

Received May 18, 2019, accepted June 18, 2019, date of publication June 26, 2019, date of current version July 15, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2925081

A Novel Design of Cryptographic SP-Network Based on Gold Sequences and Chaotic Logistic Tent System

MUHAMMAD FAHAD KHAN¹, ADEEL AHMED², KHALID SALEEM³, AND TARIQ SHAH⁴

¹Department of Software Engineering, Foundation University Islamabad, Islamabad 44000, Pakistan

²Department of Computer Science, National University of Modern Languages, Islamabad 44000, Pakistan

³Department of Computer Sciences, Quaid-i-Azam University, Islamabad 44000, Pakistan

⁴Department of Mathematics, Quaid-i-Azam University, Islamabad 44000, Pakistan

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

This work was supported by the Offices of Research, Innovation and Commercialization.

ABSTRACT Substitution permutation network (SP-network) is a chain of linked mathematical primitives used in block cipher algorithms. The proposed novel design of cryptographic SP-network consists of three cryptographic primitives: substitution box, permutation box, and random key sequences, including one key whitening operation. A new design is being proposed for each cryptographic primitive. The cryptographic strength of the proposed SP-network is evaluated by employing various standard tests; strict avalanche criterion, differential approximation probability, bit independent criterion, linear approximation probability, nonlinearity test, unified averaged changed intensity, histogram analysis, and coefficient correlation tests. The outcomes of the investigations validate that the designed cryptosystem is stable for secure communication and attains better cryptographic strength as compared with other state-of-the-art techniques.

INDEX TERMS Symmetric cryptography, block cipher, SP-network, substitution box, nonlinearity.

I. INTRODUCTION

Today's digital information age brings along many issues; among which information security and privacy is deemed to be the most important. Researchers are developing different strategies to ensure information security; cryptographic technique being one of them. Cryptography is the science of using mathematics to encrypt and decrypt data in order to ensure that data cannot be read by anyone except the intended receipt [1]. Generally, symmetric cryptographic approaches are classified into two categories; block cipher and stream cipher [1], [3]. Block cipher is a deterministic algorithm which operates on the fixed-length groups of bits, called block; having block size $n \in \mathbb{N}$. The block ciphers with block size $n = 1$ are known as substitution ciphers. The encryption function of the block ciphers has the permutation of Σ^n , when used in symmetric key approach [1], [3], [5], [6]. In literature there are two design techniques available for block ciphers; i) Substitution-Permutation Networks (SP-Network), and ii) Feistel Ciphers. The SP-Network block ciphers contain repeating rounds of

key addition (unpredictability addition), substitution (non-linear layer), and diffusion (linear scattering layer), which make them difficult for Cryptanalysis [2], [4], [7]. The most notable SP-Network block ciphers are AES (Rijndael), 3-Way, PRESENT, SAFER, SHARK and Square [3]. The decryption process is simply the reversal of encryption process, starting with cipher text (the substitution-boxes and permutation layer should be inversed where round keys are applied in reverse order). The feistel ciphers are different from the SP-Network block ciphers, in a way that they do not require invertible substitution and permutation layers. Feistel cipher has the advantage that encryption and decryption processes are very similar, even identical in some cases. The most famous Feistel design based cipher standards are DES, RC5, ICE, and Blowfish [1], [3], [5], [8].

In SP-Network, the most important layer is substitution because the strength of the substitution mechanism directly influences the resistivity against any attack. The most influential attacks for block cipher are linear and differential attacks. These attacks can only be resisted, if designed S-box attains characteristics, such as low differential uniformity and high non-linearity [2], [4], [6]. To design an efficient S-box, researchers developed different strategies for pseudo-number

The associate editor coordinating the review of this manuscript and approving it for publication was Tony Thomas.

generation, based on chaotic system [10], [17]–[19], [22], Gaussian distribution [9] and machine learning [11], [23].

Chaotic system based s-box construction strategies are widely available in literature. The most common chaotic maps are; 1D chaotic map, logistic map and tent map [9]. The chaotic system itself has many drawbacks, which can affect the overall strength of the s-box. The most common issues of the chaotic systems are; discontinuity in chaotic sequences, finite precision effect, non-uniform distribution, limited behavior and computational complexity in dependent multidimensional chaotic maps [9], [10], [24]–[33].

In literature, gold sequences are extensively used in Code-Division Multiple Access (CDMA) and Global Positioning System (GPS) to prepare long cross correlation sequences. Gold code is the pair of sequences which can be generated by a simple circuitry. For gold sequence generation, there is one condition that the preferred pairs of M-sequences must have the same degree [12], [14], [21]. The preferred M-sequences are those two sequences which have length of n with a periodic cross correlation function that takes on the possible values $\{-1, -t(m), -t(m) - 2\}$. The Gold theorem for the pair of M-sequences is as follows [12], [14].

Gold theorem: A certain pair of m sequences of length n exhibits a three-valued cross correlation function with values

$$\{-1, -t(m), -t(m)-2\} \quad \text{Where,}$$

$$t(m) = \begin{cases} 2^{(m+1/2)} + 1 & \text{odd } m \\ 2^{(m+2/2)+1} & \text{even } m \end{cases} \quad (1)$$

It has been suggested in literature that preferred pair sequences have proper correlation property but these sequences can be re-constructed by linear regression method [20], [21].

In this paper, we combine the strong characteristics of chaotic systems and gold sequences to overcome the deficiencies of the two and generate high-dimensional chaotic PN sequences, which are extremely sensitive to multidimensional initial conditions. The combination offers different advantages over other conventional PN sequences and chaotic systems, as highlighted below:

- High-dimensional chaotic PN sequence generator can generate infinite sequences
- Generate short and long sequences without any repetition
- Offer high degree of security, requiring low complexity

We present a novel method for the construction of cryptographic SP-Network by synthesizing the high-dimensional chaotic gold sequences and logistic tent system. The proposed SP-Network consists of three cryptographic primitives (substitution box, permutation box, random key sequences) and one key whitening operation for connected layers.

Remaining of the paper is organized as follows; section II describes our core contribution and section III describes proposed methodology. Section IV presents the comprehensive analysis of the designed SP-Network and conclusion is given in section V.

II. CONTRIBUTION

The core contribution of this study is summarized as:

- Novel method for the construction of cryptographic SP-Network, synthesizing Gold sequences and logistic tent system.
- The proposed SP-Network based encryption technique passes all the statistical tests, substitution box security evaluation criteria, histogram analysis, coefficient correlation tests, linear and differential approximation probability criteria.
- Novel method for the construction of substitution box primitive by using chaotic Golden sequences and logistic tent system in a linear fractional transformation.
- Newly designed S-boxes resistivity is similar to the Advanced Encryption Standard (AES) S-box, in terms of maximum non-linearity against the attacks.
- Novel method for the construction of Permutation box primitive by synthesizing chaotic Golden sequences and logistic tent system.
- Key generation method from the unpredictable higher dimensional chaotic system which is extremely sensitive to higher dimensional initial states.

III. PROPOSED DESIGN METHODOLOGY

Proposed SP-Network operates on plaintext blocks of size 256 bytes and returns cipher text blocks of the same size. It has 2 rounds and 1 key addition operation. Design of proposed SP network is depicted in figure-1. In this SP-Network, confusion between plaintext and the sub key is obtained from uniquely designed S-box₁ and S-box₂, which have high nonlinearity of 112. Alongside, diffusion is obtained from our novel key dependent design of P-box₁ and P-box₂. The whole design of SP-Network is thoroughly explained in the following steps:

Step 1: Convert plain text into a decimal number form and divide into blocks of size 256. If last block length is less than 256, then add N numbers of '0' to make the block size up to multiple of 256.

Step 2: Divide initial key into sub key of size 256. Design of initial keys generation is briefly discussed in section A.

Step 3: Perform bitwise XOR on plaintext and sub key (k_0) to obtain the key additive plaintext.

Step 4: Each value of the plaintext, obtained from step-3 is replaced with entries of the proposed novel substitution box (S-box₁). Novel design of S-boxes generation is briefly discussed in section B.

Step 5: Each value obtained from step-4 is permuted with entries of the proposed permutation box (P-box₁) technique. Design of proposed novel permutation technique is briefly discussed in section C.

Step 6: Perform XOR on sub key (k_1) and resultant values obtained from step-5.

Step 7: Each value obtained from step-6 is replaced with entries of proposed S-box₂.

Step 8: Each value obtained from step-7 is permuted with entries of proposed P-box₂.



FIGURE 1. Proposed SP-network design.

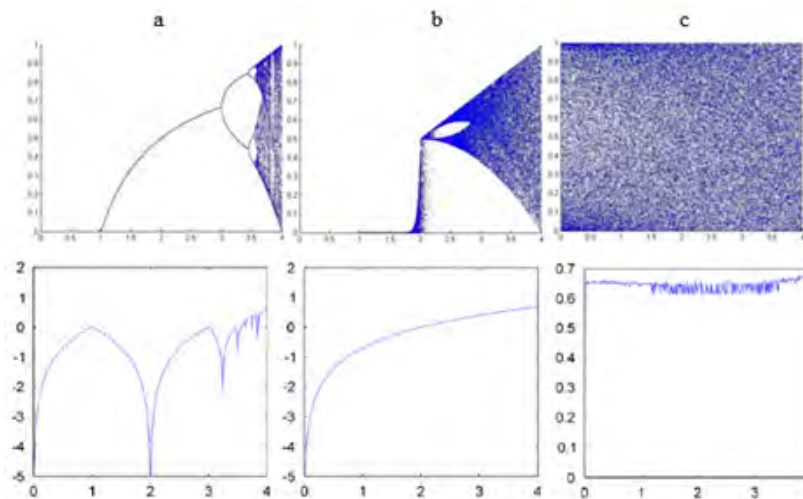


FIGURE 2. Lyapunov and bifurcation diagrams of (a). Logistic (b). Tent (c). Logistic tent system (LTS).

Step 9: Perform XOR on sub key (k_2) and resultant values obtained from step-8. After this step we get the cipher text values.

A. KEY GENERATION

Chaotic systems are extensively used in cryptography, but most of the chaotic systems and their orbits are vulnerable

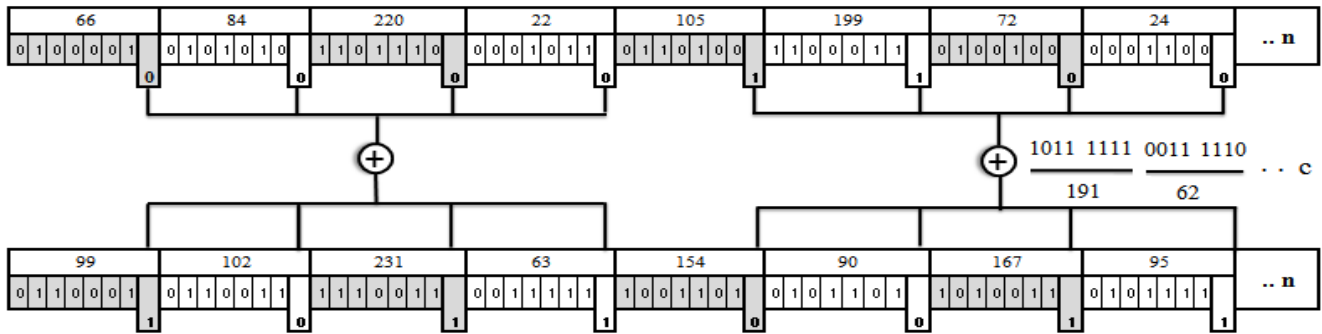


FIGURE 4. Proposed novel design to construct “c”.

chaotic behavior range. Following is the enhanced equation of Logistic Tent System (LTS):

$$z_{n+1} = \begin{cases} \left(\sigma z_n (1 - z_n) + \frac{(4 - \sigma) z_n}{2} \right) \text{ mod } 255 & z_i < 1/2 \\ \left(\sigma z_n (1 - z_n) + (4 - \sigma) (1 - z_n) / 2 \right) \text{ mod } 255 & z_i > 1/2 \end{cases} \quad (4)$$

In figure 2(c), we can see that LTS chaotic key space interval is increased for $0 \leq \sigma \leq 4$ [16]. These output sequences are divided into sub keys of size 256, in the range of 0 to 255.

B. SUBSTITUTION-BOX DESIGN

Our proposed novel design of substitution box generation method, constructs the high quality substitution boxes. Chaotic gold sequences, logistic map, tent map and improved logistic tent system are used in linear fractional transformation as:

$$f(z) = (az + b)/(cz + d) \quad (5)$$

where $cz = -d$ and $ad - bc \neq 0$ are avoided. The whole design of substitution box generation is thoroughly explained in the following steps:

Step 1: Generate golden binary sequences by using a pair of logistic map sequences and tent map sequences of $N = 2^n - 1$ [12], [13], [21]; defined as:

$$G(u, v) = \{u, v, u \oplus v, u \oplus Tv, u \oplus T^2v, \dots, u \oplus T^{N-1}v\} \quad (6)$$

‘T’ represents the cyclic shift of one in left, ‘u’ represents the logistic map sequences obtained from specific initial state and ‘v’ represents the tent map sequences obtained from specific initial state.

Step 2: For variable “a”: discard floating points from the output of golden sequences and get three random values. Figure-3 is the proposed design to produce “a” and “b”.

Step 3: Parse these three random values into their binary.

Step 4: Select least significant bit from every binary value and produce parity bits stream.

Step 5: Merge eight parity bits and parse it into their particular decimal values.

Step 6: For variable “b”: Apply XOR operation on parity bits constructed from Logistic Tent System (LTS), which is defined in equation (3) and binary sequences generated in step-1

Step 7: Convert the resultant values obtained from step-6 into their particular binary.

Step 8: Merge eight parity bits and convert to their particular decimal values.

Step 9: For variable “c”: Apply XOR operation on parity bits constructed in step-5 and values constructed in step-8. Figure-4 is the proposed design to produce “c”.

Step 10: Convert the resultant values obtained from step-9 into their particular binary.

Step 11: Merge eight parity bits and parse into their particular decimal values.

Step 12: For variable “d”: Apply XOR operation on parity bits constructed in step-8 and values constructed in step-11. Figure-5 is the proposed design to produce “d”.

Step 13: Convert the resultant values obtained from step-12 into their particular binary.

Step 14: Merge eight parity bits and parse into their particular decimal values.

Step 15: Now put sequences of “a”, “b”, “c” and “d” in equation-5 of linear fractional transformation.

Block by block sequences, generated from $f(z)$ are evaluated via nonlinear score and then transformed in substitution boxes, which are shown in Table-1 and Table-2.

C. PERMUTATION BOX DESIGN

Step-1: Apply XOR on values generated from Gold sequences in Section B step-5 and values generated from Logistic Tent System (LTS) in Section B step-8. These resultant values are in between 0 to 255 range and highly sensitive to initial states used in LTS and Golden sequences.

Step-2: Select first 256 distinct values as Permutation box.

IV. RESULTS AND EVALUATION

A. NON-LINEARITY

Nonlinearity is the capability of cryptographic function that provides resistance against linear attacks and it is represented by the non-linearity score [9]. Nonlinearity is the distance

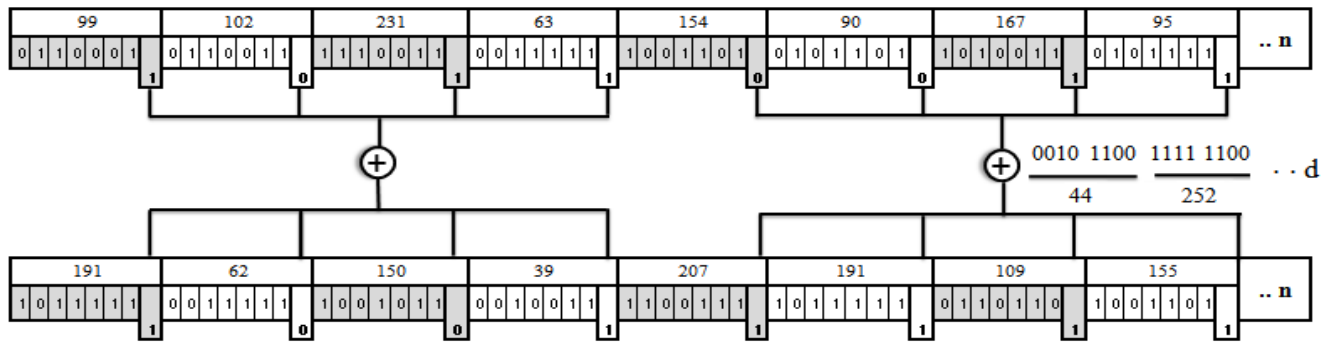


FIGURE 5. Proposed design to generate “d”.

TABLE 1. Proposed S-box-1.

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

TABLE 2. Proposed S-box-2.

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

among function and the set of all affine functions. Non-linearity represents a change in quantity of bit values in the Boolean truth table to get the nearest affine function characteristic [9], [10]. Therefore, large value of nonlinearity score is needed. Substitution Box-1 and Substitution Box-2 are generated from our novel proposed design, described

in table-1 and table-2. Maximum nonlinearity of both these substitution boxes is exactly 112 which is equal to the non-linearity score of the Advanced Encryption Standard (AES) S-box [2], [9], [34]. We observed that our obtained maximum nonlinearity scores of S-box₁ and S-box₂ are higher or equal to the state of the art research, as shown in table 3.

TABLE 3. Nonlinearity of various S-boxes.

S-box	Nonlinearity	S-box	Nonlinearity
AES	112	Jakimoski [8], 2001	98
Zhang [33], 2018	110	Khan [9], 2019	112
Yunfei [61], 2018	112	Anees [38], 2015	104
Özkaynak [39], 2018	108	Tarek [46], 2016	110
Zhang [18], 2018	112	Silva [40], 2018	106
Gangadari [56], 2016	110	Belazi [49], 2017	110
Belazi [49], 2017	112	Ahmad [11], 2015	110
Wang [34], 2010	106	Sarfraz [41], 2016	106
Belazi [49], 2017	110	Liu [46], 2014	106
Zhang [47], 2014	110	Liu [48], 2015	108
Ahmad [11], 2016	110	Lambić [45], 2017	108
Islam [35], 2017	108	Alzaidi [52], 2018	110
Solami [42], 2018	108	Tian [47], 2018	106
Belazi [49], 2017	108	Lambi [43], 2017	108
Çavuşoğlu [37], 2017	106	Lambić [45], 2014	112

TABLE 4. Bit independent criterion-S-box 1.

----	106	106	110	102	108	104	106
106	----	104	104	108	102	106	106
106	104	----	112	112	112	112	112
110	104	112	----	112	112	112	112
102	108	112	112	----	112	112	112
108	102	112	112	112	----	112	112
104	106	112	112	112	112	----	112
106	106	112	112	112	112	112	----

TABLE 5. Bit independent criterion-S-box 2.

----	108	106	100	106	108	106	106
108	----	104	106	104	100	108	100
106	104	----	100	104	106	104	104
100	106	100	----	106	108	108	104
106	104	104	106	----	112	112	112
108	100	106	108	112	----	112	112
106	108	104	108	112	112	----	112
106	100	104	104	112	112	112	----

TABLE 6. BIC dependent matrix- S-box 1.

----	.50781	.49414	.51757	.50390	.48437	.50000	.50781
.50781	----	.49804	.50781	.50195	.48828	.52343	.49804
.49414	.49804	----	.51953	.49218	.50390	.51367	.48632
.51757	.50781	.51953	----	.52148	.50195	.49023	.48046
.50390	.50195	.49218	.52148	----	.51367	.50195	.49414
.48437	.48828	.50390	.50195	.51367	----	.52734	.51562
.50000	.52343	.51367	.49023	.50195	.52734	----	.49218
.50781	.49804	.48632	.48046	.49414	.51562	.49218	----

B. BIT INDEPENDENT CRITERION (BIC)

One of the desirable property of cryptographic system is bit independent criterion (BIC), used as a standard for the evaluation of substitution boxes. The property of BIC assumes that all avalanche variables are pair-wise independent for a set of avalanche vectors, created by complementing a single plaintext bit. The outputs to affine transformation is varied with respect to nonlinear functions and number of inputs depends upon avalanche vector [9].

In tables 4, 5, 6 and 7, we can observe that the proposed S-box₁ and S-box₂ satisfy the bit independent criterion and BIC dependent matrix, near to the best achievable value.

C. STRICT AVALANCHE CRITERIA (SAC)

SAC results determine how many output bits changed when a single change is made in input [9]. It is defined as: $f : F_2^n \rightarrow F_2$ satisfies if $f(x) \oplus f(x \oplus \alpha)$ is balanced for $\alpha = 1$. The SAC result of the proposed S-box₁ and S-box₂ are given in table-8 and table-9, respectively.

TABLE 7. BIC dependent matrix- S-box 2.

----	.51171	.49804	.50390	.52343	.47851	.49023	.50976
.51171	----	.50585	.49414	.51562	.52539	.49414	.47460
.49804	.50585	----	.49218	.51367	.48242	.48046	.52734
.50390	.49414	.49218	----	.49609	.53320	.46875	.50976
.52343	.51562	.51367	.49609	----	.48632	.49414	.49609
.47851	.52539	.48242	.53320	.48632	----	.50976	.49023
.49023	.49414	.48046	.4687	.49414	.50976	----	.50781
.50976	.47460	.52734	.50976	.49609	.49023	.50781	----

TABLE 8. Strict avalanche criteria-S-box 1.

.50000	.50000	.54687	.37500	.46875	.50000	.54687	.51562
.43750	.54687	.46875	.51562	.51562	.46875	.46875	.46875
.51562	.53125	.45312	.51562	.53125	.53125	.54687	.53125
.46875	.56250	.56250	.51562	.48437	.53125	.54687	.43750
.56250	.56250	.51562	.48437	.53125	.54687	.43750	.54687
.56250	.51562	.48437	.53125	.54687	.43750	.546875	.51562
.51562	.48437	.53125	.54687	.43750	.54687	.51562	.46875
.46875	.54687	.50000	.50000	.51562	.46875	.45312	.48437

TABLE 9. Strict avalanche criteria-S-box 2.

.46875	.54687	.50000	.46875	.51562	.59375	.57812	.53125
.45312	.53125	.45312	.48437	.42187	.56250	.48437	.57812
.53125	.54687	.50000	.51562	.51562	.45312	.50000	.51562
.51562	.54687	.50000	.50000	.46875	.57812	.54687	.53125
.51562	.53125	.54687	.51562	.45312	.50000	.50000	.53125
.45312	.50000	.45312	.46875	.51562	.45312	.48437	.45312
.48437	.46875	.53125	.46875	.50000	.48437	.50000	.46875
.51562	.45312	.50000	.50000	.53125	.50000	.51562	.54687

S-box₁ average, maximum and minimum values for SAC are 0.506592, 0.562500, and 0.375000, respectively and square deviation is 0.040517. S-box₂ average, maximum and minimum, values for SAC are 0.504395, 0.593750, and 0.421875 respectively and the square deviation is 0.037192.

D. DIFFERENTIAL ANALYSIS

Diffusion characteristic of the encryption technique is measured by unified averaged changed intensity (UACI) and is number of changing pixel rate (NPCR). Both of these are also the most common assessment measures, which have the capacity to test the resistance of encryption technique against differential attacks [9], [54].

1) NPCR ANALYSIS

NPCR represented as follows [9].

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N \times M} \times 100\% \tag{7}$$

2) UACI ANALYSIS

UACI represented as follows [9].

$$UACI = \frac{1}{N \times M} \times \left[\sum_{i,j} \times \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\%$$

$$f(x) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j), \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j), \end{cases} \tag{8}$$

TABLE 10. proposed cipher comparison with AES.

Images	Loc.	NPCR		UACI	
		Proposed	AES	Proposed	AES
Lena	First	99.61	99.61	33.40	33.40
	Mid	99.65	99.66	33.51	33.32
	Last	99.63	99.61	33.62	33.52
Baboon	First	99.66	99.62	33.42	33.45
	Mid	99.64	99.61	33.44	33.46
	Last	99.63	99.62	33.48	33.53
Pepper	First	99.60	99.61	33.45	33.42
	Mid	99.65	99.66	33.50	33.35
	Last	99.62	99.62	33.49	33.47

TABLE 11. proposed cipher comparison with other cipher techniques.

Algorithms	NPCR	UACI
Proposed	99.63	33.41
Wang [18], 2018	99.59	33.45
Huang [58], 2009	99.42	24.94
Huang [59], 2013	99.54	28.27
Fouda [23], 2014	99.60	33.42
Farah [23], 2017	99.59	28.64
Guo [19] , 2018	99.60	33.46
Hussain [17], 2018	99.30	33.40
Khan [9], 2019	99.60	33.09

Comparative analysis of proposed scheme with AES is shown in table-10 and comparative analysis of proposed scheme with other various recent research works is shown in table-11.

E. LINEAR APPROXIMATION PROBABILITY (LP)

The linear approximation probability is the maximum value of the imbalance of an event in which parity of the output bits designated by the mask Γy is equal to the parity of the input bits designated by the mask Γx [9], [57].

$$LP_f = \max_{\Gamma x, \Gamma y \neq 0} \left| \frac{\#\{x \in X \mid x \cdot \Gamma x = S(x) \cdot \Gamma y\}}{2^n} - \frac{1}{2} \right| \quad (9)$$

where X is the set of all viable inputs and 2^n is the number of elements. Γx represents input mask and Γy represents output

TABLE 12. Differential approximation probability-S-box 1.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.0000	.0234	.0234	.0157	.0234	.0234	.0234	.0234	.0157	.0234	.0234	.0157	.0234	.0234	.0157	.0234
.0234	.0234	.0234	.0157	.0234	.0157	.0234	.0234	.0157	.0157	.0157	.0234	.0234	.0157	.0234	.0157
.0157	.0234	.0157	.0157	.0234	.0157	.0234	.0234	.0234	.0234	.0234	.0157	.0157	.0157	.0157	.0234
.0234	.0157	.0234	.0234	.0157	.0234	.0157	.0157	.0157	.0234	.0234	.0157	.0234	.0234	.0157	.0234
.0234	.0234	.0157	.0234	.0157	.0234	.0234	.0234	.0157	.0234	.0157	.0234	.0157	.0234	.0157	.0157
.0234	.0157	.0234	.0234	.0234	.0157	.0157	.0157	.0234	.0157	.0234	.0234	.0234	.0234	.0234	.0234
.0234	.0157	.0234	.0234	.0157	.0157	.0234	.0157	.0234	.0234	.0234	.0157	.0234	.0157	.0157	.0234
.0234	.0157	.0234	.0157	.0157	.0157	.0234	.0157	.0157	.0157	.0157	.0157	.0157	.0157	.0234	.0234
.0234	.0157	.0234	.0157	.0234	.0157	.0157	.0234	.0234	.0157	.0157	.0234	.0234	.0234	.0157	.0157
.0234	.0234	.0234	.0157	.0234	.0234	.0157	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0157	.0157
.0313	.0157	.0234	.0157	.0157	.0234	.0157	.0234	.0157	.0234	.0157	.0234	.0157	.0157	.0234	.0234
.0234	.0234	.0234	.0234	.0157	.0234	.0234	.0157	.0234	.0234	.0157	.0157	.0157	.0234	.0234	.0234
.0234	.0157	.0234	.0157	.0157	.0234	.0157	.0234	.0157	.0234	.0234	.0234	.0157	.0234	.0157	.0234
.0234	.0157	.0157	.0234	.0234	.0157	.0157	.0234	.0234	.0234	.0157	.0234	.0157	.0157	.0157	.0234
.0157	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0157	.0234	.0157	.0157	.0234

mask. Maximum value of LP for S-box₁ is 0.109 and S-box₂ is 0.117.

F. DIFFERENTIAL APPROXIMATION PROBABILITY

The differential approximation probability of Substitution box is a measure of differential uniformity. For every change in the value or order of input, there must be a distinctive change in the output. This characteristic of DP ensures uniform mapping probability for every input bit i [9]. In differential approximation probability, input differential must uniquely map to output differential $DP(\Delta x \rightarrow \Delta y)$ and it is defined as:

$$DP(\Delta x \rightarrow \Delta y) = \left[\frac{\#\{x \in X \mid (S(x) \oplus S(x \oplus \Delta x) = \Delta y)\}}{2^n} \right] \quad (10)$$

The differential approximation probability of proposed S-box₁ and S-box₂ are shown in table-12 and table-13.

G. HISTOGRAM ANALYSIS

Histogram analysis indicates how pixels spread after the encryption process. Ideal image encryption scheme transforms the plain image into encrypted image that contains the arbitrary pixels. Plain test images are shown in 6a, 8a, 10a and corresponding encrypted images are shown in 7a, 9a, and 11a. In these encrypted images, we can see that pixels are absolutely random and gives no clue about plain images. Figures 6b, 6c, 6d, 8b, 8c, 8d, 10b, 10c and 10d are the histograms of plain images in RGB channels and histogram of corresponding encrypted images in RGB channels are shown in 7b, 7c, 7d, 9b, 9c, 9d, 11b, 11c and 11d. In histogram of the plain image, we can easily see the visible patterns in every color channel but histogram of all encrypted images have no patterns and these histograms are randomly distributed in every color channel. It is the prove that histogram of encrypted images is equally uniform and does not give any clue to attacker to inject statistical attack.

TABLE 13. Differential approximation probability-S-box2.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.0000	.0234	.0313	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.01562	.0156	.0234	.0234	.0234
.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0313	.0234	.0234	.0156	.03125	.0313	.0234	.0234
.0234	.0234	.0313	.0234	.0313	.0313	.0234	.0234	.0234	.0156	.0313	.03125	.0234	.0234	.0234	.0156
.0234	.0156	.0234	.0234	.0234	.0156	.0234	.0234	.0234	.0234	.0234	.03125	.0234	.0234	.0234	.0234
.0234	.0313	.0234	.0234	.0156	.0234	.0234	.0234	.0156	.0156	.0234	.02344	.0313	.0234	.0313	.0234
.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0156	.02344	.0234	.0234	.0234	.0234
.0234	.0313	.0234	.0156	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.02344	.0234	.0234	.0313	.0234
.0234	.0234	.0234	.0156	.0234	.0234	.0234	.0313	.0313	.0234	.0234	.02344	.0313	.0234	.0234	.0234
.0234	.0234	.0234	.0313	.0234	.0234	.0234	.0234	.0234	.0234	.0156	.01562	.0234	.0313	.0234	.0313
.0234	.0156	.0234	.0234	.0234	.0156	.0234	.0156	.0234	.0234	.0234	.02344	.0234	.0234	.0234	.0313
.0156	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.02344	.0234	.0234	.0234	.0234
.0156	.0156	.0234	.0313	.0234	.0234	.0234	.0234	.0234	.0156	.0234	.02344	.0234	.0156	.0234	.0234
.0234	.0313	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.02344	.0234	.0234	.0234	.0234
.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0313	.0156	.0156	.0234	.0234	.02344	.0234	.0234	.0234
.0234	.0234	.0234	.0313	.0234	.0234	.0234	.0313	.0234	.0156	.0234	.02344	.0234	.0234	.0234	.0234
.0234	.0313	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0156	.03906	.0234	.0234	.0234	.0234	.0234

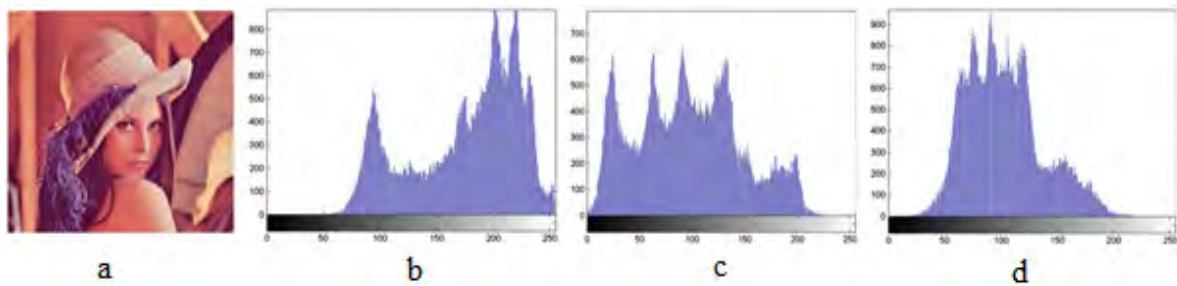


FIGURE 6. a. Plain test image lena; b. Histogram of R channel; c. Histogram of G channel; d. Histogram of B channel.

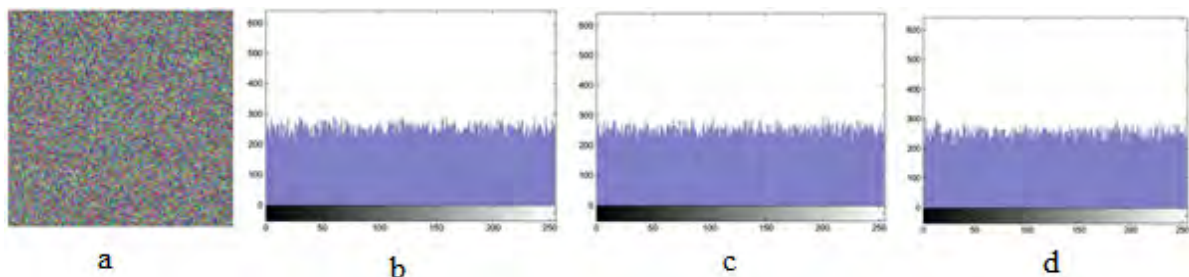


FIGURE 7. a. Encrypted image of Lena; b. Encrypted histogram of R channel; c. Encrypted histogram of G channel; d. Encrypted histogram of B channel.

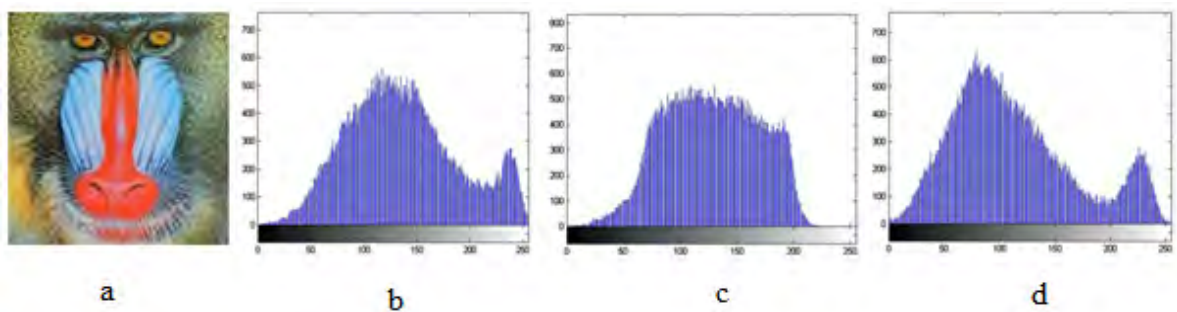


FIGURE 8. a. Plain test image baboon; b. Histogram of R channel; c. Histogram of G channel; d. Histogram of B channel.

H. CORRELATION-COEFFICIENT ANALYSIS

Adjacent pixels of images are naturally highly correlated, which gives valuable information to attackers.

Ideal encryption scheme should reduce the correlation of adjacent pixels. From the plain images (lena, baboon, pepper) and from the encrypted images (lena, baboon, pepper),

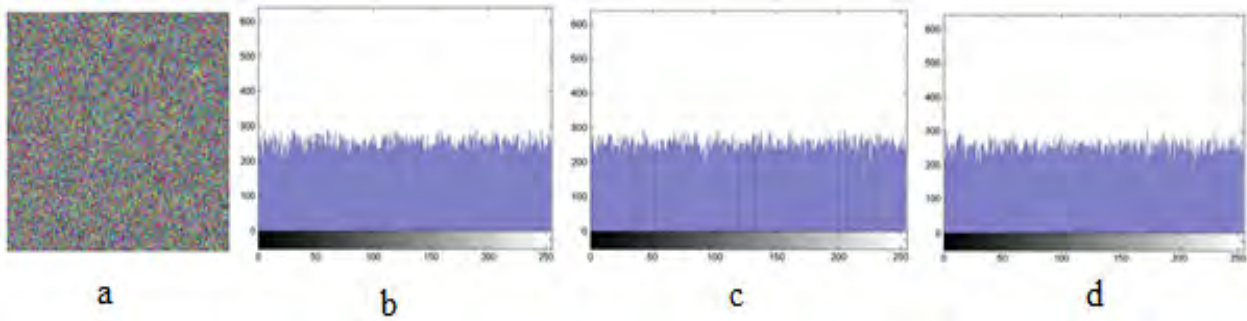


FIGURE 9. a. Encrypted image of baboon b. Encrypted histogram of R channel; c. Encrypted histogram of G channel; d. Encrypted histogram of B channel.

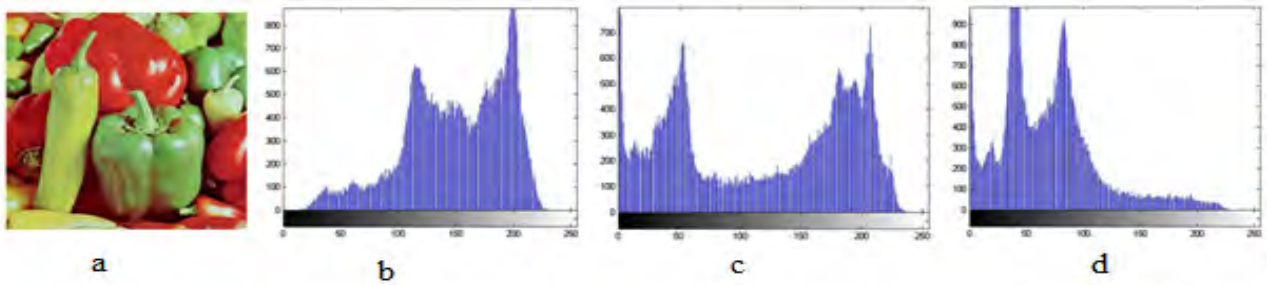


FIGURE 10. a. Plain test image pepper; b. Histogram of R channel; c. Histogram of G channel; d. Histogram of B channel.

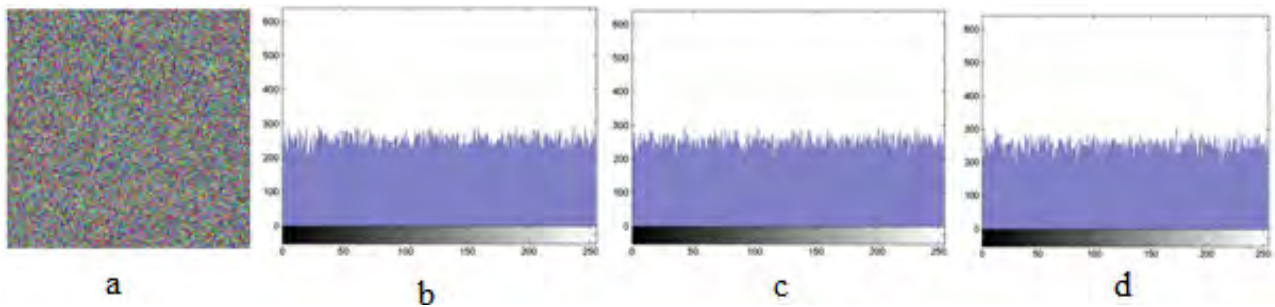


FIGURE 11. a. Encrypted image of pepper; b. Encrypted histogram of R channel; c. Encrypted histogram of G channel; d. Encrypted histogram of B channel.

10^3 adjacent pixels are selected in the horizontal, vertical and diagonal directions to calculate their correlation coefficients by using following equations [36]:

$$r_{xy} = cov(x, y) / (\sqrt{D(x)}\sqrt{D(y)}) \tag{11}$$

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \tag{12}$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2, \quad E(x) = \frac{1}{N} \sum_{i=1}^N x_i \tag{13}$$

Correlation-coefficient analysis of various plain images and their corresponding cipher images is shown in table-14. In table-14 we can see that, correlation coefficient value of adjacent pixels of plain images are near to 1 and after encryption correlation coefficient value is close to 0.

TABLE 14. Correlation-coefficient analysis of plain and cipher images.

Images	Correlation Coefficient of Plain Images			Correlation Coefficient of Encrypted Images		
	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical
Lena	0.94059	0.92432	0.96732	0.00089	0.00210	-0.00075
Baboon	0.693661	0.608783	0.607321	-0.00014	0.00031	0.000793
Pepper	0.945657	0.895111	0.941861	0.000857	-0.00137	0.000191

Correlation-coefficient value of encrypted images is entirely changed from the plain images value, so it is proved that correlation-coefficient attack fails to give any clue to attacker about original plain image. Correlation-coefficient analysis of adjacent pixels are plotted in figure-12, for results of plain image and figure-13 shows the results of encrypted image in horizontal, vertical and diagonal directions.

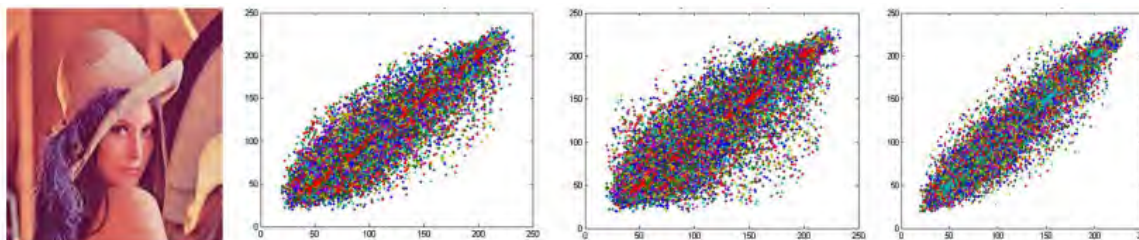


FIGURE 12. Plain image scatter plots to show the correlation-coefficient analysis of adjacent pixels in a. horizontal direction b. vertical direction c. diagonal direction.

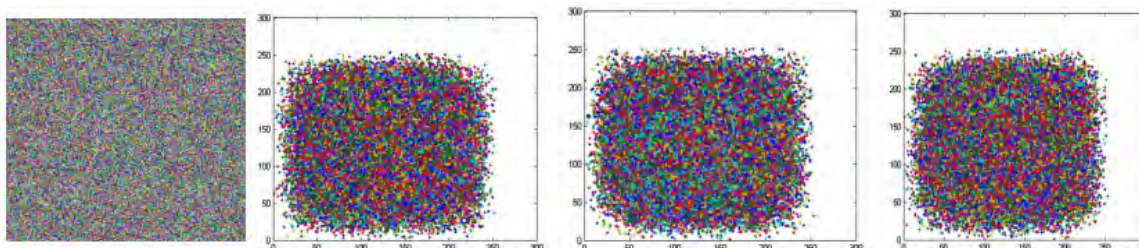


FIGURE 13. Encrypted image scatter plots to show the correlation-coefficient analysis of adjacent pixels in a. horizontal direction b. vertical direction c. diagonal direction.

V. CONCLUSION

A novel method for the construction of cryptographic SP-Network through blending the high-dimensional chaotic Gold sequences and logistic tent system has been established. The proposed SP-Network consists of three cryptographic primitives; S-box, P-box and Random key sequences, while one key whitening operation is used for connecting layers. The evaluation of the technique proves that the constructed S-box provides the required cryptographic properties. A comparison of the results of several color image quality measures, with color image encryption by chaos based schemes, has been prepared to establish the worth of this new cryptographic SP-Network. The results show that the proposed encryption method can provide a replacement for many current SP-Network based encryption systems. In future, various confusion and diffusion layers are to be used for generating SP-Network.

REFERENCES

- [1] B. Mohamed, C. Eder, and T. Hanke, *An Introduction to Cryptography*. Germany: Timo Hanke at RWTH Aachen Univ. 2018, pp. 1–145.
- [2] W. Zhang and E. Pasalic, “Highly nonlinear balanced S-boxes with good differential properties,” *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7970–7979, Dec. 2014.
- [3] M. Ratiner, “The method of S-box construction,” *J. Discrete Math. Sci. Cryptogr.*, vol. 8, no. 2, pp. 203–215, 2005.
- [4] K. Mohamed, M. N. M. Pauzi, F. H. H. M. Ali, S. Ariffin, and N. H. N. Zulkipli, “Tudy of S-box properties in block cipher,” in *Proc. Int. Conf. Comput., Commun. Control Technol. (I4CT)*, Sep. 2014, pp. 362–366.
- [5] I. Roy, C. Rebeiro, A. Hazra, and S. Bhunia, “SAFARI: Automatic synthesis of fault-attack resistant block cipher implementations,” *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, to be published.
- [6] J. Szczepanski, J. M. Amigo, T. Michalek, and L. Kocarev, “Cryptographically secure substitutions based on the approximation of mixing maps,” *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 52, no. 2, pp. 443–453, Feb. 2005.
- [7] L. Kocarev, “Chaos-based cryptography: A brief overview,” *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, Mar. 2001.
- [8] G. Jakimoski and L. Kocarev, “Chaos and cryptography: Block encryption ciphers based on chaotic maps,” *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 2, pp. 163–169, Feb. 2001.
- [9] M. F. Khan, A. Ahmed, and K. Saleem, “A novel cryptographic substitution box design using Gaussian distribution,” *IEEE Access*, vol. 7, pp. 15999–16007, 2019.
- [10] 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.
- [11] M. Ahmad, N. Mittal, P. Garg, and M. M. Khan, “Efficient cryptographic substitution box design using travelling salesman problem and chaos,” *Perspect. Sci.*, vol. 8, pp. 465–468, Sep. 2016.
- [12] S. Said, I. Fennouh, and C. Tanougast, “Hyperchaos-based spreading codes generator for DS-CDMA communication systems,” *J. Circuits, Syst. Comput.*, vol. 27, no. 13, 2018, Art. no. 1850207.
- [13] C. G. Liao and P. Liu, “Performance analysis of chaotic spread spectrum sequences,” *Adv. Mater. Res.*, vol. 852, pp. 608–612, Jan. 2014.
- [14] H.-P. Ren, C. Bai, Q. Kong, M. S. Baptista, and C. Grebogi, “A chaotic spread spectrum system for underwater acoustic communication,” *Phys. A, Stat. Mech. Appl.*, vol. 478, pp. 77–92, Jul. 2017.
- [15] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, “An efficient approach for the construction of LFT S-boxes using chaotic logistic map,” *Nonlinear Dyn.*, vol. 71, nos. 1–2, pp. 133–140, Jan. 2013.
- [16] 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.
- [17] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, “Construction of chaotic quantum magnets and matrix Lorenz systems S-boxes and their applications,” *Chin. J. Phys.*, vol. 56, no. 4, pp. 1609–1621, 2018.
- [18] X. Wang, X. Zhu, and Y. Zhang, “An image encryption algorithm based on Josephus traversing and mixed chaotic map,” *IEEE Access*, vol. 6, pp. 23733–23746, 2018.
- [19] J.-M. Guo, D. Riyono, and H. Prasetyo, “Improved beta chaotic image encryption for multiple secret sharing,” *IEEE Access*, vol. 6, pp. 46297–46321, 2018.
- [20] X. Wang, Y. Wu, and B. Caron, “Transmitter identification using embedded pseudo random sequences,” *IEEE Trans. Broadcast.*, vol. 50, no. 3, pp. 244–252, Sep. 2004.

- [21] K. Kashayp, K. K. Sarma, and M. P. Sarma, "Design of logistic map-based spreading sequence generation for use in wireless communication," in *Next Generation Wireless Network Security Privacy*. Hershey, PA, USA: IGI Global, 2015, pp. 81–121.
- [22] H. Jiang, D. Belkin, S. E. Savel'ev, S. Lin, Z. Wang, Y. Li, S. Joshi, R. Midya, C. Li, M. Rao, M. Barnell, Q. Wu, J. J. Yang, and Q. Xia, "A novel true random number generator based on a stochastic diffusive memristor," *Nature Commun.*, vol. 8, no. 1, p. 882, 2017.
- [23] 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.
- [24] C. Li, D. Arroyo, and K.-T. Lo, "Breaking a chaotic cryptographic scheme based on composition maps," *Int. J. Bifurcation Chaos*, vol. 20, no. 8, pp. 2561–2568, 2010.
- [25] C. Li, S. Li, and K.-T. Lo, "Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 2, pp. 837–843, 2011.
- [26] J. Gayathri and S. Subashini, "A survey on security and efficiency issues in chaotic image encryption," *Int. J. Inf. Comput. Secur.*, vol. 8, no. 4, pp. 347–381, 2016.
- [27] G. Zhao, G. Chen, J. Fang, and G. Xu, "Block cipher design: Generalized single-use-algorithm based on chaos," *Tsinghua Sci. Technol.*, vol. 16, no. 2, pp. 194–206, 2011.
- [28] N. Hadj-Said, B. Belmeki, and A. Belgoraf, "Chaotic behavior for the secrete key of cryptographic system," *Chaos, Solitons Fractals*, vol. 23, no. 5, pp. 1549–1552, 2005.
- [29] G. Jakimoski and L. Kocarev, "Analysis of some recently proposed chaos-based encryption algorithms," *Phys. Lett. A*, vol. 291, no. 6, pp. 381–384, 2001.
- [30] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," *Phys. Lett. A*, vol. 309, nos. 1–2, pp. 75–82, 2003.
- [31] Y. Lu, L. Li, H. Zhang, and Y. Yang, "An extended chaotic maps-based three-party password-authenticated key agreement with user anonymity," *PLoS ONE*, vol. 11, no. 4, 2016, Art. no. e0153870.
- [32] E.-J. Yoon, "Efficiency and security problems of anonymous key agreement protocol based on chaotic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 7, pp. 2735–2740, 2012.
- [33] T. Zhang, C. L. P. Chen, L. Chen, X. Xu, and B. Hu, "Design of highly nonlinear substitution boxes based on I-Ching operators," *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3349–3358, Dec. 2018.
- [34] Y. Wang, L. Yang, M. Li, and S. Song, "A method for designing S-box based on chaotic neural network," in *Proc. 6th Int. Conf. Natural Comput.*, vol. 2, Aug. 2010, pp. 1033–1037.
- [35] F. U. Islam and G. Liu, "Designing S-box based on 4D-4wing hyperchaotic system," *3D Res.*, vol. 8, no. 1, p. 9, 2017.
- [36] M. Ge and R. Ye, "A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties," *Egyptian Inform. J.*, vol. 20, no. 1, pp. 45–54, 2019.
- [37] Ü. Çavuşoğlu, A. Zengin, I. Pehlivan, and S. Kaçar, "A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system," *Nonlinear Dyn.*, vol. 87, no. 2, pp. 1081–1094, 2017.
- [38] A. Anees and M. A. Gondal, "Construction of nonlinear component for block cipher based on one-dimensional chaotic map," *3D Res.*, vol. 6, p. 17, Jun. 2015.
- [39] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," in *Neural Computing Application*. Springer, 2018, pp. 1–10.
- [40] 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.
- [41] M. Sarfraz, I. Hussain, and F. Ali, "Construction of S-box based on Mobius transformation and increasing its confusion creating ability through invertible function," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 2, p. 187, 2016.
- [42] 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.
- [43] D. Lambić, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2407–2413, 2017.
- [44] 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.
- [45] 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.
- [46] H. Liu, A. Kadir, and Y. Niu, "Chaos-based color image block encryption scheme using S-box," *AEU Int. J. Electron. Commun.*, vol. 68, no. 7, pp. 676–686, 2014.
- [47] X. Zhang, Z. Zhao, and J. Wang, "Chaotic image encryption based on circular substitution box and key stream buffer," *Signal Process., Image Commun.*, vol. 29, no. 8, pp. 902–913, 2014.
- [48] G. Liu, W. Yang, W. Liu, and Y. Dai, "Designing S-boxes based on 3-D four-wing autonomous chaotic system," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1867–1877, 2015.
- [49] 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.
- [50] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, 2016.
- [51] 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.
- [52] A. A. Alzaidi, M. Ahmad, M. N. Doja, E. Al 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.
- [53] Y. Wu, J. P. Noonan, and S. Ağaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Select. Areas Telecommun.*, vol. 1, pp. 31–38, Apr. 2011.
- [54] X. Chen and C. J. Hu, "Adaptive medical image encryption algorithm based on multiple chaotic mapping," *Saudi J. Biol. Sci.*, vol. 24, no. 8, pp. 1821–1827, 2017.
- [55] Y. Ye, N. Wu, X. Zhang, L. Dong, and F. Zhou, "An optimized design for compact masked AES S-box based on composite field and common subexpression elimination algorithm," *J. Circuits, Syst. Comput.*, vol. 27, no. 11, 2018, Art. no. 1850171.
- [56] 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.
- [57] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1993.
- [58] C. K. Huang and H.-H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Opt. Commun.*, vol. 282, pp. 2123–2127, Jun. 2009.
- [59] C. K. Huang, C.-W. Liao, S. L. Hsu, and Y. C. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system," *Telecommun. Syst.*, vol. 52, no. 2, pp. 563–571, 2013.

• • •