. The above-mentioned procedure is adopted in Advanced Encryption Standards (AES) [7]. It is considered as one of the strong cryptosystems which encrypt the plaintext and ensure
secure communication. The whole procedure consists of four steps. In the very first step byte substitution which is also named as substitution step, is done with the help of the substitution-box (S-box). This is the step that actually highlights the importance of S-box in the encryption procedure. It is the only nonlinear component and this byte substitution step creates confusion in the plaintext data that can be seen in encrypted data. Different applications of substitution

FIGURE 1. Bifurcation diagram (first row) and Lyapunov spectrum (second row) of chaotic (a) Tent map, (b) Sine map, and (c) TSS map versus parameter \( r, \alpha, \) and \( \sigma \) for \( (0, 4] \), respectively.

FIGURE 2. Flowchart of proposed S-box design method.
and permutation process on plain text data provide encrypted ciphertext data [8]–[10]. The value and capability of producing confusion are measured by variations in the output bit pattern. The selected S-box must be robust and shows opposition against any attempt of cryptanalysis. Nonlinearity is considered as the foremost performing criterion of the S-box in any encryption method. Over the years, researchers are keen to get algebraically strong and cryptographically robust S-boxes. In addition to this, chaos-based S-boxes also have their importance for secure communication of data. These S-boxes exhibit different striking properties and offer interesting results to various ciphers. But the main focus is to improve the nonlinearity of these S-boxes [11], [12]. Mathematically, an S-box can be represented as:

$$S : GF(2^a) \rightarrow GF(2^b)$$  \hspace{1cm} (1)$$

S-box holds one to one and onto relations which makes it a bijection mapping and hence its inverse is possible. A message symbol is replaced with one element of S-box. By equation (1), it is evident that an $a \times b$ S-box takes $a$ bits as the input information and gives $b$ bits as the output [13].

Due to the success of AES S-box, a number of proposals have been put forward for the design of strong S-boxes using Galois field based algebraic techniques. In [14], Cui et al. proposed an affine-power-affine (APA) structure in which same AES algebraic operations are performed but with modified affine transformation cycle. The obtained S-box found to have good cryptographic and algebraic features. Subsequently, M-T Tran et al. utilized the gray codes to improve the S-box over algebraic coefficients in [15]. They added a preprocessing step to the structure of AES S-box by performing a gray-code transformation. In [16], Hussain et al. applied the algebraic permutation group $S_8$ on the elements of AES S-box which enables them to construct sequentially as much as 40320 S-boxes with similar performance strength as that of AES S-box. The same researcher proposed another algebraic method for S-box by applying the action of projective linear group on Galois field with a particular type of linear fractional transformation in [17]. In [18], a powerful algebraic method is suggested to construct 16 strong S-boxes built on the concept of Galois field extensions of order 256. The technique is purely algebraic and has ability to construct $8 \times 8$ S-boxes of high cryptographic strengths. Farwa et al. in [19] used multiplicative cyclic group of associated Galois field for the construction of algebraic S-box. They carefully formulated a bijective nonlinear iterative algebraic map defined on $GF(2^8)$ and the algebraic S-box provided acceptable properties for application in image encryption. A new S-box generation method based on both the algebraic and chaotic structures is proposed in [20]. Wherein, chaotic Chebyshev map and a
TABLE 1. Chaotic S-box corresponds to the TSS by equation (4) for $\beta = 1$.

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

TABLE 2. Chaotic S-box corresponds to the TSS by equation (6) for $\beta = 8/9$.

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

special class of permutation subgroups of symmetric group $S_{16}$ are explored for S-box construction. The available literature makes it evident that the S-box generation using any random approach, using chaos or some other pseudo-random source, doesn’t found to have good cryptographic strengths compared to S-boxes generated via algebraic methods. The only merit with random S-boxes is that it is quite easy to get a large quantity of S-boxes. However, cryptographically strong S-boxes are found to be easily obtainable through algebraic techniques [21]. But, many of them are keyless techniques and yields static S-boxes. In literature, some of the well-known S-boxes are AES [7], APA [14], Gray [15], S8 AES [16], S8-APA [22], [23]. The performance of optimization based S-box methods lies in between the random-based and algebraic methods. With the applied heuristics, many of the researchers have obtained S-boxes better than random or chaotic S-boxes. But, the associated demerit is that they are time consuming as the optimization process takes significant time to get notable configuration of optimized S-box [24]. In this work, combination of two 1D chaotic maps to improve their chaotic range is used to construct different S-boxes. In addition, the group action of a projective general linear group is also performed on the elements of $GF(2^8)$. Hence, an improved chaos-assisted search for strong S-boxes construction using the algebraic Mobius transformation is put forward. The proposed method is key-dependent, means it also has its own set of key space. Our method is a blend
TABLE 3. Chaotic S-box corresponds to the TSS by equation (7) for $\beta = 4/5$.

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

TABLE 4. Chaotic S-box corresponds to the TSS by equation (8) for $\beta = 6/7$.

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

of chaos-based random and algebraic techniques. Therefore, it holds the advantages of ease of constructing S-boxes with cryptographic strengths similar to AES and key-dependent.

The exhaustive comparison of S-boxes performance with a number of chaos-based, algebraic-based, and optimization-based methods is also done to reflect the superiority of our method over many of the standing methods. Moreover, an image encryption application of proposed S-boxes is also carried out to show their suitability to multimedia security.

II. REVIEW OF VARIOUS CHAOTIC MAPS

In the literature, various chaotic maps have been applied for encryption, watermarking and steganography techniques. Here, two chaotic maps i.e., Tent map and Sine map will be discussed and analyzed. The combination of these maps form a Tent-Sine system (TSS) which is used for the proposed chaotic S-box method.

A. CHAOTIC TENT MAP

The Tent map is expressed as [25]:

$$y_{n+1} = \begin{cases} \frac{\tau y_n}{2} & y_n < \frac{1}{2} \\ \frac{1 + y_n}{2} & y_n \geq \frac{1}{2} \end{cases}$$

(2)

where, the range of parameter $\tau$ lies in the interval $0 < \tau \leq 4$, and state variable $y_n \in [0, 1]$. It is obvious from bifurcation diagram of chaotic tent map; the map name is due to its tent map like shape. The interval of chaotic behavior of tent map is $[2, 4]$. The bifurcation diagram and lyapunov exponent are shown in Fig 1(a). The behavior of Tent map is chaotic for

VOLUME 7, 2019
173277
TABLE 5. Chaotic S-box corresponds to the TSS by equation (9), $\beta = 10/9$.

| S-box | $n_1$ | $n_2$ | $n_3$ | $n_4$ | $n_5$ | $n_6$ | $n_7$ | $n_8$ | $n_9$ | $n_{10}$ | $n_{11}$ | $n_{12}$ |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| S-box-1 | 108  | 106  | 108  | 110  | 110  | 108  | 104  | 104  | 100  | 100  | 100  | 100  |
| S-box-2 | 108  | 106  | 108  | 110  | 110  | 108  | 104  | 104  | 100  | 100  | 100  | 100  |
| S-box-3 | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  |
| S-box-4 | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  |
| S-box-5 | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  |

TABLE 6. Nonlinearity of proposed S-boxes.

| Proposed S-box | $n_1$ | $n_2$ | $n_3$ | $n_4$ | $n_5$ | $n_6$ | $n_7$ | $n_8$ | Min $n_1$ |
|----------------|------|------|------|------|------|------|------|------|-----------|
| S-box-1        | 108  | 106  | 108  | 110  | 110  | 108  | 104  | 104  | 100       |
| S-box-2        | 108  | 106  | 108  | 110  | 110  | 108  | 104  | 104  | 100       |
| S-box-3        | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112       |
| S-box-4        | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112       |
| S-box-5        | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112  | 112       |

the specific interval only as clear from Fig. 1(a) which shows the limitations of this chaotic map.

B. CHAOTIC SINE MAP

The chaotic behaviour of well-known Logistic map and Sine map is somewhat similar to each other. This can be seen in both bifurcation and lyapunov exponent diagrams of Sine map given in Fig 1(b). The Sine map has following governing equation [26].

$$y_{n+1} = \alpha \sin(\pi y_n) / 4, \quad 0 < \alpha \leq 4; \quad (3)$$

Like Tent map, the state variable $y_n \in [0, 1]$ and $\alpha$ is system parameter. Both the Tent map and Sine map have almost identical behavior and they have common problems as well. The range of chaos in Sine map is also limited as depicted in bifurcation diagram. Moreover, the non-uniformity of its trajectory-points combine with limited chaotic range makes the application of Sine map limited.

C. CHAOTIC TENT-SINE SYSTEM

The short chaotic spread of both Tent map and Sine map demands a chaotic map whose chaotic spread is bigger than two seed maps. A unique nonlinearity combination of these two maps gives a chaotic Tent-Sine system (TSS). This arrangement of chaotic maps plays an extremely complicated chaotic role [27]. The mod1 operator is required to keep the output range lies in between 0 to 1. The assimilation of parameters of both the chaotic maps, the expression is given in equation (4).

$$y_{n+1} = F(y_n, \sigma, \beta) = \begin{cases} \left(\frac{\sigma y_n}{2} + (4 - \sigma) \sin(\pi y_n^\beta)/4\right) \mod 1 & y_i < 1/2 \\ \left(\frac{(1 - y_n)/2 + (4 - \sigma) \sin(\pi y_n^\beta)/4}\right) & y_i \geq 1/2 \end{cases} \quad (4)$$

where $0 < \sigma \leq 4, \beta > 0$ are two parameters and $y_n \in [0, 1]$ is the state variable of the TSS chaotic system. The chaotic limit of the TSS system is increased remarkably well and the output sequences are distributed uniformly which can be seen from its bifurcation and lyapunov exponent diagrams shown in Figure 1(c) for $\beta = 1$.

III. PROPOSED METHOD

A. MOBIUS TRANSFORMATION BASED CONSTRUCTION OF CHAOTIC S-BOX

The important step in any cryptographic technique is the appropriate selection of S-box. This careful selection also restricts the linear and differential attacks. With a higher chaotic range and complex properties, Tent-Sine system is considered for the structuring proposed S-boxes. The flow chart in Fig. 2 shows that the primary input for the structure of S-box is taken from chaotic Tent-Sine map.
Moreover, the mathematical foundation of the proposed method is defined by the concept of group action of a projective general linear group over a Galois finite field $GF(2^8)$ with the help of Mobius transformation. The group action and Mobius transformation is expressed as follows:

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

$$g(m) = \mu_1 \times m + \mu_2, \Rightarrow 0 \leq m \leq 255$$  \hspace{1cm} (5)
where, the four values $u_1, u_2, u_3,$ and $u_4$ are from a finite field $GF(2^8)$. The Mobius transformation has a combined effect of inversion, dilation, rotation and translation in the Galois field domain. It also serves as one to one transformer provided that its inherent conditions are satisfied. The Mobius transformation $g(m)$ has point of discontinuity at $u_3 \times m + u_4 = 0$. This point has to be avoided while using it to generate the output value $g(m)$. The existence of discontinuity point of Mobius transformation is carefully checked when generating the S-box elements during operation of proposed scheme.
TABLE 8. Majority logic criterion results for plain and substituted images.

| Images         | Contrast | Correlation | Entropy | Energy | Homogeneity |
|----------------|----------|-------------|---------|--------|-------------|
| Plain-image    | 0.445343 | 0.910666    | 7.279584| 0.135318| 0.857543    |
| Proposed S-box-1| 9.314369 | 0.089245    | 7.279584| 0.017117| 0.437896    |
| Proposed S-box-1| 10.76492| 0.078912    | 7.279584| 0.018535| 0.434900    |
| Proposed S-box-3| 9.400597 | 0.075878    | 7.279584| 0.017137| 0.428206    |
| Proposed S-box-4| 9.56152 | 0.028254    | 7.279584| 0.017690| 0.434896    |
| Proposed S-box-5| 9.426823 | 0.056952    | 7.279584| 0.017380| 0.434357    |
| AES            | 9.514212 | 0.065412    | 7.279584| 0.017541| 0.431805    |
| APA            | 9.412510 | 0.058742    | 7.279584| 0.017621| 0.427469    |
| S8 AES         | 9.741021 | 0.074290    | 7.279584| 0.017200| 0.427540    |
| Gray           | 9.987453 | 0.073548    | 7.279584| 0.017870| 0.428410    |
| Skipjack       | 10.2547  | 0.065419    | 7.279584| 0.017412| 0.435846    |

FIGURE 6. Lena plaintext image and its encrypted images with proposed S-boxes of 1, 2, 3, 4, and 5.

The scheme proceeds further only if \( u_3 \times m + u_4 \neq 0 \), else the scheme needs to loop back to avoid the possibility of this discontinuity.

The choice of four \( u_1, u_2, u_3, \) and \( u_4 \) values, allocated to Mobius transformation is selected from chaotic Tent-Sine system. The products of the proposed method are chaotic S-boxes. The algorithm depicts that loop applied in it takes values of \( u_1, u_2, u_3, \) and \( m \), from interval 0-255. The algorithm goes to the next step once it satisfies the condition of \( u_1 \times u_4 - u_2 \times u_3 \) is not equal to zero. This condition makes the transformation preclude the possibility that Mobius transformation \( g(m) \) reduces to a constant. The operational steps of proposed method are the following.

**Step I:** Initially, random values \( w_1, w_2, w_3, w_4 \) are obtained by iterating the TSS map \( F(y_0, \sigma, \beta) \) four times by using the control parameter \( \sigma \) having interval \([0, 4]\) and the initial value \( y_0 \in [0, 1] \).

**Step II:** The four values \( u_i \) are calculated out of chaotic \( w_i \) for \( i = 1, 2, 3, 4 \) obtained in Step I as:

\[
 u_i = \text{mod} (\text{floor}(w_i \times 10000), 256)
\]

If the resulting value of \( u_1 \times u_4 - u_2 \times u_3 \) is any number other than zero, we will go to the next Step else we need to start from Step I again.

**Step III:** Here, we generate a sequence \( m \) of length 256 from different entries of the finite field \( GF(2^8) \). This sequence of 256 entries will be in ascending order.
Step IV: We need to go back to step III provided that $u_3 \times m + u_4$ is equal to zero. If the result of the expression is non-zero then we would take group action of the projective general linear group $PGL(2,GF(2^5))$ on the elements of $m$. This group action is defined in equation (5).

Step V: Lastly, by iterating the above-mentioned four steps will provide us the sequence $S$ having 256 different entries. Transform its elements into $16 \times 16$ matrix. This matrix $S$ is the proposed S-box.

The flowchart of the proposed method using the TSS chaotic map and Mobius transformation is shown in Fig. 2.

**B. PROPOSED S-BOXES**

S-boxes are constructed by using various powers $\beta$ of chaotic TSS map $F(y_0, \sigma, \beta)$. The initial values for $y_0 = 0.7$ and $\sigma = 3$ with specified $\beta$ is taken for simulation. The detailed description of the map relates to the first S-box for $\beta = 1$ is specified in equation (4) and the maps of rest of the four S-boxes are given in equations (8) to (11). The bifurcation diagrams of different forms of TSS maps having different exponents are shown in Figure 3. The exponent $\beta$ of TSS map is used as a parameter for constructing different S-boxes. The tabular form of proposed chaotic S-boxes for $\beta = 1, \beta = 8/9, \beta = 4/5, \beta = 6/7, \beta = 10/9$ are provided in Tables (1) to (5), respectively. The exponents used for the construction of these S-boxes are mentioned with Tables.

$$y_{n+1} = \begin{cases} \frac{y_n}{2} + (4 - \sigma) \sin(\pi y_n^b_4)/4 \mod 1 & \text{if } y_i < 1/2 \\ \sigma (1 - y_n)/2 + (4 - \sigma) \sin(\pi y_n^b_4)/4 \mod 1 & \text{if } y_i \geq 1/2 \end{cases}$$

(6)

$$y_{n+1} = \begin{cases} \frac{y_n}{2} + (4 - \sigma) \sin(\pi y_n^b_4)/4 \mod 1 & \text{if } y_i < 1/2 \\ \sigma (1 - y_n)/2 + (4 - \sigma) \sin(\pi y_n^b_4)/4 \mod 1 & \text{if } y_i \geq 1/2 \end{cases}$$

(7)

$$y_{n+1} = \begin{cases} \frac{y_n}{2} + (4 - \sigma) \sin(\pi y_n^b_4)/4 \mod 1 & \text{if } y_i < 1/2 \\ \sigma (1 - y_n)/2 + (4 - \sigma) \sin(\pi y_n^b_4)/4 \mod 1 & \text{if } y_i \geq 1/2 \end{cases}$$

(8)

$$y_{n+1} = \begin{cases} \frac{y_n}{2} + (4 - \sigma) \sin(\pi y_n^b_4)/4 \mod 1 & \text{if } y_i < 1/2 \\ \sigma (1 - y_n)/2 + (4 - \sigma) \sin(\pi y_n^b_4)/4 \mod 1 & \text{if } y_i \geq 1/2 \end{cases}$$

(9)

**IV. SUBSTITUTION BOXES ANALYSIS**

The assessment of the S-box defines its further application in various cryptographic schemes and multimedia security [28]–[30]. For this purpose, different theoretic and statistical performance measures are being utilized to evaluate the strength of S-boxes [31]. A comprehensive demonstration of such measures, involving differential characteristics of the block cipher is discussed in [32]. These types of attacks are used in block cipher-based S-boxes like DES and AES. The cipher can be scrutinized by using information theory approach [31]. Different tests like nonlinearity score, strict avalanche criteria (SAC), bit independent criterion (BIC),
TABLE 9. Majority logic criterion analyses for plain and encrypted images (AES algorithm).

| Images     | Contrast | Correlation | Entropy | Energy  | Homogeneity |
|------------|----------|-------------|---------|---------|-------------|
| Plain-image| 0.445343 | 0.910667    | 7.279584| 0.135318| 0.857543    |
| Proposed S-box-1 | 10.51509 | -0.00114    | 7.996877| 0.015647| 0.389625    |
| Proposed S-box-2 | 10.46624 | 0.001681    | 7.996711| 0.015641| 0.390036    |
| Proposed S-box-3 | 10.43909 | 0.001395    | 7.997025| 0.015638| 0.390467    |
| Proposed S-box-4 | 10.56595 | -0.004463   | 7.997268| 0.015638| 0.388188    |
| Proposed S-box-5 | 10.41189 | 0.006517    | 7.997024| 0.015637| 0.390352    |
| AES        | 10.62102 | -0.000250   | 7.998521| 0.015640| 0.392051    |
| APA        | 10.41298 | 0.002151    | 7.996584| 0.015632| 0.386540    |
| S8 AES     | 10.52987 | -0.003251   | 7.997201| 0.015625| 0.390638    |
| Gray       | 10.53687 | 0.004152    | 7.997259| 0.015690| 0.385021    |
| Skipjack   | 10.48999 | 0.005421    | 7.996980| 0.015605| 0.386930    |

linear and differential approximation probabilities. The all eight nonlinearity scores of proposed five S-boxes are given in Table 6. The minimal score of nonlinearity is also shown to highlight that proposed S-boxes have high score of minimal nonlinearity and capable to mitigate the minimal nonlinearity based attack. Moreover, the cryptographic performance features of proposed five S-boxes are also compared with an exhaustive list of state of the art S-boxes in Table 7. We selected those S-boxes whose average nonlinearity score is about 106 for comparison in Table 7. From comparison Table, it is clear that the proposed S-boxes (preferably the S-box-3, Sbox-4 and S-box-5) have remarkably better performance compared to almost all of the S-boxes (including recent ones) listed in the comparison Table. They show exhibits similar strengths and features as that of AES, APA, Gray, S8-AES S-boxes.

V. STATISTICAL ANALYSIS

To analyze the quality of the S-box constructed with the help of chaotic tent-sine system, the Lena plaintext image is substituted with five different proposed S-boxes. Moreover, we used our proposed S-boxes in the encryption technique (encryption technique of AES is followed). Fig. 4 gives the pictorial representation of the Lena plaintext image and substituted images using proposed S-boxes. While Fig. 5 shows the corresponding histograms of plain-image and substituted images. The plain-image Lena and its encrypted images using proposed S-boxes in the AES encryption scheme are shown in Fig. 6. The histograms of the original and encrypted images are given in Fig. 7. To show the strength of our technique, some statistical analyses under Majority Logic Criteria (MLC) [56] are described below.

A. CORRELATION

Correlation is considered as one of the basic methods to calculate the similarity between two images. The correlation is given by:

\[ \text{Corr} = \sum \frac{(i - \mu_i)(j - \mu_j) p(i, j)}{\sigma_i \sigma_j} \]  

where, \( p(i, j) \) indicates the pixel value and \( i \) represent the position of row and \( j \) indicates its column value of digital images. The parameters \( \mu \) and \( \sigma \) are the variance and standard deviation respectively.

B. ENTROPY

The magnitude of the improbability of a random variable to become the part of a random process is done in entropy. This analysis is used to depict the randomness of digital images. It can be defined as:

\[ C = - \sum p(x_i) \log_2 p(x_i) \]  

where, probability of random variable is given by \( p(x_i) \).

C. CONTRAST

Contrast analysis facilitates the user to see objects vividly to identify the texture of an image. The general value of contrast is given by:

\[ C = \sum |i - j|^2 p(i, j) \]  

D. HOMOGENEITY

The nearness of the distribution in the gray level co-occurrence matrix (GLCM) to GLCM diagonal is measured in homogeneity analysis. This matrix shows the calculations of combinations of pixel brightness outcomes in tabular form. It can be given as:

\[ \text{Hom} = \sum \frac{p(i, j)}{1 + |i - j|} \]  

E. ENERGY

In a digital image, squaring and taking the sum of gray pixels give the energy of the image. It is defined as:

\[ E = \sum p(i, j)^2 \]  

These different MLC analyses are performed to assess the best suited S-box for encryption techniques and multimedia security purposes. The comparison of the results of these analyses on the proposed technique with S-boxes such as AES, APA, S8 AES, Gray, and Skipjack are also performed. The MLC results after performing substitution operation are listed in Table 8 for proposed S-boxes and AES, APA, S8-AES, Gray and Skipjack S-boxes as well. The results
Indicate that the proposed S-box offers better statistical visual distortion effect than conventional S-boxes. The value of entropy is same for plain-image and all substituted images due to the same distribution of pixels. Whereas, Table 9 is maintained to provide the results of entropy, correlation, homogeneity, energy, contrast for plain-image and encrypted images. Here, the encryption is performed by AES algorithm using mentioned S-boxes. Again, the encryption results show the strength of our proposed S-boxes compared to others. The encryption outcomes of our proposed S-boxes are sufficiently satisfactory for secure communication applications.

VI. CONCLUSION
The most crucial components in the block encryption algorithms are substitution-boxes. They play vital role in the substitution-permutation network to offer sufficient nonlinearity and confusion. In this paper, a chaotic Tent-Sine system is applied for the construction of strong S-boxes. The Mobius transformation is applied to random values obtained through the chaotic map and provides 256 unique elements of the generated S-box. The randomness produced due to the inclusion of improved chaos increases the unpredictability of the cipher. The algebraic transformation fetches strength for the S-boxes. The results of the different statistical analyses indicate the extremely good cryptographic performance of our new S-boxes. The generated S-boxes show good results as compared to some well-known S-boxes, as apparent from the different statistical analyses.

VII. ACKNOWLEDGMENT
This work was supported by the Deanship of Scientific Research at King Khalid University through the Research Groups Program under Grant R.G.P 2/58/40.

REFERENCES
[1] S. Jamal, M. Khan, and T. Shah, “A watermarking technique with chaotic fractional S-box transformation,” Wireless Pers. Commun., vol. 90, no. 4, pp. 2033–2049, 2016.
[2] M. Khan and T. Shah, “A copyright protection using watermarking scheme based on nonlinear permutation and its quality metrics,” Neural Comput. Appl., vol. 26, no. 4, pp. 845–855, May 2015.
[3] S. I. Batoool, T. Shah, and M. Khan, “A color image watermarking scheme based on affine transformation and S permutation,” Neural Comput. Appl., vol. 25, nos. 7–8, pp. 2037–2045, 2014.
[4] S. S. Jamal, T. Shah, and I. Hussain, “An efficient scheme for digital watermarking using chaotic map,” Nonlinear Dyn., vol. 73, no. 3, pp. 1469–1474, 2013.
[5] A. Belazi, M. Khan, A. A. El-Latif, and S. Belghith, “Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption,” Nonlinear Dyn., vol. 87, no. 1, pp. 337–361, 2016.
[6] A. Anees, A. M. Siddiqui, and F. Ahmed, “Chaotic substitution for highly autocorrelated data in encryption algorithm,” Commun. Nonlinear Sci. Numer. Simul., vol. 19, no. 9, pp. 3106–3118, 2014.
[7] J. Daemen and V. Rijmen, The Design of Rijndael: AES—The Advanced Encryption Standard, Berlin, Germany: Springer-Verlag, 2004.
[8] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, and M. Aldape-Pérez, “Substitution box generation using Chaos: An image encryption application,” Appl. Math. Comput., vol. 332, pp. 123–135, Sep. 2018.
[9] I. Younas and M. Khan, “A new efficient digital image encryption based on inverse left almost semi group and lorentz chaotic system,” Entropy, vol. 20, no. 12, p. 913, 2018.
[10] M. Khan, T. Shah, and S. I. Batool, “A new approach for image encryption and watermarking based on substitution box over the classes of chain rings,” Multimedia Tools Appl., vol. 76, no. 22, pp. 24027–24062, 2017.
[11] A. Ullah, S. S. Jamal, and T. Shah, “A novel construction of substitution box using a combination of chaotic maps with improved chaotic range,” Nonlinear Dyn., vol. 88, no. 4, pp. 2757–2769, 2017.
[12] 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, p. 245, May 2019.
[13] L. Dragan and M. Iordach, “Comparison of Random S-box generation methods,” Publications L’Inst. Math., vol. 93, no. 107, pp. 109–115, 2013.
[14] L. Cui and Y. Cao, “A new S-box structure named affine-power-affine,” Int. J. Innov. Comput. Inf. Control, vol. 3, no. 3, pp. 751–759, Jun. 2007.
[15] M. T. Tran, D. K. Bui, and A. D. Duong, “Gray S-box for advanced encryption standard,” Proc. Int. Conf. Comput. Intel. Secur., Dec. 2008, pp. 253–258.
[16] I. Hussain, T. Shah, and H. Mahmood, “A new algorithm to construct secure keys for AES,” Int. J. Contemp. Math. Sci., vol. 5, no. 26, pp. 1263–1270, 2010.
[17] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, “A projective general linear group based algorithm for the construction of substitution box for block ciphers,” Neural Comput. Appl., vol. 22, no. 6, pp. 1085–1093, 2013.
[18] T. Shah and D. Shah, “Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over Z2,” Multimedia Tools Appl., vol. 78, no. 2, pp. 1219–1234, 2019.
[19] S. Farwa, N. Muhammad, T. Shah, and S. Ahmad, “A novel image encryption based on algebraic S-box and Arnold transform,” 3D Res., vol. 8, no. 3, Sep. 2017.
[20] A. Ullah, A. Iaveed, and T. Shah, “A scheme based on algebraic and chaotic structures for the construction of substitution box,” Multimedia Tools Appl., vol. 78, no. 22, pp. 32467–32484, Nov. 2019, doi: 10.1007/s11456-019-07957-8.
[21] S. Pickel, M. Cupic, and L. Rotim, “A new cost function for evolution of S-boxes,” Evol. Comput., vol. 24, no. 4, pp. 695–718, 2016.
[22] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, “Construction of S8 Liu S-boxes and their applications,” Comput. Math. Appl., vol. 64, no. 8, pp. 2450–2458, 2012.
[23] K. M. Ali and M. Khan, “A new construction of confusion component of block ciphers,” Multimedia Tools Appl., vol. 78, no. 22, pp. 32585–32604, Nov. 2019, doi: 10.1007/s11456-019-07866-w.
[24] K. M. Ali and M. Khan, “Application based construction and optimization of substitution boxes over 2D mixed chaotic maps,” Int. J. Theor. Phys., vol. 58, no. 9, pp. 3091–3117, 2019.
[25] M. Alawida, A. Sansudin, and J. S. Teh, “Enhancing unimodal digital chaotic maps through hybridisation,” Nonlinear Dyn., vol. 96, no. 1, pp. 601–613, Jul. 2019.
[26] M. Alawida, A. Sansudin, J. S. Teh, and R. S. Alkhawaldeh, “A new hybrid digital chaotic system with applications in image encryption,” Signal Process., vol. 160, pp. 45–58, Jul. 2019.
[27] Y. Zou, L. Bao, and C. P. Chen, “A new 1D chaotic system for image encryption,” Signal Process., vol. 97, no. 11, pp. 172–182, 2014.
[28] S. S. Jamal, T. Shah, S. Farwa, and M. U. Khan, “A new technique of frequency domain watermarking based on a local ring,” Wireless Netw., vol. 25, no. 4, pp. 1491–1503, 2019.
[29] M. F. Khan, A. Ahmed, K. Saleem, and T. Shah, “A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system,” IEEE Access, vol. 7, pp. 84980–84991, 2019.
[30] M. Khan, A. Ahmed, and K. Saleem, “A novel cryptographic substitution box design using Gaussian distribution,” IEEE Access, vol. 7, pp. 15999–16007, 2019.
[31] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, “An efficient approach for the construction of LFT S-boxes using chaotic logistic tent system,” IEEE Access, vol. 7, pp. 84980–84991, 2019.
[32] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” J. Cryptol., vol. 4, no. 1, pp. 3–72, 1991.
[33] 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.
[34] D. Lambić, “A novel method of S-box design based on discrete chaotic map,” Nonlinear Dyn., vol. 87, no. 4, pp. 2407–2413, 2017.
[35] D. Lambić, “S-box design method based on improved one-dimensional discrete chaotic map,” J. Inf. Telecomun., vol. 2, no. 2, pp. 181–191, Dec. 2018.
[36] M. Khan and T. Shah, “A construction of novel chaos base nonlinear component of block cipher,” Nonlinear Dyn., vol. 76, no. 1, pp. 377–382, 2014.

[37] K. E. Attaullah, S. S. Jamal, and T. Shah, “A novel algebraic technique for the construction of strong substitution box,” Wireless Pers. Commun., vol. 99, no. 1, pp. 213–226, 2018.

[38] F. Ozkaynak, “Construction of robust substitution boxes based on chaotic systems,” Neural Comput. Appl., vol. 31, no. 8, pp. 3317–3326, 2019.

[39] T. Ye and L. Zhimao, “Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling,” Nonlinear Dyn., vol. 94, no. 3, pp. 2115–2126, 2018.

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

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

[42] I. Hussain, T. Shah, M. A. Gondal, and W. A. Khan, “Construction of cryptographically strong 8 × 8 S-boxes,” World Appl. Sci. J., vol. 13, no. 11, pp. 2389–2395, 2011.

[43] I. Hussain, T. Shah, M. A. Gondal, W. A. Khan, and H. Mahmood, “A group theoretic approach to construct cryptographically strong substitution boxes,” Neural Comput. Appl., vol. 23, no. 1, pp. 97–104, Jul. 2013.

[44] S. S. Jamal, T. Shah, and A. Attaullah, “A group action method for construction of strong substitution box,” J. Res., vol. 8, no. 2, p. 12, 2017.

[45] A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah, and A. Waheed, “A novel construction of substitution box involving coset diagram and a bijective map,” Secur. Commun. Netw., vol. 2017, Nov. 2017, Art. no. 5101934.

[46] L. Shuai, L. Wang, L. Miao, and X. Zhou, “S-boxes construction based on the Cayley graph of the symmetric group for UASNs,” IEEE Access, vol. 7, pp. 38826–38832, 2019.

[47] W. Yong and L. Peng, “An improved method to obtaining S-box based on chaos and genetic algorithm,” HKIE Trans., vol. 19, no. 4, pp. 53–58, 2012.

[48] M. Ahmad, M. N. Doja, and M. S. Beg, “ABC optimization based construction of strong substitution-boxes,” Wireless Personal Commun., vol. 101, no. 3, pp. 1715–1729, Aug. 2018.

[49] Y. Tian and Z. Lu, “S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm,” J. Syst. Eng. Electron., vol. 27, no. 1, pp. 232–241, Feb. 2016.

[50] M. Ahmad, D. Bhatia, and Y. Hassan, “A novel ant colony optimization based scheme for substitution box design,” Procedia Comput. Sci., vol. 57, pp. 572–580, Jan. 2015.

[51] A. A. Alzaidi, M. Ahmad, H. S. Ahmed, and E. Al Solami, “Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map,” Complexity, vol. 2018, Dec. 2018, Art. no. 9389065.

[52] T. Farah, R. Rhouma, and S. Belghith, “A novel method for designing S-box on chaotic map and teaching-learning-based optimization,” Nonlinear Dyn., vol. 88, no. 2, pp. 1059–1074, 2017.

[53] H. A. Ahmed, M. F. Zolkipli, and M. Ahmad, “A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map,” Neural Comput. Appl., vol. 31, no. 11, pp. 7201–7210, 2019, doi: 10.1007/s00521-018-3557-3.

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

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

[56] A. Ullah, S. S. Jamal, and T. Shah, “A novel scheme for image encryption using substitution box and chaotic system,” Nonlinear Dyn., vol. 91, no. 1, pp. 359–370, 2018.

SAJJAD SHAUKAT JAMAL received the Ph.D. degree in mathematics from Quaid-i-Azam University, Islamabad, Pakistan. He is currently an Assistant Professor with the Department of Mathematics, King Khalid University, Abha, Saudi Arabia. His research interests are number theory, cryptography, digital watermarking, and steganography.

AMIR ANEES received the B.S. degree in electrical engineering from HITEC University, Taxila Cantt, Pakistan, in 2011, the M.S. degree in electrical engineering from the Military College of Signals, National University of Sciences and Technology, Pakistan, in 2014, and the Ph.D. degree in computer science from La Trobe University, Melbourne, Australia, in 2019. His research interests include image encryption, image hashing, and chaos-based encryption.

MUHAMMAD FAHAD KHAN is currently an Assistant Professor with Foundation University, and also a Ph.D. Scholar with the Department of Computer Science, Quaid-i-Azam University Islamabad. He is the author of more than 30 research articles. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, and optimization techniques.

IQTADAR HUSSAIN received the Ph.D. degree in mathematics, specializing in the area of algebraic cryptography, in 2014. He is currently an Assistant Professor with Qatar University. His current research interests include the applications of mathematical concepts in the field of secure communication and cybersecurity, where he has published 63 articles in well-known journals. His H-index score is 23 and i-10 index score is 34. His articles have 1320 Google scholar citations.