



OPEN

## Multilevel information fusion for cryptographic substitution box construction based on inevitable random noise in medical imaging

Muhammad Fahad Khan<sup>1,2✉</sup>, Khalid Saleem<sup>1</sup>, Mohammed Ali Alshara<sup>3</sup> & Shariq Bashir<sup>4</sup>

Block cipher has been a standout amongst the most reliable option by which data security is accomplished. Block cipher strength against various attacks relies on substitution boxes. In literature, extensively algebraic structures, and chaotic systems-based techniques are available to design the cryptographic substitution boxes. Although, algebraic and chaotic systems-based approaches have favorable characteristics for the design of substitution boxes, but on the other side researchers have also pointed weaknesses in these approaches. First-time multilevel information fusion is introduced to construct the substitution boxes, having four layers; Multi Sources, Multi Features, Nonlinear Multi Features Whitening and Substitution Boxes Construction. Our proposed design does not hold the weakness of algebraic structures and chaotic systems because our novel s-box construction relies on the strength of true random numbers. In our proposed method true random numbers are generated from the inevitable random noise of medical imaging. The proposed design passes all the substitution box security evaluation criteria including Nonlinearity, Bit Independence Criterion (BIC), Strict Avalanche Criterion (SAC), Differential Approximation Probability (DP), Linear Approximation Probability (LP), and statistical tests, including resistance to Differential Attack, Correlation Analysis, 2D, 3D histogram analysis. The outcomes of the evaluation criteria validate that the proposed substitution boxes are effective for block ciphers; furthermore, the proposed substitution boxes attain better cryptographic strength as compared to very recent state-of-the-art techniques.

Information security is the protection of information and information systems from unauthorized access and manipulation. Block cipher has been a standout amongst the most reliable options by which data security is accomplished<sup>1,2</sup>. Block ciphers are deterministic cryptographic algorithms that operate on a plaintext block of  $n$  bits, to produce a block of cipher text of  $m$  bits. Here  $n$  and  $m$  length are not necessarily to same. Block cipher contains repeating rounds of key mixing, permutation and substitution layers, which make it difficult for cryptanalysis or attacks. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are the most famous examples of block cipher. For block ciphers such as AES and DES, linear and differential cryptanalysis attacks are considered as powerful attacks. These cryptanalysis attacks are based on probabilistic characteristics of cipher parameters and output. Such an attack identifies the strength of the encryption algorithm by exponentially growing the number of rounds. For example, a differential attack examines how the differences in input reflect as differences in output. The ultimate goal of the attacker is to find the non-random behavior of the output which helps the attacker to attack the algorithm. For this purpose, attacker tries to put specific set of inputs to trace the differences in the output of every round. In linear cryptanalysis, the attacker tries to learn the probabilistic linear relations between the parity bits of plaintext, cipher text, and the key, by running the cipher several times<sup>3,4</sup>. Responsibility to make the correlation between cipher text and the key, as undetectable as possible, is on Substitution box (S-box). An S-box is an  $m \times n$  mapping  $S: \{0, 1\}^m \rightarrow \{0, 1\}^n$ , transforming input vector  $x = [x_{n-1}, x_{n-2}, x_{n-3} \dots x_0]$  into output vector  $y = [y_{n-1}, y_{n-2}, y_{n-3} \dots y_0]$ .

The noise of medical imaging which captured from multi sensors, multi-sources is an inevitable random phenomenon caused by the numerous intrinsic and inevitable switching factors including sensors temperature,

<sup>1</sup>Department of Computer Sciences, Quaid-i-Azam University, Islamabad, Pakistan. <sup>2</sup>Department of Software Engineering, Foundation University Islamabad, Islamabad, Pakistan. <sup>3</sup>Department of Information Technology, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia. <sup>4</sup>DMPs Computer Science Section, The College of Arts and Sciences, University of Nizwa, Nizwa, Sultanate of Oman. ✉email: mfkhan@cs.qau.edu.pk

spectral density, trap state, mobility fluctuation, charge trapping, free carriers, thermal motion of the ions, pulse sequence, field strength, charged particles scattering, optical density fluctuation and so on. Correlation and distribution of noise values captured from a single sensor, a single source of medical images is noticeably different from noise values that are captured from the multi-sensors, multi-sources. Noise captured from a single sensor and a single source has cohesiveness, more patterns, less uniform distribution compare to noise captured from the multi-sensors, multi-sources.

Remaining paper is organized as follows; "**Contribution**" section presents our core contribution; "**Weaknesses in existing S-box designs**" section describes weaknesses in existing s-box designs. "**Proposed information fusion design**" section explains the proposed multilevel information fusion for the construction of S-boxes. "**Results and evaluation: S-box analysis**" section presents the results and its evaluation; "**Conclusion**" section gives the concluding remarks.

**Contribution.** The main contribution of this research is summarized in the following:

1. First-time multilevel information fusion is introduced to construct the cryptographic substitution boxes.
2. Extraction of true random numbers from the inevitable random noise of medical imaging, to synthesize the multi-level information fusion, for the construction of substitution boxes.
3. We introduce a novel nonlinear multi features whitening technique.
4. The proposed design passes all substitution box security evaluation criteria including Nonlinearity, Bit Independence Criterion (BIC), Strict Avalanche Criterion (SAC), Differential Approximation Probability(DP), Linear Approximation Probability(LP), and Statistical tests including resistance to Differential Attack, Correlation Analysis, 2D,3D histogram analysis.
5. The substitution-boxes constructed from our proposed design does not bear weaknesses of algebraic structures and chaotic systems.

**Weaknesses in existing S-box designs.** In literature, extensively algebraic structures and chaotic systems-based methods are available for designing the S-boxes. Although algebraic and chaotic systems base approaches provide favourable characteristics for the S-box design, but researchers have also pointed weaknesses in these approaches. S-box designs of pure algebraic structures are jeopardized due to the intrinsic algebraic structure. Various algebraic attacks are available for algebraic construction of S-boxes including linear and differential attacks<sup>3–17</sup>, interpolation attacks<sup>18–21</sup>, Gröbner basis attack<sup>22–28</sup>, side-channel attacks<sup>29–37</sup>, SAT solver<sup>38–45</sup>, XSL attack<sup>46–55</sup>, XL attacks<sup>56–60</sup>.

Similarly, chaotic systems widely adopted in the designs of substitution boxes<sup>61–74</sup>. But due to the inherent algorithmic evolution of control parameters and periodic nature of chaotic maps, many weaknesses also exist in the literature, including discontinuity in chaotic sequences<sup>1,67,75–78</sup>, non-uniform distribution of chaotic sequences<sup>1,75,76,79,80</sup>, predictability<sup>66,81–91</sup>, finite precision effect<sup>1,75,78,92,93</sup>, dynamical degradation of chaotic systems<sup>61,78,92–94</sup>, small number of control parameters<sup>79,82,83,95</sup>, frail chaos<sup>67,94</sup>, short quantity of randomness<sup>1,11,67,75–77,79,80,84,92,93,96–99</sup>. Inherent intrinsic evolution of algebraic structures and its automorphism nature is an essential problem. Alternatively, researchers endorse the true random sequences for cryptography due to the fact that these sequences rely on the strength of naturally occurring processes to generate the true randomness<sup>100–107</sup>. True random sequences are irreversible, unpredictable, and unreproducible, even if their internal structure and response history are known to adversaries.

The objective of this research is extraction of true random numbers from the inevitable random noise of medical imaging, to synthesize the multi-level information fusion, for the construct of cryptographically strong substitution boxes.

### Proposed information fusion design

The proposed design of multilevel information fusion for substitution boxes construction have four layers Multi Sources, Multi Features, Nonlinear Multi Features Whitening and Substitution Boxes Construction. The whole design is thoroughly explained in the following layers and depicted in Fig. 1.

**Multi sources (L0: DAI-DAO).** This layer takes multiple medical imaging objects as input and gives raw objects to layer 1. One hundred medical imaging objects of random sources and random organs are taken from the UACI, Kaggle, SpineWeb, softnetaMedDream, OASIS, TCIA repositories.

**Multi features (L1: DAI-FEO).** Noise is an inevitable random phenomenon caused by the numerous intrinsic and inevitable switching factors including sensors temperature, spectral density, trap state, mobility fluctuation, charge trapping, free carriers, thermal motion of the ions, pulse sequence, field strength, charged particles scattering, optical density fluctuation and so on. In this layer primary four types of noise features are extracted from the raw objects of layer 1. First type is Thermal noise which is an inevitable energy equilibrium fluctuation phenomenon caused by the thermal agitation of electrons in resistances. Thermal noise always presents in medical imaging sensors and devices pre-eminently in multimodality imaging. The spectrum of thermal noise is flat over a wide range of frequencies. Features of the thermal noise extracted using<sup>108,109</sup>. Second is shot noise which is caused by the fact that current flowing across a junction isn't smooth but is comprised of individual electrons arriving at random times. This non-uniform flow gives rise to broadband white noise that gets worse with increasing average. Features of the shot noise extracted using<sup>106</sup>. Third is speckle noise, which is a multiplicative noise that accompanies all coherent imaging modalities, in which images are produced by inter-

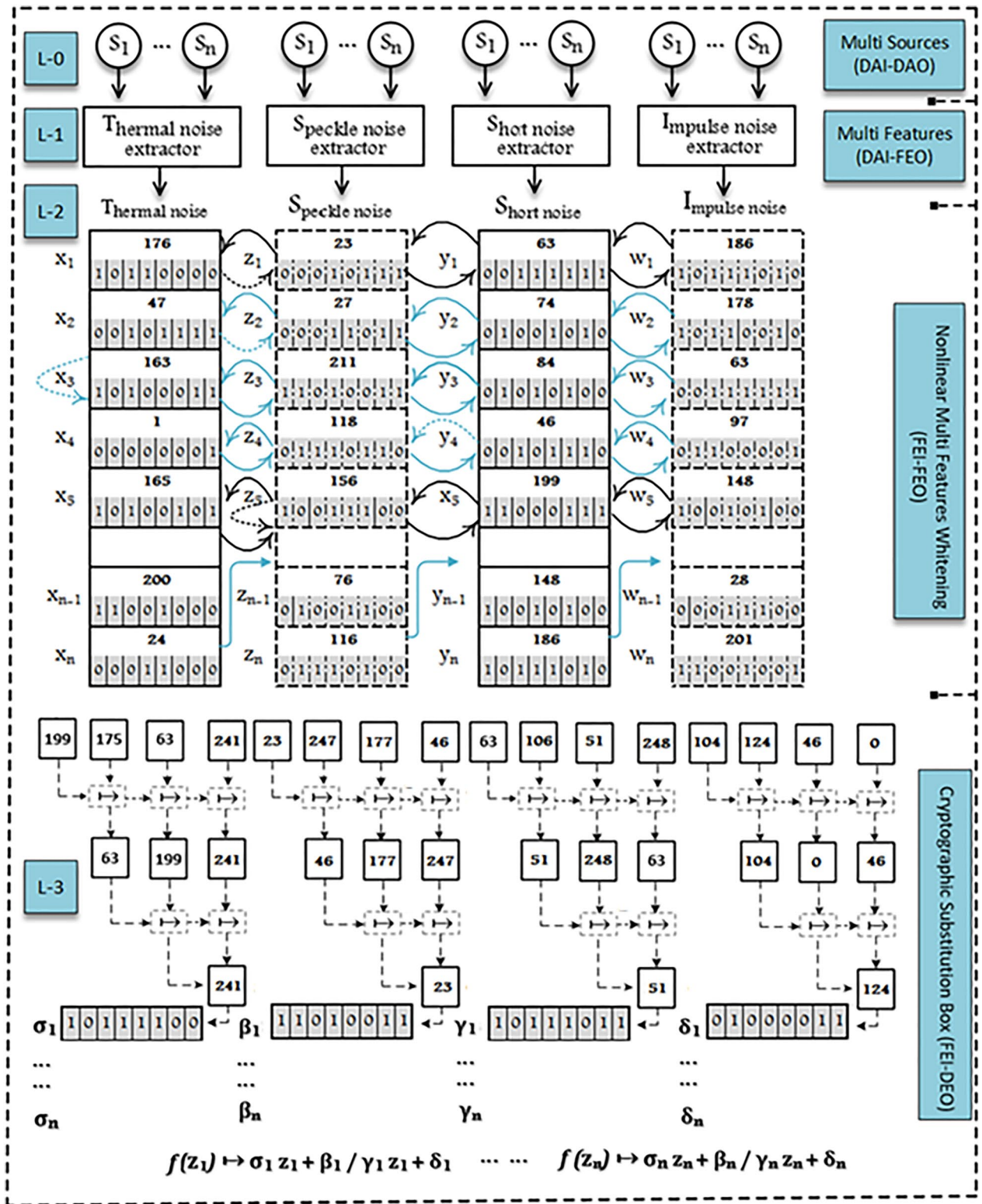


Figure 1. Multilevel information fusion for substitution boxes construction.

fering echoes of a transmitted waveform and backscattered reflection. Forth is impulse noise, which is the most common noise that exists in medical modalities. Normally, impulse noise generated during the image acquisition, storage and transmission. In impulse noise some of the pixels are replaced by outliers while the rest remain unchanged. This layer gives features of these four noises to layer 2. Features of the speckle noise and impulse noise extracted using<sup>88,110–112</sup> respectively.

NIST tests	Noise features			
	Thermal	Speckle	Shot	Impulse
Frequency (Monobit) Test	Pass	Fail	Fail	Fail
Frequency Test within a Block	Fail	Fail	Fail	Fail
Runs Test	Fail	Fail	Fail	Pass
Longest Run of Ones in a Block	Fail	Pass	Fail	Fail
Binary Matrix Rank Test	Pass	Pass	Fail	Pass
Discrete Fourier Transform Test	Fail	Fail	Fail	Fail
Non-overlapping Template Matching Test	Fail	Pass	Fail	Fail
Overlapping Template Matching Test	Fail	Pass	Pass	Fail
Maurer's Universal Statistical Test	Pass	Fail	Pass	Pass
Linear Complexity Test	Pass	Pass	Pass	Pass
Serial Test	Pass	Pass	Pass	Pass
Approximate Entropy Test	Fail	Fail	Fail	Fail
Cumulative Sums Test	Pass	Pass	Pass	Pass

**Table 1.** Noise features of medical imaging objects.

**Nonlinear multi features whitening (L2: FEI-FEO).** Inherently various characteristics of the true randomness are existing in the noise features of medical imaging, which captured from multi sensors, multi-sources but these characteristics are unable to pass each NIST statistical randomness tests. In Table 1, we can see that various NIST randomness criteria failed, thus requiring a technique that is able to decrease the correlation, cohesiveness, and periodicity among multi-features, creating a highly random output that appears independent from multi-sources and uniformly distributed. To adhere to these requirements, we propose a technique called the “Nonlinear Multi Features Whitening”, which takes Multi features of the noise as input and returns uniformly distributed output that has no cohesiveness and calculable periodicity. The output of the proposed scheme has good statistical properties, including the elimination of statistical autocorrelation among multi-features. Thus, making the suggested multi-features fusion technique suitable for symmetric encryption.

The nonlinear multi features whitening design has two basic transformations: horizontal permutation and vertical permutation. This layer takes multi noise features including thermal, speckle, shot and impulse from the layer-1 and returns highly random output that appears independent from the input features. This layer also decreases the correlation, cohesiveness, and periodicity among the input features. The whole design of nonlinear multi features whitening thoroughly explained in the following steps and depicted in L2 of the Fig. 1.

#### Horizontal permutation.

*Step 1:* Convert Thermal noise ( $T_{nf}$ ), Speckle noise ( $Sp_{nf}$ ), Shot ( $Sh_{nf}$ ), Impulse noise ( $I_{nf}$ ) values into their respective binary representation. Where vector  $x$  holds  $T_{nf}$  binaries, vector  $z$  holds  $Sp_{nf}$  binaries, vector  $y$  holds  $Sh_{nf}$  binaries and  $w$  holds  $I_{nf}$  binaries.

*Step 2:* Select the LSB of the  $x_i$  and check if the selected bit is ‘0’ then execute step-3 to step-8 and if the selected bit is ‘1’ then execute step-9 to step-14. A visual representation of the vector  $x, y$  pair and vector  $z, w$  pair are depicted in Fig. 2.

*Step 3:* If the frequency of 0's in leftmost 6 bits of  $x_i$  are greater than frequency of 0's in leftmost 6 bits of  $y_i$  then permute twice the  $x_i, z_i, y_i, w_i$  from left to right respectively.

*Step 4:* If the frequency of 0's in leftmost 6 bits of  $x_i$  are less than frequency of 0's in leftmost 6 bits of  $y_i$  then permute twice the  $y_i, w_i, x_i, z_i$  from right to left respectively.

*Step 5:* If the frequency of 0's in leftmost 6 bits of  $x_i$  and leftmost 6 bits of  $y_i$  are the same then execute step-6 or step-7, accordingly.

*Step 6:* If the frequency of 0's in leftmost 6 bits of  $z_i$  are greater than frequency of 0's in leftmost 6 bits of  $w_i$  then permute twice the  $z_i, y_i, w_i, x_i$  from left to right respectively.

*Step 7:* If the frequency of 0's in leftmost 6 bits of  $z_i$  are less than frequency of 0's in leftmost 6 bits of  $w_i$  then permute twice the  $w_i, y_i, z_i, x_i$  from right to left respectively.

*Step 8:* If the frequency of 0's in leftmost 6 bits of  $z_i$  and leftmost 6 bits of  $w_i$  are same then discard the  $x_i, z_i, y_i, w_i$ .

*Step 9:* If the frequency of 1's in leftmost 6 bits of  $x_i$  are greater than frequency of 1's in leftmost 6 bits of  $y_i$  then permute twice the  $x_i, z_i, y_i, w_i$  from left to right, respectively.

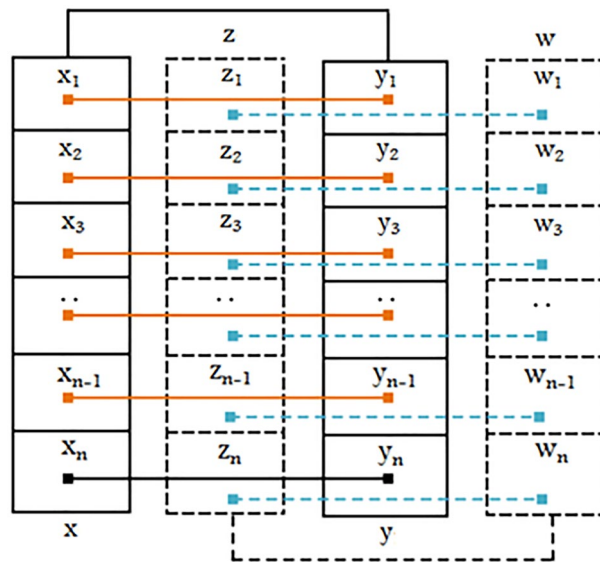
*Step 10:* If the frequency of 1's in leftmost 6 bits of  $x_i$  are less than frequency of 1's in leftmost 6 bits of  $y_i$  then permute twice the  $y_i, w_i, x_i, z_i$  from right to left respectively.

*Step 11:* If the frequency of 1's in leftmost 6 bits of  $x_i$  and leftmost 6 bits of  $y_i$  are the same then execute step-12 or step-13 accordingly.

*Step 12:* If the frequency of 1's in leftmost 6 bits of  $z_i$  are greater than frequency of 1's in leftmost 6 bits of  $w_i$  then permute twice the  $z_i, y_i, w_i, x_i$  from left to right respectively.

*Step 13:* If the frequency of 1's in leftmost 6 bits of  $z_i$  are less than frequency of 1's in leftmost 6 bits of  $w_i$  then permute twice the  $w_i, y_i, z_i, x_i$  from right to left respectively.





**Figure 2.** Pairs of vectors  $x, y$  and vector  $z, w$ .

*Step 14:* If the frequency of 1's in leftmost 6 bits of  $z_i$  and leftmost 6 bits of  $w_i$  are also same then discard the  $x_i, z_i, y_i, w_i$ .

*Vertical permutation.*

*Step 1:* Assign fused octet values according to the following:

1st bit  $\leftarrow$  2nd bit of  $z_i$   
 2nd bit  $\leftarrow$  1st bit of  $z_{i+1}$   
 3rd bit  $\leftarrow$  3rd bit of  $z_{i-1}$   
 4th bit  $\leftarrow$  4th bit of  $w_{i+1}$   
 5th bit  $\leftarrow$  5th bit of  $w_{i-1}$   
 6th bit  $\leftarrow$  6th bit of  $y_{i+1}$   
 7th bit  $\leftarrow$  7th bit of  $y_{i-1}$   
 8th bit  $\leftarrow$  8th bit of  $y_i$

A visual representation of vertical permutation depicted in Fig. 3.

*Step 2:* For variable 'K': Parse left-most 6 bits of the fused byte into corresponding decimal value.

*Step 3:* If 1st bit of the fused octet is '0' then K times cyclically permute the  $column_x$  in the top to bottom manner.

*Step 4:* If 1st bit of the fused octet is '1' then K times cyclically permute the  $column_y$  in the bottom to top manner.

*Step 5:* If 2nd bit of the fused octet is '0' then K times cyclically permute the  $column_z$  in the top to bottom manner.

*Step 6:* If 2nd bit of the fused octet is '1' then K times cyclically permute the  $column_w$  in the bottom to top manner.

**Substitution boxes construction (L3: FEI-DEO).** This layer takes highly correlated true random numbers from the L2 and generates substitution boxes. The complete design of this layer is thoroughly described in the following steps:

*Step 1:* Traverse each value of  $column_x, column_y, column_z,$  and  $column_w$ , row by row and then concatenate the subsequent rows in a one dimensional vector. A visual representation of steps 2 to 11 is depicted in Fig. 4.

*Step 2:* Split one-dimensional vector into blocks of 6 bytes. If the length of last block is less than 6 then exclude last block.

*Step 3:* Convert each block of step-2 into binary representation and then split into blocks of 3 bits.

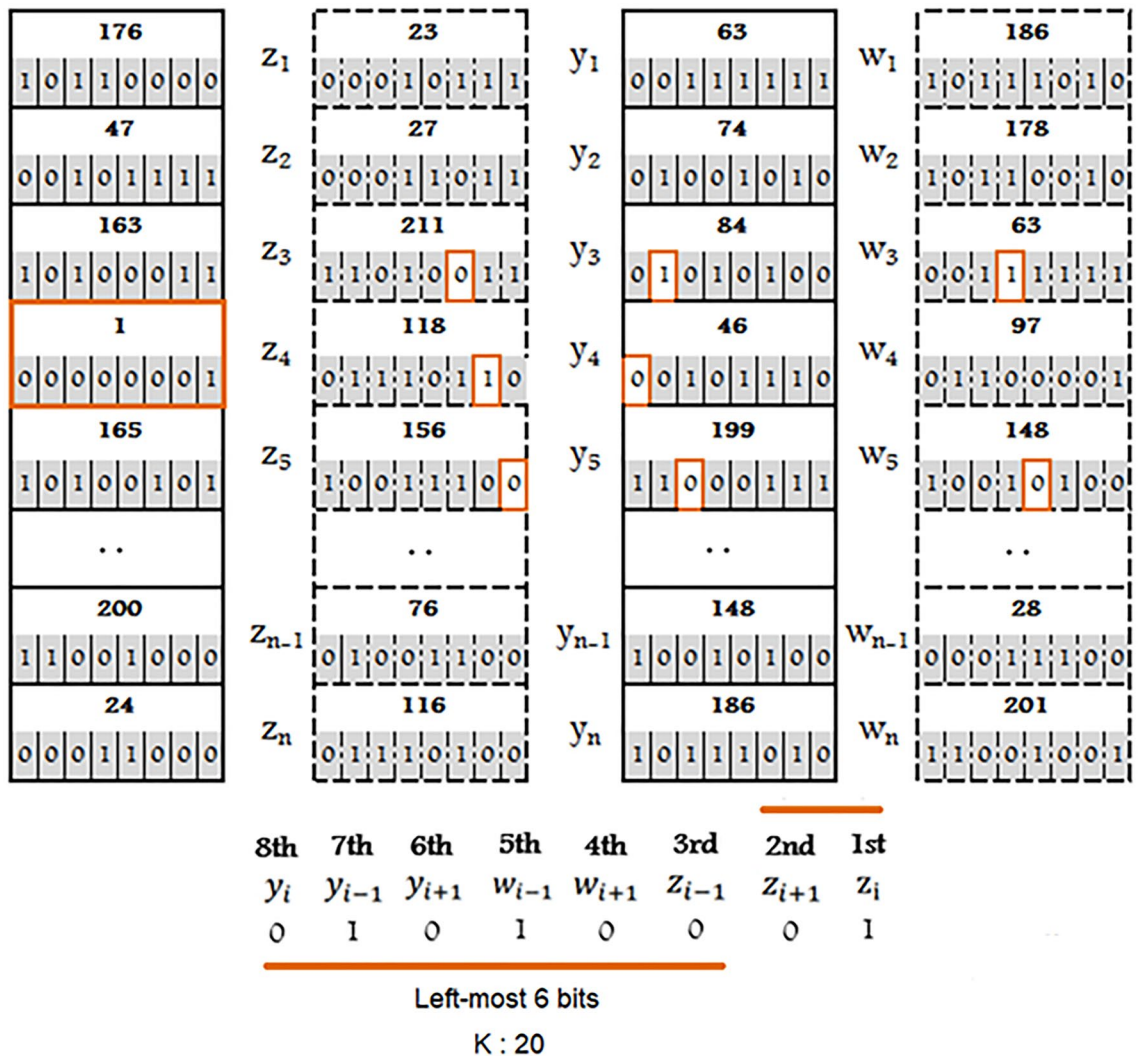
*Step 4:* Get frequency of 0's in every block which are obtained from step-3.

*Step 5:* Consider the block-0 to block-3 values of step-4 as the 1st row of matrix  $Map^1$ .

*Step 6:* Consider the block-4 to block-7 values of step-4 as the 2nd row of matrix  $Map^1$ .

*Step 7:* Consider the block-8 to block-11 values of step-4 as the 3rd row of matrix  $Map^1$ .

*Step 8:* Consider the block-12 to block-15 values of step-4 as the 4th row of matrix  $Map^1$ .



**Figure 3.** Vertical permutation.

*Step 9:* To create the matrix  $Map^2$ : Traverse  $Map^1$  in the Z-order format. Consider quadrant NW as a 1st column, quadrant NE as a 3rd column, quadrant SW as 2nd column and quadrant SE as a 4th column of  $Map^2$ .  
*Step 10:* Traverse first 4 unique values of  $Map^2$  from row-major order.  
*Step 11:* Sublevel-1 indexes assignment: Consider the values of step-10 as indexes of the first-4 unique elements which are obtained from step-2. A visual representation of the steps 12 to 14 is shown in the sublevel-1 of Fig. 5.  
*Step 12:* To Get 1st  $right_{index}$ : Use each index of the left most block to select a row of  $Map^1$  and the second left-most index of a block to select a column of  $Map^1$ .  
*Step 13:* To Get 2nd  $right_{index}$ : For first parameter, take index from step-12 and for second parameter, take the index of third left-most element which gained from step-11. Use first and second parameters to select a row and column of  $Map^1$ .  
*Step 14:* To Get 3rd  $right_{index}$ : For first parameter, take index from step-13 and for second parameter, take the index of fourth left-most element which gained from step-11. Use first and second parameters to select a row and column of  $Map^1$ .  
*Step 15:* Get 1st permuted element of sublevel-2: To obtain index, execute the step-12 over  $Map^2$ , except  $Map^1$ , and get permuted element through the retrieved index. A visual representation of the steps 15 to 19 is shown in the sublevel-2 of Fig. 5.  
*Step 16:* Get 2nd permuted element of sublevel-2: To obtain index, execute the step-13 over  $Map^2$ , except  $Map^1$ , and get permuted element through the retrieved index.  
*Step 17:* Get 3rd permuted element of sublevel-2: To obtain index, execute the step-14 over  $Map^2$ , except  $Map^1$ , and get permuted element through the retrieved index.  
*Step 18:* To Get 4th  $right_{index}$ : For first parameter, take the index of output of the step-15 and for second parameter, take the index of output of the step-16. Use first and second parameter to select a row and column of  $Map^1$ .

**Blocks of 6 bytes**

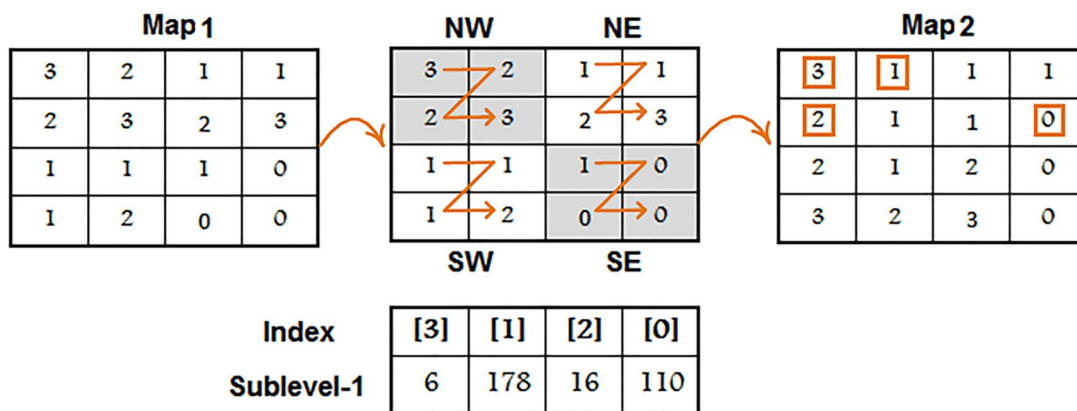
<b>6</b>	<b>178</b>	<b>16</b>	<b>110</b>	<b>253</b>	<b>63</b>	<b>n</b>
000001101011001000010000011011101111110100111111						

**Blocks of 3 bits**

000001101011001000010000011011101111110100111111																												<b>n</b>
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----------

**Frequency of 0's**

3	2	1	1	2	3	2	3	1	1	1	0	1	2	0	0	<b>n</b>
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	----------



**Figure 4.** Visual representation of steps 2 to 11.

*Step 19:* To Get 5th  $right_{index}$ : For first parameter, take the index of output of the step-18. For second parameter, take the index of output of the step-17. Use first and second parameters to select a row and column of Map<sup>1</sup>.  
*Step 20:* Get 1st permuted element of sublevel-3: To obtain index, execute the step-14 over Map<sup>2</sup>, except Map<sup>1</sup>, by passing resultant values of step-18 and step-19 as parameters. Fetch permuted element through the retrieved index.  
*Step 21:* To Get 6th  $right_{index}$ : Take index of the 1st permuted element of sublevel-3  
*Step 22:* To acquire arbitrary bits of permuted elements: Obtain indexes from step-12 to step-14, step-18 to step-19, and step-21. Acquire the respective bits of permuted elements from these indexes.  
*Step 23:* Get a most significant bit and least significant bit from the permuted element of step-15.  
*Step 24:* Subsequently, generate  $\sigma_i, \beta_i, \gamma_i, \delta_i$ : Concatenate the bits of step-22 and step-23 thus parse these bits into their particular decimal value.  
*Step 25:* Put values of  $\sigma_i, \beta_i, \gamma_i, \delta_i$  in linear fraction transform  $f(z_i) \mapsto (\sigma_i z_i + \beta_i) / (\gamma_i z_i + \delta_i)$  where  $\gamma_i z_i = -\delta_i$  and  $\sigma_i \delta_i - \beta_i \gamma_i \neq 0$ . Remove repeating elements from the  $f(z_i)$  block of 256 size and transformed elements in a s-box of size  $8 \times 8$ .

**Results and evaluation: S-box analysis**

This section covers the results and evaluation of the results. The resultant S-boxes evaluated through the standard S-box evaluation criteria<sup>65,69,74,113-124</sup> including Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), Linear Approximation Probability(LP), Differential Approximation Probability(DP), Nonlinearity, and through the statistical tests including resistance to Differential Attack, Correlation Analysis, 2D, 3D histogram analysis. From the proposed design the total number of 4562 S-boxes constructed, where the nonlinearity of 821 S-boxes are less-than 109, the nonlinearity of 3728 S-boxes are equal to 110 and the nonlinearity of 13 S-boxes is equal to 112. Two S-boxes picked randomly from the resultant S-boxes as samples and shown in the Table 2a, b. The nonlinearity of S-boxes which are shown in Table 2a, b are 110 and 112 respectively.

**Nonlinearity.** The nonlinearity is the ability of substitution box that provides immunity from the linear cryptanalysis and it is exhibited by the nonlinearity score<sup>1,128,129,142,145,154,155,158-175</sup>. The nonlinearity of a substitution box  $h(x)$  described as the Walsh spectrum (WS):

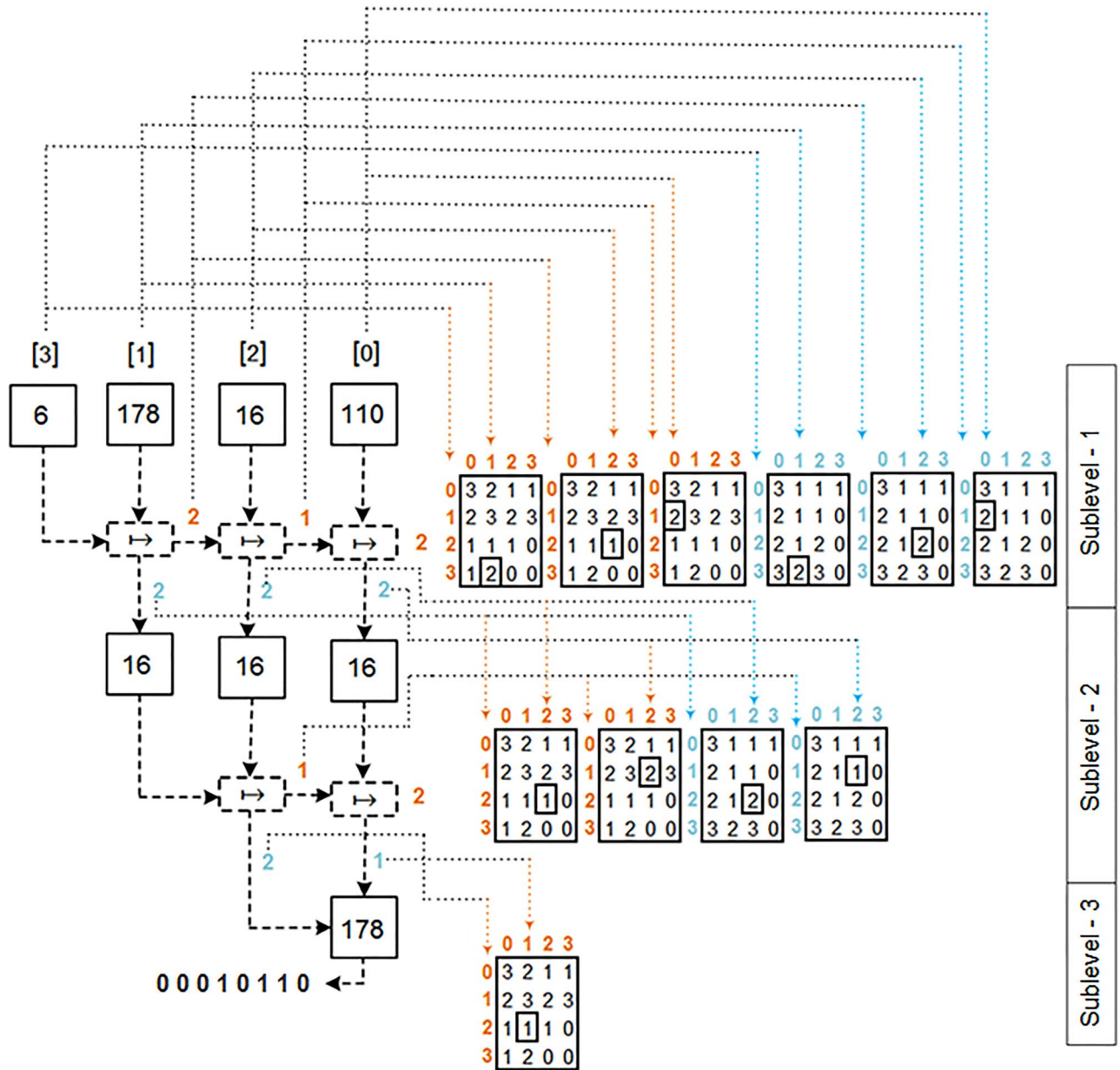


Figure 5. Visual representation of steps 15 to 19.

$$N_h = 2^{m-1} \left( 1 - 2^{-m} \max_w |S_{(g)}(w)| \right) \tag{1}$$

The WS,  $h(x)$  defined as:

$$S_{(h)}(x) = \sum_{x \in GF(2^n)} (-1)^{h(x) \oplus x \cdot X} \tag{2}$$

where  $x \in GF(2^n)$  and  $x \cdot X$  is the dot product of  $x$  and  $X$ , which is defined as:

$$x \cdot X = x_1 \oplus X_1 + x_2 \oplus X_2 + \dots + x_n \oplus X_n \tag{3}$$

The nonlinearity score of substitution box-1 and substitution box-2 is 110 and 112 respectively. We observed that the Nonlinearity score of both these S-boxes are better than to the thirty state-of-the-art (2018 to 2020 year) S-boxes, mentioned in Table 3.

**Bit independence criterion (BIC).** One of the desirable characteristic of substitution box is bit independence criterion. BIC property is defined as all the avalanche variables should be pair-wise independent for a given



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

**Table 2.** (a) Substitution box 1. (b) Substitution box 2.

Substitution box	Max. nonlinearity	Substitution box	Max. nonlinearity
Özkaynak <sup>130</sup> , 2020	104	Azam <sup>143</sup> , 2019	108
El-Latif <sup>131</sup> , 2020	104	Özkaynak <sup>120</sup> , 2019	108
Zahir <sup>132</sup> , 2020	104	Hussam <sup>144</sup> , 2019	108
El-Latif <sup>133</sup> , 2020	106	Amjad <sup>157</sup> , 2019	108
Artuğer <sup>134</sup> , 2020	107	Özkaynak <sup>146</sup> , 2018	106
D. Lambic <sup>135</sup> , 2020	108	Tian <sup>102</sup> , 2018	106
H. Liu <sup>136</sup> , 2020	108	Silva <sup>74</sup> , 2018	106
Zhang <sup>137</sup> , 2020	108	Attaullah <sup>146</sup> , 2018	107
Cassal <sup>138</sup> , 2020	108	Alzaidi <sup>147</sup> , 2018	107
Bin <sup>139</sup> , 2020	104	Alzaidi <sup>148</sup> , 2018	107
KM <sup>124</sup> , 2019	106	Solami <sup>149</sup> , 2018	108
Tanyildizi <sup>140</sup> , 2019	106	Hayat <sup>150</sup> , 2018	108
Açikkapi <sup>141</sup> , 2019	106	Wang <sup>151</sup> , 2018	108
Özkaynak <sup>72</sup> , 2019	107	Liu <sup>152</sup> , 2018	108
Zahid <sup>156</sup> , 2019	108	Zhimao <sup>153</sup> , 2018	108

**Table 3.** Nonlinearity of the state-of-the-art S-boxes.

a							
–	0.507812	0.460938	0.503906	0.503906	0.513672	0.500000	0.482422
0.507812	–	0.476562	0.480469	0.482422	0.503906	0.511719	0.513672
0.460938	0.476562	–	0.474609	0.462891	0.513672	0.525391	0.535156
0.503906	0.480469	0.474609	–	0.509766	0.525391	0.507812	0.496094
0.503906	0.482422	0.462891	0.509766	–	0.503906	0.498047	0.517578
0.513672	0.503906	0.513672	0.525391	0.503906	–	0.490234	0.462891
0.500000	0.511719	0.525391	0.507812	0.498047	0.490234	–	0.482422
0.482422	0.513672	0.535156	0.496094	0.517578	0.462891	0.482422	–
b							
–	0.480469	0.492188	0.496094	0.492188	0.503906	0.519531	0.515625
0.480469	–	0.490234	0.482422	0.486328	0.484375	0.490234	0.505859
0.492188	0.490234	–	0.484375	0.519531	0.527344	0.515625	0.517578
0.496094	0.482422	0.484375	–	0.500000	0.488281	0.480469	0.521484
0.492188	0.486328	0.519531	0.500000	–	0.513672	0.478516	0.507812
0.503906	0.484375	0.527344	0.488281	0.513672	–	0.468750	0.470703
0.519531	0.490234	0.515625	0.480469	0.478516	0.468750	–	0.533203
0.515625	0.505859	0.517578	0.521484	0.507812	0.470703	0.533203	–

**Table 4.** (a) Bit independence criterion of the S-box1. (b) Bit independence criterion of the S-box2.

a							
0.500000	0.468750	0.531250	0.468750	0.468750	0.500000	0.500000	0.546875
0.484375	0.500000	0.515625	0.562500	0.531250	0.593750	0.562500	0.546875
0.531250	0.546875	0.500000	0.515625	0.500000	0.531250	0.515625	0.468750
0.437500	0.531250	0.515625	0.515625	0.453125	0.421875	0.500000	0.578125
0.546875	0.484375	0.500000	0.453125	0.531250	0.531250	0.578125	0.437500
0.468750	0.500000	0.531250	0.500000	0.390625	0.546875	0.468750	0.468750
0.453125	0.546875	0.500000	0.562500	0.453125	0.453125	0.546875	0.500000
0.515625	0.500000	0.546875	0.468750	0.500000	0.453125	0.437500	0.484375
b							
0.515625	0.515625	0.484375	0.515625	0.500000	0.453125	0.468750	0.484375
0.453125	0.453125	0.468750	0.515625	0.578125	0.562500	0.515625	0.531250
0.531250	0.531250	0.500000	0.453125	0.531250	0.468750	0.484375	0.531250
0.531250	0.453125	0.515625	0.484375	0.484375	0.500000	0.531250	0.515625
0.546875	0.500000	0.484375	0.468750	0.484375	0.562500	0.515625	0.500000
0.515625	0.531250	0.468750	0.546875	0.453125	0.500000	0.546875	0.500000
0.453125	0.515625	0.453125	0.468750	0.515625	0.515625	0.531250	0.484375
0.515625	0.437500	0.484375	0.515625	0.453125	0.500000	0.515625	0.484375

**Table 5.** (a) Strict Avalanche Criterion of the S-box1. (b) Strict Avalanche Criterion of the S-box2.

set of avalanche vectors, created by complementing of only one plaintext bit. Bit independent criterion is examined by altering every input bit from the plaintext<sup>1</sup>. Suppose Boolean functions are  $S_1, S_2, \dots, S_n$  and if two Boolean functions output bits,  $S_j$  and  $S_k$  satisfy BIC, the nonlinearity and SAC must be met by  $S_j \oplus S_k$  ( $j \neq k, 1 \leq j, k \leq n$ ). The average of BIC-SAC matrix of the S-box1 is 0.499 and the S-box2 is also 4.99, which is very close to 0.5. Result shows that our proposed S-boxes are competent enough to fulfil the bit independent criteria. BIC results of the S-box1 and S-box2 are presented in Table 4a, b, respectively.

**Strict avalanche criterion (SAC).** The confusion strength of the substitution box is examined through the strict avalanche criteria. SAC determines how many output bits changed when a single change is made in input<sup>1</sup>. It is defined as:  $f : F_2^n \rightarrow F_2$  satisfies if  $f(x) \oplus f(x \oplus \alpha)$  is balanced for  $\alpha = 1$ . Variance, Maximum, Minimum and Average SAC results of the S-box1 are 0.041869, 0.593750, 0.390625 and 0.503174, respectively. Variance, Maximum, Minimum and Average SAC results of the S-box2 are 0.032103, 0.578125, 0.437500 and 0.500488, respectively. The average SAC value of S-box1 and S-box2 dependency matrix are 0.503174 and 0.500488 which are exactly same to the ideal SAC. So, our proposed S-boxes satisfy the avalanche criteria. S-box1 and S-box2 results of the SAC are presented in Table 5a, b, respectively.

a															
0.00000	0.03125	0.02343	0.02343	0.03125	0.03125	0.02343	0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.03125	0.02343	0.03125
0.02343	0.02343	0.03125	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.03120	0.01562	0.02343	0.03906	0.03125	0.02343
0.03125	0.02343	0.03125	0.02343	0.02343	0.03125	0.03125	0.03125	0.02343	0.03125	0.02343	0.02343	0.03125	0.02343	0.03125	0.03125
0.02343	0.03906	0.02343	0.03125	0.02343	0.02343	0.01562	0.02343	0.02343	0.03125	0.02343	0.02343	0.03906	0.02343	0.03125	0.03125
0.02343	0.03125	0.03125	0.02343	0.02343	0.02343	0.03125	0.02343	0.03125	0.03125	0.03125	0.03125	0.02343	0.02343	0.02343	0.01562
0.02343	0.02343	0.02343	0.03125	0.03125	0.03125	0.02343	0.03125	0.02343	0.03125	0.03125	0.02343	0.02343	0.02343	0.02343	0.03125
0.03125	0.02343	0.02343	0.03125	0.03125	0.01562	0.03125	0.02343	0.02343	0.03906	0.02343	0.02343	0.03125	0.02343	0.03125	0.03125
0.03906	0.02343	0.02343	0.03125	0.03125	0.03125	0.03125	0.02343	0.03906	0.02343	0.03125	0.02343	0.02343	0.02343	0.02343	0.02343
0.03906	0.03125	0.02343	0.02343	0.01562	0.02343	0.03125	0.02343	0.03125	0.03125	0.03125	0.02343	0.02343	0.02343	0.03125	0.02343
0.02343	0.02343	0.02343	0.03125	0.03125	0.02343	0.02343	0.03125	0.03125	0.02343	0.03125	0.02343	0.03125	0.02343	0.03125	0.03125
0.03125	0.03125	0.02343	0.02343	0.02343	0.02343	0.03125	0.02343	0.03906	0.03125	0.04687	0.02343	0.02343	0.03125	0.02343	0.02343
0.02343	0.03125	0.03125	0.02343	0.03125	0.02343	0.02343	0.03125	0.02343	0.02343	0.03125	0.02343	0.03125	0.03125	0.03125	0.02343
0.03125	0.03125	0.03125	0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.02343	0.02343	0.03125	0.02343	0.03125	0.02343	0.03125
0.02343	0.02343	0.02343	0.02343	0.03125	0.02343	0.03125	0.02343	0.02343	0.02343	0.01562	0.03125	0.02343	0.01562	0.03125	0.02343
0.02343	0.03125	0.02343	0.02343	0.02343	0.03125	0.03125	0.03125	0.03125	0.03125	0.05468	0.02343	0.02343	0.03125	0.02343	0.02343
0.02343	0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.03125	0.02343	0.02343	0.02343	0.02343	0.03125	0.03906	0.02343	0.02343
b															
0.00000	0.02343	0.03906	0.02343	0.02343	0.02343	0.02343	0.03125	0.03125	0.02343	0.03125	0.02343	0.02343	0.02343	0.03125	0.02343
0.03125	0.02343	0.03125	0.03125	0.03125	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.02343	0.02343
0.02343	0.03125	0.02343	0.02343	0.02343	0.03125	0.03125	0.02343	0.02343	0.02343	0.02343	0.03125	0.03125	0.02343	0.02343	0.03125
0.02343	0.03125	0.03125	0.02343	0.02343	0.03906	0.02343	0.03125	0.03125	0.02343	0.02343	0.02343	0.03125	0.03125	0.02343	0.02343
0.02343	0.03125	0.02343	0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.02343	0.01562	0.03125	0.02343	0.02343	0.02343	0.03125
0.03125	0.02343	0.02343	0.02343	0.02343	0.03906	0.02343	0.02343	0.02343	0.03125	0.02343	0.03906	0.02343	0.03125	0.02343	0.02343
0.03125	0.03125	0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.03906	0.02343	0.03125	0.02343	0.02343	0.02343	0.03125	0.02343
0.02343	0.02343	0.03125	0.02343	0.03125	0.02343	0.02343	0.03125	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.03906	0.02343
0.03125	0.02343	0.03906	0.03906	0.03125	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.03125	0.03125	0.02343
0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.03125	0.03906	0.02343
0.03125	0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.02343	0.02343	0.02343	0.03906	0.02343	0.02343	0.02343	0.02343	0.02343
0.02343	0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.03125	0.02343	0.02343	0.02343	0.02343	0.02343	0.03125	0.03125	0.03125
0.02343	0.03125	0.02343	0.02343	0.03125	0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.03125	0.03125	0.02343	0.02343	0.02343
0.03125	0.02343	0.02343	0.02343	0.02343	0.03906	0.02343	0.02343	0.02343	0.02343	0.03125	0.02343	0.03125	0.03125	0.02343	0.03125
0.03125	0.03125	0.03125	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.02348	0.02343	0.02343	0.02343	0.02343
0.03125	0.03125	0.03125	0.03125	0.02343	0.02343	0.02343	0.02343	0.02343	0.02343	0.03125	0.02343	0.02343	0.03125	0.03906	0.03125

**Table 6.** (a) DP of the S-box1. (b) DP of the proposed S-box2.

**Linear approximation probability (LP).** The imbalance of an event among input and output bit is identified by LP<sup>79,80</sup>. LP is the biggest disparity of an event, in which parity of the output bits is equal to the parity of the input bits. Here parity of the input bits is selected by the mask  $\Omega x$  and parity of the output bits is selected by the mask  $\Omega y$ .<sup>56,74</sup>  $2^n$  is the number of elements and  $X$  is the set of all feasible inputs. Maximum LP of our S-box1 is 0.140625 and S-box2 is 0.1171875, which satisfy the LP criteria.

$$LP_f = \max_{\Omega x, \Omega y \neq 0} \left| \frac{\#\{x \in X | x \cdot \Omega x = S(x) \cdot \Omega y\}}{2^n} - \frac{1}{2} \right| \tag{4}$$

**Differential approximation probability (DP).** Differential uniformity of substitution box is measured through the differential approximation probability. For any change in the input either sequence or value, there has to be a change in the output. In DP, the input differential  $\Delta x_i$  should uniquely map to an output differential  $\Delta y_i$ , therefore ensuring a uniform mapping probability for each  $i$ . In Table 6a, b we can see that the results of our S-box1 and S-box2 fully fills the DP criteria, represented as follows<sup>1</sup>:

$$DP(\Delta x \rightarrow \Delta y) = \frac{\#\{x \in X | (S(x) \oplus S(x \oplus \Delta x)) = \Delta y\}}{2^n} \tag{5}$$

**Evaluation: statistical analysis.** *Resistance to differential attack.* Number of changing pixel rate (NPCR) and Unified Averaged Changed Intensity (UACI) are the performance indicators that have the ability to assess the resilience of cipher against differential attacks<sup>9,74</sup>. Mathematically they are defined in Eqs. (6) and (7).

Images	Location	NPCR	UACI
Baboon	Last	99.82	33.47
	Mid	99.83	33.43
	First	99.87	33.45
Cameraman	Last	99.85	33.49
	Mid	99.78	33.52
	First	99.84	33.55
Parrot	Last	99.85	33.42
	Mid	99.83	33.46
	First	99.81	33.45
Fruits	Last	99.91	33.58
	Mid	99.89	33.59
	First	99.82	33.51

**Table 7.** NPCR and UACI.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N \times M} \times 100\% \quad (6)$$

$$UACI = \frac{1}{N \times M} \times \left[ \sum_{i,j} \times \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\% \quad (7)$$

In Eq. (8)  $C_1(i,j)$  and  $C_2(i,j)$  are two encrypted images obtained from plaintext images that are slightly different. where  $N$  is the width,  $M$  is height of the encrypted image and  $D(i,j)$  is the difference function between encrypted images. Difference is given as:

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

To evaluate the impact of pixels change, in the plain images over the encrypted images various test images are evaluated through the NPCR and UACI measures. Experimental results of the NPCR and UACI for each channel (R, G, B) of baboon, cameraman, parrot and fruits are presented in Table 7. Constantly NPCR values of our results are close to 99.9 which is the perfect value. Similarly, all the values of UACI are greater than 33.5 which is also the perfect value.

**Histogram analysis.** Here histogram analysis is used to examine the resistance of encryption algorithm against the statistical attacks. It shows, how plain image pixels scatter after the encryption process and it indicates the frequency distribution of encrypted pixels. Ideal encryption technique reconstructs the plain image into encrypted image that bears the random pixel values and sequences. We examined the 2D and 3D histograms of various color images.

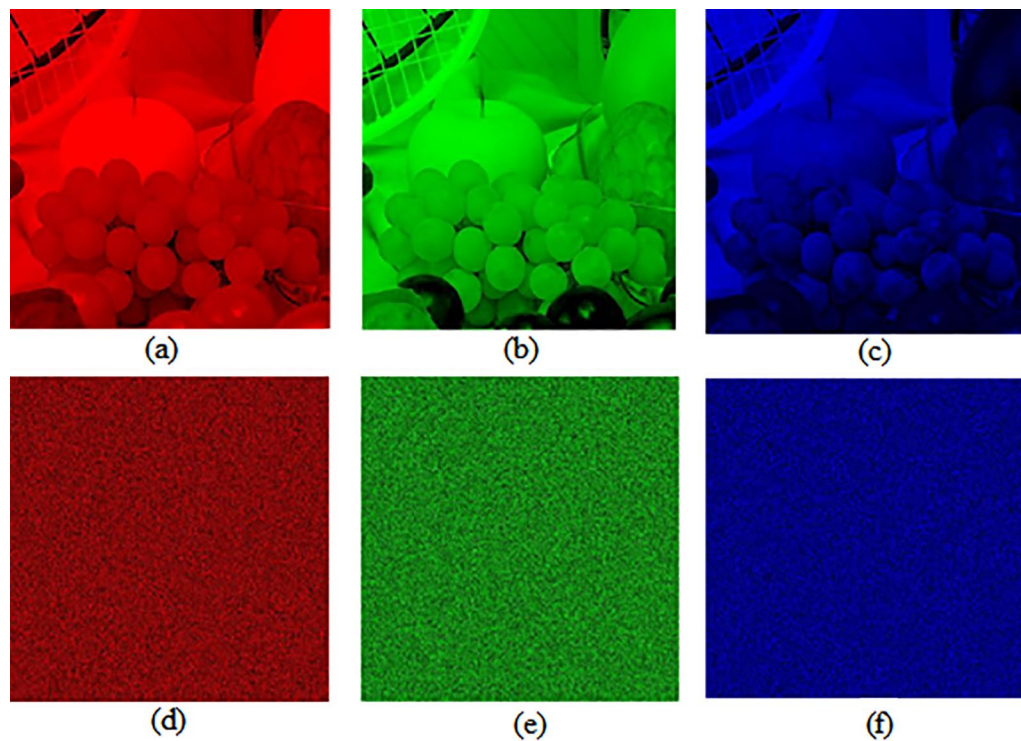
Test images of fruit and parrot with their corresponding encrypted images are shown in Figs. 6 and 7 respectively. Two-dimensional histogram of the plain test images (fruit Fig. 8g, parrot Fig. 9g) over RGB channels are shown in Figs. 8c–e and 9c–e and their corresponding encrypted images histograms are shown in Figs. 8h–j and 9h–j respectively. Histogram of the test images (Figs. 8a and 9a) and their corresponding encrypted images histograms are shown in Figs. 8b,f and 9b, f respectively.

Three-dimensional histogram of the plain test images (fruit, parrot) over RGB channels are shown in Figs. 10b–d and 11b–d and their corresponding encrypted images histograms are shown in Figs. 10f–h and 11f–h respectively. Histogram of the color plain test images (fruit, parrot) are shown in Figs. 10a and 11a and their corresponding encrypted images histograms are shown in Figs. 10e and 11e respectively.

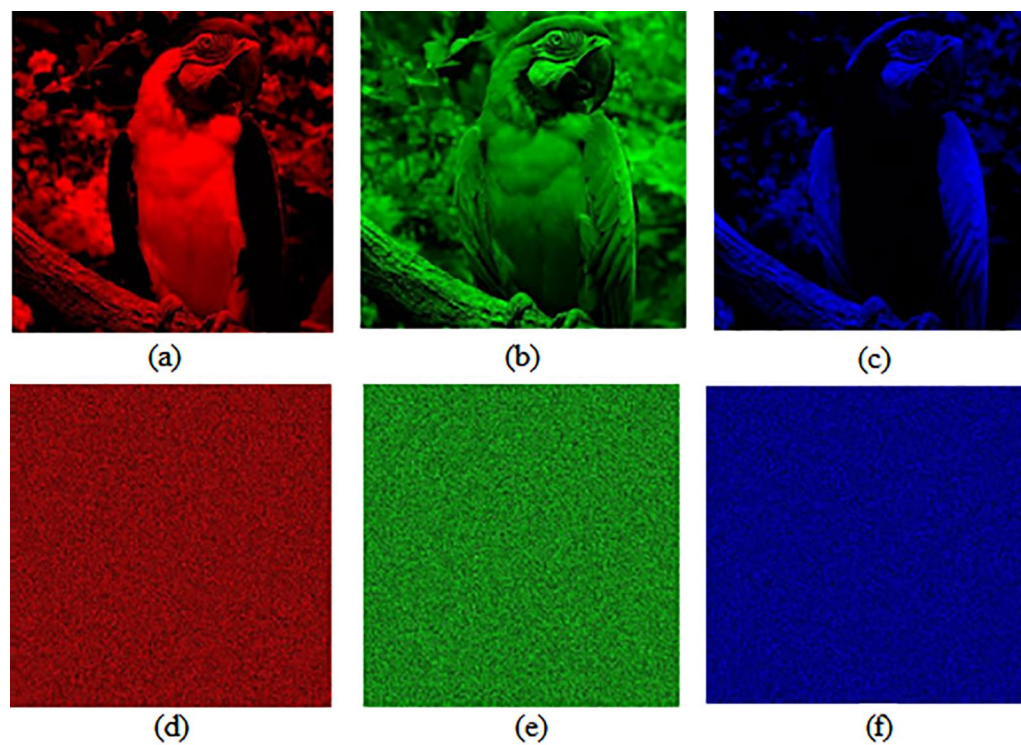
It is clearly visible that the proposed algorithm shows a uniform two dimensional and 3-dimensional histogram for encrypted image. The uniformity of random pixels indicates a good encryption and resist against several types of statistical attacks. So, histogram analysis fails to provide any clue about encrypted image.

**Correlation-coefficient analysis.** Adjacent pixels of the plain images are highly correlated, that provides significant visual traits to the attacker. Strong cipher should reduce the correlation of adjacent pixels. Adjacent pixel pairs in every direction of the sailboat image are plotted in Figs. 12, 13, and 14 From the plain images and from the encrypted images,  $10^3$  adjacent pixels are selected in the horizontal, vertical and diagonal directions to calculate their correlation coefficients by using Eqs. (9), (10), (11). The results of the Correlation-coefficient analysis for each channel (R, G, B) of Peppers, parrot, baboon, and sailboat are presented in Table 8. It is clear that the distribution of adjacent pixel pairs in every direction and in every channel (R, G, B) are entirely changed after the encryption. Correlation coefficients are calculated by the following formulas:

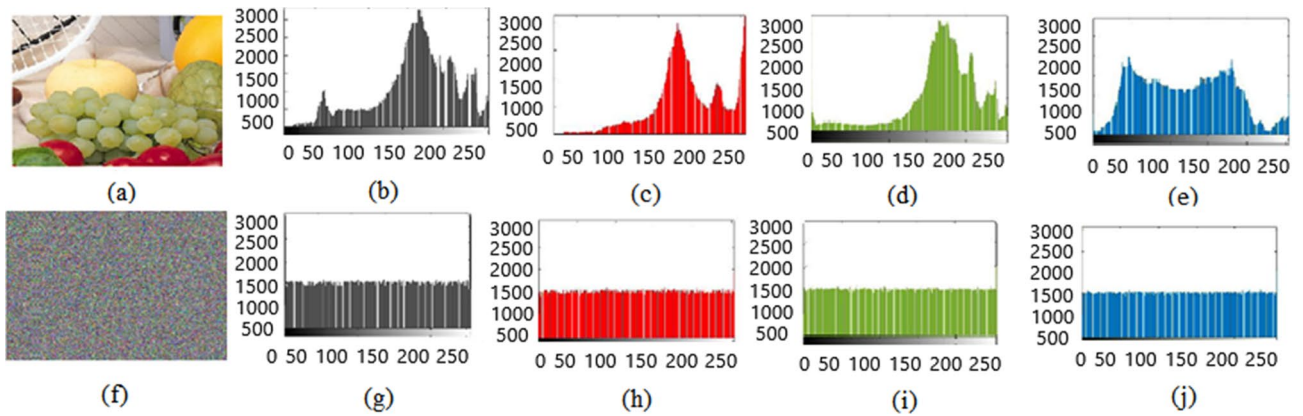




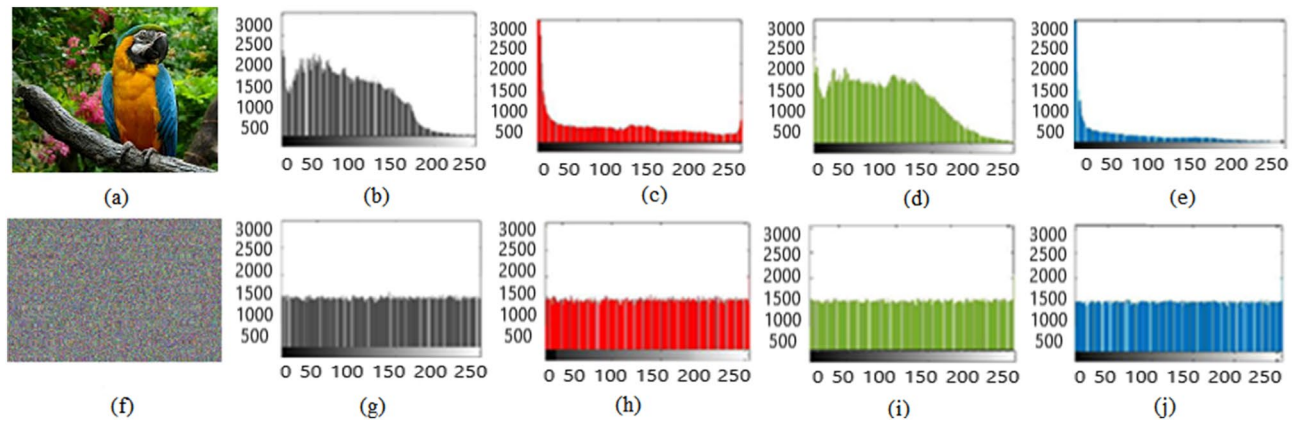
**Figure 6.** Plain and encrypted images of fruit. (a) R channel; (b) G channel; (c) B channel; (d) Encrypted R channel; (e) Encrypted G channel; (f) Encrypted B channel.



**Figure 7.** Plain and encrypted images of parrot. (a) R channel; (b) G channel; (c) B channel; (d) Encrypted R channel; (e) Encrypted G channel; (f) Encrypted B channel.



**Figure 8.** Plain and encrypted images of fruit. (a) Color image; (b) Histogram of color image; (c) Plain R channel; (d) Plain G channel; (e) Plain B channel; (f) Encrypted color image; (g) Histogram of encrypted image; (h) Encrypted R channel; (i) Encrypted G channel; (j) Encrypted B channel.



**Figure 9.** Plain and encrypted images of parrot. (a) Color image; (b) Histogram of color image; (c) Plain R channel; (d) Plain G channel; (e) Plain B channel; (f) Encrypted color image; (g) Histogram of encrypted image; (h) Encrypted R channel; (i) Encrypted G channel; (j) Encrypted B channel.

$$r_{xy} = cov(x, y) / (\sqrt{\psi(x)}\sqrt{\psi(y)}) \tag{9}$$

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \tag{10}$$

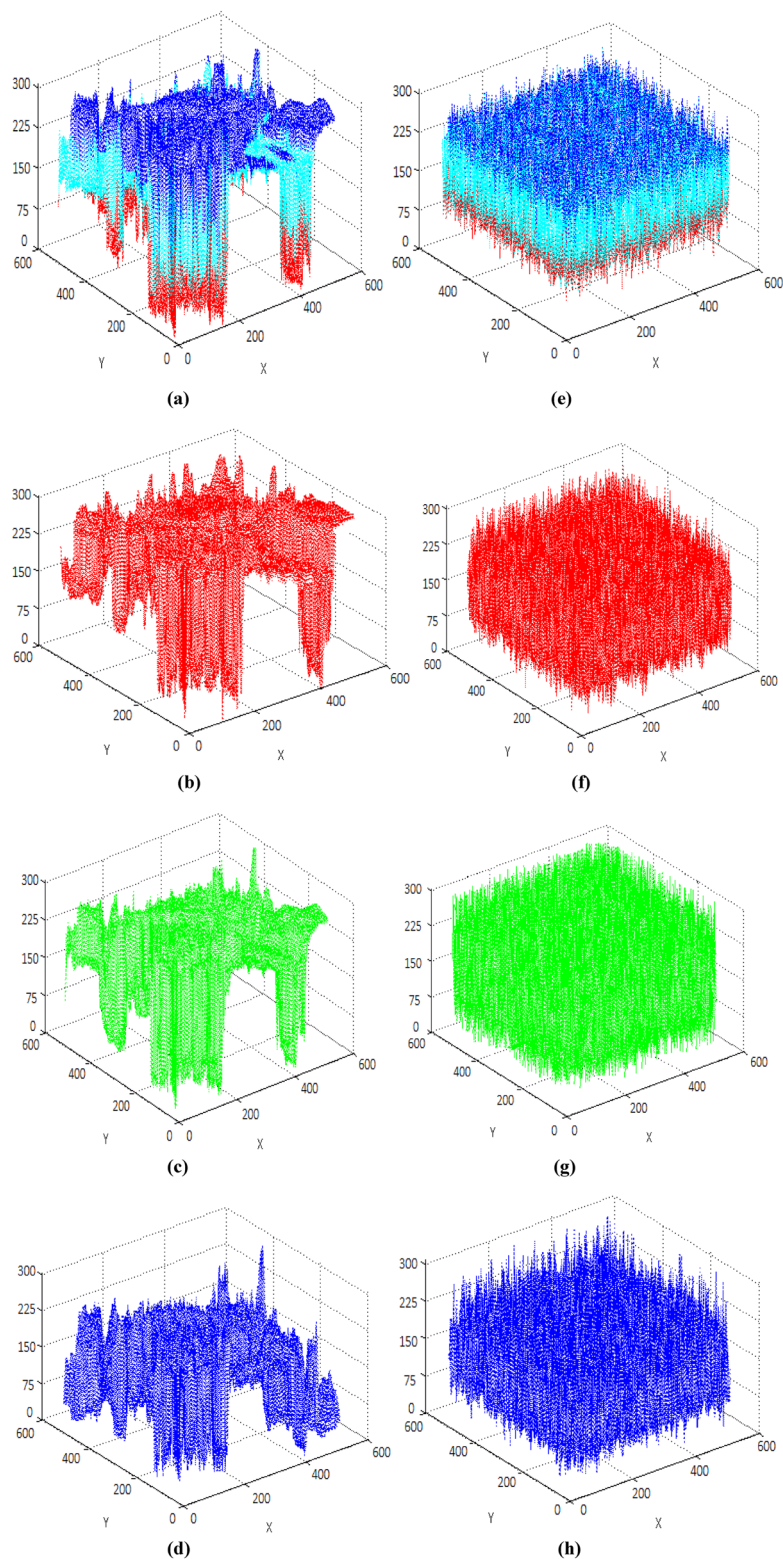
$$\psi(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2, E(x) = \frac{1}{N} \sum_{i=1}^N x_i \tag{11}$$

where  $x, y$  shows 2 adjacent pixels (whatever diagonal, vertical, or horizontal),  $N$  is the total size of  $x_i$  and  $y_i$  acquired from the image.  $E(x)$  is the mean value of  $x_i$ ; and  $E(y)$  is the mean value of  $y_i$ .

Results presented in Table 8 show that before encryption, correlation-coefficient values of plain images are close to 1 and after encryption, these values are close to 0 which validates that correlation-coefficient analysis fails to provide any clue of plain images.

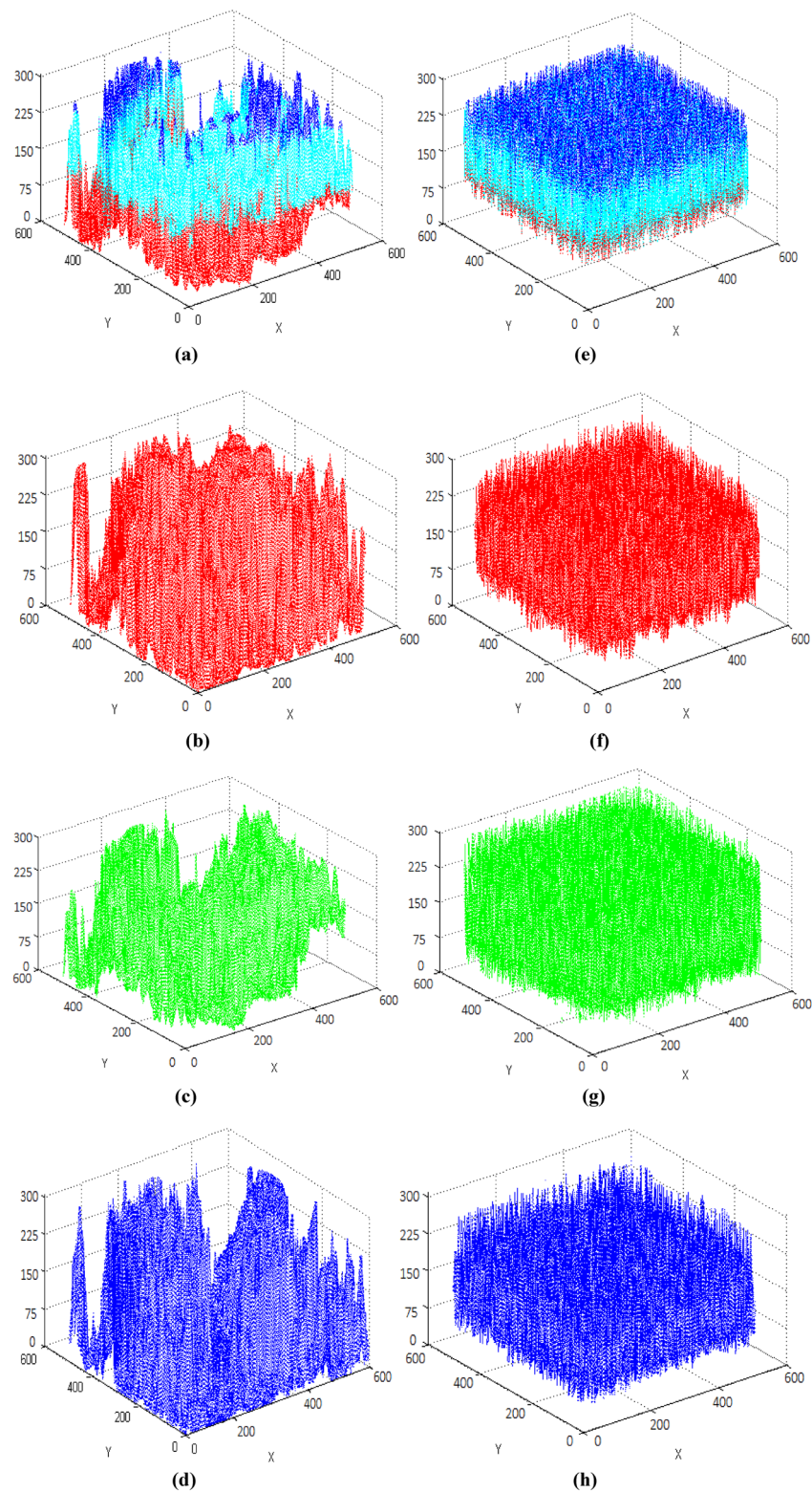
Assume that our proposed S-box and any existing s-box (such as the AES) are identical, even in this case our proposed S-box does not hold those vulnerabilities which are highlighted in above "Weaknesses in existing S-box designs" section. Instead of well-understood mathematical principles, we introduce the true random numbers for the design of S-boxes due to the reason that, true random numbers are irreversible, unpredictable, and unreproducible, even if their internal structure and response history are known to adversaries.

The asymptotic computational complexity of our technique is  $O(n^2)$ , detailed derivation is attached in Annex C. The asymptotic computational complexity of  $f^1$  and  $f^5$  is  $O(n^4)$  and  $O(n^5)$  respectively. The asymptotic computational complexity of  $f^{125-127}$  is  $O(n^3)$ .



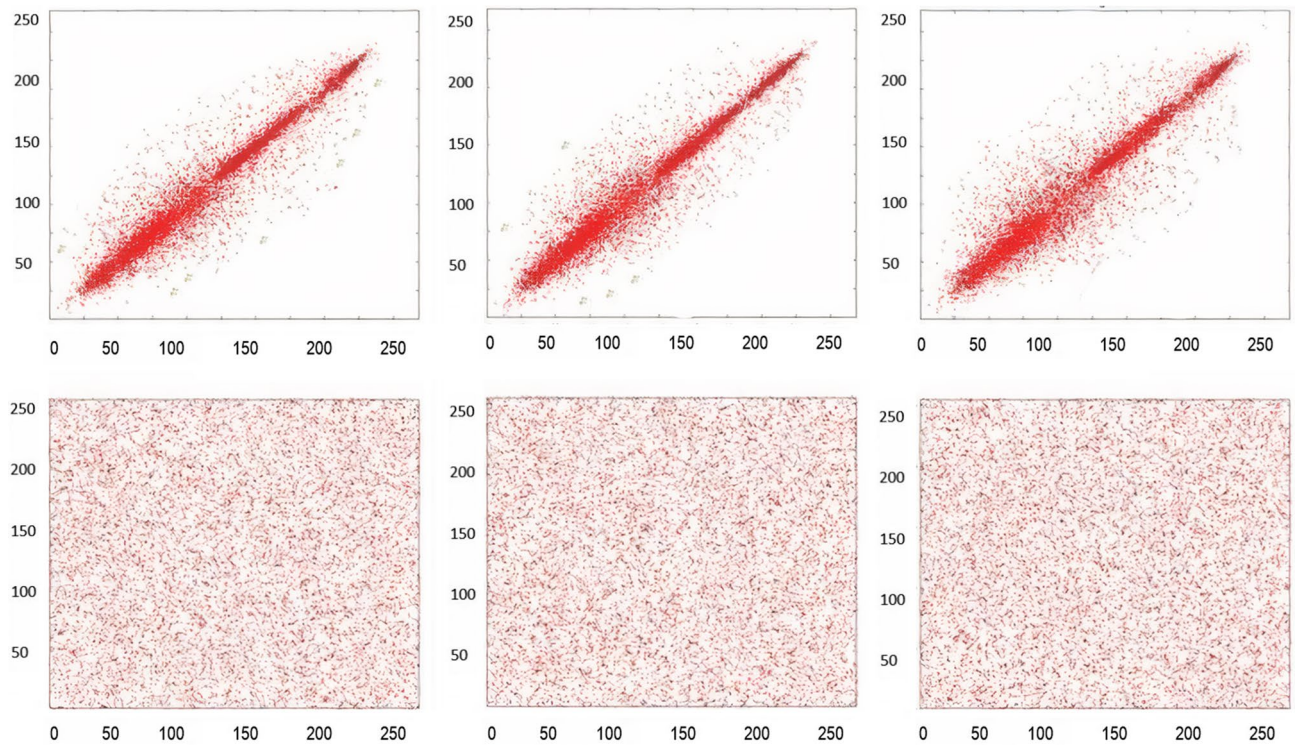
**Figure 10.** Three-dimensional histogram of fruit. (a) Color plain image; (b) R channel of plain image; (c) G channel of plain image; (d) B channel of plain image; (e) Color encrypted image; (f) R channel of encrypted image; (g) G channel of encrypted image; (h) B channel of encrypted image.





**Figure 11.** Three-dimensional histogram of parrot. (a) Color plain image; (b) R channel of plain image; (c) G channel of plain image; (d) B channel of plain image; (e) Color encrypted image; (f) R channel of encrypted image; (g) G channel of encrypted image; (h) B channel of encrypted image.



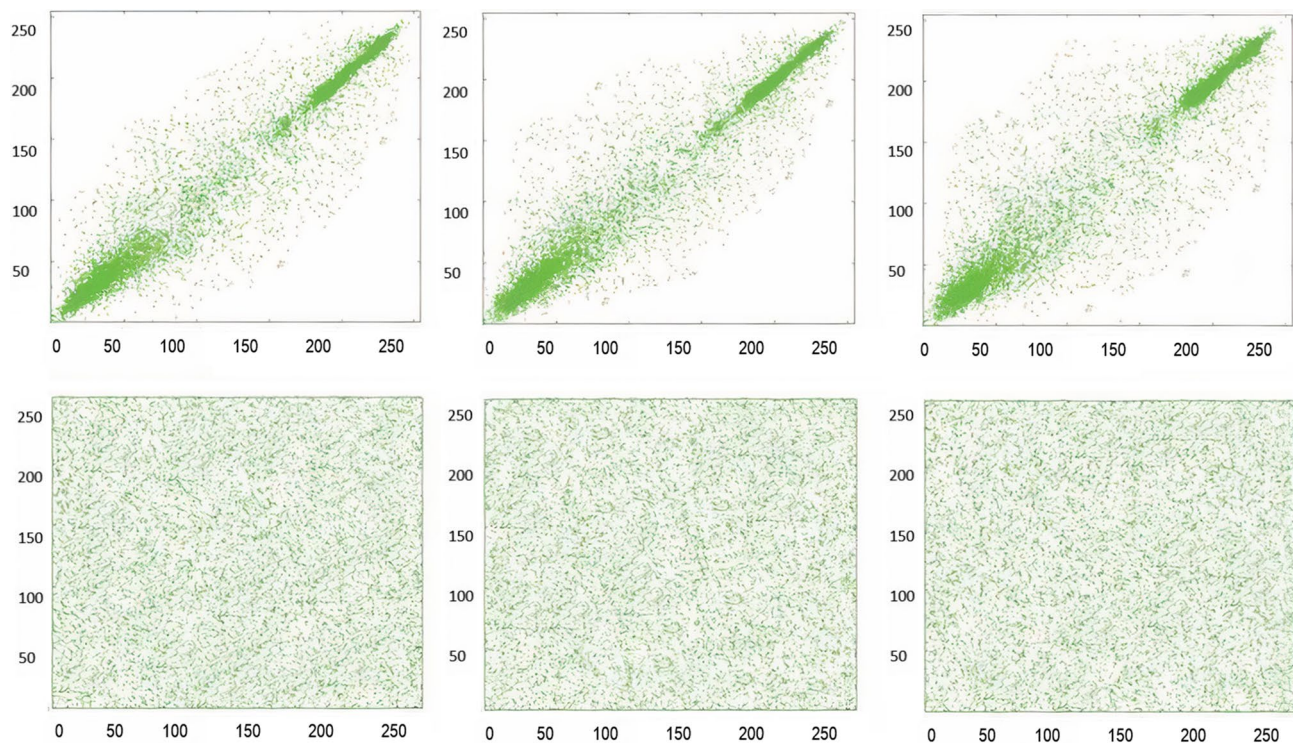


**Figure 12.** Red channel scatter plots of the Sailboat, to indicate the correlation-coefficient analysis of neighbouring pixels. **(a)** Plain image horizontal direction; **(b)** Plain image vertical direction; **(c)** Plain image diagonal direction; **(d)** Encrypted image horizontal direction; **(e)** Encrypted image vertical direction; **(f)** Encrypted image diagonal direction.

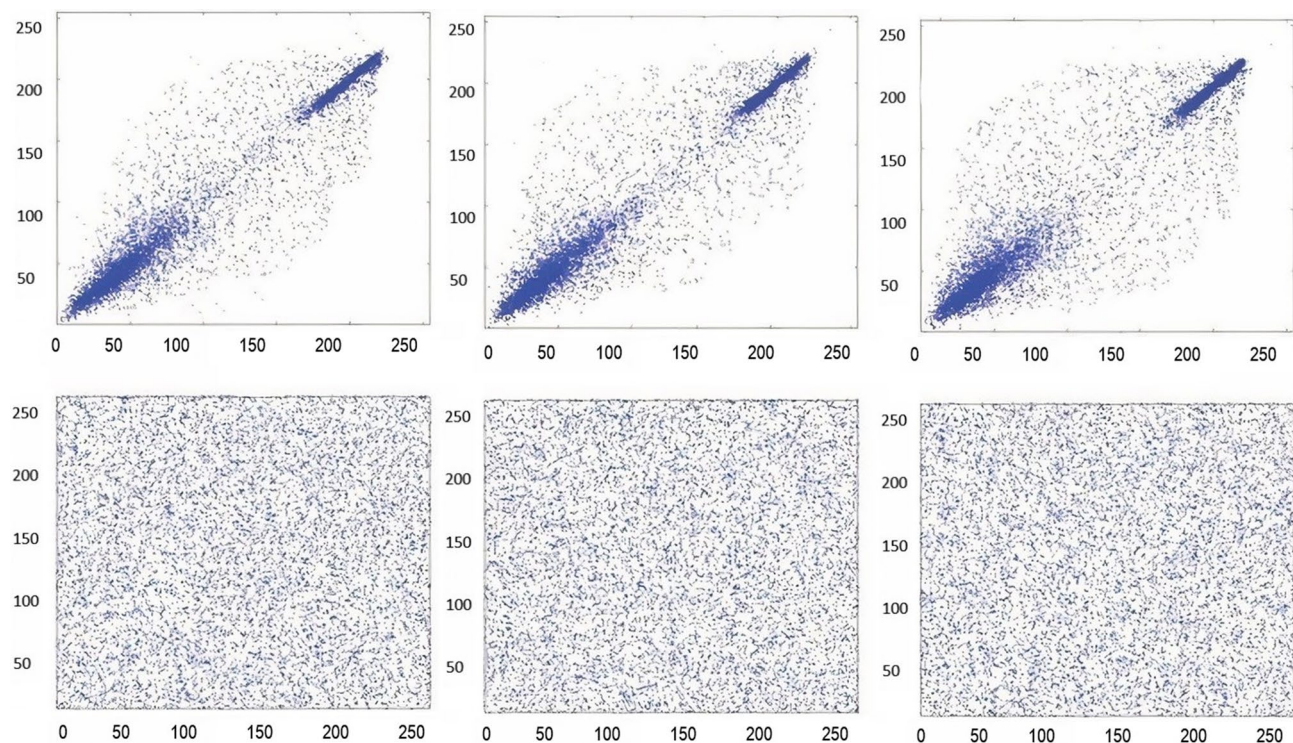
## Conclusion

Protecting confidential data is a major worldwide challenge and block ciphers has been a standout amongst the most reliable option by which data security is accomplished. Block cipher strength against various attacks rely on substitution box. Various weakness in the algebraic and chaos-based S-box designs are pointed in the literature. On the other hand, researchers endorse the true random sequences for cryptography due to the fact that these sequences rely on the strength of naturally occurring processes to generate the true randomness. The objective of this research is extraction of inevitable random noise from the medical imaging, and to synthesize the multi-level information fusion for the construction of strong substitution boxes. Various security evaluation criteria, statistical tests and comparison with various very recent state-of-the-art techniques validate our proposed technique. In future, we will extend our proposed information fusion design for the construction of lattice cryptographic primitive.





**Figure 13.** Green channel scatter plots of the Sailboat, to indicate the correlation-coefficient analysis of neighbouring pixels. (a) Plain image horizontal direction; (b) Plain image vertical direction; (c) Plain image diagonal direction; (d) Encrypted image horizontal direction; (e) Encrypted image vertical direction; (f) Encrypted image diagonal direction.



**Figure 14.** Blue channel scatter plots of the Sailboat, to indicate the correlation-coefficient analysis of neighbouring pixels. (a) Plain image horizontal direction; (b) Plain image vertical direction; (c) Plain image diagonal direction; (d) Encrypted image horizontal direction; (e) Encrypted image vertical direction; (f) Encrypted image diagonal direction.

Images	Horizontal			Vertical			Diagonal		
	R	G	B	R	G	B	R	G	B
Plain Peppers	0.9853	0.9931	0.9819	0.9788	0.9862	0.9854	0.9866	0.9754	0.9767
Encrypted Peppers	-0.0210	-0.0054	-0.0003	-0.0114	-0.0115	-0.0201	-0.0037	-0.0018	-0.0043
Plain Parrot	0.9659	0.9468	0.9546	0.9402	0.9303	0.9753	0.9784	0.9010	0.9182
Encrypted Parrot	-0.0016	-0.0072	-0.0069	0.0002	-0.0015	0.0007	-0.0008	0.0014	0.0006
Plain Baboon	0.9195	0.8519	0.9325	0.8567	0.8982	0.8413	0.8478	0.8886	0.8689
Encrypted Baboon	-0.0069	-0.0143	-0.0048	-0.0203	-0.0187	-0.0032	-0.0019	-0.0164	-0.0053
Plain Sailboat	0.9548	0.9552	0.9637	0.9573	0.9627	0.9507	0.9322	0.9147	0.9246
Encrypted Sailboat	-0.0002	-0.0084	-0.001	-0.0019	-0.0018	0.0038	0.0009	0.005	0.0011

**Table 8.** Correlation-coefficient analysis.

Received: 30 September 2020; Accepted: 18 February 2021

Published online: 12 July 2021

## References

- Khan, M. F. *et al.* A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system. *IEEE Access* **7**, 84980–84991 (2019).
- Bernstein, D. J. & Lange, T. Post-quantum cryptography. *Nature* **549**(7671), 188–194 (2017).
- Jinomeiq, L., Baoduui, W. & Xinmei, W. One AES S-box to increase complexity and its cryptanalysis. *J. Syst. Eng. Electron.* **18**(2), 427–433 (2007).
- Cho, J. Y. Linear cryptanalysis of reduced-round PRESENT. In *Cryptographers' Track at the RSA Conference* 302–317 (Springer, 2010).
- Selçuk, A. A. On probability of success in linear and differential cryptanalysis. *J. Cryptol.* **21**(1), 131–147 (2008).
- Blondeau, C. & Gérard, B. Multiple differential cryptanalysis: Theory and practice. In *International Workshop on Fast Software Encryption* 35–54 (Springer, 2011).
- Blondeau, C. & Nyberg, K. New links between differential and linear cryptanalysis. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* 388–404 (Springer, 2013).
- Musa, M. A., Schaefer, E. F. & Wedig, S. A simplified AES algorithm and its linear and differential cryptanalyses. *Cryptologia* **27**(2), 148–177 (2003).
- Wang, M., Sun, Y., Mouha, N. & Preneel, B. Algebraic techniques in differential cryptanalysis revisited. In *Australasian Conference on Information Security and Privacy* 120–141 (Springer, 2011).
- Blondeau, C. & Nyberg, K. Links between truncated differential and multidimensional linear properties of block ciphers and underlying attack complexities. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* 165–182 (Springer, 2014).
- Kazlauskas, K. & Kazlauskas, J. Key-dependent S-box generation in AES block cipher system. *Informatica* **20**(1), 23–34 (2009).
- Jing-mei, L., Bao-dian, W., Xiang-guo, C. & Xin-mei, W. Cryptanalysis of Rijndael S-box and improvement. *Appl. Math. Comput.* **170**(2), 958–975 (2005).
- Khan, M. A., Ali, A., Jeoti, V. & Manzoor, S. A chaos-based substitution box (S-Box) design with improved differential approximation probability (DP). *Iran. J. Sci. Technol., Trans. Electr. Eng.* **42**(2), 219–238 (2018).
- Hermelin, M. & Nyberg, K. Linear cryptanalysis using multiple linear approximations. *IACR Cryptol. ePrint Arch.* **2011**, 93 (2011).
- Lu, J. A methodology for differential-linear cryptanalysis and its applications. *Des. Codes Crypt.* **77**(1), 11–48 (2015).
- Tiessen, T., Knudsen, L. R., Kölbl, S. & Lauridsen, M. M. Security of the AES with a secret S-box. In *International Workshop on Fast Software Encryption* 175–189 (Springer, 2015).
- Canteaut, A. & Roué, J. On the behaviors of affine equivalent Sboxes regarding differential and linear attacks (2015).
- Youssef, A. M. & Gong, G. On the interpolation attacks on block ciphers. In *FSE 2000. LNCS Vol. 1978* (ed. Schneier, B.) 109–120 (Springer, 2001).
- Dinur, I., Liu, Y., Meier, W. & Wang, Q. Optimized interpolation attacks on LowMC. In *International Conference on the Theory and Application of Cryptology and Information Security* 535–560 (Springer, 2015).
- Li, C. & Preneel, B. Improved interpolation attacks on cryptographic primitives of low algebraic degree. In *International Conference on Selected Areas in Cryptography* 171–193 (Springer, 2019).
- Courtois, N. T. The inverse S-box, non-linear polynomial relations and cryptanalysis of block ciphers. In *International Conference on Advanced Encryption Standard* 170–188 (Springer, 2004).
- Bulygin, S. & Brickenstein, M. Obtaining and solving systems of equations in key variables only for the small variants of AES. *Math. Comput. Sci.* **3**(2), 185–200 (2010).
- Buchmann, J., Pyshkin, A. & Weinmann, R.-P. Block ciphers sensitive to Gröbner basis attacks. In *Cryptographers' Track at the RSA Conference* 313–331 (Springer, 2006).
- Buchmann, J., Pyshkin, A. & Weinmann, R.-P. A zero-dimensional Gröbner basis for AES-128. In *International Workshop on Fast Software Encryption* 78–88 (Springer, 2006).
- Cid, C. & Weinmann, R.-P. Block ciphers: Algebraic cryptanalysis and Groebner bases. In *Groebner Bases, Coding, and Cryptography* 307–327 (Springer, 2009).
- Pyshkin, A. *Algebraic Cryptanalysis of Block Ciphers Using Gröbner Bases* (Technische Universität, 2008).
- Zhao, K., Cui, J. & Xie, Z. Algebraic cryptanalysis scheme of AES-256 using Gröbner basis. *J. Electr. Comput. Eng.* **2017**, 1–9 (2017).
- Faugère, J.-C. Interactions between computer algebra (Gröbner bases) and cryptology. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation* 383–384 (2009).
- Prouff, E. DPA attacks and S-boxes. In *International Workshop on Fast Software Encryption* 424–441 (Springer, 2005).
- Carlet, C. On highly nonlinear S-boxes and their inability to thwart DPA attacks. In *International Conference on Cryptology in India* 49–62 (Springer, 2005).



31. Kim, H., Kim, T., Han, D. & Hong, S. Efficient masking methods appropriate for the block ciphers ARIA and AES. *ETRI J.* **32**(3), 370–379 (2010).
32. Oswald, E., Mangard, S., Pramstaller, N. & Rijmen, V. A side-channel analysis resistant description of the AES S-box. In *FSE 2005. LNCS Vol. 3557* (eds Gilbert, H. & Handschuh, H.) 413–423 (Springer, 2005).
33. Oswald, E. & Schramm, K. An efficient masking scheme for AES software implementations. In *WISA 2005. LNCS Vol. 3786* (eds Song, J.-S. et al.) 292–305 (Springer, 2006).
34. Rivain, M., Dottax, E. & Prouff, E. Block ciphers implementations provably secure against second order side channel analysis. In *FSE 2008. LNCS Vol. 5086* (ed. Nyberg, K.) 127–143 (Springer, 2008).
35. Rivain, M. & Prouff, E. Provably secure higher-order masking of AES. In *CHES 2010. LNCS Vol. 6225* (eds Mangard, S. & Standaert, F.-X.) 413–427 (Springer, 2010).
36. Bogdanov, A. & Pyshkin, A. *Algebraic Side-Channel Collision Attacks on AES*. <https://eprint.iacr.org/2007/477.pdf> (2007).
37. Carlet, C., Faugere, J.-C., Goyet, C. & Renault, G. Analysis of the algebraic side channel attack. *J. Cryptogr. Eng.* **2**(1), 45–62 (2012).
38. Gwynne, M., Kullmann, O. Attacking AES via SAT. PhD diss., BSc dissertation (Swansea) (2010).
39. Jovanovic, P. & Kreuzer, M. Algebraic attacks using SAT-solvers. *Groups Complex. Cryptol.* **2**(2), 247–259 (2010).
40. Semenov, A., Zaikin, O., Otpuschennikov, I., Kochemazov, S. & Ignatiev, A. On cryptographic attacks using backdoors for SAT. In *Thirty-Second AAAI Conference on Artificial Intelligence* (2018).
41. Lafitte, F., Nakahara, J. & Van Heule, D. Applications of SAT solvers in cryptanalysis: Finding weak keys and preimages. *J. Satisf., Boolean Model. Comput.* **9**(1), 1–25 (2014).
42. Bard, G. On the rapid solution of systems of polynomial equations over lowdegree extension fields of GF (2) via SAT-solvers. In *8th Central European Conf. on Cryptography* (2008).
43. Magalhães, H. M. M. Applying SAT on the linear and differential cryptanalysis of the AES (2009).
44. Bard, G. V., Courtois, N. T. & Jefferson, C. Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over GF (2) via SAT-solvers (2007).
45. Bard, G. V. Extending SAT-solvers to low-degree extension fields of GF (2). In *Central European Conference on Cryptography*, Vol. 2008 (2008).
46. Cid, C. Some algebraic aspects of the advanced encryption standard. In *Advanced Encryption Standard—AES* (eds Dobbertin, H., Rijmen, V. & Sowa, A.). No. 3373 in *Lecture Notes in Computer Science* 58–66 (Springer, 2005).
47. Cid, C. & Leurent, G. An analysis of the XSL algorithm. In *Advances in Cryptology—ASIACRYPT 2005* (ed Roy, B.). No. 3788 in *Lecture Notes in Computer Science* 333–352 (Springer, 2005).
48. Choy, J., Yap, H. & Khoo, K. An analysis of the compact XSL attack on BES and embedded SMS4. In *International Conference on Cryptology and Network Security* 103–118 (Springer, 2009).
49. Choy, J., Chew, G., Khoo, K. & Yap, H. Cryptographic properties and application of a generalized unbalanced Feistel network structure. In *Australasian Conference on Information Security and Privacy* 73–89 (Springer, 2009).
50. Ji, L. Y., Ye, Y. P., Lin, W. Y., Wu, P. & Fang, S. The optimum and the combination algorithm of AES and RSA. *J. Foshan Univ. (Natural Sci. Edit.)* **6**, 1–132 (2009).
51. Blondeau, C. & Nyberg, K. Joint data and key distribution of simple, multiple, and multidimensional linear cryptanalysis test statistic and its impact to data complexity. *Des., Codes Cryptogr.* **82**(1–2), 319–349 (2017).
52. Oren, Y. & Wool, A. Side-channel cryptographic attacks using pseudo-boolean optimization. *Constraints* **21**(4), 616–645 (2016).
53. Yi, W., Lu, L. & Chen, S. Integral and zero-correlation linear cryptanalysis of lightweight block cipher MIBS. *J. Electron. Inform. Technol.* **38**(4), 819–826 (2016).
54. Wei, H. R. & Zheng, Y. F. Algebraic techniques in linear cryptanalysis. In *Advanced Materials Research*, Vol. 756, 3634–3639 (Trans Tech Publications Ltd., 2013).
55. Liu, J., Chen, S. & Zhao, L. Lagrange interpolation attack against 6 rounds of Rijndael-128. In *2013 5th International Conference on Intelligent Networking and Collaborative Systems* 652–655 (IEEE, 2013).
56. Courtois, N. T. & Pieprzyk, J. Cryptanalysis of block ciphers with overdefined systems of equations. In *Advances in Cryptology—ASIACRYPT 2002*. No. 2501 in *Lecture Notes in Computer Science* (ed Zheng, Y.) 267–287 (Springer, 2002).
57. Diem, C. The XL-algorithm and a conjecture from commutative algebra. In *International Conference on the Theory and Application of Cryptology and Information Security* (Springer, 2004).
58. Sugita, M. K. & Imai, H. Relation between the XL algorithm and Gröbner basis algorithms. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **E89-A**, 11–18 (2006).
59. Diem, C. The XL-algorithm and a conjecture from commutative algebra. In *Advances in Cryptology—ASIACRYPT 2004*, Vol. 3329 of *Lecture Notes in Computer Science* (ed Lee, P. J.) 323–337 (2004).
60. Nicolas, C. & Pieprzyk, J. Cryptoanalysis of block ciphers with overdefined system of equations. In *Advances in Cryptology—Asiacrypt 2002*, Vol. 2501 of *Lecture Notes in Computer Science* (ed. Zheng, Y.) 267–287 (Springer-Verlag, 2002).
61. Zhang, L. Y. et al. A chaotic image encryption scheme owning temp-value feedback. *Commun. Nonlinear Sci. Numer. Simul.* **19**(10), 3653–3659 (2014).
62. Zhang, Y. et al. A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations. *Signal Process.: Image Commun.* **28**(3), 292–300 (2013).
63. Niyat, A. Y., Moattar, M. H. & Torshiz, M. N. Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Opt. Lasers Eng.* **90**, 225–237 (2017).
64. Khan, M. & Asghar, Z. A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S 8 permutation. *Neural Comput. Appl.* **29**(4), 993–999 (2018).
65. Özkaynak, F. & Yavuz, S. Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dyn.* **74**(3), 551–557 (2013).
66. Hua, Z. & Zhou, Y. Image encryption using 2D logistic-adjusted-sine map. *Inf. Sci.* **339**, 237–253 (2016).
67. Hua, Z. et al. 2D logistic-sine-coupling map for image encryption. *Signal Process.* **149**, 148–161 (2018).
68. Zhang, Y. The unified image encryption algorithm based on chaos and cubic S-box. *Inf. Sci.* **450**, 361–377 (2018).
69. Ullah, A., Jamal, S. S. & Shah, T. A novel scheme for image encryption using substitution box and chaotic system. *Nonlinear Dyn.* **91**(1), 359–370 (2018).
70. Guo, J.-M., Riyono, D. & Prasetyo, H. Improved beta chaotic image encryption for multiple secret sharing. *IEEE Access* **6**, 46297–46321 (2018).
71. Wang, H. et al. Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map. *Signal Process.* **144**, 444–452 (2018).
72. Chai, X. et al. A color image cryptosystem. *Signal Process.* **155**, 44–62 (2019).
73. Hussain, I. et al. Construction of S-box based on chaotic map and algebraic structures. *Symmetry* **11**(3), 351 (2019).
74. Belazi, A. et al. Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. *Nonlinear Dyn.* **87**(1), 337–361 (2017).
75. Khan, M. F., Ahmed, A. & Saleem, K. A novel cryptographic substitution box design using Gaussian distribution. *IEEE Access* **7**, 15999–16007 (2019).
76. Zhou, Y., Bao, L. & Chen, C. L. P. A new 1D chaotic system for image encryption. *Signal Process.* **97**, 172–182 (2014).
77. Xie, E. Y. et al. On the cryptanalysis of Fridrich's chaotic image encryption scheme. *Signal Process.* **132**, 150–154 (2017).



78. Li, C. *et al.* Dynamic analysis of digital chaotic maps via state-mapping networks. *IEEE Trans. Circuits Syst. I Regul. Pap.* **66**(6), 2322–2335 (2019).
79. Pak, C. & Huang, L. A new color image encryption using combination of the 1D chaotic map. *Signal Process.* **138**, 129–137 (2017).
80. Parvaz, R. & Zarebnia, M. A combination chaotic system and application in color image encryption. *Opt. Laser Technol.* **101**, 30–41 (2018).
81. Hua, Z. & Zhou, Y. Dynamic parameter-control chaotic system. *IEEE Trans. Cybern.* **46**(12), 3330–3341 (2015).
82. Chen, G., Chen, Y. & Liao, X. An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. *Chaos, Solitons, Fractals* **31**(3), 571–579 (2007).
83. Alawida, M. *et al.* A new hybrid digital chaotic system with applications in image encryption. *Signal Process.* **160**, 45–58 (2019).
84. Lan, R. *et al.* Integrated chaotic systems for image encryption. *Signal Process.* **147**, 133–145 (2018).
85. Zhu, C. & Sun, K. Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps. *IEEE Access* **6**, 18759–18770 (2018).
86. Preishuber, M. *et al.* Depreciating motivation and empirical security analysis of chaos-based image and video encryption. *IEEE Trans. Inf. Forensics Secur.* **13**(9), 2137–2150 (2018).
87. Arroyo, D., Diaz, J. & Rodriguez, F. B. Cryptanalysis of a one round chaos-based substitution permutation network. *Signal Process.* **93**(5), 1358–1364 (2013).
88. Li, C. *et al.* Breaking a novel colour image encryption algorithm based on chaos. *Nonlinear Dyn.* **70**(4), 2383–2388 (2012).
89. Zhang, L. Y. *et al.* On the security of a class of diffusion mechanisms for image encryption. *IEEE Trans. Cybern.* **48**(4), 1163–1175 (2017).
90. Li, Y., Wang, C. & Chen, H. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Opt. Lasers Eng.* **90**, 238–246 (2017).
91. Zhang, L. Y. *et al.* Cryptanalyzing a chaos-based image encryption algorithm using alternate structure. *J. Syst. Softw.* **85**(9), 2077–2085 (2012).
92. Liu, Y. *et al.* Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation. *Int. J. Bifurc. Chaos* **27**(03), 1750033 (2017).
93. Deng, Y. *et al.* A general hybrid model for chaos robust synchronization and degradation reduction. *Inf. Sci.* **305**, 146–164 (2015).
94. Hua, Z., Zhou, B. & Zhou, Y. Sine chaotification model for enhancing chaos and its hardware implementation. *IEEE Trans. Ind. Electron.* **66**(2), 1273–1284 (2018).
95. Cao, C., Sun, K. & Liu, W. A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. *Signal Process.* **143**, 122–133 (2018).
96. Alawida, M., Teh, J. S. & Samsudin, A. An image encryption scheme based on hybridizing digital chaos and finite state machine. *Signal Process.* **164**, 249–266 (2019).
97. Li, C. Cracking a hierarchical chaotic image encryption algorithm based on permutation. *Signal Process.* **118**, 203–210 (2016).
98. Wu, X. *et al.* A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. *Inf. Sci.* **349**, 137–153 (2016).
99. Zahmoul, R., Ejbali, R. & Zaied, M. Image encryption based on new Beta chaotic maps. *Opt. Lasers Eng.* **96**, 39–49 (2017).
100. Sunar, B., Martin, W. J. & Stinson, D. R. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Trans. Comput.* **56**(1), 109–119 (2006).
101. Lee, K. *et al.* TRNG (true random number generator) method using visible spectrum for secure communication on 5G network. *IEEE Access* **6**, 12838–12847 (2018).
102. Bernardo-Gavito, R. *et al.* Extracting random numbers from quantum tunnelling through a single diode. *Sci. Rep.* **7**(1), 17879 (2017).
103. Ray, B. & Milenković, A. True random number generation using read noise of flash memory cells. *IEEE Trans. Electron Dev.* **65**(3), 963–969 (2018).
104. Aghamohammadi, C. & Crutchfield, J. P. Thermodynamics of random number generation. *Phys. Rev. E* **95**(6), 062139 (2017).
105. Abutaleb, M. M. A novel true random number generator based on QCA nanocomputing. *Nano Commun. Netw.* **17**, 14–20 (2018).
106. Marangon, D. G. *et al.* Long-term test of a fast and compact quantum random number generator. *J. Lightwave Technol.* **36**(17), 3778–3784 (2018).
107. Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* **464**(7291), 1021 (2010).
108. Goossens, B., Luong, H., Pizurica, A. & Philips, W. An improved non-local denoising algorithm. In *2008 International Workshop on Local and Non-Local Approximation in Image Processing (LNLA 2008)* 143–156 (2008).
109. Soto, M. E., Pezoa, J. E. & Torres, S. N. Thermal noise estimation and removal in MRI: A noise cancellation approach. In *Iberoamerican Congress on Pattern Recognition* 47–54 (Springer, 2011).
110. Toprak, A. & Güler, İ. Suppression of impulse noise in medical images with the use of fuzzy adaptive median filter. *J. Med. Syst.* **30**(6), 465–471 (2006).
111. Srinivasan, K. S. & Ebenezer, D. A new fast and efficient decision-based algorithm for removal of high-density impulse noises. *IEEE Signal Process. Lett.* **14**(3), 189–192 (2007).
112. Toprak, A. & Güler, İ. Impulse noise reduction in medical images with the use of switch mode fuzzy adaptive median filter. *Digit. Signal Process.* **17**(4), 711–723 (2007).
113. Özkaynak, F., Çelik, V. & Özer, A. B. A new S-box construction method based on the fractional-order chaotic Chen system. *Signal, Image Video Process.* **11**(4), 659–664 (2017).
114. Khan, M., Shah, T. & Batool, S. I. Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Comput. Appl.* **27**(3), 677–685 (2017).
115. Abd el-Latif, A. A., Abd-el-Atty, B., Amin, M. & Iliyasu, A. M. Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Sci. Rep.* **10**(1), 1–16 (2020).
116. Khan, M., Shah, T., Mahmood, H. & Gondal, M. A. An efficient method for the construction of block cipher with multi-chaotic systems. *Nonlinear Dyn.* **71**(3), 489–492 (2013).
117. Özkaynak, F. & Özer, A. B. A method for designing strong S-boxes based on chaotic Lorenz system. *Phys. Lett. A* **374**(36), 3733–3738 (2010).
118. Çavuşoğlu, Ü., Zengin, A., Pehlivan, I. & Kaçar, S. A novel approach for strong S-box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dyn.* **87**(2), 1081–1094 (2017).
119. Hussain, I., Shah, T., Gondal, M. A., Khan, W. A. & Mahmood, H. A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Comput. Appl.* **23**(1), 97–104 (2013).
120. Khan, M., Shah, T., Mahmood, H., Gondal, M. A. & Hussain, I. A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. *Nonlinear Dyn.* **70**(3), 2303–2311 (2012).
121. Khan, M. & Shah, T. An efficient construction of substitution box with fractional chaotic system. *SIVIP* **9**(6), 1335–1338 (2015).
122. Hussain, I., Shah, T., Mahmood, H. & Gondal, M. A. A projective general linear group based algorithm for the construction of substitution box for block ciphers. *Neural Comput. Appl.* **22**(6), 1085–1093 (2013).

123. Hussain, I., Shah, T., Gondal, M. A. & Mahmood, H. An efficient approach for the construction of LFT S-boxes using chaotic logistic map. *Nonlinear Dyn.* **71**(1–2), 133–140 (2013).
124. Hussain, I., Shah, T. & Gondal, M. A. A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. *Nonlinear Dyn.* **70**(3), 1791–1794 (2012).
125. Jamal, S. S., Anees, A., Ahmad, M., Khan, M. F. & Hussain, I. Construction of cryptographic S-boxes based on mobius transformation and chaotic tent-sine system. *IEEE Access* **7**, 173273–173285 (2019).
126. Beg, S. *et al.* S-box design based on optimize LFT parameter selection: A practical approach in recommendation system domain. *Multimed. Tools Appl.* **79**, 1–18 (2020).
127. Shah, T., Qureshi, A. & Khan, M. F. Designing more efficient novel S 8 S-boxes. *Int. J. Inform. Technol. Secur.* **12**(2), 826 (2020).
128. Lambić, D. A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. *Nonlinear Dyn.* **100**, 1–13 (2020).
129. Azam, N. A., Hayat, U. & Ullah, I. Efficient construction of a substitution box based on a mordell elliptic curve over a finite field. *Front. Inf. Technol. Electron. Eng.* **20**(10), 1378–1389 (2019).
130. El-Latif, A. A. A., Abd-El-Atty, B., Mazurczyk, W., Fung, C. & Venegas-Andraca, S. E. Secure data encryption based on quantum walks for 5G internet of things scenario. *IEEE Trans. Netw. Serv. Manag.* **17**(1), 118–131 (2020).
131. Özkaynak, F. Construction of robust substitution boxes based on chaotic systems. *Neural Comput. Appl.* **31**(8), 3317–3326 (2019).
132. Liu, H., Kadir, A. & Xu, C. Cryptanalysis and constructing S-box based on chaotic map and backtracking. *Appl. Math. Comput.* **376**, 125153 (2020).
133. Ahmed, H. A., Zolkipli, M. F. & Ahmad, M. A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. *Neural Comput. Appl.* **31**(11), 7201–7210 (2019).
134. El-Latif, A. A. A., Abd-El-Atty, B., Amin, M. & Ilyasu, A. M. Quantuminspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Sci. Rep.* **10**(1), 1–16 (2020).
135. Zahid, A. H. & Arshad, M. J. An innovative design of substitution-boxes using cubic polynomial mapping. *Symmetry* **11**(3), 437 (2019).
136. Artuğer, F. & Özkaynak, F. A novel method for performance improvement of chaos-based substitution boxes. *Symmetry* **12**(4), 571 (2020).
137. Özkaynak, F. On the effect of chaotic system in performance characteristics of chaos-based S-box designs. *Phys.: A Stat. Mech. Appl.* **550**, 124072 (2020).
138. Muhammad, Z. M. Z. & Özkaynak, F. A cryptographic confusion primitive based on Lotka–Volterra chaotic system and its practical applications in image encryption. In *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)* 694–698 (IEEE, 2020).
139. Silva-Garcia, V. M. *et al.* Substitution box generation using Chaos: An image encryption application. *Appl. Math. Comput.* **332**, 123–135 (2018).
140. Zhang, Y.-Q., Hao, J.-L. & Wang, X.-Y. An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map. *IEEE Access* **8**, 54175–54188 (2020).
141. Attaullah, A., Jamal, S. S. & Shah, T. A novel algebraic technique for the construction of strong substitution box. *Wirel. Pers. Commun.* **99**(1), 213–226 (2018).
142. Cassal-Quiroga, B. B. & Campos-Canton, E. Generation of dynamical S-boxes for block ciphers via extended logistic map. *Math. Probl. Eng.* **2020**, 1–12 (2020).
143. Alzaidi, A. A., Ahmad, M., Doja, M. N., Al Solami, E. & Beg, M. S. A new 1D chaotic map and  $\beta$ -hill climbing for generating substitution-boxes. *IEEE Access* **6**, 55405–55418 (2018).
144. Faheem, Z. B., Ali, A., Khan, M. A., Ul-Haq, M. E. & Ahmad, W. Highly dispersive substitution box (S-box) design using chaos. *ETRI J.* **42**, 619–632 (2020).
145. Alzaidi, A. A., Ahmad, M., Ahmed, H. S. & Solami, E. A. Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map. *Complexity* **2018**, 1–16 (2018).
146. Ali, K. M. & Khan, M. Application based construction and optimization of substitution boxes over 2D mixed chaotic maps. *Int. J. Theor. Phys.* **58**(9), 3091–3117 (2019).
147. Zhang, Y.-Q. & Wang, X.-Y. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. *Inf. Sci.* **273**, 329–351 (2014).
148. Tanyildizi, E. & Özkaynak, F. A new chaotic S-box generation method using parameter optimization of one-dimensional chaotic maps. *IEEE Access* **7**, 117829–117838 (2019).
149. Hayat, U., Azam, N. A. & Asif, M. A method of generating 8×8 substitution boxes based on elliptic curves. *Wirel. Pers. Commun.* **101**(1), 439–451 (2018).
150. Açikkapi, M. Ş, Özkaynak, F. & Özer, A. B. Side-channel analysis of chaos-based substitution box structures. *IEEE Access* **7**, 79030–79043. <https://doi.org/10.1109/ACCESS.2019.2921708> (2019).
151. Wang, X. *et al.* A chaotic system with infinite equilibria and its S-box constructing application. *Appl. Sci.* **8**(11), 2132 (2018).
152. Özkaynak, F. Construction of robust substitution boxes based on chaotic systems. *Neural Comput. Appl.* **31**, 1–10 (2019).
153. Liu, L., Zhang, Y. & Wang, X. A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. *Appl. Sci.* **8**(12), 2650 (2018).
154. Zahid, A. H., Arshad, M. J. & Ahmad, M. A novel construction of efficient substitution-boxes using cubic fractional transformation. *Entropy* **21**(3), 245 (2019).
155. Ye, T. & Zhimao, L. Chaotic S-box: Six-dimensional fractional Lorenz-Duffing chaotic system and O-shaped path scrambling. *Nonlinear Dyn.* **94**(3), 2115–2126 (2018).
156. Hua, Z., Zhou, Y. & Huang, H. Cosine-transform-based chaotic system for image encryption. *Inf. Sci.* **480**, 403–419 (2019).
157. Zhu, H., Zhao, Y. & Song, Y. 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption. *IEEE Access* **7**, 14081–14098 (2019).
158. Zhang, X., Zhao, Z. & Wang, J. Chaotic image encryption based on circular substitution box and key stream buffer. *Signal Process. Image Commun.* **29**(8), 902–913 (2014).
159. El Assad, S. & Farajallah, M. A new chaos-based image encryption system. *Signal Process.: Image Commun.* **41**, 144–157 (2016).
160. Belazi, A. *et al.* Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Opt. Lasers Eng.* **88**, 37–50 (2017).
161. Luo, Y. *et al.* A chaotic map-control-based and the plain image-related cryptosystem. *Nonlinear Dyn.* **83**(4), 2293–2310 (2016).
162. Ping, P. *et al.* Designing permutation–substitution image encryption networks with Henon map. *Neurocomputing* **283**, 53–63 (2018).
163. Özkaynak, F., Çelik, V. & Özer, A. B. A new S-box construction method based on the fractional-order chaotic Chen system. *Signal, Image Video Process* **11**(4), 659–664 (2017).
164. Muhammad, K. *et al.* Secure surveillance framework for IoT systems using probabilistic image encryption. *IEEE Trans. Ind. Inf.* **14**(8), 3679–3689 (2018).
165. Khan, J. S. & Ahmad, J. Chaos based efficient selective image encryption. *Multidimens. Syst. Signal Process.* **30**(2), 943–961 (2019).
166. Zhu, Z.-L. *et al.* A chaos-based symmetric image encryption scheme using a bit-level permutation. *Inf. Sci.* **181**(6), 1171–1186 (2011).

167. Wang, Y. *et al.* A new chaos-based fast image encryption algorithm. *Appl. Soft Comput.* **11**(1), 514–522 (2011).
168. Liu, H., Kadir, A. & Niu, Y. Chaos-based color image block encryption scheme using S-box. *AEU-Int. J. Electron. Commun.* **68**(7), 676–686 (2014).
169. Belazi, A., El-Latif, A. A. A. & Belghith, S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Process.* **128**, 155–170 (2016).
170. Çavuşoğlu, Ü. *et al.* Secure image encryption algorithm design using a novel chaos based S-box. *Chaos, Solitons Fractals* **95**, 92–101 (2017).
171. Zhang, W. *et al.* Image encryption based on three-dimensional bit matrix permutation. *Signal Process.* **118**, 36–50 (2016).
172. Kaur, S. & Kaur, S. MRI denoising using non-local PCA with DWT. In *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)* 507–511 (IEEE, 2016).
173. Yang, J. *et al.* Local statistics and non-local mean filter for speckle noise reduction in medical ultrasound image. *Neurocomputing* **195**, 88–95 (2016).
174. Chandrasekharappa, T. G. S. Enhancement of confidentiality and integrity using cryptographic techniques (2012).
175. Razaq, A. *et al.* A novel construction of substitution box involving coset diagram and a bijective map. *Secur. Commun. Netw.* **2017**, 5101934 (2017).

## Author contributions

M.F.K.: Wrote the main manuscript. K.S.: Reviewed and edited the manuscript. M.A.A.: Reviewed the manuscript. S.B.: Reviewed the manuscript.

## Competing interests

The authors declare no competing interests.

## Additional information

**Supplementary Information** The online version contains supplementary material available at <https://doi.org/10.1038/s41598-021-93344-z>.

**Correspondence** and requests for materials should be addressed to M.F.K.

**Reprints and permissions information** is available at [www.nature.com/reprints](http://www.nature.com/reprints).

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



**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2021