Wireless Personal Communications (2020) 112:467–480
https://doi.org/10.1007/s11277-020-07052-4

Construction of Non-linear Component of Block Cipher by Means of Chaotic Dynamical System and Symmetric Group

Adnan Javeed[1] · **Tariq Shah**[1] · **Atta Ullah**[1]

Published online: 10 January 2020

Abstract
The interesting features of chaos theory are utilized now a day's in information security. The simplest chaotic dynamical system is the double pendulum. Here in this article, two double pendulums are used to enhance the chaotic behavior of a dynamical system. This system is sensitive to initial conditions and bears complex and chaotic trajectory. Moreover, being multi dimensional system it endures grander solution space for the generation of large number of S-boxes. Furthermore, a permutation comprising on only two cycles of symmetric group of order 256 is applied to generate integer values for the construction of desired substitution box. The algebraic analysis of suggested S-box emphasis on its application, thereafter, an image is encrypted with the help of this S-box, whose statistical analysis validates its efficacy.

Keywords Chaotic dynamical system · Symmetric group · Substitution box (S-box) · Image encryption

1 Introduction

The exploration of chaotic systems started some 200 years ago. A system whose current state cannot be determined by initial conditions is known as chaotic system. The current state of the system is the consequence of the past initial conditions, medium of communication, the noise and external circumstances beyond the control of the observer. Hence randomness, ergodicity and sensitivity to initial conditions are ultimate topographies of chaotic system. These features attract cryptographers to use such system for secure communications of media using cryptographic algorithms. The purpose of cryptography in secure transmission is to convert valuable and meaningfull messages into the bogus ones. Such targets are achieved specifically in symmetric key cryptography and assymetric key cryptography, the two main divisions of cryptography. This paper make use of symmetric key cryptography. These are further divided by gauging mode of applications like block ciphers and stream ciphers.

✉ Adnan Javeed
ajaveed@math.qau.edu.pk

[1] Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan

Block cryptosytem works by selecting blocks of input data for further application of cryptographic procedures. The two main objectives of block cryotograms are to induce confusion and diffusion in the plain-text message. This was the idea introduced by Shannon [1]. Diffusion is attained by distorting the statistical configuration i.e. the original bits are scattered in cipher text. While confusion is achieved by modification of original bits. These two are attained in many block cryptosystems by means of round repetition of an algorithm. The four steps of recent block cryptograms include permutation, substitution, addition of key and mixing [2–5].

The usage of chaotic systems in cryptography specifically in block cryptosystems like the case here in this article is due to the fact of their peculier behaviour. These systems exhibt random behaviour, unpredictability and sensitivity towards initial inputs and parameters [6, 7]. An assaulter can not predict the chaotic system and the results obtained from this without having the knowledge of initial conditions. Chaotic dynamical systems are useful in the the design of cryptostem for acquiring confusion and dissusuion in the ciphered text. Henceforth, chaos is getting place in recent cryptosystem [8–12].

Secure communication using wireless channels is mandatory since cryptanalysts are always in line to extract the vital information. Thus, use of cryptography is only way to tackle such situations. The main aim of cryptographic algorithms is to create ambiguity in the enciphered information which is achieved using substitution boxes. These are only nonlinear components of block ciphers generating pandemonium in cryptosystems. Many articles are available in literature to construct such non-linear components utilizing different algebraic and chaotic maps, some of them are listed here. [13–18], but the chaotic dynamical systems are utilized very often in the field of cryptography.

The motivation behind the utilization of chaotic dynamical systems like double pendulum in the design of cryptosystems is due to the fact of the unpredictability and complex behaviour of the system. These systems are governed by the differential equtions. A physical system is modelled initially by finding derivatives of the function. These systems are key sensitive i.e. for a different set of initial conditions and parameters, a totally dissimilar chaotic trajectory is obtained. Moreover, with the involvement of numerous equations and conditions, chaotic dynamical systems are having enriched key space as compared to one dimensional systems like [7, 10, 15, 16, 19].

2 Double Pendulum

The simplest chaotic dynamical system is double pendulum. Whenever initial angels are slightly changed, the bifurcation pattern of this system changes exponentially. Being sensitive to initial conditions, the chaotic dynamical system is found prolific in generating confusion and diffusion in the cryptosystem. In this article, two double pendulums having same inclinations initially are used to generate integer values to design the non-linear components of block cipher. The mathematical formulation of a double pendulum shown in Fig. 1 is explained as follow

$$x_1 = l_1 \sin \varphi_1 \tag{1}$$

$$x_2 = l_1 \sin \varphi_1 + l_2 \sin \varphi_2 \tag{2}$$

$$y_1 = -l_1 \cos \varphi_1 \tag{3}$$

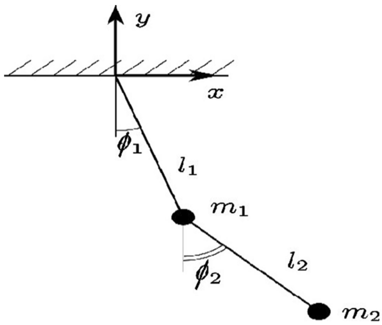

Fig. 1 Double pendulum attached end to end

$$y_2 = -l_1 \cos\varphi_1 - l_2 \cos\varphi_2 \tag{4}$$

where x_1 and x_2 are horizontal components and y_1 and y_2 are vertical components of masses m_1 and m_2 respectively. Now the potential energy P for case of double pendulum is given as

$$P = -m_1 g l_1 \cos\varphi_1 - m_2 g\left(l_1 \cos\varphi_1 + l_2 \cos\varphi_2\right) \tag{5}$$

And kinetic energy K is obtained by finding derivatives of Eqs. (1)–(4), we get

$$K = \frac{1}{2}m_1\left(\dot{\varphi}_1^2 l_1^2\right) + \frac{1}{2}m_2\left(\dot{\varphi}_1^2 l_1^2 + \dot{\varphi}_2^2 l_2^2 + 2\dot{\varphi}_1 l_1 \dot{\theta}_2 l_2 \cos\left(\varphi_1 - \varphi_2\right)\right) \tag{6}$$

The Langrangian (L) of a system is defined as the difference of kinetic energy and potential energy, which, for the case of a double pendulum is

$$\begin{aligned} L = &\frac{1}{2}\left(m_1 + m_2\right)L_1^2\dot{\varphi}_1^2 + \frac{1}{2}m_2 L_2^2 \dot{\varphi}_2^2 + m_2 L_1 L_2 \dot{\varphi}_1 \dot{\varphi}_2 \cos\left(\varphi_1 + \varphi_2\right) \\ &+ \left(m_1 + m_2\right) g L_1 \cos\varphi_1 + m_2 g L_2 \cos\varphi_2 \end{aligned} \tag{7}$$

Then,

$$\frac{\partial L}{\partial \varphi_1} = -L_1 g\left(m_1 + m_2\right)\sin\varphi_1 - m_2 L_1 L_2 \dot{\varphi}_1 \dot{\varphi}_2 \sin\left(\varphi_1 - \varphi_2\right) \tag{8}$$

$$\frac{\partial L}{\partial \dot{\varphi}_1} = \left(m_1 + m_2\right)L_1^2 \dot{\varphi}_1 + m_2 L_1 L_2 \dot{\varphi}_2 \cos\left(\varphi_1 - \varphi_2\right) \tag{9}$$

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{\varphi}_1}\right) = \left(m_1 + m_2\right)L_1^2 \ddot{\varphi}_1 + m_2 L_1 L_2 \ddot{\theta}_2 \cos\left(\varphi_1 - \varphi_2\right) - m_2 L_1 L_2 \ddot{\varphi}_2 \sin\left(\varphi_1 - \varphi_2\right)\left(\ddot{\varphi}_1 - \ddot{\varphi}_2\right) \tag{10}$$

Since Langrangian of a system satisfies the Euler-Langrange differential equation

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{\varphi}_1}\right) - \frac{\partial L}{\partial \varphi_1} = 0. \tag{11}$$

Substituting Eqs. (9) and (10) in above equation we get

$$\left(m_1 + m_2\right)L_1^2 \ddot{\varphi}_1 + m_2 L_1 L_2 \ddot{\theta}_2 \cos\left(\varphi_1 - \varphi_2\right) - m_2 L_1 L_2 \ddot{\varphi}_2^2 \sin\left(\varphi_1 - \varphi_2\right) + g L_1\left(m_1 + m_2\right)\sin\varphi_1 = 0 \tag{12}$$

Extracting $\ddot{\varphi}_1$ from the above equ, we get:

$$\ddot{\varphi}_1 = \frac{-m_2L_2\ddot{\varphi}_2\cos\left(\varphi_1-\varphi_2\right)-m_2L_2\ddot{\varphi}_2^2\sin\left(\varphi_1-\varphi_2\right)-g\left(m_1+m_2\right)\sin\varphi_1}{\left(m_1+m_2\right)L_1} \tag{13}$$

Similarly, we can derive an equation using Euler–Langrange equation for φ_2, which is as follow

$$\ddot{\varphi}_2 = \frac{-L_1\ddot{\varphi}_1\cos\left(\varphi_1-\varphi_2\right)-L_1\ddot{\varphi}_1^2\sin\left(\varphi_1-\varphi_2\right)-g\sin\varphi_2}{L_2} \tag{14}$$

Solving above two equations simultaneously to derive the following differential equations

$$\ddot{\varphi}_1 = \frac{-m_2L_1\ddot{\varphi}_1^2\sin\left(\varphi_1-\varphi_2\right)\cos\left(\varphi_1-\varphi_2\right)-m_2L_2\ddot{\varphi}_2^2\sin\left(\varphi_1-\varphi_2\right)+m_2gsin\left(\varphi_2\right)\cos\left(\varphi_1-\varphi_2\right)-g\left(m_1+m_2\right)\sin\varphi_1}{\left(m_1+m_2\right)L_1-m_2L_1\cos^2\left(\varphi_1-\varphi_2\right)}$$

$$\ddot{\varphi}_2 = \frac{m_2L_2\ddot{\varphi}_2^2\sin\left(\varphi_1-\varphi_2\right)\cos\left(\varphi_1-\varphi_2\right)+L_1\ddot{\varphi}_1^2\sin\left(\varphi_1-\varphi_2\right)\left(m_1+m_2\right)+gsin\left(\varphi_1\right)\cos\left(\varphi_1-\varphi_2\right)\left(m_1+m_2\right)-g\left(m_1+m_2\right)\sin\varphi_1}{\left(m_1+m_2\right)L_2-m_2L_2\cos^2\left(\varphi_1-\varphi_2\right)}$$

Now replacing $\varphi_1, \varphi_2, \ddot{\varphi}_1$and $\ddot{\varphi}_1$ by $\zeta_1, \zeta_2, \zeta_3, and\zeta_4$ respectively. Differentiation of these yields the following four first order differential equations after substituting $\ddot{\varphi}_1$ and $\ddot{\varphi}_2$:

$$\dot{\zeta}_1 = \ddot{\varphi}_1$$

$$\dot{\zeta}_2 = \ddot{\varphi}_2$$

$$\dot{\zeta}_3 = \frac{-m_2L_1\zeta_3^2\sin\left(\zeta_1-\zeta_2\right)\cos\left(\zeta_1-\zeta_2\right)-m_2L_2\zeta_4^2\sin\left(\zeta_1-\zeta_2\right)+m_2gsin\left(\zeta_2\right)\cos\left(\zeta_1-\zeta_2\right)-g\left(m_1+m_2\right)\sin\zeta_1}{\left(m_1+m_2\right)L_1-m_2L_1\cos^2\left(\zeta_1-\zeta_2\right)}$$

$$\dot{\zeta}_4 = \frac{m_2L_2\zeta_4^2\sin\left(\zeta_1-\zeta_2\right)\cos\left(\zeta_1-\zeta_2\right)+L_1\zeta_4^2\sin\left(\zeta_1-\zeta_2\right)\left(m_1+m_2\right)+gsin\left(\zeta_1\right)\cos\left(\zeta_1-\zeta_2\right)\left(m_1+m_2\right)-g\left(m_1+m_2\right)\sin\zeta_2}{\left(m_1+m_2\right)L_2-m_2L_2\cos^2\left(\zeta_1-\zeta_2\right)}$$

Solving the above four first order differential equations for two double pendulums in MATLAB for 50 s. The graph given in Fig. 2 depicts the chaotic nature of this dynamical system. The trajectories of two double pendulums are represented by colors in figure i.e. blue and red.

The initial inclinations of two double pendulums along with initial conditions of differential equations are responsible to determine the chaotic trajectory of dynamical system. A slight change in their values generate a different bifurcation pattern as demonstarted in Fig. 3. In other words, the solution space is sensitive to initial keys. This concept is very useful in cryptography for the generation of S-boxes. The robustness of the scheme based on such systems increases exponentially. For the case of two double pendulums, slight variation in initial parameters generated the following different bifurcation pattern. It implies that with theses values one can generate a totally different substitution box. Hence the suggested method is key sensitive.

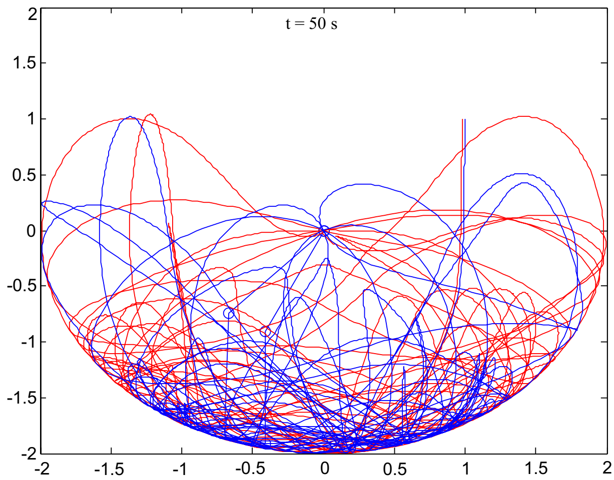

Fig. 2 Bifurcation diagram for double pendulum. (Color figure online)

The dominance of chaotic dynamical systems over low dimensional discrete chaotic systems is due to the fact that they have larger and complex solution space. Their larger key space and key sensitivity are also contributing in their supremacy. Moreover, chaotic range of continuous chaotic systems is bigger than discrete systems. Additionally, with the invention of modern computing devices, the chance of resistance attacks like brute force etc. are minimum for chaotic dynamical systems as compared to 1D and 2D systems.

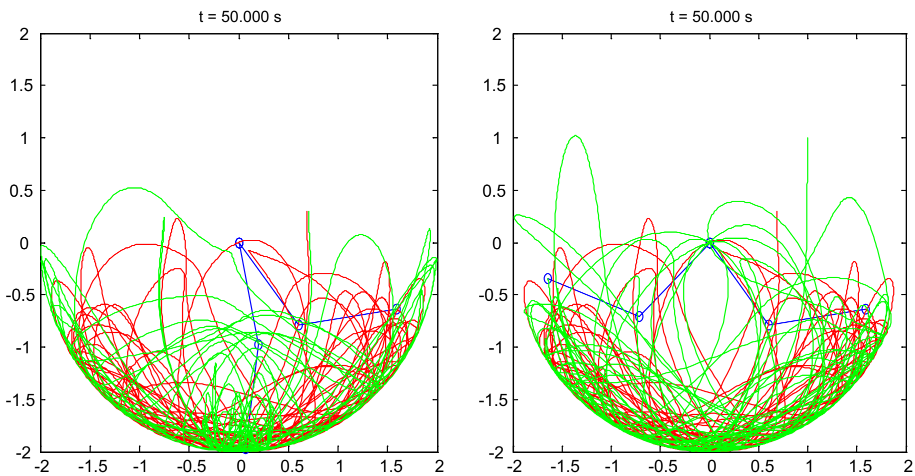

Fig. 3 Trajectory plot of the system for different initial conditions

3 Review of S-Boxes Connected to the Suggested Scheme

This section includes the contextual background regarding the suggested scheme. System of differential equations like Chaotic Lorenz system and Rabionvich–Fabrikant system is used by [13, 20, 21] to generate S-box. Khan et al. used multi chaotic systems for the construction of block cipher in [22]. The chaotic maps with improved chaotic range are utilized in [7] to synthesize nonlinear component of block cipher. The chaotic behavior of tent and sine maps are used to encipher the image by Zhou et al. in [5] and Attaullah et al. in [23]. Chaotic Gingerbreadman and symmetric group of order 8 was used for the design of an S-box in [24]. Authors used ABC optimization [25] and three dimensional baker maps for the production of S-boxes [17]. In [26] authors used the concept of coset diagram with bijecteive map and in [27] primitive irreducible polynomials over the field Z_2 for the construction of S-boxes. There is enough relevant material available in literature for the construction of S-boxes based on chaotic maps [19, 28–31] but chaotic dynamical systems are less utilized in cybersecurity.

4 Construction of Substitution Box

The confidentiality in any cryptosystem is increased utilizing substitution boxes. We suggest a new scheme for the design of S-box based on chaotic dynamical system. The simplest chaotic dynamical system is double pendulum. Two double pendulums making an extreme chaotic trajectory are used to construct S-box in this scheme. The result analysis of nonlinearity, strict avalanche criterion (SAC), bit independence criterion (BIC) and linear and differential approximation probability validates the proficiency of the suggested S-box. Substitution box construction involves the following steps.

- Initially, from the solution space of two double pendulums a chaotic sequence $U(1 \times 256)$ of integers is generated using MATLAB.
- Find the sequence $V(1 \times 256)$ as follow.

$$V(i) = U(256) - U(i) 1 \leq i \leq 256$$

- Arranging $V(i)$ in ascending order to obtain $W(i)$.
- After that each element of $W(i)$ is replaced by its order in $U(i)$ to obtain $Z(i)$.
- A new sequence $Z'(i)$ is obtained by the following relation

$$Z'(i) = Z(1) - Z(i) 1 \leq i \leq 256$$

- Permuting the position of $Z'(i)$ with random permutation generated by MATLAB to obtain the 16×16 matrix M_{16} given in Table 1.
- In the last step, a permutation μ from symmetric group S_{256}, containing only two cycles, is utilized for permuting the entries of M_{16}. This process leads us to obtain the desired substitution box given in Table 2.

Table 1 16 × 16 matrix

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

Table 2 Designed substitution box

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

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

Table 3 Evaluation of suggested S-box for nonlinearity analysis

S-box	Ref. [7]	Ref. [16]	Ref. [17]	Ref. [20]	Ref. [34]	Ref. [35]	Proposed
Average	106.75	103.3	103	104.7	105.25	112	111.5
Minimum	106	99	100	102	102	112	110
Maximum	108	106	106	108	108	112	112

Table 4 Evaluation of suggested S-box for average values

S-boxes	Ref. [7]	Ref. [16]	Ref. [17]	Ref. [20]	Ref. [34]	Ref. [35]	Proposed
BIC nonlinearity	106.6	103.3	103.1	104.1	103.8	112	111.357
BIC-SAC	0.4989	0.4987	0.5050	0.5058	0.4956	0.504	0.5053

4.1 Nonlinearity

It is the most imperative property of a cryptosystem. Principally, the nonlinearity of an outstanding cryptographic system is higher. It measures the confrontation of a system against linear cryptanalysis as given in Table 3. For a set of affine Boolean functions f_j, the following equation describes the nonlinearity of a Boolean function v:

$$NL_u = d\left(v,f_j\right) = \min\ d(v,\delta);\quad \delta \in f_j$$

4.2 Bit Independence Criterion

The statistical property of output bit independent criterion (BIC) for an S-box given by Webster and Tavares [32] is delineated as, for a certain collection of avalanche vectors, altogether the avalanche variables should be pairwise autonomous. This principle highlights the efficacy of confusion function. BIC values for the suggested S-box are tabultaed in Table 4.

Table 5 Evaluation of suggested S-box for SAC analysis

S-boxes	Ref. [7]	Ref. [16]	Ref. [17]	Ref. [20]	Ref. [34]	Ref. [35]	Proposed
Minimum	0.4219	0.4140	0.4218	0.3906	0.4297	0.453	0.4375
Average	0.4939	0.499	0.500	0.506	0.496	0.504	0.5053
Maximum	0.5625	0.6015	0.6093	0.5937	0.5313	0.562	0.5781

Table 6 Evaluation of suggested S-box for LP analysis

S-boxes	Ref. [7]	Ref. [16]	Ref [17].	Ref. [34]	Ref. [20]	Ref. [35]	Suggested
Max. LP	0.1250	0.1328	0.1289	0.1562	0.1250	0.062	0.0703
Max value	160	164	162	168	160	144	146

4.3 Strict Avalanche Criterion

The Strict avalanche effect (SAC) introduced by Webster and Tavares in 1985, basically elaborates the generality of avalanche effect and completeness given in Table 5. It states that the chances of variation in output bits must by 0.5 for alteration of sole input bit. Mathematically, for

$$h : GF(2)^n \to GF(2)^m$$

$$Prob\left(h\left(x^j\right)\right)_i \neq Prob(g(x))_i = \frac{1}{2} \qquad \forall \quad j \in [1, n] \quad and \quad i \in [1, m]$$

4.4 Linear Approximation Probability

The linear approximation probability (LAP) is used to measure the maximum amount of discrepancy of an event. For a set S containing total members 2^p of possible input bits. If τ_i *and* τ_o are denoting input and output values respectively, then (LAP) values for the proposed S-box given in Table 6, is explained by the following equation:

$$LAP = \max_{\tau_i, \tau_o \neq 0} \left| \frac{\#\left\{u/u.u = \tau(u).\tau_o\right\}}{2^p} - \frac{1}{2} \right|$$

4.5 Differential Approximation Probability

The differential homogeneity is an ultimate trait of a substitution box. The degree of a differential equality is also known as differential approximation probability. The corresponding values of DP are depicted in Table 7. Mathemaitcally, it is defined as follow:

Table 7 Assessment of DP entities for various S-boxes

S-boxes	Suggested	Ref. [7]	Ref. [16]	Ref. [17]	Ref. [34]	Ref. [20]
Max. DP	0.01563	0.0625	0.03906	0.05469	0.03906	0.04688

$$DP_f = \left(\frac{\#\{u \in U \wedge f(u) \oplus f(u \oplus \Delta u) = \Delta z\}}{2^k} \right)$$

5 Majority Logic Criterion

Majority logic criterion (MLC) is used to gauge the texture of an encrypted image after enciphering of an input image by an S-box. It includes the analyses like homogeneity, contrast, correlation, entropy and energy [33]. These analyses are used to establish the statistical strength of nonlinear component of block ciphers by measuring the amount of alterations occurred in an image after encryption. Some very brief details of these analysis are given hereafter.

5.1 Information Entropy Analysis

The rate of disorder in the cipher image gives the information entropy. The entropy for an image having total pixels N and the probability $p\left(u_j\right)$ for the pixel u_j will be calculated by:

$$\mathrm{E(U)} = \sum_{j=1}^{N} p\left(u_j\right) \log_2 p\left(u_j\right)$$

For a grayscale image, if $p\left(u_j\right)$ of occurance for any pixel u_j is equal then the hypothetical value of entropy is 8. Hence, the information entropy for the suggested scheme should approximately be 8, to validate its efficacy. Table 7 compares the entropy outcomes for the suggested scheme with [4, 7, 34].

Table 8 Evaluation of the proposed S-box for the Cameraman Image in comparison of varous S-boxes

Images	Contrast	Entropy	Correlation	Homogeneity	Energy
Original	0.4785	7.1025	0.9292	0.8964	0.1679
Proposed S-box	10.2584	7.9845	0.0023	0.3952	0.0157
Ref. [4]	8.2314	7.9591	−0.0441	0.4151	0.0202
Ref. [7]	8.3154	7.9812	−0.0045	0.4091	0.0177
Ref. [34]	8.2113	7.9431	0.0155	0.4248	0.0219
Ref. [35]	8.3124	7.9561	0.0554	0.4662	0.0202

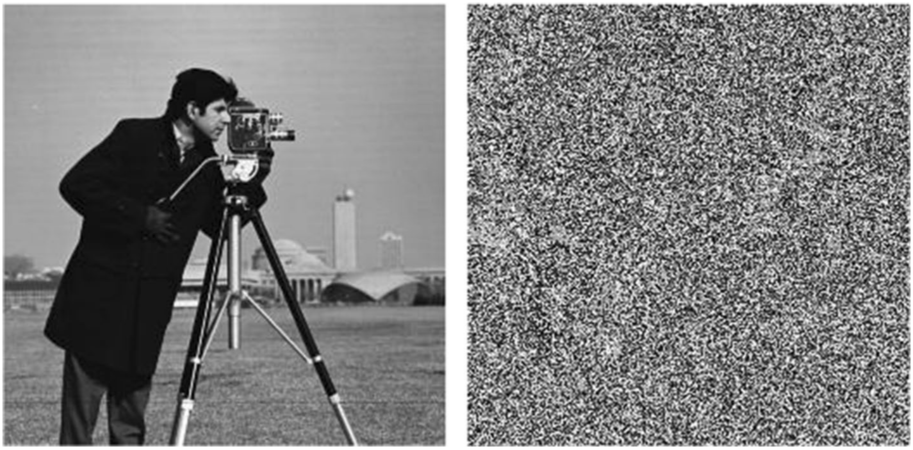

Fig. 4 Original and the processed cameraman image

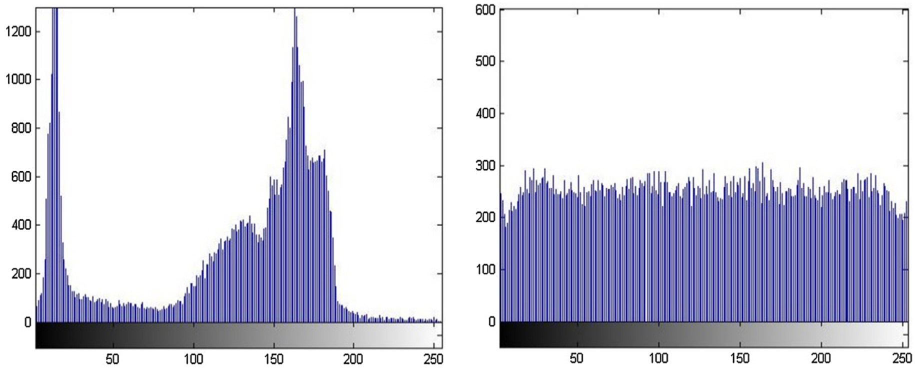

Fig. 5 Histogram of the Host and encrypted cameraman image

5.2 Correlation Analysis

The adjoining pixels (horizontally, vertically and diagonally) of the host image are highly correlated. A secure and robust encryption procedure make these adjacent pixels unrelated, i.e. the correlation of adjacent pixels approaches to zero of an enciphered image. The correlation for the neighbouring pixels r and s for a grayscale image is given by:

$$\Lambda_{rs} = \frac{\sum_{i=1}^{N} \left(\{ r_i - \bar{r} \} \{ s_i - \bar{s} \} \right)}{\sqrt{\sum_{i=1}^{N} \left(r_i - \bar{r} \right)^2} \sqrt{\sum_{i=1}^{N} \left(s_i - \bar{s} \right)^2}}$$

The outcomes generated by above relation are shown in Table 8. The correlation values of the processed image is almost zero as required.

5.3 Contrast, Homogeneity and Energy Analyses

An appropriate amount of brightness is present in the host image, which vanishes in the enciphered image. This loss is measured by the contrast analysis. The secure encryption yields the higher values of contrast for the encrypted image. Furthermore, the texture of an encrypted image is measured utilizing homogeneity and energy analysis (Figs. 4, 5).

6 Conclusion

To increase the vagueness of a cryptosystem, use of chaotic maps in the construction of a substitution box is a recent trend. In this paper, the simplest chaotic dynamical system i.e. double pendulum is used for the first time to generate integer values along with the application of symmetric group in construction of non-linear components of block cipher. The amalgamation of these two yields confusion and diffusion in the suggested cryptosystem. For a practical application, an image is encrypted afterwards with the designed S-box. The standard algebraic and statistical analyses available in literature validate the efficacy of the proposed system for the safe communication of data. Hence, designed chaotic S-box generated by means of chaotic dynamical system and symmetric group has the ability to become hurdle in the path of cryptanalysts.

Compliance with Ethical Standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell Systems Technical Journal, 28,* 656–715.
2. Kocarev, L. (2001). Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Magazine, 1,* 6–21.
3. Dachselt, F., & Schwarz, W. (2001). Chaos and cryptography. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48*(12), 1498–1509.
4. Khan, M., Shah, T., & Batool, S. I. (2016). Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Computing and Applications, 27*(3), 677–685.
5. Zhou, Y., Bao, L., & Chen, C. L. P. (2014). A new 1D chaotic system for image encryption. *Signal Processing, 97,* 172–182.
6. Jakimoski, G., & Kocarev, L. (2001). Chaos and cryptography: Block encryption ciphers. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48*(2), 163–169.
7. Ullah, A., Jamal, S. S., & Shah, T. (2017). A novel construction of substitution box using a combination of chaotic maps with improved chaotic range. *Nonlinear Dynamics*. https://doi.org/10.1007/s11071-017-3409-1.
8. Li, X., Wang, L., Yan, Y., & Liu, P. (2016). An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems. *Optik-International Journal for Light and Electron Optics, 127*(5), 2558–2565.
9. Hussain, I., Shah, T., & Gondal, M. A. (2012). A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. *Nonlinear Dynamics, 70*(3), 1791–1794.
10. Khan, M., & Shah, T. (2014). A novel image encryption technique based on Henon chaotic map and S8 symmetric group. *Neural Computing and Applications, 25*(7), 1717–1722.

11. Zhang, Y., & Xiao, D. (2014). Self-adaptive permutation and combined global diffusion or chaotic color image encryption. *International Journal of Electronics and Communications, 68*(4), 361–368.
12. Zhang, W., Yu, H., Zhao, Y., & Zhu, Z. (2016). Image encryption based on three-dimensional bit matrix permutation. *Signal Processing, 118,* 36–50.
13. Özkaynak, F., & Özer, A. B. (2010). A method for designing strong S-boxes based on chaotic Lorenz system. *Physics Letters A, 374*(36), 3733–3738.
14. Brown, R., & Chua, L. O. (1996). Clarifying chaos: examples and counter examples. *International Journal of Bifurcation and Chaos, 6*(2), 219–242.
15. Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos, 8*(6), 1259–1284.
16. Tang, G., Liao, X., & Chen, Y. (2005). A novel method for designing S-boxes based on chaotic maps. *Chaos, Solitons & Fractals, 23*(2), 413–419.
17. Chen, G., Chen, Y., & Liao, X. (2007). An extended method for obtaining S-boxes based on 3-dimensional chaotic baker maps. *Chaos, Solitons & Fractals, 31*(3), 571–579.
18. Arroyo, D., Diaz, J., & Rodriguez, F. B. (2013). Cryptanalysis of a one round chaos-based substitution permutation network. *Signal Processing, 93*(5), 1358–1364.
19. Ullah, A., Javeed, A., & Shah, T. (2019). A scheme based on algebraic and chaotic structures for the construction of substitution box. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-019-07957-8.
20. Khan, M., Shah, T., Mahmood, H., Gondal, M. A., & Hussain, I. (2012). A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. *Nonlinear Dynamics, 70*(3), 2303–2311.
21. Javeed, A., Shah, T., & Ullah, A. Design of an S-box using Rabinovich–Fabrikant system of differential equations perceiving third order nonlinearity. Multimedia Tools and Applications, https://doi.org/10.1007/s11042-019-08393-4.
22. Khan, M., Shah, T., Mahmood, H., & Gondal, M. A. (2013). An efficient method for the construction of block cipher with multi chaotic systems. *Nonlinear Dynamics, 71*(3), 489–492.
23. Ullah, A., Jamal, S. S., & Shah, T. (2018). A novel scheme for image encryption using substitution box and chaotic system. *Nonlinear Dynamics, 91*(1), 359–370.
24. Khan, M., & Asghar, Z. (2018). A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation. *Neural Comput & Applications, 29*(4), 993–999.
25. Ahmad, M., Doja, M. N., & Beg, M. M. S. (2018). ABC optimization based construction of strong substitution-boxes. *Wireless Personal Communications, 101*(3), 1715–1729.
26. Razaq, A., Yousaf, A., Shuaib, U., Siddiqui, N., Ullah, A., & Waheed, A. (2017). A novel construction of substitution box involving coset diagram and a bijective map. *Security and Communication Networks, 2017,* 5101934.
27. Shah, T., & Shah, D. (2019). Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over Z_2. *Multimdeia Tools and Applications, 78*(2), 1219–1234.
28. Khan, M., & Munir, N. (2019). A novel Image encryption technique based on generalized advanced encryption standard based on field of any characteristic. *Wireless and Personal Communication, 109*(2), 849–867.
29. Wang, X. Y., Feng, L., & Zhao, H. (2019). Fast image encryption algorithm based on parallel computing system. *Information Sciences, 486,* 340–358.
30. Khan, M., Hussain, I., Jamal, S. S., & Amin, M. (2019). A privacy scheme for digital images based on quantum particles. *Intrnational Journal of Theoretical Physics*. https://doi.org/10.1007/s10773-019-04301-6.
31. Wang, X. Y., & Gao, S. (2020). Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory. *Information Sciences, 507,* 16–36.
32. Webster, A. F., & Tavares, S. (1986). On the design of S-boxes. In: *Advances in cryptology: Proceedings of CRYPTO'85*. Lecture Notes in Computer Science, pp. 523–534.
33. Hussain, I., Shah, T., Gondal, M. A., & Mahmood, H. (2012). Generalized majority logic criterion to analyze the statistical strength of S-boxes. *Zeitschrift für Naturforschung A, 67,* 282–288.
34. Belazi, A., Khan, M., El-Latif, A. A., & Belghith, S. (2016). Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. *Nonlinear Dynamics, 87,* 337–361.
35. Daemen, J., & Rijmen, V. (2002). *The design of Rijndael-AES: The advanced encryption standard*. Berlin: Springer.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Adnan Javeed is currently a Ph.D. scholar in the department of Mathematics at Quaid-i-Azam University. He has done his masters and M.Phil. from the same university. His research interests are Groups and Loops, Cryptography, cybersecurity and digital watermarking.

Dr. Tariq Shah currently serving as Professor in department of Mathematics at Quaid-i-Azam University. His topics of research are commutative algebra, algebraic coding theory, cryptography, wireless communication, generalization of algebraic structure, fuzzy and soft structures in development of economics.

Atta Ullah is currently a Ph.D. scholar in the department of Mathematics at Quaid-i-Azam University. He has done his M.Phil. from the same university. His research interests are Algebra, Functional Analysis and Cryptography.