Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 2532497, 20 pages
https://doi.org/10.1155/2022/2532497

Research Article

Human Psychological Disorder towards Cryptography: True Random Number Generator from EEG of Schizophrenics and Its Application in Block Encryption's Substitution Box

Muhammad Fahad Khan,[1,2] **Khalid Saleem**,[1] **Mohammad Mazyad Hazzazi**,[3] **Mohammed Alotaibi**,[4] **Piyush Kumar Shukla**,[5] **Muhammad Aqeel**,[6] **and Seda Arslan Tuncer**[7]

[1]*Department of Computer Science, Quaid-i-Azam University, Islamabad, Pakistan*
[2]*Department of Software Engineering, Foundation University Islamabad, Islamabad, Pakistan*
[3]*Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia*
[4]*Department of Management Information Systems, College of Business Administration, University of Tabuk, Tabuk, Saudi Arabia*
[5]*Department of Computer Science & Engineering, University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, Madhya Pradesh, India*
[6]*Department of Psychology, Foundation University Islamabad, Islamabad, Pakistan*
[7]*Department of Software Engineering, Firat University Faculty of Engineering, Elazig, Turkey*

Correspondence should be addressed to Muhammad Fahad Khan; fahad.khan@fui.edu.pk

Received 23 March 2022; Revised 21 April 2022; Accepted 30 April 2022; Published 21 June 2022

Academic Editor: Arpit Bhardwaj

Schizophrenia is a multifaceted chronic psychiatric disorder that affects the way a human thinks, feels, and behaves. Inevitably, natural randomness exists in the psychological perception of schizophrenic patients, which is our primary source of inspiration for this research because true randomness is the indubitably ultimate valuable resource for symmetric cryptography. Famous information theorist Claude Shannon gave two desirable properties that a strong encryption algorithm should have, which are confusion and diffusion in his fundamental article on the theoretical foundations of cryptography. Block encryption strength against various cryptanalysis attacks is purely dependent on its confusion property, which is gained through the confusion component. In the literature, chaos and algebraic techniques are extensively used to design the confusion component. Chaos- and algebraic-based techniques provide favorable features for the design of the confusion component; however, researchers have also identified potential attacks on these techniques. Instead of existing schemes, we introduce a novel methodology to construct cryptographic confusion component from the natural randomness, which are existing in the psychological perception of the schizophrenic patients, and as a result, cryptanalysis of chaos and algebraic techniques are not applicable on our proposed technique. The psychological perception of the brain regions was captured through the electroencephalogram (EEG) readings during the sensory task. The proposed design passed all the standard evaluation criteria and validation tests of the confusion component and the random number generators. One million true random bits are assessed through the NIST statistical test suite, and the results proved that the psychological perception of schizophrenic patients is a good source of true randomness. Furthermore, the proposed confusion component attains better or equal cryptographic strength as compared to state-of-the-art techniques (2020 to 2021). To the best of our knowledge, this nature of research is performed for the first time, in which psychiatric disorder is utilized for the design of information security primitive. This research opens up new avenues in cryptographic primitive design through the fusion of computing, neuroscience, and mathematics.

1. Introduction

Schizophrenia is a multifaceted psychiatric disorder, which consists of several varied causes such as environmental, developmental, and genetic factors. Due to numerous complications of its causes, inevitable natural randomness exists in the electroencephalographic readings of patient's psychological responses. Patients who suffer from schizophrenia show randomness in their clinical presentation of symptoms, characteristics, and related prognosis. It is distinguished by three major clusters of symptoms consisting of cognitive symptoms including impairment of short- or long-term working memory, negative symptoms like social withdrawal, and positive symptoms like hallucinations or delusions. These symptoms stimulate diverse neural activities in the different regions of brain. Natural randomness has been acknowledged as the ideal method for cryptography and a lot of researchers endorse the true random numbers for cryptography due to the reason that true random numbers are irreversible, unpredictable, and unreproducible, even if their internal construction and response history are identifiable to the adversaries [1–8].

Naturally, in the characteristics of the schizophrenic patients, diverse spectrum of disorders inevitably exists, which was our core source of inspiration because these disorders are the potential source of natural randomness. For example, in the delusion characteristic, patients lose their brain control due to their delusionary beliefs about the world around them. The loss of control stimulates uncertain and indistinct neural activities in different parts of the brain. These delusions could include grandiose, erotomaniac, and persecutory. Another characteristic of schizophrenic patients is the variation in the presentation of their sensory hallucinations, which differs between each patient. These hallucinations could be auditory, visual, tactile, gustatory, or olfactory. These hallucinations are also responsible for the arbitrariness of neural activities in brain regions. The third characteristic is a derailment, in which patients have variations in the thinking patterns and these disorganized thinking patterns are also a cause of irregular neural activity in different brain regions. The last characteristic is grossly disorganized or catatonic behavior, which causes variation in their presentation of motor behavior due to the imbalanced neural activities. These involuntary motor behaviors can range from childlike "silliness" to unpredictable agitation, which causes difficulty in goal-directed behavior.

Protecting secret information is a global challenge, and block cipher has been a standout among the most reliable option by which security is accomplished [9–12]. Block ciphers belong to the family of deterministic algorithms that operate on the fixed length of bits (n), called a block. A block cipher algorithm divides the plaintext into several fixed-length blocks of n bits, to produce a block of ciphertext of k bits. Block cipher combines both confusion and diffusion components within a round function and repeats the function multiple times to produce a ciphered text. Advanced Encryption Standard and Data Encryption Standard are the most prominent block ciphers. For the block ciphers, differential and linear attacks are considered very powerful attacks [13–17]. The main objective of the differential attack is to find the nonrandom pattern of the output, and for this objective, the attacker attempts to impose a certain set of input to track the differences in the output. Similarly, the main objective of the linear attack is to try to learn the linear association between the parity bits of cipher text, plaintext, and the symmetric key. Responsibility to make the correlation between ciphertext and the key, as undetectable as possible, is only on the confusion component, as well as resistance against the cryptanalysis attacks totally depends upon the confusion component [13–22]. The confusion component of the block cipher is normally known as substitution box (S-box) or nonlinear block cipher primitive. Nonlinear block cipher primitive transforms m bits input to n bits output by using S: $\{0,1\}^n \longrightarrow \{0,1\}^k$.

The ultimate goal of this research is to propose a methodology for the problem "how to construct the nonlinear primitive of block cipher using the strength of true randomness." The core concept of this research is to extract true random bits, by calculating the difference between each electrode reading of one patient and those of all other patients, and to design a technique for the generation of nonlinear primitive of block cipher. The remaining study is arranged as follows: Section 2 presents our main contribution; Section 3 describes attacks on existing confusion component designs; Section 4 explains the proposed scheme; Section 5 presents the results and its evaluation; and Section 6 presents the application of the proposed dynamic confusion components in image encryption technique.

2. Contribution

The main contribution of this research is as follows:

(a) A novel method is proposed, to generate true random bits from the psychological perception of schizophrenic patients. As test, one million true random bits are assessed through the NIST statistical test suite, and the results proved that the psychological perception of schizophrenic patients is outstanding source of true randomness.

(b) Instead of algebraic structures and chaotic systems, our technique relies on inevitable natural randomness, which are existing in EEG of schizophrenic patients for the design of confusion component, and as a result, attacks of algebraic- and chaos-based techniques are not applicable and irrelevant for our proposed technique.

(c) To the best of our knowledge, this nature of research is performed for the first time, in which psychiatric disorder is utilized for the design of any block cipher primitive.

(d) This research opens up new avenues in cryptographic primitive design through the fusion of computing, neuroscience, and mathematic.

(e) As the application of our proposed dynamic confusion components, an image cipher based on confusion-diffusion principal is also developed and

the resultant encrypted images are examined through various security analyses and statistical tests. All the results of these tests are passed, and it also confirms that the proposed confusion components are competent enough for the image cipher.

3. Attacks on Confusion Component Design Schemes

As mentioned earlier, chaos- and algebraic-based techniques are extensively used to design the confusion component. Chaos- and algebraic-based techniques provide favorable features for the design of confusion components; however, researchers have also identified various cryptanalysis on these techniques including interpolation attacks [9–12], Gröbner basis attack [13–19], SAT solver [20–27], linear and differential attacks [28–42], XL attacks [43–45], and XSL attack [9, 46–55]. Similarly, chaos-based techniques are also commonly applied in the designs of confusion components [56–68], dynamical degradation of chaotic systems [69–73], predictability [74–85], discontinuity in chaotic sequences [70, 86–90], small number of control parameters [76, 77, 91, 92], finite precision effect [70–72, 86, 88], and short quantity of randomness [71, 72, 86, 88–90, 93–96].

On the other side, a lot of researchers endorse the true random numbers for cryptography due to the purpose that true random numbers are unpredictable, unreproducible, and irreversible, even if their inner structure and past responses are known to the adversary. [1–8]. Our proposed technique extracts true random bits, from the readings of patient's electrode scalp sites (Fz, FCz, Cz, FC3, FC4, C3, C4, CP3, CP4) during the sensory task.

4. Proposed Design

The proposed technique has two phases: true random bits extraction and dynamic generation of confusion components. The system architecture diagram is depicted in Figure 1 and the whole design is explained in the following phases.

Phase 1. True random bits extraction

(a) Acquire EEG readings from the basic sensory button press task

The dataset that is used in this research was obtained from Refs. [97, 98], and for this, forty-nine schizophrenia patients were selected by professional and clinical psychologists after the initial screening of schizophrenia symptoms. Symptoms of the schizophrenia are assessed through three standardized psychological instruments: Scale for Negative Symptoms (SANS), Scale for Positive Symptoms (SAPS), and Positive and Negative Syndrome Scale (PANSS). The age range of the schizophrenia patients is 20 to 60 ($\mu = 42.82$, $\sigma = 13.12$) years, and different subtypes of schizophrenic patients included such as residual schizophrenia, paranoid schizophrenia, undifferentiated schizophrenia, schizophrenia unknown subtype, schizoaffective disorder, and disorganized schizophrenia. Event-related potential (ERP) averages of nine electrode scalp sites (Fz, FCz, Cz, FC3, FC4, C3, C4, CP3, CP4) are obtained, and readings of the electroencephalography are continuously digitalized at 1024 Hz. The topological positions of the 64-channel, active-electrode layout is illustrated in Figure 2 [98]. The sensory task given to the participants consisted of a button press at every 1–2 seconds, to deliver 1000 Hz, 80 dB sound pressure level, and tones with zero delay between press and tone onset. The task was stopped after 100 tones had been delivered.

(b) Difference calculation between each electrode reading of one patient and each electrode reading of all other patients

Each reading of the 1st channel is subtracted, from the 1st channel reading, of all other patients. Similarly, each reading of the 2nd channel is subtracted, from the 2nd channel reading of all other patients. Subtracted readings of every channel are stored individually in vector data structure and then parsed into binary format. This process is repeated over the readings of 64 channels and 4900 vectors generated. As test, one million of these binary bits are assessed through the NIST statistical test suite, and the results of Table 1 proved that the psychological perception of schizophrenic patients is a good source of true randomness.

(c) True Random Bits Fusion

The output of the last step is fused through the proposed DIFFERENCE_FUSION () algorithm, which is attached in annexed (Figure S1). A visual representation of the algorithm is depicted in Figure 3. This algorithm takes true random bits in the multiple of four vectors and then traverse in a specific order based on z-ordering. If the value of quadrant NW is 0, then retrieve bits from left to right, and if the value of quadrant NW is 1, then retrieve bits from right to left. Two variations of the z-ordering scheme are implemented here: the first is local *z,* which operates on 2×2 bits, and the second is global *z,* which operates on 2×2 local *z*.

Phase 2. Dynamic generation of confusion components

(a) Difference-based Two-Dimensional Map Generation (D2DMG)

Vectors of the last step are passed as parameters to the D2DMG() algorithm for the generation of two-dimensional maps. Visual representation of the algorithm is depicted in Figure 4, and the D2DMG() algorithm is attached in annexed (Figure S2).

(b) Dynamic Confusion Component Generator (DCCG)

Pairwise randomly traverse all vectors from Phase 1 and then assign arbitrary indexes. Arbitrary indexes are produced simply by applying the module 3 operation on every byte of the vector. Here, arbitrary indexes work as indexes of the vector elements. To get the values of the confusion component, parameters (pair of vectors with their arbitrary index and map

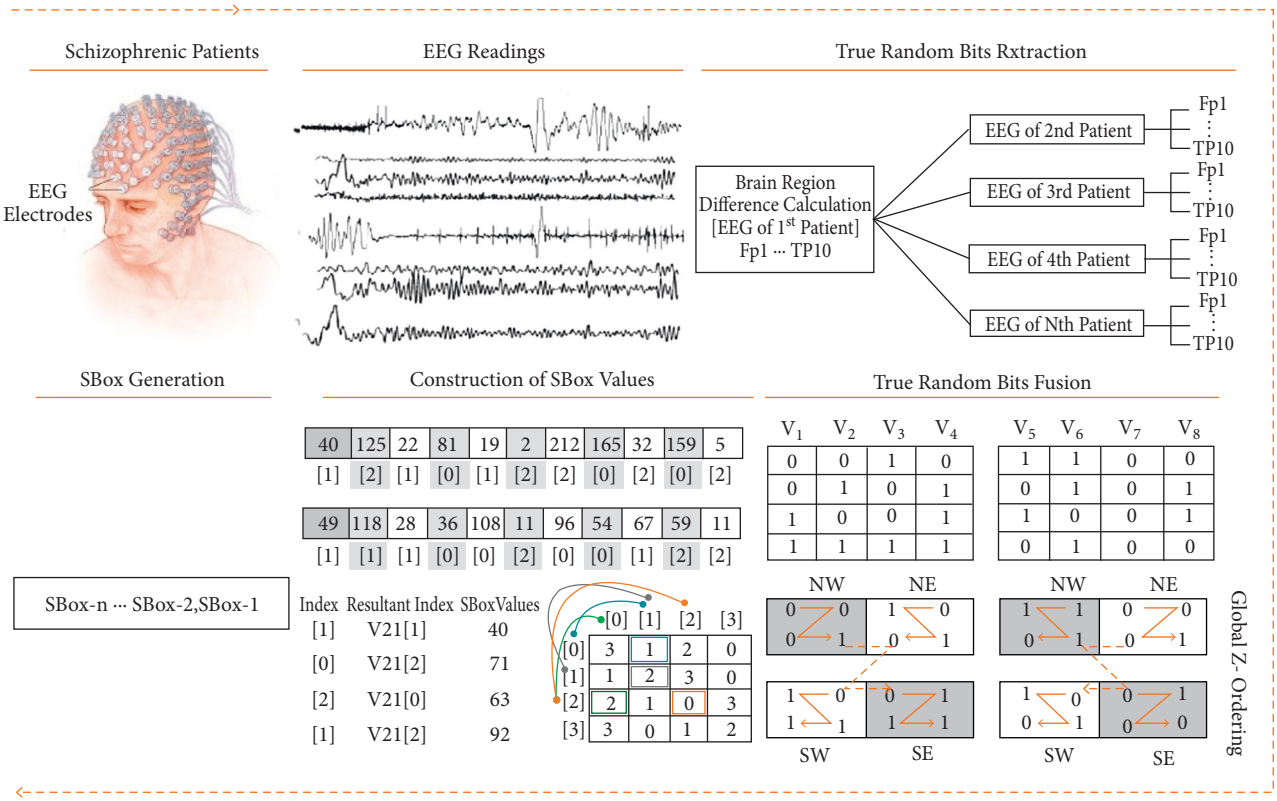

Figure 1: Proposed system design.

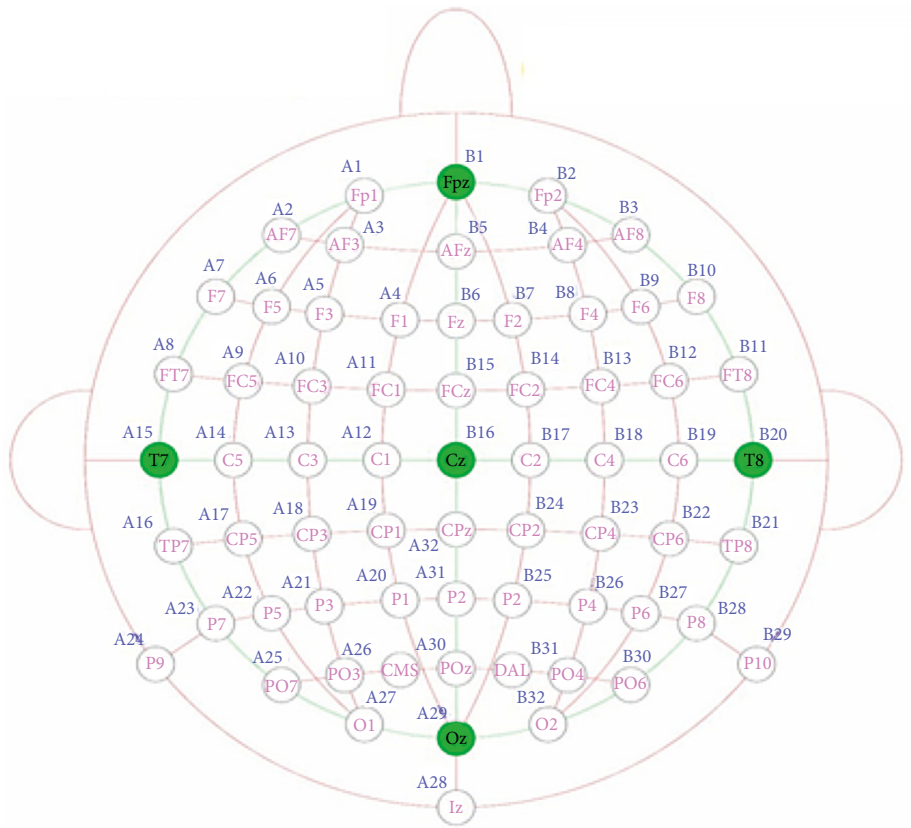

Figure 2: 64-channel active-electrode layout.

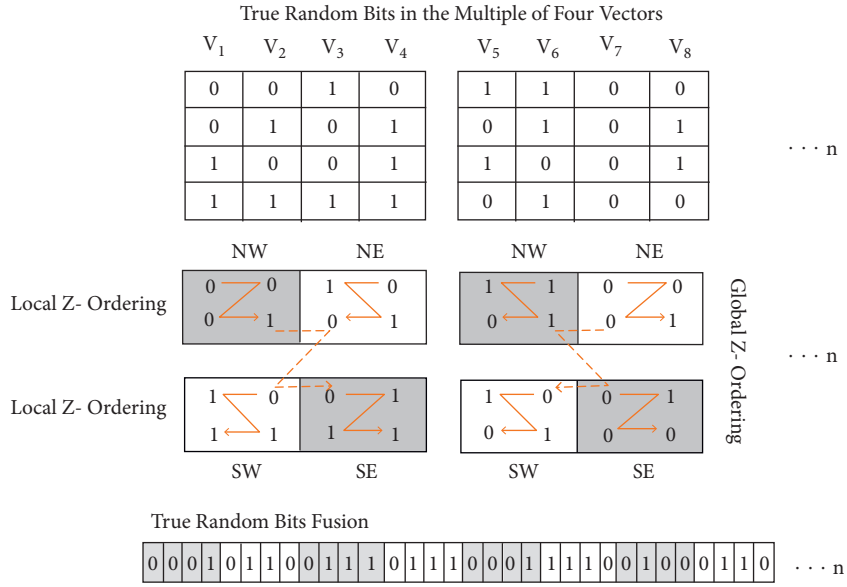

Figure 3: True random bits fusion.

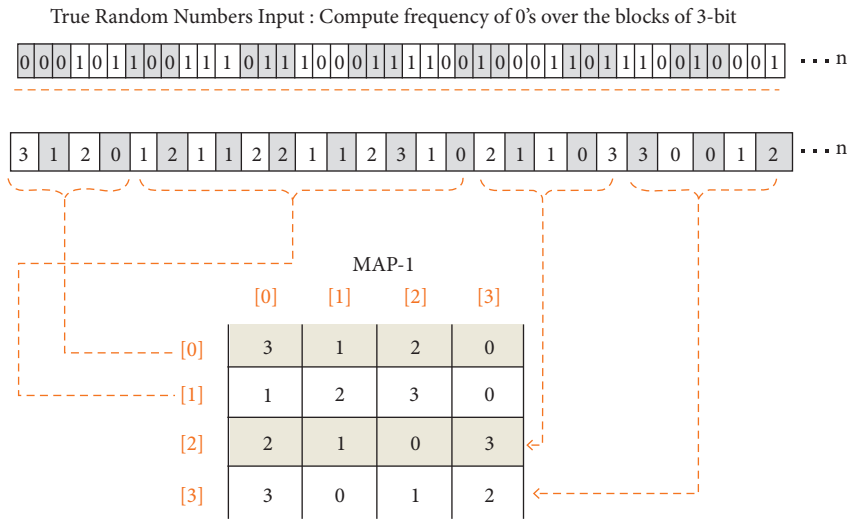

Figure 4: Difference-based two-dimensional map generation.

with its index) are passed to the ConfusionValuesGenerator() algorithm. ConfusionValuesGenerator algorithm is attached in annexed (Figure S3), and the visual representation of the algorithm is depicted in Figure 5. Due to the pure randomized nature, on every call, this algorithm returns 0 to 8 values. Resultant stream of the ConfusionValuesGenerator( ) algorithm was passed to the DCCG() algorithm for the generation of dynamic confusion components. The DCCG algorithm returns dynamic confusion components depending upon the size of stream; the DCCG algorithm is attached in annexed (Figure S4). From the results, six confusion components are randomly picked as samples, and first randomly picked confusion component and its inverse is shown in Tables 2 and 3 respectively, and the remaining five confusion components are shown in annexed (Table S1). The reverse S-box algorithm is shown in Algorithm 1.

5. Results Evaluation

In this section, sample confusion components of Section 4 are evaluated through the standard confusion component evaluation criteria [32–44], which includes bit independence criterion(BIC), linear approximation probability (LP), strict avalanche criterion (SAC), nonlinearity score, and differential approximation probability (DP).

5.1. Nonlinearity. Nonlinearity is one of the most important confusion component properties, which indicates the resistance ability of confusion components against the linear attacks, and the nonlinearity of cipher is expressed by the nonlinearity score. It is known as the smallest distance of

Table 1: NIST statistical tests of SP-800-22.

Type of test		*P*-value
Frequency test (monobit)		0.64785502
Frequency test within a block		0.673576240
Run test		0.170731649
Longest run of ones in a block		0.875317043
Binary matrix rank		0.285809935
Discrete Fourier transform (spectral)		0.465626931
Nonoverlapping template matching		0.879441943
Cumulative sums (reverse)		0.896802069
Cumulative sums (forward)		0.631657291
Overlapping template matching		0.687280196
Serial test		0.625578760
Linear complexity		0.185625430
Random excursions variant		
State	Chi-squared	*P*-value
−4	2.693559056	0.747103374
−3	4.472941176	0.483511959
−2	2.645606391	0.754424291
−1	8.647058824	0.123997312
1	12.29411765	0.030972537
2	1.730573711	0.885025702
3	3.344094118	0.647097954
4	3.152387486	0.676505457
Random excursions variant test		
State	Counts	*P*-value
−9	2	0.532681604
−8	5	0.595163147
−7	7	0.634322683
−6	7	0.605094946
−5	7	0.567551017
−4	6	0.475830847
−3	5	0.357385716
−2	8	0.372857936
−1	9	0.170066961
1	21	0.492716677
2	16	0.921126555
3	17	1
4	16	0.948317021
5	17	1
6	27	0.605094946
7	39	0.295361031
8	46	0.19909242
9	50	0.169870808

Boolean function from the set of affine functions. The nonlinearity score is the total number of bits altered to get the nearest affine function in the Boolean truth table. To calculate the nonlinearity score, the distance of all affine functions and Boolean function is determined. When the initial distance is calculated, the nearest affine function is achieved by changing the amount of bit values in the Boolean function's truth table. The Walsh spectrum defines the nonlinearity of a Boolean function by using the following formula:

$$N_g = 2^{n-1}\left(1 - 2^{-n} \max_{\varphi \varepsilon \mathrm{GF}(2^n)} |S(g)(\varphi)|\right), \tag{1}$$

where $S_{(g)}(\varphi)$ is defined as

```
in: 2D array of integers, sbox [16, 16];
out: 2D array of integers, ReverseSbox [16, 16];
(1) ReverseSbox ⟶ |16||16|
(2) for row ⟶ 0 ... (16) do
(3)       for col ⟶ 0 ... (16) do
(4)          rowIS ⟶ sbox row,col div 16
(5)          colIS ⟶ sbox row,col mod 16
(6)          value ⟶ row ∗ 16 + col
(7)             ReverseSbox rowIS, colIS ⟶ value
(8)       end for
(9) end for
(10) return ReverseSbox
```

Algorithm 1: Reverse S-box (S-box).

$$S_{(g)}(\varphi) = \sum_{\varphi \in \mathrm{GF}(2^n)} (-1)^{g(x) \oplus x.\varphi}, \tag{2}$$

where φ is a n-bit vector and $\varphi \in \mathrm{GF}(2^n)$. The dot product between x and φ is denoted as $x \cdot \varphi$:

$$x \cdot \varphi = x1 \oplus \varphi 1 + x2 \oplus \varphi 2 \cdots + xn \oplus \varphi n. \tag{3}$$

The nonlinearity score of our randomly picked confusion components 1,2,3,4,5,6 is 110.50, 106.75, 106.50, 106.75, 107.50, and 107.25, respectively. In Table 4 we can see that the nonlinearity score of our proposed confusion components is higher or equal from the state-of-the-art techniques(year 2020 to 2021).

5.2. Strict Avalanche Criteria (SAC). SAC specify that all the output bits will be modified with 1/2 probability by flipping a bit of input. SAC analyze the impact of avalanche effects in encryption. The change in the input generates a number of changes in the output. Having an even output pattern prevents linear attacks. Therefore, the changes in the output bits must be independent. SAC counts the number of changed output bits caused by complementing a single bit of input. All output bits will deviate with the probability of one half for an algorithm to be more secure. To test the SAC of the confusion component, we used the dependency matrix. S-box fulfils the SAC property, if all the elements and mean value in the dependency matrix are approximately equal to 0.5. The offsets of the dependence matrix are calculated by the following formula:

$$S(g) = \frac{1}{n^2} \sum_{1 \le r \le n} \sum_{1 \le w \le n} \left| \frac{1}{2} - Qr, w(g) \right|, \tag{4}$$

where

$$Qr, \quad w(g) = 2^{-n} \sum_{x \varepsilon B^n} gw(x) \oplus gw(x \oplus e_r), \tag{5}$$

$e_r = [\theta r, 1\theta r, 2 \ldots \theta r, n]^T$ is the transpose of matrix $\theta_{r,w} = 0, r \neq w$ Or $\theta_{r,w}\theta_{r,w} = 1, r = w$

The SAC (average) score of our randomly picked six confusion components (1,2,3,4,5,6) is 0.498779, 0.500244, 0.503662, 0.497314, 0.500732, and 0.508545, respectively.

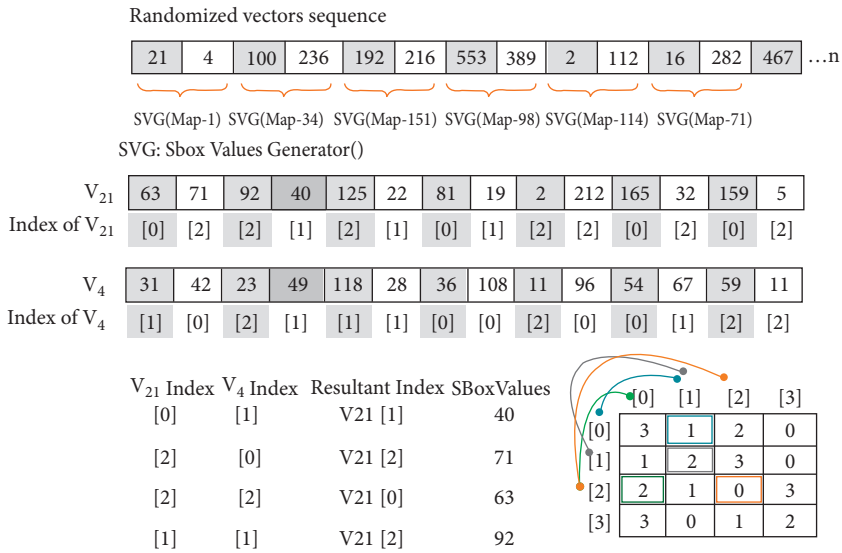

Figure 5: Confusion value generator.

Table 2: Proposed confusion component-1.

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

Table 3: Inverse of confusion component-1.

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

These results proved that our proposed confusion components are enough capable. The SAC result of confusion component-1 presented in Table 5 is the sample

5.3. BIT Independent Criterion (BIC). BIC is used to analyze the output bits behavior by changing the input bits. Confusion component holds the BIC property when output bits behave independently from each other. BIC characteristic states that output bits j and k will modify individually if any single input bit i is reversed. This will improve the proficiency of confusion function. The independence between pair of avalanche variables is measured through the coefficient of correlation. The bit independence of the j^{th} and k^{th} bits of B^{ei} is

$$\text{BIC}\left(b_j, b_k\right) = \max_{1\le i\le n}\left|\text{corr}\left(b_j^{ei}, b_j^{ei}\right)\right|. \tag{6}$$

Shannon's confusion function(C) is represented as C: {0, 1}^{n} ⟶{0, 1}^{n}. BIC parameter for Shannon's confusion function is measured by the given mathematical expression:

$$\text{BIC}\,(C) = \max_{1\le j,k\le n} \text{BIC}\left(b_j, b_k\right). \tag{7}$$

The shift in output bits is an important parameter for determining the strength of the encryption process. The average BIC score of our randomly picked confusion components from 1 to 6 is 0.50105, 0.50272, 0.50112, 0.50223, 0.50105, and 0.50105, respectively. These results proved that our proposed confusion components strongly fulfill the bit independent criteria. The SAC-BIC results of confusion component-1 presented in Table 6 are the sample.

5.4. Linear Approximation Probability (LP). LP is another important criteria for evaluating Shannon's confusion component. LP is the function's capability to avoid linear attacks and is the highest value of the disparity of an event. The input bit's parity selected by the mask γ^1 and the output bit's parity selected by the γ^2 mask are equal. The masks of input and output bits are evaluated to obtain the imbalance of an event. Linear approximation probability is measured by the following mathematical expression:

$$\text{LP}_f = \max_{\gamma 1,\gamma 2\neq 0}\left|\frac{\{x\varepsilon X \mid x\cdot\gamma 1 = S(x).\gamma 2\}}{2^n} - \frac{1}{2}\right|, \tag{8}$$

where γ^1 represents the input mask and γ^2 represents the output mask in the above equation. X represents the set of all possible inputs, and 2^n is the total number of elements in the confusion component. The maximum LP score of our confusion components(1 to 6) is 0.1171875,0.1328125,0.12500, 0.1328125, 0.140625, and 0.140625, respectively; these results also fulfills the LP criteria.

5.5. Differential Approximation Probability (DP). DP characteristic examines the XOR distribution among the input and output bits. In order to be resilient against the differential attacks, the XOR values of all outputs must have equal probability with the XOR values of all inputs. In the differential approximation table, the probability of all the XOR values of input and the probability of all XOR values of output are equal. The exclusive-or distribution among the inputs and outputs of S-box is calculated by

$$\text{DP}\ (\Delta w \longrightarrow \Delta z) = \left[\frac{\#\{w\varepsilon X \mid S(w)\oplus S(w\oplus\Delta w) = \Delta z\}}{2^i}\right]. \tag{9}$$

Here X represents the set of all possible input values and 2^i represents cardinality of set. The maximum DP score of our confusion components (1 to 6) is 0.046875, 0.046875, 0.046875, 0.054688, 0.039062, and 0.054688, respectively; here, we can see that these results also fulfills the DP criteria. As a sample, the DP results of the confusion component-1 are presented in Table 7.

Table 4: Nonlinearity of state-of-the-art techniques.

State-of-the-art confusion components	Nonlinearity score gained
[99], 2021	106.25
[101], 2021	106.5
[103], 2021	102.25
[105], 2020	106.5
[107], 2020	106.87
[109], 2020	104.25
[111], 2020	102.50
[113], 2020	106.25
[115], 2020	105.5
[117], 2021	106.75
[114], 2020	103.5
[118], 2020	106.5
[119], 2020	106.3
[121], 2021	104.0
[122], 2021	108.5
[100], 2021	109.75
[102], 2021	106.5
[104], 2021	105.5
[106], 2021	107.0
[108], 2020	105.25
[110], 2020	100.5
[112], 2020	104.0
[114], 2020	103.5
[116], 2020	105.0
[118], 2020	106.5
[111], 2020	102.5
[109], 2020	104.25
[120], 2020	101.75
[121], 2021	104.0
[123], 2021	105.25

6. Application of Proposed Dynamic Confusion Components in Image Encryption

As the application of our proposed dynamic confusion components, an image cipher based on confusion-diffusion principal is developed, which is depicted in Figure 6. The structure of the mage cipher is depicted in Figure 6. It consists of repeating rounds of dynamic confusion layers, static diffusion layer, and the key addition, which make them

Table 5: SAC of confusion component-1.

0.453125	0.500000	0.500000	0.531250	0.515625	0.500000	0.484375	0.500000
0.453125	0.562500	0.515625	0.515625	0.500000	0.468750	0.484375	0.453125
0.531250	0.515625	0.515625	0.468750	0.515625	0.500000	0.500000	0.515625
0.515625	0.468750	0.500000	0.468750	0.500000	0.500000	0.531250	0.515625
0.546875	0.515625	0.500000	0.468750	0.468750	0.546875	0.500000	0.453125
0.531250	0.515625	0.484375	0.578125	0.468750	0.515625	0.546875	0.468750
0.437500	0.515625	0.468750	0.484375	0.515625	0.500000	0.515625	0.484375
0.500000	0.406250	0.484375	0.515625	0.484375	0.500000	0.500000	0.500000

Table 6: SAC of BIC.

—	0.490234	0.505859	0.501953	0.513672	0.509766	0.507812	0.498047
0.490234	—	0.503906	0.513672	0.486328	0.494141	0.488281	0.480469
0.505859	0.503906	—	0.488281	0.503906	0.513672	0.513672	0.527344
0.501953	0.513672	0.488281	—	0.507812	0.490234	0.503906	0.513672
0.513672	0.486328	0.503906	0.507812	—	0.513672	0.480469	0.501953
0.509766	0.494141	0.513672	0.490234	0.513672	—	0.474609	0.470703
0.507812	0.488281	0.513672	0.503906	0.480469	0.474609	—	0.531250
0.498047	0.480469	0.527344	0.513672	0.501953	0.470703	0.531250	—

Table 7: DP of the confusion component-1.

.00000	.02344	.03125	.02344	.02344	.03125	.02344	.02344	.03125	.02344	.02344	.02344	.02344	.02344	.02344	.02344
.02344	.03125	.02344	.03125	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.03125	.03125	.03125	.03125	.03125
.02344	.02344	.02344	.02344	.02344	.02344	.03125	.02344	.03125	.02344	.02344	.01562	.03125	.02344	.02344	.01562
.02344	.02344	.02344	.02344	.02344	.03125	.03125	.03125	.02344	.03125	.03125	.02344	.02344	.02344	.02344	.03125
.02344	.03125	.03125	.03125	.02344	.02344	.02344	.02344	.02344	.03125	.02344	.03125	.02344	.02344	.02344	.03125
.02344	.03906	.03125	.02344	.02344	.03125	.03125	.02344	.02344	.03125	.02344	.02344	.03125	.02344	.03125	.03125
.03125	.03125	.02344	.02344	.02344	.03125	.03906	.02344	.03125	.02344	.03125	.02344	.03125	.02344	.04687	.03125
.02344	.03125	.02344	.02344	.02344	.02344	.02344	.02344	.03125	.03125	.03125	.02344	.02344	.03125	.01562	.02344
.03125	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.01562	.02344	.02344	.02344	.03125	.02344
.02344	.02344	.02344	.02344	.02344	.02344	.02344	.03125	.02344	.02344	.03125	.02344	.02344	.03125	.02344	.02344
.02344	.03125	.03125	.02344	.03125	.02344	.03125	.02344	.03125	.02344	.03125	.02344	.02344	.02344	.02344	.03125
.02344	.02344	.01562	.02344	.02344	.03125	.02344	.02344	.02344	.02344	.03125	.02344	.02344	.03125	.01562	.03125
.02344	.02344	.02344	.02344	.02344	.02344	.02344	.02344	.03906	.03125	.03125	.03906	.03906	.03125	.02344	.02344
.03125	.02344	.02344	.01562	.02344	.03125	.02344	.02344	.02344	.02344	.02344	.03906	.03125	.03125	.02344	.02344
.02344	.015625	.02344	.02344	.03125	.03125	.03125	.02344	.02344	.02344	.02344	.01562	.02344	.03125	.02344	.02344
.03125	.02344	.03125	.02344	.02344	.02344	.03906	.03125	.02344	.02344	.03125	.02344	.02344	.02344	.03906	.03125

hard for cryptanalysis. For the key generation process, the chaotic interval of the logistic map and tent map is enhanced by synthesizing the parameters of both maps to obtain the increased keyspace [86]. The chaotic field of the logistic map only lies in the range between $3.57 \le \sigma \le 4$, and similarly, the chaotic field of the tent map lies in the range between $2 \le \sigma \le 4$. Logistic map and tent map are defined in (10) and (11), respectively, and their enhanced chaotification structure of logistic tent system(LTS) is defined in (12). Finally for the subkey generation, divide the resultant values of LTS into the blocks of 256 bytes. In the same way for the permutation process, apply XOR operation on the values generated from (11) and (12). These resultant values are in the range between 0 and 255. Select first 256 distinct values as permutation. We examined the encrypted images through various security analyses and statistical tests including NPCR, UACI, correlation-coefficient analysis, and 2D, 3D histogram analysis. All the results of these tests are passed; it also confirms that the proposed confusion is competent enough for the image cipher:

$$z_{n+1} = \sigma z_n (1 - z_n), \quad 0 < \sigma \le 4;\ z_n \in [0, 1]. \tag{10}$$

$$z_{n+1} = \begin{cases} \gamma \dfrac{z_n}{2} z_i < \dfrac{1}{2}, \\ \dfrac{\gamma (1 - z_n)}{2} z_i > \dfrac{1}{2}, \end{cases} \quad 0 < \sigma \le 4;\ z_n \in [0, 1]. \tag{11}$$

$$z_{n+1} = \begin{cases} (\sigma z_n (1 - z_n) + (4 - \sigma) z_n / 2) \bmod 255 z_i < (1/2) \\ (\sigma z_n (1 - z_n) + (4 - \sigma)(1 - z_n)/2) \bmod 255 z_i > (1/2) \end{cases}. \tag{12}$$

6.1. Resistance against Differential Analysis. The key requirement of the encryption algorithm is its ability to resist

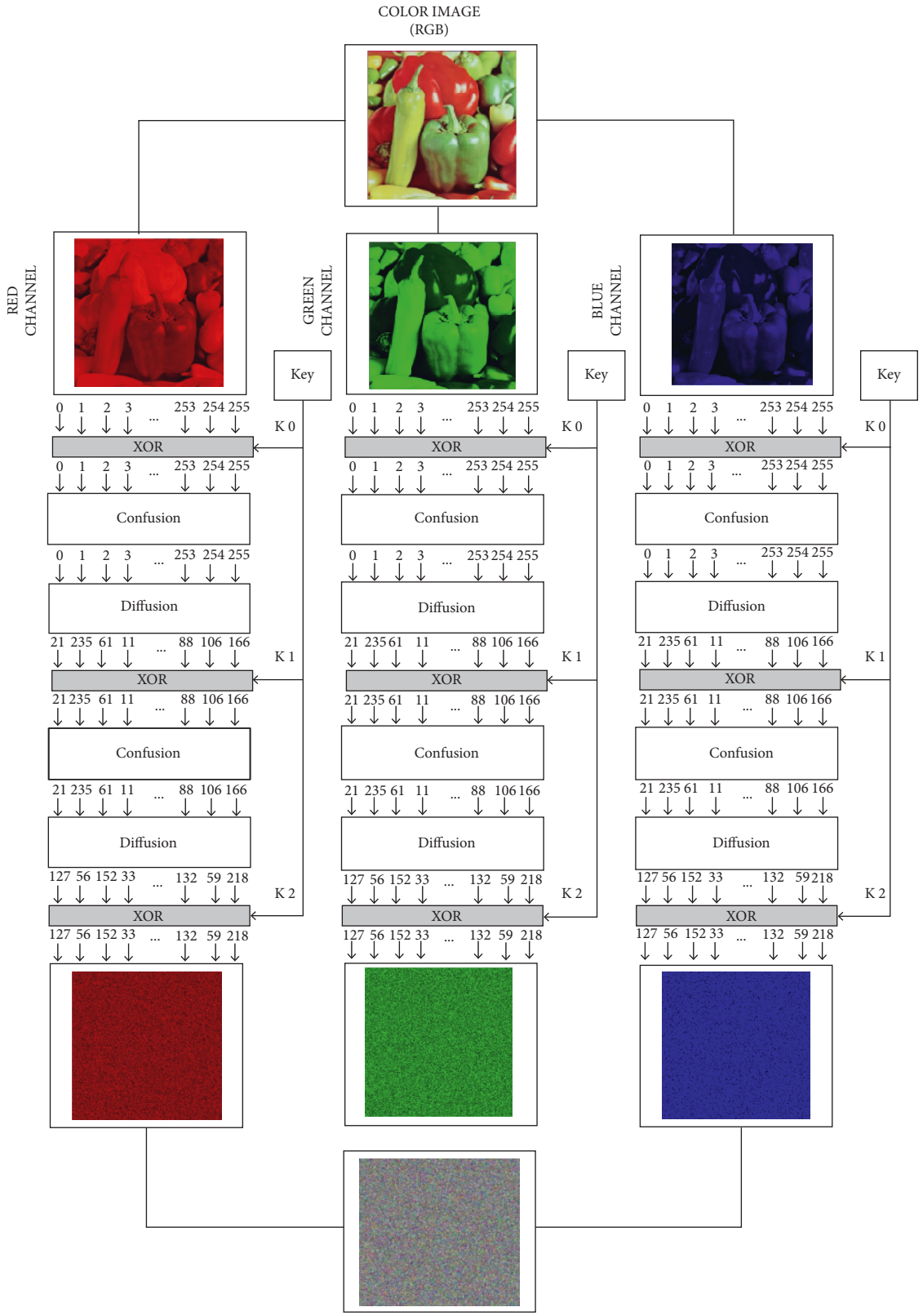

Figure 6: Confusion- and diffusion-based image cipher.

the differential attacks. Differential cryptanalysis is difficult when a small shift in original image will generate completely different ciphered image. We examined the image encryption results on various standard color test images (Lena, pepper, nature, bird, baboon, grapes, sparrow, butterfly), and here as a sample, original image pepper over the

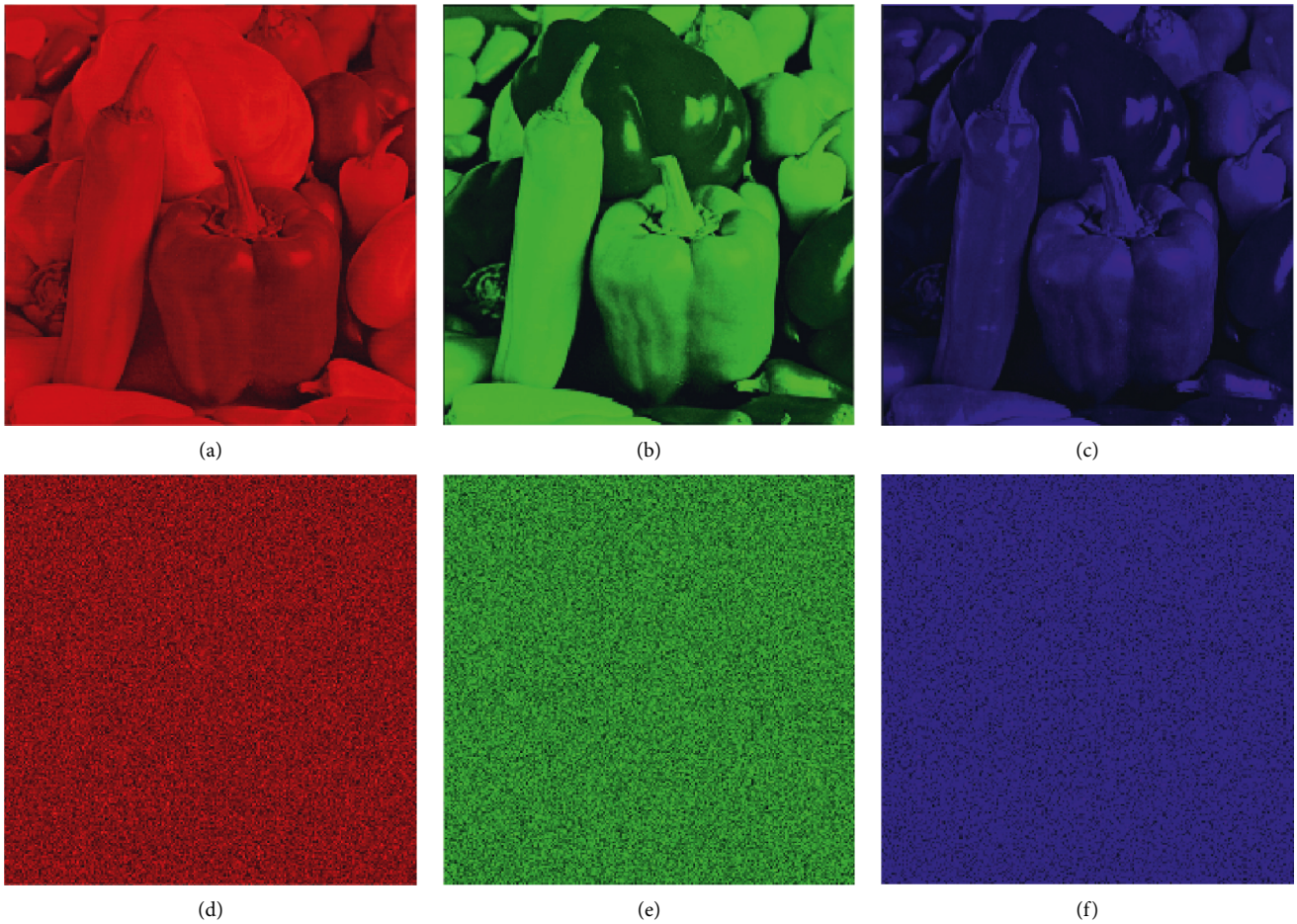

FIGURE 7: Original and encrypted test image of the pepper. (a) Before encryption(Channel:R); (b) before encryption (Channel:G); (c) before encryption (Channel:B); (d) after encryption(Channel:R); (e) after encryption (Channel:G); (f) after encryption (Channel:B).

RGB channels is shown in Figures 7(a)–7(c) and their correspondent cipher pictures are presented in Figures 7(d), 7(e), and 7(f). The NPCR and UACI are the two frequently used tests of the image cipher to check the strength against the differential attacks. NPCR is defined as follows [124, 125]:

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%. \tag{13}$$

$D_{(i,j)}$ is described as $D_{(i,j)} = 0$ if $I(i,j) = J(i,j)$, $D_{(i,j)} = 1$ if $I(i,j) = J(i,j)$

UAIC measure the mean variation of pixel intensity of two encrypted images at same location. It is determined by

$$\text{UACI} = \frac{1}{W \times H} \times \left[\sum_{i,j} \times \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\%, \tag{14}$$

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

where $C1(i,j)$ and $C2(i,j)$ indicate the pixel value of two encrypted images at location (i,j). W represents the number of rows and H presents the number of columns of the plain image. The encryption security is improved with a large UACI value. The NPCR and UACI are measured through the following formulas:

$$\text{NPCR}_E = \left(1 - 2^{-n}\right) \times 100\%,$$

$$\text{UACI}_E = \frac{1}{2^{2n}} \frac{\sum_{i=1}^{2^n - 1} i(i+1)}{2^n - 1} \times 100\% = \frac{1}{3}\left(1 + 2^{-n}\right) \times 100\%, \tag{15}$$

where n is the number of bits used to denote the various bit planes of an image. High values of UACI and NCPR have strong resistance against differential attacks. Table 8 indicates the values of NPCR and UACI. NPCR and UACI values of our encrypted images are near to 99.63 and 336.50, respectively, which are very good results.

6.2. Correlation Coefficient Analysis. Neighbor pixels of the unencrypted images are extremely correlated and can show visual traits to the adversaries. An efficient cipher technique would reduce the correlation between adjacent pixels of an encrypted image in all the three directions. Before the encryption, the correlation coefficient value should be around 1

Table 8: NPC and UACI.

Images	Location	NPCR Proposed	UACI Proposed
Lena	R	99.6221	33.5514
	G	99.6127	33.5158
	B	99.5517	33.5212
Pepper	R	99.6231	33.4525
	G	99.6462	33.4642
	B	99.6652	33.4935
Nature	R	99.5925	33.6789
	G	99.6186	33.4987
	B	99.6245	33.6506
Bird	R	99.6621	33.4065
	G	99.6651	32.9154
	B	99.6266	32.9365
Baboon	R	99.6578	33.6534
	G	99.6256	33.6385
	B	99.6344	33.7265
Grapes	R	99.6231	33.7596
	G	99.6652	32.7821
	B	99.6632	33.5063
Sparrow	R	99.6551	33.4798
	G	99.6225	33.4125
	B	99.6432	32.9098
Butterfly	R	99.6591	33.5215
	G	99.6652	32.9952
	B	99.6063	33.0563

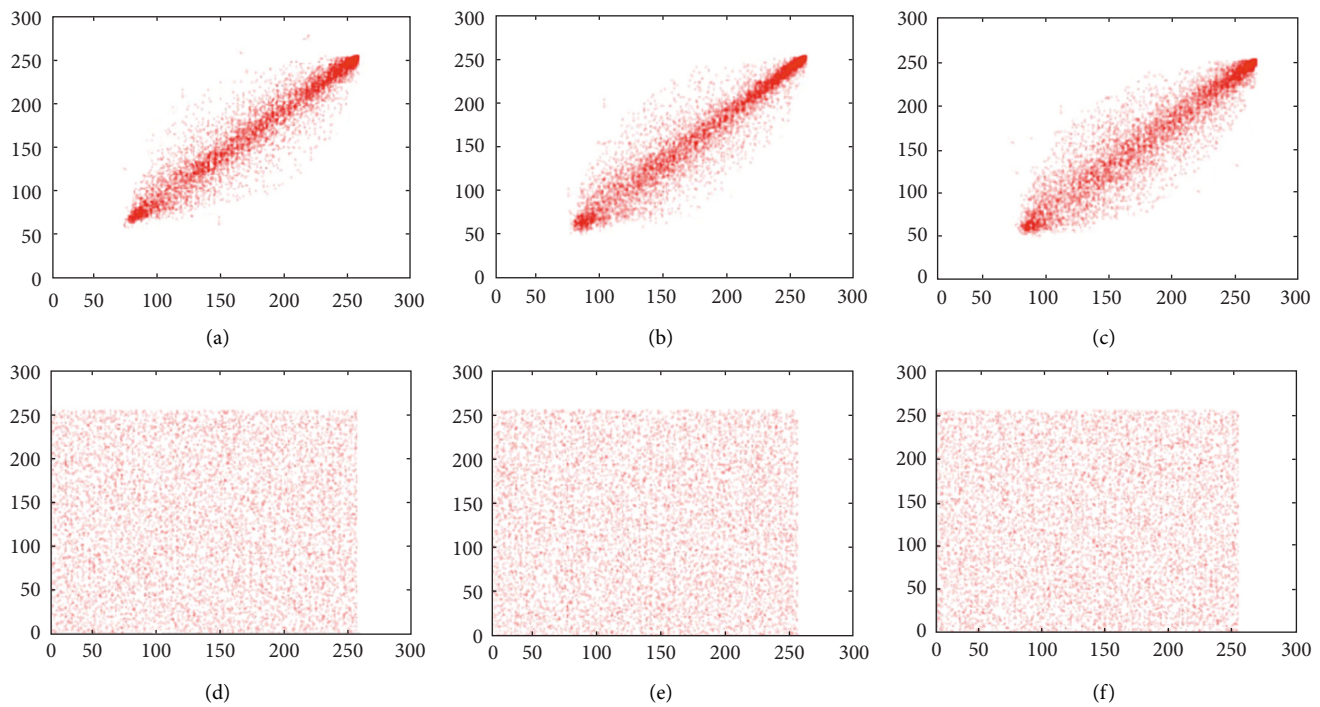

Figure 8: Scatter plots of the test image pepper over the R channel. (a) Plain image (direction: horizontal); (b) plain image (direction: vertical); (c) plain image (direction: diagonal); (d) cipher image (direction: horizontal); (e) cipher image (direction: vertical); (f) cipher image (direction: diagonal).

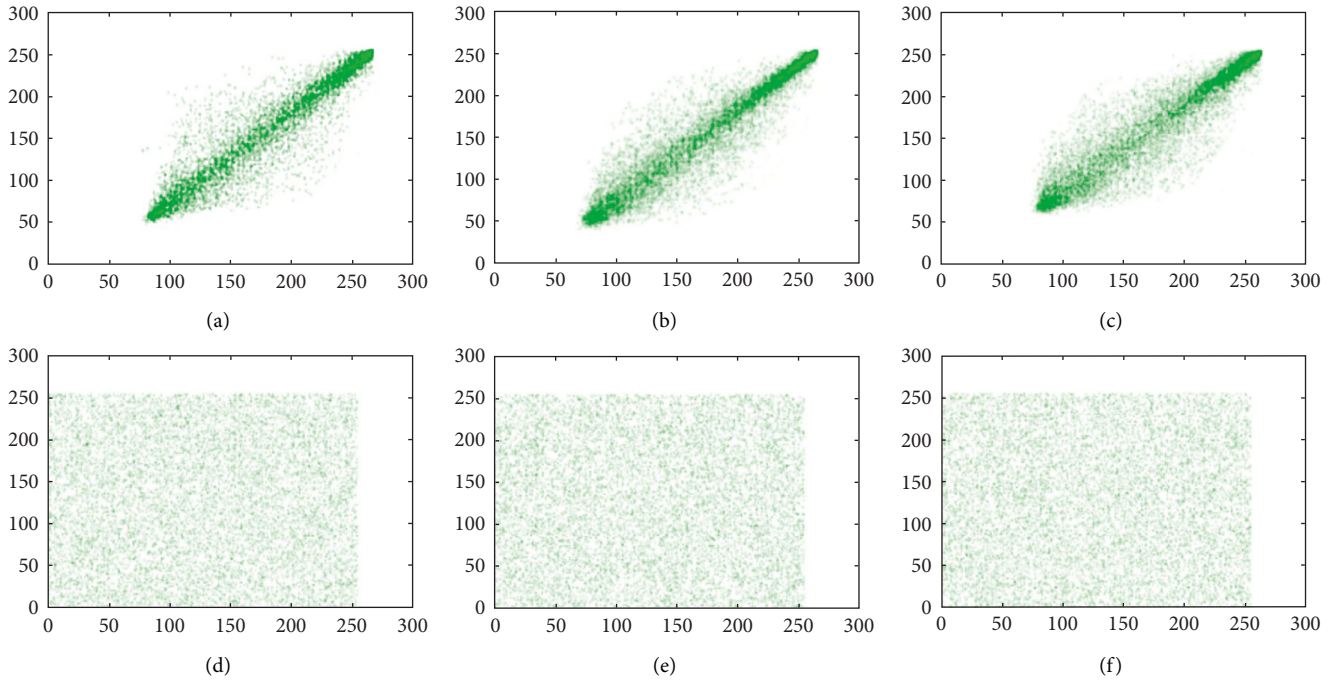

Figure 9: Scatter plots of the test image pepper over the G channel. (a) Plain image (direction: horizontal); (b) plain image (direction: vertical); (c) plain image (direction: diagonal); (d) cipher image (direction: horizontal); (e) cipher image (direction: vertical); (f) cipher image (direction: diagonal).

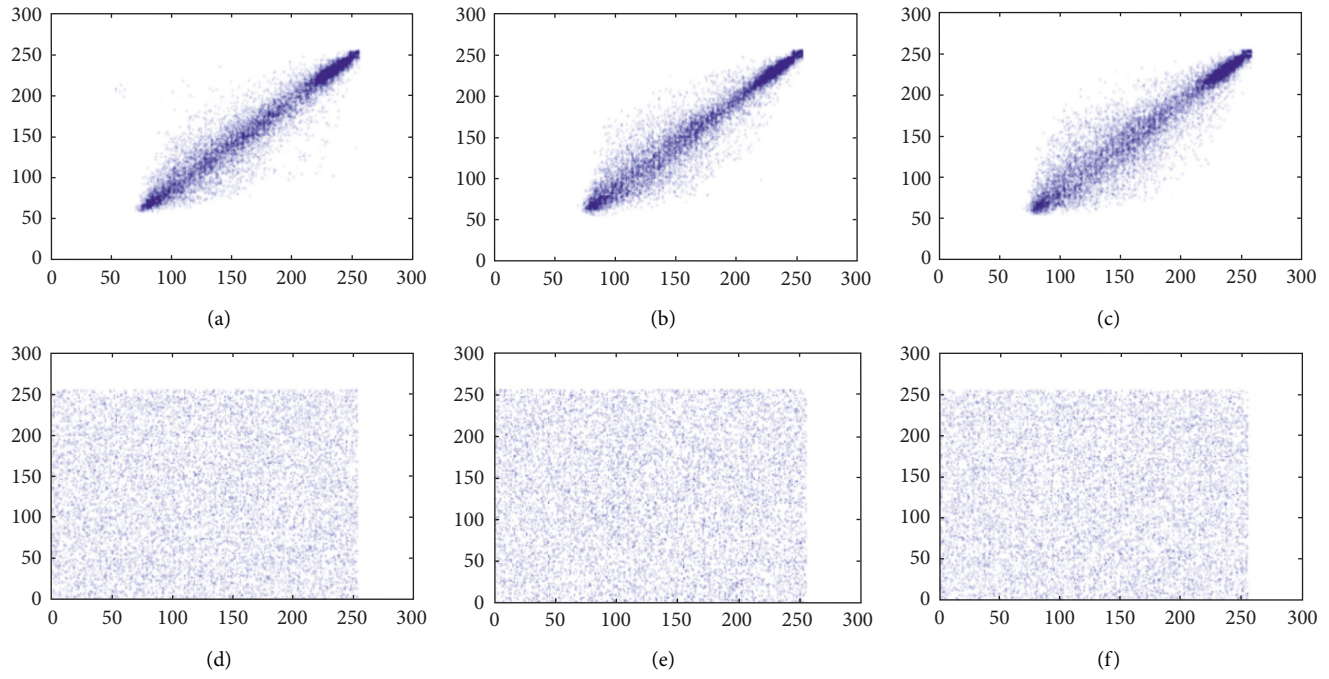

Figure 10: Scatter plots of the test image pepper over the B channel. (a) Plain image (direction: horizontal); (b) plain image (direction: vertical); (c) plain image (direction: diagonal); (d) cipher image (direction: horizontal); (e) cipher image (direction: vertical); (f) cipher image (direction: diagonal).

Table 9: Correlation analysis of the adjacent pixels.

Images	Location	Horizontal		Vertical		Diagonal	
		Plain	Encrypted	Plain	Encrypted	Plain	Encrypted
Lena	R	.9302	−.000005	.9806	.00011	.9306	.000071
	G	.9426	−.000462	.9752	−.00005	.9360	−.000051
	B	.9061	.000012	.9503	.00078	.8803	.000077
Pepper	R	.9252	.000021	.9303	.00026	.8745	.000048
	G	.9566	−.000295	.9806	−.00008	.9363	−.000065
	B	.9312	.000212	.9308	.00015	.8896	.00023
Nature	R	.9472	−.000012	.9512	.00015	.9101	−.000069
	G	.8833	.000352	.9313	−.00012	.8693	.000019
	B	.9702	.000009	.9708	−.00082	.9513	.000038
Bird	R	.9806	.000021	.9705	.00010	.9596	−.000007
	G	.9612	−.000005	.9603	.00006	.9298	.000201
	B	.9633	−.000511	.9512	.00007	.9319	−.000039
Baboon	R	.9659	−.00008	.9519	−00006	.9127	.000047
	G	.9559	.000615	.9201	−.000031	.8539	−.00078
	B	.9313	−.000018	.9499	−.00002	.9206	.000071
Grapes	R	.9836	.000051	.9826	.00005	.9568	.000068
	G	.9852	.000005	.9756	−.000031	.9627	−.000064
	B	.9788	−.000047	.9702	.00003	.9608	−0.00051
Sparrow	R	.8866	.000057	.9236	−.00004	.9906	−.000043
	G	.9503	−.000049	.8352	.00008	.9804	.000059
	B	.9306	−.000008	.7952	−.00070	.9402	.000021
Butterfly	R	.9512	−.000048	.9800	−0.0006	.8845	−.000034
	G	.8999	−.000007	.8306	.00021	.9269	.000062
	B	.8802	−.000008	.7789	.00056	.8417	.000081

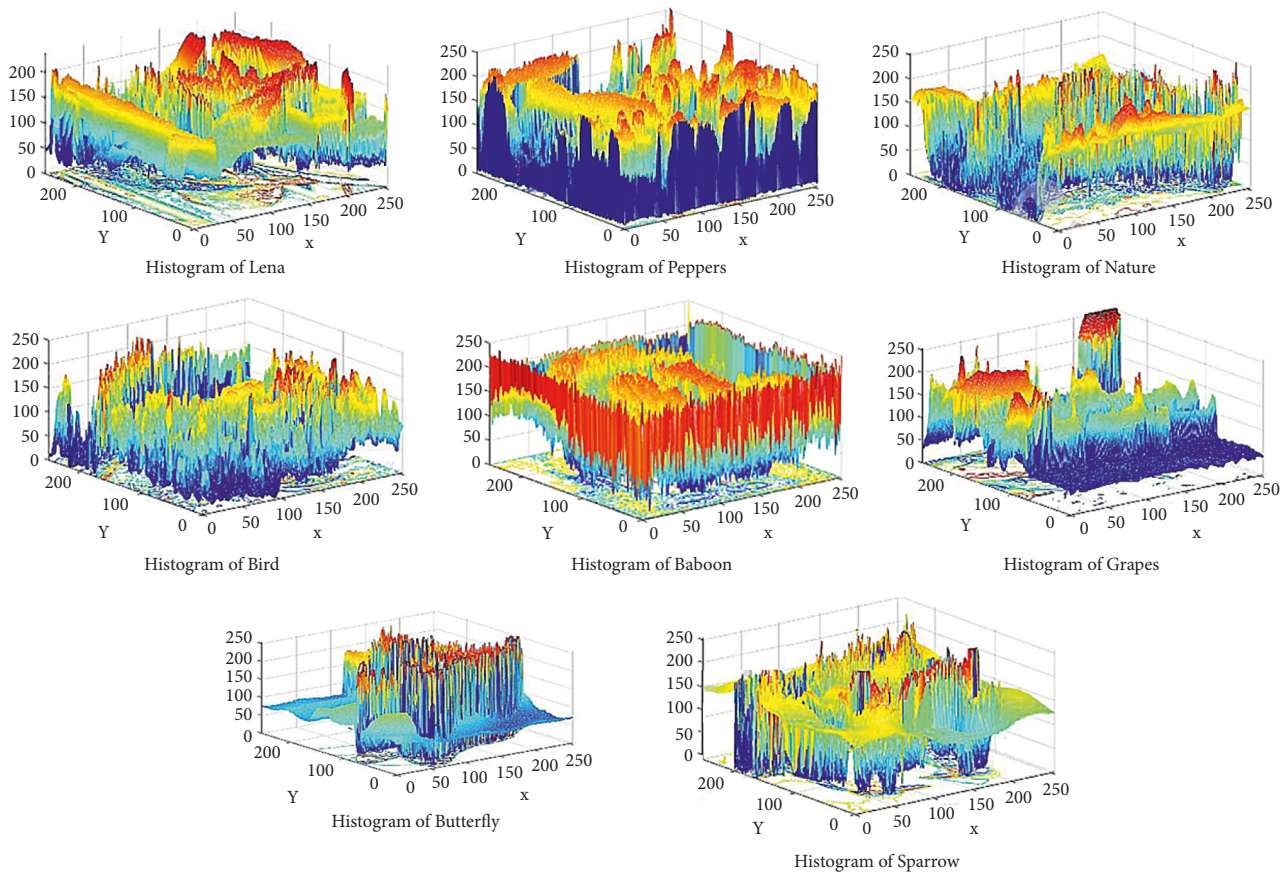

Figure 11: 3D Histogram of the original images.

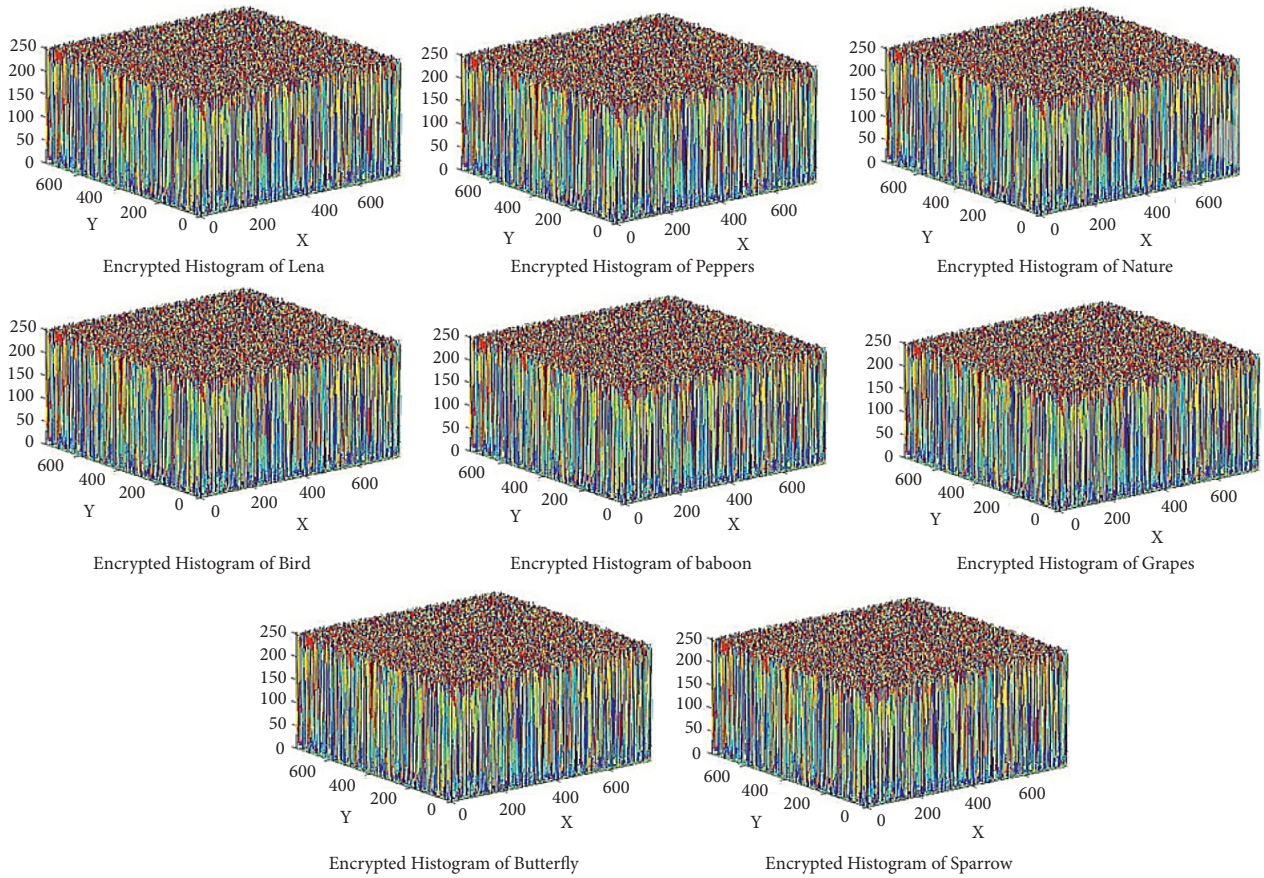

Figure 12: 3D Histogram of the encrypted images.

and after the encryption should be around 0. Adjacent pixel pairs of the test image pepper are plotted in Figures 8, 9 and 10. From the both original and encrypted images, 1000 pixels are plotted in the diagonal, horizontal, and vertical direction. Correlation coefficient among two neighboring pixels are calculated by

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right), \tag{16}$$

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

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

where x_i and y_i show the values of two adjacent pixels and N is the total number of duplets. The mean value of x_i is denoted by $E(x)$, and the mean value of y_i is denoted by $E(y)$. The calculated value of the correlation coefficient in plain images is closer to 1 along diagonal, horizontal, and vertical directions, whereas the value of correlation coefficient in encrypted image is closer to 0. We can see that the values of the correlation coefficient over the encrypted images are totally different from the values of plain images, so the correlation coefficient attack fails to provide any clue of the original image. The results of the correlation coefficient analysis on horizontal, vertical, and diagonal directions are displayed in Table 9.

6.3. Histogram Analysis. The histogram is the graphical representation of the distribution of pixels in the picture by measuring a number of pixels at each intensity level. Analyzing the histogram shows how pixels are distributed over encrypted image. Effective cipher encrypts the original image into the cipher image, which contains random RGB pixel. In Figure 11, we can see that 3D histogram of the standard test images shows some information, but in Figure 12, encrypted test images have uniformly random pixel values. The histogram of the encrypted and original images are completely different, so the attacker cannot extract any relation between encrypted image and plain image.

7. Conclusion

Randomness is a fundamental feature in nature and a valuable resource for the cryptography. First time, this nature of research is performed in which psychiatric disorder is utilized for the generation of truly random bits, and based on these

true random bits, confusion components are constructed. Instead of algebraic- and chaotic-based approaches, our technique relies on inevitable natural randomness, which exists in the EEG of schizophrenic patients, and as a result, attacks of chaos- and algebraic-based techniques are bypassed in our proposed approach. For the evaluation of the true random bits, NIST statistical test suite was adopted, and for the evaluation of the confusion component, standard evaluation criteria were adopted. As a test case, one million true random bits are assessed through the NIST statistical test suite, and the results proved that the psychological perception of schizophrenic patients is a good source of true randomness. Confusion components are evaluated through SAC, LP, DP, BIC, and nonlinearity. The outcomes of these criteria verified that the proposed confusion component is effective for block ciphers. We will expand this research in future, for the dynamic generation of lattice primitives [70].

Data Availability

The datasets "EEG data from basic sensory task in Schizophrenia," which analyzed during the current study are available in the Kaggle repository at https://www.kaggle.com/datasets/broach/button-tone-sz.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

The authors extend their gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through research groups program under grant number R. G. P. 2/109/43. The author would like to thank Brain Roach and Dr. Ford for sharing their EEG dataset. The initial data collection was supported by the National Institute of Mental Health.

Supplementary Materials

Figure S1: DIFFERENCE_FUSION() algorithm. Figure S2: D2DMG() algorithm. Figure S3: CONFUSIONVALUES_GENERATOR() algorithm. Figure S4: DCCG() algorithm. Table S1: confusion components. . (*Supplementary Materials*)

References

[1] S. Pironio, A. Acín, S. Massar et al., "Random numbers certified by Bell's theorem," *Nature*, vol. 464, no. 7291, pp. 1021–1024, 2010.

[2] R. Bernardo-Gavito, I. E. Bagci, J. Roberts et al., "Extracting random numbers from quantum tunnelling through a single diode," *Scientific Reports*, vol. 7, no. 1, Article ID 17879, 2017.

[3] B. Sunar, W. Martin, and D. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *IEEE Transactions on Computers*, vol. 56, no. 1, pp. 109–119, 2007.

[4] B. Ray and A. Milenkovic, "True random number generation using read noise of flash memory cells," *IEEE Transactions on Electron Devices*, vol. 65, no. 3, pp. 963–969, 2018.

[5] C. Aghamohammadi and J. P. Crutchfield, "Thermodynamics of random number generation," *Physical Review*, vol. 95, no. 6, Article ID 062139, 2017.

[6] K. Lee, S. Y. Lee, C. Seo, and K. Yim, "TRNG (True Random Number Generator) method using visible spectrum for secure communication on 5G network," *IEEE Access*, vol. 6, Article ID 12847, 2018.

[7] M. M. Abutaleb, "A novel true random number generator based on QCA nanocomputing," *Nano Communication Networks*, vol. 17, pp. 14–20, 2018.

[8] D. G. Marangon, A. Plews, M. Lucamarini et al., "Long-term test of a fast and compact quantum random number generator," *Journal of Lightwave Technology*, vol. 36, no. 17, pp. 3778–3784, 2018.

[9] A. M. Youssef and G. Gong, "On the interpolation attacks on block ciphers," in *Fast Software Encryption*, B. Schneier, Ed., vol. 1978pp. 109–120, 2001.

[10] I. Dinur, Y. Liu, W. Meier, and Q. Wang, "Optimized interpolation attacks on LowMC," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 535–560, Springer, Berlin, Heidelberg, December 2015.

[11] C. Li and B. Preneel, "Improved interpolation attacks on cryptographic primitives of low algebraic degree," in *Proceedings of the International Conference on Selected Areas in Cryptography*, pp. 171–193, Springer, Waterloo, ON, Canada, August 2019.

[12] N. T. Courtois, "The inverse S-box, non-linear polynomial relations and cryptanalysis of block ciphers," in *Proceedings of the International Conference on Advanced Encryption Standard*, pp. 170–188, Springer, Bonn, Germany, May 2004.

[13] S. Bulygin and M. Brickenstein, "Obtaining and solving systems of equations in key variables only for the small variants of AES," *Mathematics in Computer Science*, vol. 3, no. 2, pp. 185–200, 2010.

[14] J. Buchmann, A. Pyshkin, and R.-P. Weinmann, "Block ciphers sensitive to gröbner basis attacks," in *Topics in Cryptology - CT-RSA 2006*, pp. 313–331, Springer, Berlin, Heidelberg, 2006.

[15] J. Buchmann, A. Pyshkin, and R.-P. Weinmann, "A zero-dimensional gröbner basis for AES-128," in *Proceedings of the International Workshop on Fast Software Encryption*, pp. 78–88, Springer, Graz, Austria, March 2006.

[16] C. Cid and R.-P. Weinmann, "Block ciphers: algebraic cryptanalysis and gröbner bases," in *Gröbner Bases, Coding, and Cryptography*, pp. 307–327, Springer, Berlin, Heidelberg, 2009.

[17] A. Pyshkin, *Algebraic cryptanalysis of block ciphers using Gröbner Bases*, Technische Universität, Berlin, Heidelberg, Ph.D Dissertion, 2008.

[18] K. Zhao, J. Cui, and Z. Xie, "Algebraic cryptanalysis scheme of AES-256 using gröbner basis," *Journal of Electrical and Computer Engineering*, vol. 2017, Article ID 9828967, 9 pages, 2017.

[19] J.-C. Faugère, "Interactions between computer algebra (Gröbner bases) and cryptology," in *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, pp. 383-384, New York, NY, USA, July 2009.

[20] M. Gwynne and K. Oliver, *Attacking AES via SAT*, BSc Dissertation (Swansea), Ph.D Dissertion, Swansea, UK, 2010.

[21] P. Jovanovic and M. Kreuzer, "Algebraic attacks using SAT-solvers," *Groups Complexity Cryptology*, vol. 2, no. 2, pp. 247–259, 2010.

[22] A. Semenov, O. Zaikin, I. Otpuschennikov, S. Kochemazov, and A. Ignatiev, "On cryptographic attacks using backdoors for SAT," in *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence*, Irkutsk, Russia, March 2018.

[23] F. Lafitte, J. Nakahara, and D. V. Heule, "Applications of SAT solvers in cryptanalysis: finding weak keys and preimages," *Journal on Satisfiability, Boolean Modeling and Computation*, vol. 9, no. 1, pp. 1–25, 2014.

[24] G. Bard, "On the rapid solution of systems of polynomial equations over lowdegree extension fields of GF (2) via SAT-solvers," in *Proceedings of the 8th Central European Conferance. on Cryptography*, Gruz Austria, July 2008.

[25] H. M. M. Magalhães, "Applying SAT on the Linear and Differential Cryptanalysis of the AES," 2009.

[26] G. V. Bard, N. T. Courtois, and C. Jefferson, "Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariate Polynomials over GF (2) via SAT-Solvers," 2007.

[27] G. V. Bard, "Extending SAT-solvers to low-degree extension fields of GF (2)," in *Proceedings of the Central European Conference on Cryptography*, Sydney, Australia, July 2008.

[28] L. Jinomeiq, W. Baoduui, and W. Xinmei, "One AES S-box to increase complexity and its cryptanalysis," *Journal of Systems Engineering and Electronics*, vol. 18, no. 2, pp. 427–433, 2007.

[29] J. Y. Cho, "Linear cryptanalysis of reduced-round PRESENT," in *Topics in Cryptology - CT-RSA 2010*, pp. 302–317, Springer, Berlin, Heidelberg, 2010.

[30] A. A. Selçuk, "On probability of success in linear and differential cryptanalysis," *Journal of Cryptology*, vol. 21, no. 1, pp. 131–147, 2008.

[31] C. Blondeau and B. Gérard, "Multiple differential cryptanalysis: theory and practice," *Fast Software Encryption*, Springer, pp. 35–54, Berlin, Heidelberg, 2011.

[32] C. Blondeau and K. Nyberg, "New links between differential and linear cryptanalysis," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 388–404, Springer, Athens, Greece, May 2013.

[33] M. A. Musa, E. F. Schaefer, and S. Wedig, "A simplified AES algorithm and its linear and differential cryptanalyses," *Cryptologia*, vol. 27, no. 2, pp. 148–177, 2003.

[34] M. Wang, Y. Sun, N. Mouha, and B. Preneel, "Algebraic techniques in differential cryptanalysis revisited," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 120–141, Springer, Melbourne, Australia, July 2011.

[35] C. Blondeau and K. Nyberg, "Links between truncated differential and multidimensional linear properties of block ciphers and underlying attack complexities," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 165–182, Springer, Kaoshiung, Taiwan, December 2014.

[36] K. Kazlauskas and J. Kazlauskas, "Key-dependent S-box generation in AES block cipher system," *Informatica*, vol. 20, no. 1, pp. 23–34, 2009.

[37] L. M. Jing, W. D. Bao, C. G. Xiang, and W. M. Xin, "Cryptanalysis of rijndael S-box and improvement," *Applied Mathematics and Computation*, vol. 170, no. 2, pp. 958–975, 2005.

[38] M. A. Khan, A. Ali, V. Jeoti, and S. Manzoor, "A chaos-based substitution box (S-Box) design with improved differential approximation probability (DP)," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 42, no. 2, pp. 219–238, 2018.

[39] M. Hermelin and K. Nyberg, "Linear cryptanalysis using multiple linear approximations," *IACR Cryptology ePrint Archive*, vol. 2011, p. 93, 2011.

[40] J. Lu, "A methodology for differential-linear cryptanalysis and its applications," *Designs, Codes and Cryptography*, vol. 77, no. 1, pp. 11–48, 2015.

[41] T. Tiessen, L. R. Knudsen, S. Kölbl, and M. M. Lauridsen, "Security of the AES with a secret S-box," in *Fast Software Encryption*, pp. 175–189, Springer, Berlin, Heidelberg, 2015.

[42] A. Canteaut and J. Roué, "On the behaviors of affine equivalent sboxes regarding differential and linear attacks," *Advances in Cryptology -- EUROCRYPT 2015*, Springer, in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 45–74, 2015.

[43] N. T. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," in *Proceedings of the Advances in Cryptology — ASIACRYPT*, Y. Zheng,, Ed., pp. 267–287, Springer, Queenstown, New Zealand, December 2002.

[44] C. Diem, "The XL-algorithm and a conjecture from commutative algebra," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, December 2004.

[45] M. Sugita, M. Kawazoe, and H. Imai, "Relation between the XL algorithm and Gr¨obner basis algorithms," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci*, vol. E89, pp. 11–18, 2006.

[46] C. Cid, "Some algebraic aspects of the advanced encryption standard," in *Advanced Encryption Standard – AES*, H. Dobbertin, V. Rijmen, and A. Sowa, Eds., pp. 58–66, Springer, Berlin Heidelberg, 2004.

[47] C. Cid and G. Leurent, "An analysis of the XSL algorithm," in *Proceedings of the Advances in Cryptology - ASIACRYPT*, B. Roy,, Ed., pp. 333–352, Springer, Chennai, India, December 2005.

[48] J. Choy, H. Yap, and K. Khoo, "An analysis of the compact XSL attack on BES and embedded SMS4," in *Proceedings of the International Conference on Cryptology and Network Security*, pp. 103–118, Springer, Kanazawa, Japan, December 2009.

[49] J. Choy, G. Chew, K. Khoo, and H. Yap, "Cryptographic properties and application of a generalized unbalanced Feistel network structure," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 73–89, Springer, Berlin, Heidelberg, 2009.

[50] L. Y. Ji, Y. E. Yu-Peng, L Wei-Yang, W. U. Pei, and S. M. Fang, "The optimum and the combination algorithm of AES and RSA," *Journal of Foshan University (Natural Science Edition*, vol. 6, 2009.

[51] C. Blondeau and K. Nyberg, "Joint data and key distribution of simple, multiple, and multidimensional linear cryptanalysis test statistic and its impact to data complexity," *Designs, Codes and Cryptography*, vol. 82, no. 1-2, pp. 319–349, 2017.

[52] Y. Oren and A. Wool, "Side-channel cryptographic attacks using pseudo-boolean optimization," *Constraints*, vol. 21, no. 4, pp. 616–645, 2016.

[53] W. Yi, L. Lu, and S. Chen, "Integral and zero-correlation linear cryptanalysis of lightweight block cipher MIBS," *Journal of Electronics and Information Technology*, vol. 38, no. 4, pp. 819–826, 2016.

[54] H. R. Wei and Y. F. Zheng, "Algebraic techniques in linear cryptanalysis," *Advanced Materials Research*, vol. 756-759, pp. 3634–3639, 2013.

[55] J. Liu, S. Chen, and L. Zhao, "Lagrange interpolation attack against 6 rounds of rijndael-128," in *Proceedings of the2013 5th International Conference on Intelligent Networking and Collaborative Systems*, pp. 652–655, IEEE, Xi'an, China, Sebtember 2013.

[56] M. Khan and S. S. Jamal, "Lightweight chaos-based nonlinear component of block ciphers," *Wireless Personal Communications*, vol. 120, no. 4, pp. 3017–3034, 2021.

[57] L. S. Khan, M. M. Hazzazi, M. Khan, and S. S. Jamal, "A novel image encryption based on rossler map diffusion and particle swarm optimization generated highly non-linear substitution boxes," *Chinese Journal of Physics*, vol. 72, pp. 558–574, 2021.

[58] K. M. Ali and M. Khan, "Application based construction and optimization of substitution boxes over 2D mixed chaotic maps," *International Journal of Theoretical Physics*, vol. 58, no. 9, pp. 3091–3117, 2019.

[59] M. Khan and T. Shah, "A novel construction of substitution box with Zaslavskii chaotic map and symmetric group," *Journal of Intelligent and Fuzzy Systems*, vol. 28, no. 4, pp. 1509–1517, 2015.

[60] 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 Dynamics*, vol. 88, no. 4, pp. 2757–2769, 2017.

[61] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-Box," *Information Sciences*, vol. 450, pp. 361–377, 2018.

[62] A. Ullah, S. S. Jamal, and T. Shah, "A novel scheme for image encryption using substitution box and chaotic system," *Nonlinear Dynamics*, vol. 91, no. 1, pp. 359–370, 2018.

[63] J. M. Guo, D. Riyono, and H. Prasetyo, "Improved beta chaotic image encryption for multiple secret sharing," *IEEE Access*, vol. 6, Article ID 46321, 2018.

[64] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 144, pp. 444–452, 2018.

[65] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[66] I. Hussain, A. Anees, T. Al-Maadeed, and M. Mustafa, "Construction of S-Box based on chaotic map and algebraic structures," *Symmetry*, vol. 11, no. 3, p. 351, 2019.

[67] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation," *Neural Computing & Applications*, vol. 29, no. 4, pp. 993–999, 2018.

[68] S. S. Jamal, T. Attaullah, T. Shah, A. H. AlKhaldi, and M. N. Tufail, "Construction of new substitution boxes using linear fractional transformation and enhanced chaos," *Chinese Journal of Physics*, vol. 60, pp. 564–572, 2019.

[69] L. Y. Zhang, X. Hu, Y. Liu, K. W. Wong, and J. Gan, "A chaotic image encryption scheme owning temp-value feedback," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 10, pp. 3653–3659, 2014.

[70] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 6, pp. 2322–2335, 2019.

[71] Y. Liu, Y. Luo, S. Song, L. Cao, J. Liu, and J. Harkin, "Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation," *International Journal of Bifurcation and Chaos*, vol. 27, no. 03, Article ID 1750033, 2017.

[72] Y. Deng, H. Hu, N. Xiong, W. Xiong, and L. Liu, "A general hybrid model for chaos robust synchronization and degradation reduction," *Information Sciences*, vol. 305, pp. 146–164, 2015.

[73] Z. Hua, B. Zhou, and Y. Zhou, "Sine chaotification model for enhancing chaos and its hardware implementation," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1273–1284, 2019.

[74] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[75] Z. Hua and Y. Zhou, "Dynamic parameter-control chaotic system," *IEEE Transactions on Cybernetics*, vol. 46, no. 12, pp. 3330–3341, 2016.

[76] G. Chen, Y. Chen, and X. Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps," *Chaos, Solitons & Fractals*, vol. 31, no. 3, pp. 571–579, 2007.

[77] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019.

[78] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, "Integrated chaotic systems for image encryption," *Signal Processing*, vol. 147, pp. 133–145, 2018.

[79] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, 18770.

[80] M. Preishuber, T. Hutter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2137–2150, 2018.

[81] D. Arroyo, J. Diaz, and F. B. Rodriguez, "Cryptanalysis of a one round chaos-based substitution permutation network," *Signal Processing*, vol. 93, no. 5, pp. 1358–1364, 2013.

[82] C. Li, L. Y. Zhang, R. Ou, K.-W. Wong, and S. Shu, "Breaking a novel colour image encryption algorithm based on chaos," *Nonlinear Dynamics*, vol. 70, no. 4, pp. 2383–2388, 2012.

[83] L. Y. Zhang, Y. Liu, F. Pareschi et al., "On the security of a class of diffusion mechanisms for image encryption," *IEEE Transactions on Cybernetics*, vol. 48, no. 4, pp. 1163–1175, 2018.

[84] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, 2017.

[85] L. Y. Zhang, C. Li, K.-W. Wong, S. Shu, and G. Chen, "Cryptanalyzing a chaos-based image encryption algorithm using alternate structure," *Journal of Systems and Software*, vol. 85, no. 9, pp. 2077–2085, 2012.

[86] M. F. Khan, A. Ahmed, K. Saleem, and T. Shah, "A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system," *IEEE Access*, vol. 7, 84991.

[87] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.

[88] M. F. Khan, A. Ahmed, and K. Saleem, "A novel cryptographic substitution box design using Gaussian distribution," *IEEE Access*, vol. 7, 16007.

[89] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.

[90] E. Y. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal Processing*, vol. 132, pp. 150–154, 2017.

[91] C. Pak and L. Huang, "A New Color Image Encryption Using Combination of the 1D Chaotic Map," *Signal Processing*, vol. 138, pp. 129–137, 2017.

[92] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Processing*, vol. 143, pp. 122–133, 2018.

[93] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Optics & Laser Technology*, vol. 101, pp. 30–41, 2018.

[94] M. Alawida, J. S. Teh, and A. Samsudin, *An Image Encryption Scheme Based on Hybridizing Digital Chaos and Finite State Machine*, Signal Processing, vol. 164, 2019.

[95] C. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," *Signal Processing*, vol. 118, pp. 203–210, 2016.

[96] X. Wu, D. Wang, J. Kurths, and H. Kan, "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system," *Information Sciences*, vol. 349-350, pp. 137–153, 2016.

[97] J. M. Ford, V. A. Palzes, B. J. Roach, and D. H. Mathalon, "Did I do that? Abnormal predictive processes in schizophrenia when button pressing to deliver a tone," *Schizophrenia Bulletin*, vol. 40, no. 4, pp. 804–812, 2014.

[98] B. Roach, "EEG data from basic sensory task in Schizophrenia," *EEG data from basic sensory task in Schizophrenia | Kaggle*, vol. 12, 2021.

[99] U. Hayat, N. A. Azam, H. R. Gallegos-Ruiz, S. Naz, and L. Batool, "A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings," *Arabian Journal for Science and Engineering*, vol. 46, no. 9, pp. 8887–8899, 2021.

[100] M. Long and L. Wang, "S-box design based on discrete chaotic map and improved artificial bee colony algorithm," *IEEE Access*, vol. 9, 86154.

[101] S. Ibrahim and A. M. Abbas, "Efficient key-dependent dynamic S-boxes based on permutated elliptic curves," *Information Sciences*, vol. 558, pp. 246–264, 2021.

[102] R. Soto, B. Crawford, F. G. Molina, and R. Olivares, "Human behaviour based optimization supported with self-organizing maps for solving the S-box design problem," *IEEE Access*, vol. 9, 84618.

[103] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, and A. Alzamil, "Implementing a symmetric lightweight cryptosystem in highly constrained IoT devices by using a chaotic S-box," *Symmetry*, vol. 13, no. 1, pp. 1–20, 2021.

[104] W. Yan and Q. Ding, "A novel S-box dynamic design based on nonlinear-transform of 1D chaotic maps," *Electronics*, vol. 10, no. 11, p. 1313, 2021.

[105] W. Gao, B. Idrees, S. Zafar, and T. Rashid, "Construction of nonlinear component of block cipher by action of modular group PSL(2, Z) on projective line PL(GF(28))," *IEEE Access*, vol. 8, 136749.

[106] P. Zhou, J. Du, K. Zhou, and S. Wei, "2D mixed pseudo-random coupling PS map lattice and its application in S-box generation," *Nonlinear Dynamics*, vol. 103, no. 1, pp. 1151–1166, Jan. 2021.

[107] S. Hussain, S. S. Jamal, T. Shah, and I. Hussain, "A power associative loop structure for the construction of non-linear components of block cipher," *IEEE Access*, vol. 8, 123506.

[108] F. Özkaynak, "On the effect of chaotic system in performance characteristics of chaos based s-box designs," *Physica A: Statistical Mechanics and Its Applications*, vol. 550, 124072.

[109] Y. Q. Zhang, J. L. Hao, and X. Y. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, 54188.

[110] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "'Secure data encryption based on quantum walks for 5G Internet of Things scenario," *IEEE Trans. Netw. Service Manage.*vol. 17, no. 1, pp. 118–131, 2020.

[111] H. Liu, A. Kadir, and C. Xu, "Cryptanalysis and constructing S-Box based on chaotic map and backtracking," *Applied Mathematics and Computation*, vol. 376, pp. 125–153, 2020.

[112] Z. M. Z. Muhammad and F. Özkaynak, "A cryptographic confusion primitive based on lotka–volterra chaotic system and its practical applications in image encryption"" in *Proceedings of the 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, pp. 694–698, IEEE, Lviv-Slavske, Ukraine, Febrary2020.

[113] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dynamics*, vol. 99, no. 4, pp. 3041–3064, 2020.

[114] A. A. Abd El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Scientific Reports*, vol. 10, no. 1, pp. 1–16, 2020.

[115] Z. Bin Faheem, A. Ali, M. A. Khan, M. E. Ul-Haq, and W. Ahmad, "Highly dispersive substitution box (S-box) design using chaos," *ETRI Journal*, vol. 42, no. 4, pp. 619–632, 2020.

[116] F. Artuğer and F. Özkaynak, "A novel method for performance improvement of chaos-based substitution Boxes," *Symmetry*, vol. 12, no. 4, p. 571, 2020.

[117] F. Artuğer and F. Özkaynak, "An effective method to improve nonlinearity value of substitution boxes based on random selection," *Information Sciences*, vol. 576, pp. 577–588, 2021.

[118] D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlinear Dynamics*, vol. 100, no. 1, pp. 699–711, 2020.

[119] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, 25678.

[120] B. B. Cassal-Quiroga and E. Campos-Canton, "Generation of Dynamical S-Boxes for Block Ciphers via Extended Logistic Map," *Mathematical Problems in Engineering*, vol. 2020, Article ID 2702653, 12 pages, 2020.

[121] N. Siddiqui, A. Naseer, and M. Ehatisham-ul-Haq, "A novel scheme of substitution-box design based on modified pascal's triangle and elliptic curve," *Wireless Personal Communications*, vol. 116, no. 4, pp. 3015–3030, 2021.

[122] H. S. Alhadawi, M. A. Majid, D. Lambić, and M. Ahmad, "A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm," *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 7333–7350, 2021.

[123] Z. Hua, J. Li, Y. Chen, and S. Yi, "Design and application of an S-box using complete Latin square," *Nonlinear Dynamics*, vol. 104, no. 1, pp. 807–825, 2021.

[124] M. Asif, S. Mairaj, Z. Saeed, M. U. Ashraf, K. Jambi, and R. M. Zulqarnain, "A Novel Image Encryption Technique Based on Mobius Transformation," *Computational Intelligence and Neuroscience*, vol. 2021, Article ID 1912859, 14 pages, 2021.

[125] H. Zhang and S. Yang, "Image Encryption Based on Hopfield Neural Network and Bidirectional Flipping," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 7941448, 7 pages, 2022.