IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 26 February 2023, accepted 18 March 2023, date of publication 27 March 2023, date of current version 13 April 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3262313

RESEARCH ARTICLE

Construction and Optimization of Dynamic S-Boxes Based on Gaussian Distribution

ADEL R. ALHARBI[1], SAJJAD SHAUKAT JAMAL[2], MUHAMMAD FAHAD KHAN[3], MOHAMMAD ASIF GONDAL[4], AND AAQIF AFZAAL ABBASI[3]

[1]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
[2]Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia
[3]Department of Software Engineering, Foundation University Islamabad, Islamabad 44000, Pakistan
[4]Department of Mathematics, Dhofar University, Salalah 211, Oman

Corresponding author: Adel R. Alharbi (aalharbi@ut.edu.sa)

The authors extend their appreciations to the Deanship of Scientific Research for funding this work through research group no. R.G.P. 2/86/43. The authors extend their appreciations to the Deanship of Scientific Research at University of Tabuk for funding this work through research group no. S-0112-1443.

ABSTRACT Block ciphers are widely used for securing data and are known for their resistance to various types of attacks. The strength of a block cipher against these attacks often depends on the S-boxes used in the cipher. There are many chaotic map-based techniques in the literature for constructing the dynamic S-Boxes. While chaos-based approaches have certain attractive properties for this purpose, they also have some inherent weaknesses, including finite precision effect, dynamical degradation of chaotic systems, non-uniform distribution, discontinuity in chaotic sequences. These weaknesses can limit the effectiveness of chaotic map-based substitution boxes. In this paper, we propose an innovative approach for constructing dynamic S-boxes using Gaussian distribution-based pseudo-random sequences. The proposed technique overcomes the weaknesses of existing chaos-based S-box techniques by leveraging the strength of pseudo-randomness sequences. However, one of the main drawbacks of using Gaussian distribution-based pseudo-random sequences is the low nonlinearity of the resulting S-boxes. To address this limitation, we introduce the use of genetic algorithms (GA) to optimize the nonlinearity of Gaussian distribution-based S-boxes while preserving a high level of randomness. The proposed technique is evaluated using standard S-box performance criteria, including nonlinearity, bit independence criterion (BIC), linear approximation probability (LP), strict avalanche criterion (SAC), and differential approximation probability (DP). Results demonstrate that the proposed technique achieves a maximum nonlinearity of 112, which is comparable to the ASE algorithm.

INDEX TERMS Symmetric cipher, block cipher, S-Box optimization, PRNG, S-Box construction, Gaussian distribution, genetic algorithm.

I. INTRODUCTION

Cryptographic algorithms are essential tools for securing sensitive data transmitted through computer and communication technology. With the increasing reliance on the internet and electronic communication, it is important to ensure that the transmitted data is protected from unauthorized access and tampering. Cryptographic algorithms are used to secure communications and protect data by encoding it in a way that makes it difficult for unauthorized individuals to access [1]. Cryptographic algorithms can generally be divided into two categories: symmetric and asymmetric. Symmetric algorithms utilize the same key for both encryption and decryption, which means that the key must be shared between the sender and recipient of the encrypted message. Asymmetric algorithms, on the other hand, use a different key for each process [2]. In an asymmetric cryptographic algorithm, the sender uses a publicly-available key to encrypt the message, and the recipient uses a private key to decrypt it. This allows for secure communication without the need for the sender and

The associate editor coordinating the review of this manuscript and approving it for publication was Alessandra De Benedictis.

recipient to share a single key. Asymmetric algorithms can provide a higher level of security than symmetric algorithms, which use the same key for both encryption and decryption. However, symmetric algorithms are generally faster and more efficient at encrypting large amounts of data [4].

They are also more reliable, as they do not rely on complex mathematical problems and are less susceptible to attacks. Some examples of popular symmetric algorithms include AES, DES, and Blowfish [3], [5]. A block cipher is a type of symmetric cipher that operates on fixed-size blocks of data. It uses a secret key to encrypt and decrypt the data, with the key typically being the same size as the block. The block size is usually chosen to be a power of 2, such as 128 or 256 bits, to allow for efficient implementation using Boolean operations. A key component of a block cipher is the substitution box, or S-box, which is a non-linear transformation that is applied to the input data to produce the output. The S-box plays a vital role in the security and efficiency of the block cipher, as it provides confusion and diffusion, which are two important principles of cryptography. Confusion refers to the complexity of the relationship between the input and output of the S-box, making it difficult for an attacker to determine the key used in the encryption process. Diffusion refers to the property of the S-box to evenly distribute the input patterns over the output patterns, making it difficult for an attacker to identify patterns in the encrypted data. The design of the S-box is critical to the security and efficiency of the block cipher, as it determines the level of confusion and diffusion achieved. A good S-box should have a high level of non-linearity, which measures the complexity of the relationship between the input and output. It should also have good algebraic immunity, which measures the resistance to attacks based on algebraic properties. The S-box should also be resilient to other types of attacks, such as differential and linear cryptanalysis. The design of the S-boxes plays a crucial role in determining the efficiency of a block cipher.

Various methods have been proposed for constructing S-boxes, including the use of chaos, polynomials, DNA sequences, TDERC numbers, galois fields(GF),neural network,inversion mapping, and pseudo random number generators(PRNGs) [6], [9]. In the past ten years, there has been significant research on using chaotic systems for the construction of S-boxes. The use of chaotic maps has been widely documented in the literature on this topic.

There are several favorable properties of chaotic systems that make them useful for encryption, including a continuous broad-band power spectrum, strong randomness, periodic states, non-convergence, and sensitivity to initial conditions. The effectiveness of chaotic ciphers for encryption depends on both the chaotic system being used and the encryption scheme chosen. Chaotic systems can be classified into one-dimensional and multi-dimensional types, each with its own advantages and disadvantages. The cryptographic strength of a chaotic cipher can vary depending on the number of independent or dependent parameters in the chaotic system. In general, it is important to carefully consider the characteristics of the chaotic system being used in order to ensure the security of the resulting cipher. Chaotic maps have been widely used in the design of S-boxes in cryptographic systems. Some of the most commonly used chaotic maps for this purpose include the Gingerbreadman, Henon, Lorenz, Logistic, and Chen maps.

While chaotic systems offer several favorable properties for encryption, such as strong randomness and sensitivity to initial conditions, there are also some potential weaknesses that have been identified by researchers. These include non-uniform data distribution, discontinuity in chaotic sequences, limited randomness, the impact of finite precision, and computational complexity [10], [30], [37], [53], [54]. It is important to carefully consider these factors when using chaotic systems for encryption in order to ensure the security of the resulting cipher. Gaussian distribution is a common method for generating pseudo-random numbers [11]. These types of random number generators can produce high-quality random numbers that are suitable for use in various simulation environments. Gaussian based random number generators can be classified into four main categories: cumulative density function (CDF), inversion transformation, rejection, and recursive methods.

One method for generating Gaussian random numbers is to use the cumulative density function(CDF). This involves inverting the CDF to produce random numbers that follow a specified distribution [13], [15], [16]. Other methods, such as inversion transformation and rejection, involve more complex processes for generating random numbers from a Gaussian distribution. Recursive methods involve using a recursive function to generate random numbers that follow a Gaussian distribution. Regardless of the method used, Gaussian random number generators can be an effective tool for generating high-quality random numbers for use in simulations and other applications. There are several algorithms that are commonly used to generate random numbers using a Gaussian distribution, including the Box-Muller, polarization, and the central limit. The results of a comparison between chaos and Gaussian-based random numbers are presented in Table 1. In order to compare the quality of pseudo-randomness produced by these methods, we selected five different chaotic maps based and 3 different Gaussian distribution-based random number generation techniques and evaluated them using the NIST randomness suite. The results of the assessment show that Gaussian distribution-based pseudo-random numbers generally perform better than chaos-based pseudo-random numbers. While chaos-based techniques offer a number of favorable cryptographic properties, they may still need further improvements in order to keep up with advances in cryptanalysis techniques. In general, it is important to carefully consider the quality of pseudo-random numbers when selecting a method for use in cryptographic systems, as the security of the resulting cipher can depend on the randomness of the numbers used.

TABLE 1. Comparing Techniques of Gaussian and Chaos Theory.

NIST TESTS	Lorenz Map	Chen System	Henon Map	Gingerbread man map	Logistic Map	Box–Muller Transform	Polarization Decision	Central Limit Algorithm
Frequency	P	P	P	P	--	P	P	P
Frequency Within A Block	--	--	--	--	--	P	P	P
Runs	P	P	--	P	--	P	P	P
Longest Run Of Ones(Block)	--	-	--	--	P	p	P	P
Random Binary Matrix Rank	--	--	P	--	--	P	--	--
Non-Overlapping Template Matching	--	--	--	--	--	P	P	P
Maurer's Universal Statistical	P	P	P	P	--	--	--	--
Cumulative Sum	P	--	P	P	--	P	P	P
Discrete Fourier Transform	--	P	--	--	P	P	P	P
Rank Test	--	--	--	--	--	P	P	P

Gaussian distribution-based methods may be a good option due to their generally higher quality and performance compared to chaos-based methods. In recent years, hybrid chaotic S-box construction approaches have been proposed in order to address the need for more secure ciphers as cryptanalysis techniques continue to advance. The use of randomized S-Boxes can significantly increase the resilience of IoT systems to cyber-attacks. With the vast number of interconnected devices and the increasing amount of data being transmitted through them, IoT systems are becoming more vulnerable to attacks, which can have significant consequences. One of the key benefits of using randomized S-Boxes in IoT systems is that they can help protect against attacks that target the encryption algorithm. In many cases, IoT devices use standardized encryption algorithms, which are widely known and studied by attackers. By using randomized S-Boxes in the encryption process, the output becomes less predictable, making it harder for attackers to exploit vulnerabilities in the algorithm and extract sensitive data. Moreover, randomized S-Boxes can help protect against brute-force attacks. Brute-force attacks are commonly used to guess encryption keys by trying every possible combination. However, the use of randomized S-Boxes makes the encryption keys more complex and harder to guess, which makes it more difficult for attackers to break the encryption.

Single chaos-based techniques have not been able to meet the higher standards of security that are now required, so hybrid approaches that combine multiple chaotic maps or integrate chaotic maps with other cryptographic techniques have been proposed as a solution. Chaos-based S-boxes are known to be highly sensitive to initial conditions. This means that small changes in the input can result in significant changes in the output. Gaussian distribution based S-boxes, on the other hand, are less sensitive to initial conditions, which makes them more robust and less susceptible to differential attacks. The Gaussian distribution is a smooth function with continuous derivatives, which makes it more robust and less prone to abrupt changes. This reduces the probability of differential attacks and makes it more difficult for an attacker to exploit the input-output differences to extract the secret key. The reduced sensitivity to initial conditions also makes Gaussian distribution based S-boxes more resistant to side-channel attacks, which are attacks that exploit information leaked during the execution of a cryptographic algorithm such as power consumption, electromagnetic radiation, or timing measurements. Side-channel attacks rely on exploiting the sensitive dependence of the output on the input. These hybrid approaches may offer improved security and resistance to cryptanalysis compared to single chaotic map techniques. Gaussian distribution based Pseudo-Random Number Generators (PRNGs) do not require random extraction methods, such as von Neumann extractors, to pass NIST statistical tests. The reason is that these PRNGs utilize the Box-Muller transform, polarization decision method, and the central limit theorem to generate statistically random values with a continuous probability distribution that can produce an infinite number of possible values without repetition. For the proposed design, we have chosen to use the Box-Muller, polarization decision, and central limit technique to design the S-box, rather than relying on chaotic maps. These algorithms are well-established and offer good performance for generating pseudo-random numbers from a Gaussian distribution. By using these algorithms, we aim to achieve a high level of security and resistance to cryptanalysis in the resulting cipher. In the proposed technique, we first designed the S-boxes using the three different Gaussian distribution based PRNG techniques, instead of chaotic maps. The following is the mathematical description of each method: The Box-Muller transform is based on the fact that if you have two independent random variables x and y that are uniformly distributed between −1 and 1, then the variables X and Y defined by the equations:

$$f_X(x) = \frac{1}{\sqrt{2\pi\delta}} e^{-\frac{x^2}{2\delta^2}} \tag{1}$$

$$f_Y(y) = \frac{1}{\sqrt{2\pi\delta}} e^{-\frac{y^2}{2\delta^2}} \tag{2}$$

A pair of random numbers, referred to as r and θ, can be generated from the X and Y coordinates. These numbers are independent of each other and can be described as follows:

$$f_R(r) = \int_0^{2\pi} \frac{r}{2\pi\delta^2} e^{-\frac{r^2}{2\delta^2}} d\theta, \quad 0 \le \mathrm{r} \le \infty \tag{3}$$

$$f_\theta(\theta) = \int_0^{\infty} \frac{r}{2\pi\delta^2} e^{-\frac{r^2}{2\delta^2}} dr, \quad 0 \le \theta \le 2\pi \tag{4}$$

The probability density of R and θ, which are jointly distributed according to the Rayleigh distribution and normal distribution, respectively, can be described as follows: $f_{R\theta}(r,\theta) = f_R(r) \times f_\theta(\theta)$ is statistically independent. This means that the distribution of R and θ is independent of one another and can be described as:

$$F_R(r) = \int_0^{r} \frac{r'}{\delta^2} e^{-\frac{r^2}{2\delta^2}} dr \tag{5}$$

$$F_\Theta(\theta) = \int_0^{\theta} \frac{1}{2\pi} d\theta^r = \frac{\theta}{2\pi} \tag{6}$$

The inverse transformation method can be used to generate Gaussian random variables, because both $F_R(r)$ and $F_\theta(\theta)$ are in closed form. This means that they can be easily transformed into their corresponding Gaussian distributions using the inverse transformation method. The polarization decision method of Gaussian distribution is a statistical technique used to classify data points into one of two categories based on their likelihood of belonging to a particular group. This method is based on the assumption that the data follows a normal distribution, which means that the data points are distributed around a central mean value, with a certain standard deviation. The polarization decision method uses the mean value and standard deviation of the data to determine a boundary, or threshold, between the two categories. Points that are above the threshold are classified as belonging to one category, while points that are below the threshold are classified as belonging to the other category. This function is defined as follows:

$$F = \int_{-\infty}^{+\infty} f_X(x)dx = \int_{-\infty}^{+\infty} f_Y(y)dy \tag{7}$$

The square of the transformed function F in polar coordinates is given by equation 8:

$$\begin{aligned} F^2 &= \frac{1}{2\pi\delta^2} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} e^{-\frac{x^2+y^2}{2\delta^2}} d(x)d(y) \\ &= \frac{1}{2\pi\delta^2} \int_0^{2\pi} \int_0^{+\infty} re - \frac{r^2}{2\delta^2} drd\theta \end{aligned} \tag{8}$$

This approach is near to Box-Muller in that it involves transforming the coordinates to polar form. This transformation results in a uniform distribution of θ from 0 to 2π. The normalized distribution function for the radial distance r is:

$$P(r < a) = \int_0^{a} re^{-\frac{r^2}{2}} dr \tag{9}$$

A uniform random number U, with values in the interval [0 1], is also used in this method. To generate a new point, the radial distance r is multiplied by the original point: r : (rcos (2πU), rsin (2πU)) The inverse transformation of these points results in two standard normal variables.

The central limit theorem is a fundamental result in probability theory that states that the distribution of the sum or average of a large number of independent and identically distributed random variables is approximately normal, regardless of the underlying distribution of the individual variables. This means that if you have a large number of random variables with a certain mean and standard deviation, and you calculate the sum or average of these variables, the resulting distribution will be approximately normal, with a mean equal to the sum or average of the means of the individual variables, and a standard deviation equal to the standard deviation of the individual variables divided by the square root of the number of variables. Here 'n' number of independent and identically distributed uniform numbers $\mathrm{U_i} \sim$ U (0, 1) then sum of $\mathrm{U_i}$ is:

$$S = \sum_{i=1}^{n} U_i \tag{10}$$

The probability distribution of S can be estimated using the following equation

$$F_s(s) = \Phi\left(\frac{s - n\mu}{\sqrt{n\sigma^2}}\right) \tag{11}$$

The mean and variance of the distribution can be calculated using the equations $\mu = 1/2$ and $\sigma = 1/12$, The variable z can be selected in such a way that:

$$z = \frac{s - \frac{n}{2}}{\frac{1}{12}\sqrt{n}} \tag{12}$$

The probability distribution of z can be represented as:

$$f_z(z) = \frac{n}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \tag{13}$$

In this paper, we designed S-boxes using various Gaussian distribution techniques and then enhance their nonlinearity value using a novel approach based on genetic algorithm. The paper is structured as follows: The contribution of our work is outlined in Section II. The proposed methodology is explained in Section III. The results and evaluation are presented in Section IV. Finally, the conclusion is given in Section V.

II. CONTRIBUTION

a- A method is proposed for the construction of dynamic S-boxes by using the box Box-Muller transformation, the polarization decision method, and the central limit theorem.

b- A method is proposed for the optimization of dynamic S-boxes by using the Genetic Algorithm. More than 500000 dynamic S-boxes optimized and results demonstrate that the proposed technique achieves a maximum nonlinearity of 112, which is similar to the ASE algorithm.

c- Proposed approach passes the standard S-box performance criteria, including nonlinearity, bit independence criterion(BIC), linear approximation probability(LP), strict avalanche criterion(SAC), and differential approximation probability(DP).

d- Proposed technique overcomes the weaknesses of existing chaos-based S-box construction techniques.

III. PROPOSED DESIGN METHODLOGY

The proposed technique consists of two phases: Construction of S-boxes and the optimization of the constructed S-boxes. The algorithm for constructing the S-boxes is described in the following steps, while the algorithm for optimizing the S-boxes is depicted in Figure 2. Specifically, the first phase involves constructing the S-boxes using a specific set of algorithms and procedures, while the second phase involves adjusting and refining the S-boxes to improve their performance.

A. CONSTRUCTION OF S-BOXES

The proposed design algorithm involves the use of linear fractional transformations with parameters a, b, and c drawn from the Box-Muller, polarization decision and central limit algorithm respectively. In order to ensure the proper functioning of the methodology, it is necessary to avoid certain conditions, such as cz = −d and ad – bc ≠ 0.

$$f(z) = \frac{az+b}{cz+d} \tag{14}$$

Step 1: To generate the parameters a, b, and c, we used three approaches: the Box-Muller, the polarization decision, and the central limit. The proposed design for generating these parameters is illustrated in Figure 1a.

Step 2: To create three sequences of random numbers, removed the floating point values from the original sequences and Get resulting sequences.

Step 3: To obtain binary representations of the three sequences of random numbers, convert each sequence into its corresponding binary form by using: Sequence-1 = (Sequence-1 x RandomNo) %255. Sequence-2 = (Sequence-2 x RandomNo) %255. Sequence-3 = (Sequence-3 x Random No) %255.

Step 4: To generate a stream of parity bits, Select LSB from each of the binary sequences.

Step 5: To obtain decimal numbers, append 8 parity bits and convert the resulting groups of bits into decimal form.

Step 6: To generate the parameter d: Perform a bitwise XOR operation on the parity bits obtained from the Box-Muller technique and the polarization decision technique. The proposed design for generating d is illustrated in Figure 1b.

Step 7: Perform (Binary of step-6) x (RandomNo) }mod 255.

Step 8: To obtain decimal numbers, append 8 parity bits and convert the resulting groups of bits into decimal form.

Step 9: Convert the resultant output of Step-8 into its corresponding binary form.

Step 10: To obtain decimal numbers, append 8 parity bits and convert the resulting groups of bits into decimal form.

Step 11: Perform LFT of equation (14).

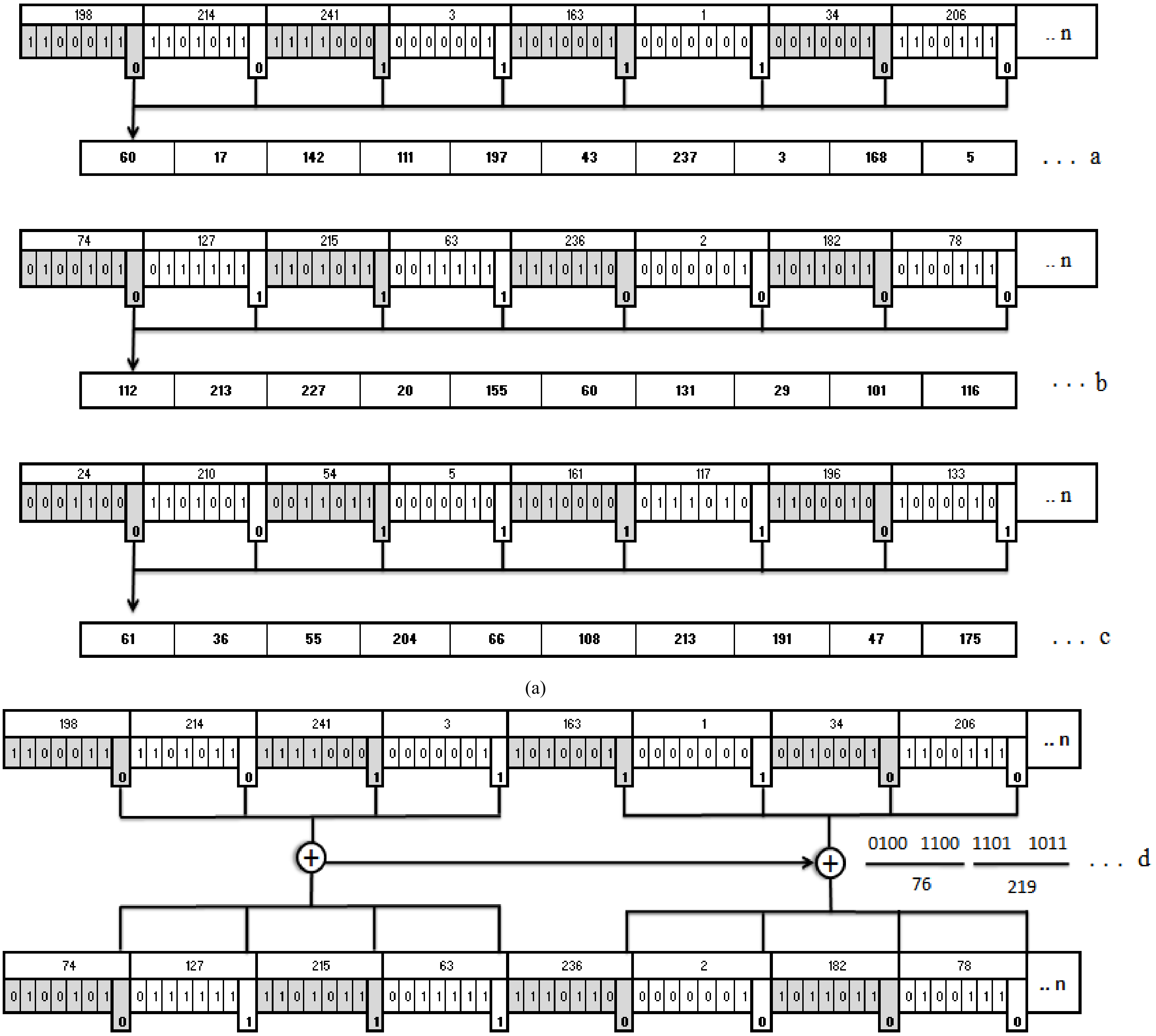
For the results, we constructed a total of 100,000 S-boxes and found that the NL of 12431 S-boxes were ≤ 99, the NL of 21246 S-boxes were between 100 and 102, the NL of 37275 S-boxes were between 103 and 104, the NL of 24297 S-boxes were between 105 and 106, the NL of 4751 S-boxes were between 107 and 109.

B. OPTIMIZATION OF S-BOXES

GA states that the most fit individuals are more likely to survive and reproduce. In a GA, selection, crossover, and mutation are standard processes. For our case, we used the selection process to acquire all substitution boxes with NL scores between 100 and 107 as the initial population. This process is based on the idea that these S-boxes are the fittest and therefore most likely to be successful in the optimization. In crossover, we used a one-point crossover scheme, which involves exchanging half of each parent's genetic information with the other parent to create new offspring. This scheme is illustrated in yellow in the flowchart shown in Figure 2. Specifically, we selected pairs of parents and exchanged the relevant information to generate new offspring according to the one-point crossover scheme.

This process helps to introduce new genetic diversity into the population and can potentially improve the overall performance of the S-boxes. In the standard GA, crossover and mutation are separate steps, but in our method for generating S-boxes, we combine these steps together. This is because the S-boxes produced by the crossover operation often do not have the bijective property. To ensure that the S-boxes produced have the bijective property, we adopted a simple strategy in the mutation process to remove any repetition from the new offspring. In mutation, we flip a single bit from the right side to the left side, and then check the corresponding value within s-box. If value is unique, stop the flipping step. If it is not unique, we continue flipping bits until we find a unique number. In many cases, we are able to achieve the bijective property through the flipping process. However, in a few cases, even after flipping all eight bits, we are unable to find a unique value in the s-box. In these cases, we simply add 1 to the original value and begin the flipping procedure again. When bits are flipped from right to left then on every flip small change occur in the actual value, if we flip bits from left to right then very big change will occur in the actual decimal value of the S-box.

Mutation procedure is shown by the green color in flowchart of Figure 2. Our results show that many S-boxes



(a)

(b)

FIGURE 1. **(a) Design for parameters a, b and c. (b) Design for parameter d.**

and their subsets are repeated, so we use hash-based searching to remove these repetitions. This process is depicted by the blue color in the flowchart. The optimization process using a GA has been shown to significantly improve the overall quality of S-boxes. When comparing the highest quality S-boxes produced by the GA method to those produced using a Gaussian distribution based S-boxes. For our experiment, we optimized 500,000 S-boxes and compared the performance of the highest quality 100,000 optimized S-boxes with Gaussian distribution based S-boxes. It can be seen that the GA method produces zero S-boxes with non-linearity less than or equal to 99. Additionally, the GA method produced 9817 new S-boxes with non-linearity of 110 and 112, which were not discovered using Gaussian based approach. The detailed comparison is shown in the Figure 3.

IV. RESULTS AND EVALUATION

Here we evaluated the sample S-box of the previous section using standard S-box evaluation criteria. The proposed method achieved a maximum non-linearity of 112, equal to ASE. Other statistical analysis also proves that our scheme has high resistance to attacks.

A. STANDARD S-BOX EVALUATION MEASURE

1) NON-LINEARITY

The nonlinearity of a function is a measure of how different it is from a set of affine functions. It can be quantified by the minimum number of bits that must be altered in the truth table in order to obtain the closest affine function. In cryptographic contexts, the nonlinearity of a function is a key factor in its resistance to linear attacks. A higher nonlinearity score is

TABLE 2. Proposed S-box.

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
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

generally considered to be desirable, as it indicates a higher level of resistance to these types of attacks. In our analysis, we calculated the nonlinearity value of our sample S-box and found it to be 112, as shown in Table 2. In order to compare the security of our sample S-box with other S-boxes that have been proposed in the literature, we also calculated the nonlinearity scores of 30 state-of-the-art S-boxes. The results of this comparison are shown in Table 3. By comparing the nonlinearity score of our sample S-box with these other S-boxes, The results showed that the nonlinearity score of our S-box is equal to or greater than that of state-of-the-art S-boxes.

TABLE 3. Nonlinearity of state of the art S-boxes.

Substitution box	Nonlinearity	Substitution box	Nonlinearity
[60]	112	[6]	98
[27]	112	[43]	106
[28]	112	[45]	106
[29]	110	[43]	106
[9]	106	[46]	106
[38]	110	[47]	108
[39]	110	[48]	108
[40]	108	[49]	110
[41]	106	[50]	106
[42]	107	[51]	112
[59]	108	[55]	110
[41]	110	[56]	108
[60]	108	[57]	110
[54]	108	[58]	112
[52]	106	[53]	110

2) BIT INDEPENDENT CRITERION(BIC)

It is determined by evaluating the function's truth table and counting the number of input combinations that yield a unique output. A function with a high bit independent criterion is less likely to be vulnerable to linear attacks, as it is more difficult for an attacker to predict the output of the function based on the inputs. In cryptographic contexts, the bit independent criterion is an important consideration, as it can help to ensure the security and confidentiality of data.

The average value of the BIC-SAC matrix for sample S-box 1 is 0.498, which is very close to the ideal value of 0.5. This indicates that our proposed S-boxes are able to effectively meet the bit independent criteria. The BIC results for sample S-box can be found in Tables 4 and 5.

TABLE 4. BIC of the sample S-box.

----	104	100	100	106	106	104	106
104	----	116	102	104	102	104	104
100	116	----	104	106	108	100	104
100	102	104	----	106	104	100	106
106	104	106	106	----	106	106	100
106	102	108	104	106	----	102	104
104	104	100	100	106	102	----	104
106	104	104	106	100	104	104	----

TABLE 5. Dependent matrix of sample S-box.

----	.48828	.47656	.50781	.50195	.49804	.52148	.50976
.48828	----	.48242	.49218	.50195	.48632	.49804	.49804
.47656	.48242	----	.48437	.52539	.52539	.50976	.50781
.50781	.49218	.48437	----	.50000	.48632	.48242	.51562
.50195	.50195	.52539	.50000	----	.50976	.48632	.49609
.49804	.48632	.52539	.48632	.50976	----	.47656	.46875
.52148	.49804	.50976	.48242	.48632	.47656	----	.52929
.50976	.49804	.50781	.51562	.49609	.46875	.52929	----

3) STRICT AVALANCHE CRITERIA(SAC)

The strict avalanche criterion is a measure of the sensitivity of a Boolean function to changes in its inputs. It is determined by evaluating the function's truth table and counting the number of input combinations that result in a change in the output. A function with a high strict avalanche criterion is considered

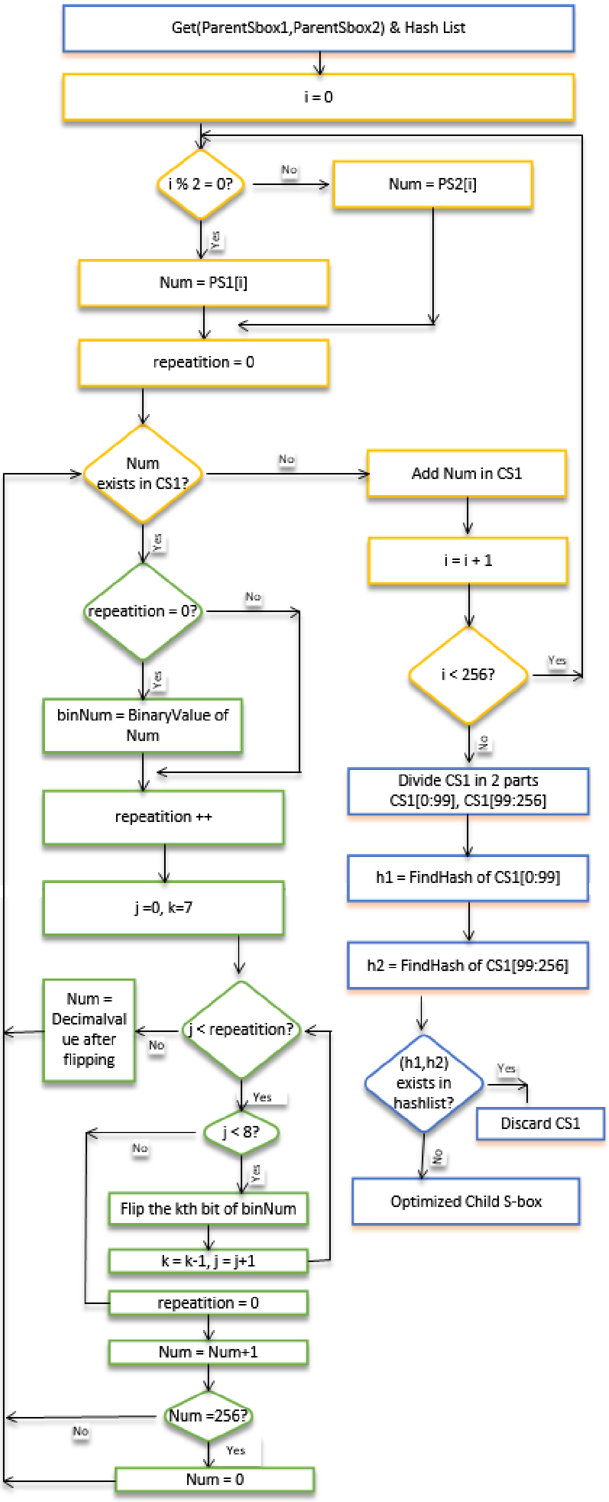


FIGURE 2. GA based Optimization.

to be highly sensitive to changes in its inputs, making it less vulnerable to certain types of attacks. In cryptographic contexts, the strict avalanche criterion is an important consideration, as it can help to ensure the security and confidentiality of data. The results of the SAC analysis for the sample S-box are presented in Table 6.

TABLE 6. Strict avalanche criteria.

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

The results of the SAC analysis for sample S-box show that it performs well, with minimum, maximum, and average values of 0.453125, 0.031122, and 0.500488, respectively.

4) RESISTANCE AGAINST DIFFERENTIAL ATTACKS

The resistance of an encrypted image to differential attacks can be gauged by its NPCR and UACI values. Differential attacks involve attempting to uncover the secret key used to encrypt a message or image by examining how the encryption impacts the original data. A high NPCR value indicates that many pixels in the encrypted image have been altered, making it more challenging for an attacker to apply differential analysis to determine the key. A high UACI value signifies that the encrypted image differs significantly from the original, also hindering an attacker's ability to use differential techniques to determine the key. As a result, image encryption algorithms with high NPCR and UACI values tend to be more secure against differential attacks. The mathematical definitions of UACI and NPCR can be found in equations 15 and 16, respectively.

NPCR Analysis:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N \times M} \times 100\% \tag{15}$$

UACI Analysis:

$$UACI = \frac{1}{N \times M} \times \left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\% \tag{16}$$

Equation 16 presents the determination of the UACI by means of two encrypted images, C1(i,j) and C2(i,j), that have been derived from slightly altered original images. N and M stand for the width and height of the encrypted image, respectively, and D(i,j) is the discrepancy function between the two encrypted images. The discrepancy is defined as:

$$f(x) = \begin{cases} 0, & \textit{if } \mathrm{C}_1(\mathrm{i},\mathrm{j}) = \mathrm{C}_2(\mathrm{i},\mathrm{j}), \\ 1, & \text{if } \mathrm{C}_1(\mathrm{i},\mathrm{j}) \neq C_2(\mathrm{i},\mathrm{j}), \end{cases}$$

Tables 7 and 8 present a comparative analysis of NPCR and UACI with the proposed method for the test image Lena.

TABLE 7. Comparative of NPCR and UACI.

Dataset Image	Loc.	NPCR		UACI	
		Our Proposed	AES	Our Proposed	AES
Camera man	Start	99.54	99.60	30.55	33.52
	Mid	99.56	99.59	37.39	33.51
	End	99.53	99.60	34.29	33.57
Lena	Start	99.63	99.62	33.39	33.39
	Mid	99.64	99.65	31.92	33.33
	End	99.59	99.59	33.93	33.50
Baboon	Start	99.73	99.60	30.39	33.47
	Mid	99.89	99.60	28.90	33.48
	End	99.90	99.61	31.29	33.55

TABLE 8. NPCR and UACI Comparison.

Algorithms	NPCR	UACI
Our Proposed	99.59	33.37
[25]	99.61	33.41
[20]	98.48	32.29
[21]	99.45	24.88
[22]	99.56	28.32
[23]	99.61	33.43
[19]	99.59	28.64
[26]	99.59	33.49
[24]	99.33	33.42

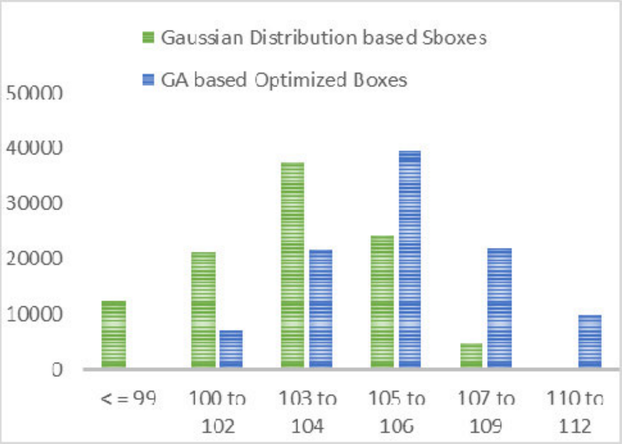


FIGURE 3. NL comparison of Gaussian & GA based approach.

5) LINEAR APPROXIMATION PROBABILITY (LP)

It is determined by evaluating the function's truth table and calculating the probability that a linear function will accurately approximate the output of the function for a given set of inputs. Functions with low linear approximation probabilities are considered to be more resistant to linear attacks, as they are more difficult to approximate using linear functions. The maximum LP value of our S-box is 0.125, which meets the LP criteria.

$$LP_f = \max_{\Gamma x, \Gamma y \neq 0} \left| \frac{\{x \in X \mid x \cdot \Gamma x = \mathrm{S}(x) \cdot \Gamma y\}}{2^n} - \frac{1}{2} \right| \quad (17)$$

Γx, Γy are masks used for the input and output. The set of all possible inputs is represented by X and 2^n is the quantity of elements that are in that set.

6) DIFFERENTIAL APPROXIMATION PROBABILITY(DP)

The differential uniformity of S-box is a key factor in its effectiveness for use in cryptography. To measure this property, we can use differential approximation probability (DP). This metric assesses the extent to which any change in the input of the substitution box, whether in terms of the sequence or the value, results in a corresponding change in the output. To ensure a high degree of differential uniformity, it is desirable for the input differential, represented by Δxi, to be uniquely mapped to an output differential, represented by Δyi. This ensures that the substitution box provides a uniform mapping probability for each input value, which is important for maintaining the security and confidentiality of data. DP is represented as [17] and [18]. Table 9 illustrates the DP result of proposed s-box.

$$DP(\Delta x \to \Delta y) = \left[\frac{\#\{x \in X | (\mathrm{S}(\mathrm{x}) \oplus S(x \oplus \Delta x) = \Delta y)\}}{2^n} \right]$$

Algorithm 1 ReverseSbox (S-Box)

```
in: 2D array of integers, sbox [16], [16];
out: 2D array of integers, ReverseSbox [16], [16];
ReverseSbox → |16||16|
for row → 0 ...(16) do
    for col → 0 ...(16) do
        rowIS → sbox row,col div 16
        colIS → sbox row,col mod 16
        value → row ∗16+col
        ReverseSbox rowIS,colIS → value
    end for
end for
return ReverseSbox
```

7) HISTOGRAM ANALYSIS

Histogram analysis is a technique that can be used to assess the robustness of cipher against cryptanalysis. This method involves examining the distribution of pixels in a plain image after it has been encrypted, and it provides insight into the frequency of different pixel values in the encrypted image. An effective encryption technique should be able to transform the image into an encrypted version that has randomly distributed pixels and sequences, which helps to protect the confidentiality of the data being secured. Proposed approach clearly generates a two-dimensional histogram that is evenly distributed for the encrypted image.

This uniformity among the random pixels demonstrates the effectiveness of the encryption and its resistance to various statistical attacks. As a result, histogram test is ineffective at providing any information about the encrypted image. Test image is depicted in Figure 4a and its histogram is presented in Figure 4c. Similarly encrypted image is depicted in

TABLE 9. Differential approximation probability.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.00000	.02343	.03906	.02343	.02343	.02343	.02343	.03125	.03125	.02343	.03125	.02343	.02343	.02343	.03125	.02343
.03125	.02343	.03125	.03125	.03125	.02343	.02343	.02343	.02343	.02343	.02343	.03125	.02343	.02343	.02343	.02343
.02343	.03125	.02343	.02343	.02343	.03125	.03125	.02343	.02343	.02343	.02343	.03125	.03125	.02343	.02343	.03125
.02343	.03125	.03125	.02343	.02343	.03906	.02343	.03125	.03125	.02343	.02343	.02343	.03125	.03125	.02343	.02343
.02343	.03125	.02343	.02343	.03125	.02343	.02343	.02343	.03125	.02343	.02343	.03125	.03125	.02343	.02343	.02343
.03125	.02343	.02343	.02343	.02343	.03906	.02343	.02343	.02343	.03125	.02343	.03125	.03125	.02343	.03125	.03125
.03125	.03125	.03125	.02343	.02343	.02343	.02343	.02343	.02343	.02343	.02343	.02343	.02343	.02343	.02343	.02343
.03125	.03125	.03125	.03125	.02343	.02343	.02343	.02343	.02343	.03125	.02343	.02343	.03125	.03906	.03125	.03125
.03125	.02343	.03906	.03906	.03125	.02343	.02343	.02343	.02343	.02343	.02343	.02343	.02343	.03125	.03125	.02343
.02343	.02343	.02343	.03125	.02343	.02343	.02343	.02343	.02343	.02343	.03125	.02343	.02343	.03125	.03906	.02343
.03125	.02343	.02343	.02343	.03125	.02343	.02343	.02343	.02343	.02343	.03906	.02343	.02343	.02343	.02343	.02343
.02343	.02343	.02343	.02343	.03125	.02343	.02343	.03125	.02343	.02343	.02343	.02343	.02343	.03125	.03125	.03125
.02343	.03125	.02343	.02343	.02343	.02343	.03125	.02343	.02343	.02343	.01562	.03125	.02343	.02343	.02343	.03125
.03125	.02343	.02343	.02343	.02343	.03906	.02343	.02343	.02343	.03125	.02343	.03906	.02343	.03125	.02343	.02343
.03125	.03125	.02343	.02343	.02343	.03125	.02343	.02343	.03906	.02343	.03125	.02343	.02343	.02343	.03125	.02343
.02343	.02343	.03125	.02343	.03125	.02343	.02343	.03125	.02343	.02343	.02343	.02343	.02343	.02343	.03906	.02343

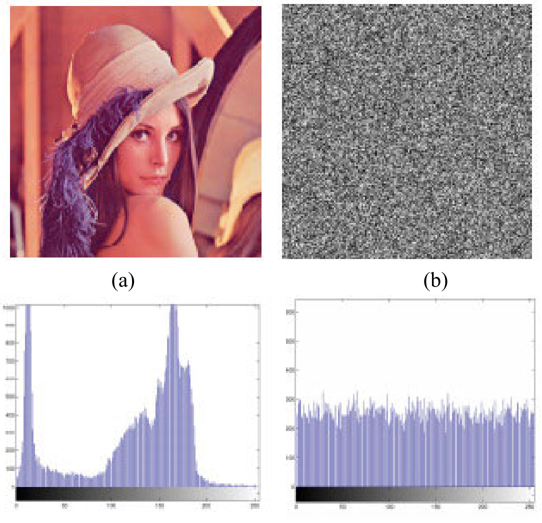
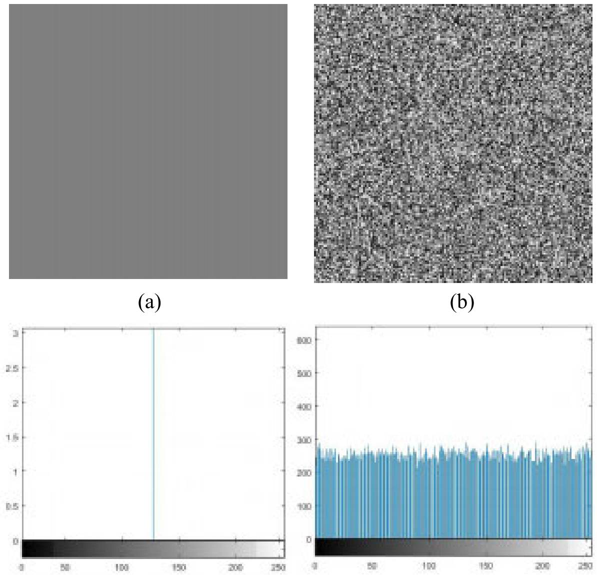

(a)
(b)
(c)
(d)

FIGURE 4. Figure 4a shows the plain image of Lena and its histogram in Figure 4c, while Figure 4b depicts the encrypted image and its histogram is in Figure 4d.

Figure 4b and its histogram is presented in Figure 4d. It can be observed that the encrypted Lena image bears no resemblance to the original image, indicating the effectiveness of our S-box. Additionally, the histogram of the encrypted image in Figure 4d exhibits a uniform distribution.

To further assess the performance of our proposed method, we tested it on a gray image with 125 gray values, as shown in Figure 5a. Figure 5c shows the corresponding histogram. Figure 5b displays gray image(encrypted) produced by proposed S-box. As shown in results, the pixels of the encrypted image appear to be randomly distributed. Furthermore, the histogram of gray encrypted image is uniform.



(a)
(b)
(c)
(d)

FIGURE 5. Figure 5a shows a one gray scale image and its histogram in Figure 5c, while Figure 5b depicts the encrypted image and its histogram is in Figure 2d.

V. CONCLUSION

In literature, extensively S-box construction methods are based on chaotic maps but chaos-based approaches have certain attractive properties for this purpose, they also have some inherent weaknesses, including finite precision effect, dynamical degradation of chaotic systems, non-uniform distribution, discontinuity in chaotic sequences. These weaknesses can limit the effectiveness of chaotic map-based substitution boxes. In this paper, we propose an innovative approach for constructing dynamic S-boxes using three Gaussian distribution-based random number generation techniques: the Box-Muller transform, the polarization decision method, and the central limit theorem. By utilizing the Gaussian distribution-based method, our proposed approach overcomes the deficiencies of current chaos-based S-box techniques. However, one of the main drawbacks of using Gaussian distribution-based pseudo-random sequences is the low nonlinearity of the resulting S-boxes. To address this limitation, we introduce the use of genetic algorithms (GAs) to optimize the nonlinearity of Gaussian distribution-based S-boxes. Our proposed method demonstrated a high degree of nonlinearity, reaching a peak value of 112, similar to that achieved by the ASE algorithm.

REFERENCES

[1] W. Zhang and E. Pasalic, "Highly nonlinear balanced S-boxes with good differential properties," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7970–7979, Dec. 2014.

[2] M. Ratiner, "The method of S-box construction," *J. Discrete Math. Sci. Cryptogr.*, vol. 8, no. 2, pp. 203–215, 2005.

[3] K. Mohamed, M. N. M. Pauzi, F. H. H. M. Ali, S. Ariffin, and N. H. N. Zulkipli, "Study of S-box properties in block cipher," in *Proc. Int. Conf. Comput., Commun., Control Technol. (I4CT)*, Sep. 2014, pp. 362–366.

[4] J. Szczepanski, J. M. Amigo, T. Michalek, and L. Kocarev, "Cryptographically secure substitutions based on the approximation of mixing maps," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 52, no. 2, pp. 443–453, Feb. 2005.

[5] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, Mar. 2001.

[6] G. Jakimoski and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 2, pp. 163–169, Feb. 2001.

[7] T. T. K. Hue, T. M. Hoang, and D. Tran, "Chaos-based S-box for lightweight block cipher," in *Proc. IEEE 5th Int. Conf. Commun. Electron. (ICCE)*, Jul. 2014, pp. 572–577.

[8] D. Lambić, "S-box design method based on improved one-dimensional discrete chaotic map," *J. Inf. Telecommun.*, vol. 2, no. 2, pp. 181–191, Dec. 2018.

[9] Y. Wang, L. Yang, M. Li, and S. Song, "A method for designing S-box based on chaotic neural network," in *Proc. 6th Int. Conf. Natural Comput.*, Aug. 2010, pp. 1033–1037.

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

[11] D. B. Thomas, W. Luk, P. H. W. Leong, and J. D. Villasenor, "Gaussian random number generators," *ACM Comput. Surv.*, vol. 39, no. 4, p. 11, 2007.

[12] D. B. Thomas, "FPGA Gaussian random number generators with guaranteed statistical accuracy," in *Proc. IEEE 22nd Annu. Int. Symp. Field-Program. Custom Comput. Mach.*, May 2014, pp. 149–156.

[13] Y. Hu, Y. Wu, Y. Chen, and G. C. Wan, "Gaussian random number generator based on FPGA," 2018, *arXiv:1802.07368*.

[14] P. H. W. Leong, J. D. Villasenor, R. C. C. Cheung, and W. Luk, "Ziggurat-based hardware Gaussian random number generator," in *Proc. Int. Conf. Field Program. Logic Appl.*, 2005, pp. 275–280.

[15] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *NPJ Quantum Inf.*, vol. 2, p. 16021, Jun. 2016.

[16] T. Shinzato, "Box Müller method," Hitotsubashi Univ. Tokyo, Kunitachi, Japan, Tech. Rep. 0605570, 2007.

[17] A. Altaleb, M. S. Saeed, I. Hussain, and M. Aslam, "An algorithm for the construction of substitution box for block ciphers based on projective general linear group," *AIP Adv.*, vol. 7, no. 3, Mar. 2017, Art. no. 035116.

[18] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal, and U. Y. Bhatti, "Some analysis of S-box based on residue of prime number," *Proc. Pakistan Acad. Sci.*, vol. 48, no. 2, pp. 111–115, 2011.

[19] K. Loukhaoukha, J.-Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on Rubik's cube principle," *J. Electr. Comput. Eng.*, vol. 2012, pp. 1–13, Jan. 2012.

[20] G. A. Sathishkumar, K. Bhoopathy, and R. Sriraam, "Image encryption based on diffusion and multiple chaotic maps," *Int. J. Netw. Secur. Appl.*, vol. 3, pp. 181–194, Mar. 2011.

[21] C. K. Huang and H.-H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Opt. Commun.*, vol. 282, pp. 2123–2127, Jun. 2009.

[22] C. K. Huang, C.-W. Liao, S. L. Hsu, and Y. C. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system," *Telecommun. Syst.*, vol. 52, no. 2, pp. 563–571, 2013.

[23] J. S. Fouda, A. Eyebe, J. Y. Effa, S. L. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 3, pp. 578–588, 2014.

[24] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, "Construction of chaotic quantum magnets and matrix Lorenz systems S-boxes and their applications," *Chin. J. Phys.*, vol. 56, no. 4, pp. 1609–1621, Aug. 2018.

[25] J. M. Hassan and F. A. Kadhim, "New S-box transformation based on chaotic system for image encryption," in *Proc. 3rd Int. Conf. Eng. Technol. Appl. (IICETA)*, Sep. 2020, pp. 214–219.

[26] J.-M. Guo, D. Riyono, and H. Prasetyo, "Improved beta chaotic image encryption for multiple secret sharing," *IEEE Access*, vol. 6, pp. 46297–46321, 2018.

[27] M. F. Khan, K. Saleem, M. Alotaibi, M. M. Hazzazi, E. Rehman, A. A. Abbasi, and M. A. Gondal, "Construction and optimization of TRNG based substitution boxes for block encryption algorithms," *Comput., Mater. Continua*, vol. 73, no. 2, pp. 2679–2696, 2022.

[28] M. F. Khan, A. Ahmed, K. Saleem, and T. Shah, "A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system," *IEEE Access*, vol. 7, pp. 84980–84991, 2019.

[29] B. R. Gangadari and S. R. Ahamed., "Design of cryptographically secure AES like S-box using second-order reversible cellular automata for wireless body area network applications," *Healthcare Technol. Lett.*, vol. 3, no. 3, pp. 177–183, 2016.

[30] H. R. Yassein, N. M. G. Al-Saidi, and A. K. Farhan, "A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 2, pp. 523–542, Feb. 2022.

[31] J. Gayathri and S. Subashini, "A survey on security and efficiency issues in chaotic image encryption," *Int. J. Inf. Comput. Secur.*, vol. 8, no. 4, pp. 347–381, 2016.

[32] G. Zhao, G. Chen, J. Fang, and G. Xu, "Block cipher design: Generalized single-use-algorithm based on chaos," *Tsinghua Sci. Technol.*, vol. 16, no. 2, pp. 194–206, 2011.

[33] N. Hadj-Said, B. Belmeki, and A. Belgoraf, "Chaotic behavior for the secrete key of cryptographic system," *Chaos, Solitons Fractals*, vol. 23, no. 5, pp. 1549–1552, 2005.

[34] G. Jakimoski and L. Kocarev, "Analysis of some recently proposed chaos-based encryption algorithms," *Phys. Lett. A*, vol. 291, no. 6, pp. 381–384, 2001.

[35] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," *Phys. Lett. A*, vol. 309, nos. 1–2, pp. 75–82, Mar. 2003.

[36] Y. Lu, L. Li, H. Zhang, and Y. Yang, "An extended chaotic maps-based three-party password-authenticated key agreement with user anonymity," *PLoS ONE*, vol. 11, no. 4, Apr. 2016, Art. no. e0153870.

[37] E.-J. Yoon, "Efficiency and security problems of anonymous key agreement protocol based on chaotic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 7, pp. 2735–2740, 2012.

[38] A. H. Zahid and M. J. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, 2019.

[39] M. F. Khan, K. Saleem, M. M. Hazzazi, M. Alotaibi, P. K. Shukla, M. Aqeel, and S. A. Tuncer, "Human psychological disorder towards cryptography: True random number generator from EEG of schizophrenics and its application in block encryption's substitution box," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–20, Jun. 2022.

[40] F. U. Islam and G. Liu, "Designing S-box based on 4D-4wing hyperchaotic system," *3D Res.*, vol. 8, no. 1, pp. 1–9, Mar. 2017.

[41] Ü. Çavuşoğlu, A. Zengin, I. Pehlivan, and S. Kaçar, "A novel approach for strong S-box generation algorithm design based on chaotic scaled Zhongtang system," *Nonlinear Dyn.*, vol. 87, no. 2, pp. 1081–1094, 2017.

[42] M. Ahmad, N. Mittal, P. Garg, and M. M. Khan, "Efficient cryptographic substitution box design using travelling salesman problem and chaos," *Perspect. Sci.*, vol. 8, pp. 465–468, Sep. 2016.

[43] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3317–3326, Aug. 2019.

[44] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[45] H. Nasry, A. A. Abdallah, A. K. Farhan, H. E. Ahmed, and W. I. E. Sobky, "Multi chaotic system to generate novel S-box for image encryption," *J. Phys., Conf. Ser.*, vol. 2304, no. 1, Aug. 2022, Art. no. 012007.

[46] M. Sarfraz, I. Hussain, and F. Ali, "Construction of S-box based on Mobius transformation and increasing its confusion creating ability through invertible function," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 2, p. 187, 2016.

[47] E. A. Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyperchaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, 2018.

[48] D. Lambić, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2407–2413, 2017.

[49] M. F. Khan, K. Saleem, T. Shah, M. M. Hazzazi, I. Bahkali, and P. K. Shukla, "Block cipher's substitution box generation based on natural randomness in underwater acoustics and Knight's tour chain," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–17, May 2022.

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

[51] A. H. Zahid, M. Ahmad, A. Alkhayyat, M. J. Arshad, M. M. U. Shaban, N. F. Soliman, and A. D. Algarni, "Construction of optimized dynamic S-boxes based on a cubic modular transform and the sine function," *IEEE Access*, vol. 9, pp. 131273–131285, 2021.

[52] H. Liu, A. Kadir, and Y. Niu, "Chaos-based color image block encryption scheme using S-box," *AEU-Int. J. Electron. Commun.*, vol. 68, no. 7, pp. 676–686, Jul. 2014.

[53] X. Zhang, Z. Zhao, and J. Wang, "Chaotic image encryption based on circular substitution box and key stream buffer," *Signal Process., Image Commun.*, vol. 29, no. 8, pp. 902–913, 2014.

[54] G. Liu, W. Yang, W. Liu, and Y. Dai, "Designing S-boxes based on 3-D four-wing autonomous chaotic system," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1867–1877, 2015.

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

[56] A. H. Zahid, M. J. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Entropy*, vol. 21, no. 3, p. 245, May 2019.

[57] M. F. Khan, K. Saleem, M. A. Alshara, and S. Bashir, "Multilevel information fusion for cryptographic substitution box construction based on inevitable random noise in medical imaging," *Sci. Rep.*, vol. 11, no. 1, pp. 1–23, Jul. 2021.

[58] A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," *IEEE Access*, vol. 8, pp. 150326–150340, 2020.

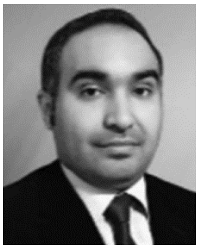
[59] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, Jan. 2017.

[60] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of cryptographic S-boxes based on Mobius transformation and chaotic tent-sine system," *IEEE Access*, vol. 7, pp. 173273–173285, 2019.

[61] C. Li, D. Arroyo, and K.-T. Lo, "Breaking a chaotic cryptographic scheme based on composition maps," *Int. J. Bifurcation Chaos*, vol. 20, no. 8, pp. 2561–2568, 2010.

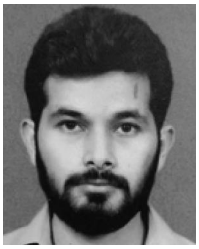
[62] C. Li, S. Li, and K.-T. Lo, "Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 2, pp. 837–843, 2011.

[63] J. Daemen and V. Rijmen, *The Design of RIJNDAEL: AES—The Advanced Encryption Standard*. Berlin, Germany: Springer-Verlag, 2002.



ADEL R. ALHARBI received the B.S. degree in computer science from Qassim University, Saudi Arabia, in 2008, and the M.S. degrees in security engineering and computer engineering and the Ph.D. degree in computer engineering from Southern Methodist University, Dallas, TX, USA, in 2013, 2015, and 2017, respectively. He has been a Faculty Staff Member with the College of Computing and Information Technology, University of Tabuk, Saudi Arabia, since 2009. He acquired several academic certificates and published several scientific articles.

SAJJAD SHAUKAT JAMAL received the Ph.D. degree in mathematics from Quaid-i-Azam University, Islamabad, Pakistan. Currently, he is an Assistant Professor with the Department of Mathematics, King Khalid University, Abha, Saudi Arabia. He has several quality research articles in well-reputed journals on the application of mathematics in multimedia security. His research interests include mathematics, number theory, cryptography, digital watermarking, and steganography.



MUHAMMAD FAHAD KHAN is currently an Assistant Professor with Foundation University Islamabad and also a Ph.D. Scholar with the Department of Computer Science, Quaid-i-Azam University, Islamabad. He is the author of more than 50 research articles. His research interests include steganography, cryptography, and multimedia communication.

MOHAMMAD ASIF GONDAL is a Professor and the Director of the Department of Scientific Research, Dhofar University. He is the author of more than 200 research articles. His research interests include steganography, cryptography, and multimedia communication.

AAQIF AFZAAL ABBASI is an Associate Professor with Foundation University Islamabad. He published more than 50 papers in well reputed journals and conferences. His research interests include the IoT, multimedia communication, and 4G.