Flower Pollination Based Strategy and Chaos for Designing Bijective Substitution Boxes

Hussam S. Alhadawi
Information Technology Department, Midland Oil Company, Ministry of Oil, 10001 Baghdad, Iraq
hussam.alddin@outlook.com

Keywords: Substitution Boxes, Flower Pollination Algorithm, Cryptography.

Abstract: Substitution-boxes (S-boxes) are essential nonlinear elements in modern symmetric cryptographic systems, offering confusion and resilience against cryptanalysis. The rising need for secure communication highlights the imperative to develop resilient S-boxes with formidable cryptographic properties. This work aims to develop novel 8×8 S-boxes utilizing a hybrid approach that integrates the flower pollination algorithm (FPA) with chaotic maps. The suggested method uses a one-dimensional discrete chaotic map to generate high-quality initial S-boxes, addressing the constraints of traditional FPA techniques that may become trapped in local optima. These preliminary solutions facilitate an effective optimization procedure. The FPA metaheuristic optimizes the S-box configurations by refining a fitness function that embodies critical cryptographic requirements. The produced S-boxes are assessed using conventional metrics, such as bijectivity, rigorous avalanche criterion, nonlinearity, input/output XOR distribution, bit independence criterion, and maximal predicted linear probability. The results are juxtaposed with alternative approaches for S-box generation utilizing optimization techniques. The results demonstrate that the suggested technique generates S-boxes with robust cryptographic attributes and enhanced resilience to various forms of cryptanalytic assaults. This paper offers both theoretical and practical advances by presenting an effective hybrid optimization framework for S-box designs, enhancing the security of contemporary encryption systems.

1 INTRODUCTION

An $n \times n$ S-box is mathematically mapped as $S: \{0,1\}^n \rightarrow \{0,1\}^n$; it is deployed for a nonlinear transformation of an input string of n-bits size into a relatively sized output string. The relationship between the I/O values of an S-box can be determined to satisfy the security criteria [1]. One of the most important criteria that is responsible for resisting linear cryptanalysis and for achieving the required level of confusion in ciphers is nonlinearity [2]. The advancement of cryptanalysis attacks on DES S-boxes has transformed the challenge of producing S-boxes with superior cryptographic attributes. Nonetheless, several unresolved issues persist concerning the design of S-boxes for cryptographic applications[3]. The creation of the S-box, capable of withstanding cryptanalysis, is regarded as an NP-hard issue [3]. It is hard to design an S-box with flawless cryptographic features; hence, a compromise is considered required [4]. The S-box may often be generated by one of three broad approaches:[5], algebraic techniques, random search, or metaheuristic methods. These strategies provide distinct advantages and drawbacks. For instance, although it is the most straightforward strategy, the random search method typically produces S-boxes with subpar cryptographic characteristics. Algebraically produced S-boxes have superior cryptographic characteristics [6], although it is infeasible to identify an extensive collection of robust S-boxes by this methodology. Metaheuristic algorithms are the foundation of the third approach for S-box design, which is extensively researched across many applications. Since the 1990s, a great deal of research has demonstrated that using metaheuristic optimization algorithms is a very successful approach for S-box design, especially considering how well they work in both software and hardware implementations. Numerous optimization techniques, including both evolutionary and swarm intelligence approaches, have been investigated. Researchers have created S-boxes with remarkable cryptography properties by employing a variety of optimization

strategies. Despite these developments, there are still a number of unsolved problems with S-box design and analysis. A solitary meta-heuristic-based S-box cannot assert superiority over its alternatives. Therefore, investigating a novel metaheuristic-based S-box design technique is a valuable pursuit. The flower pollination algorithm (FPA) is a population-based algorithm developed by Yang [7] that stimulates the pollination behavior of flowering plants. This paper employs a one-dimensional discrete chaotic map to enhance the efficacy of the Flower Pollination Algorithm, resulting in the designation of the proposed system as the "Chaotic Flower Pollination Algorithm (CFPA)." The remainder of the paper was organized as follows: The suggested CFPA was described in Section 2, and the outcomes of the suggested method-based S-boxes were shown in Section 3. The performance analysis of the acquired findings was described in Section 4. The conclusion of the research is given in Section 5.

2 THE PROPOSED ALGORITHM (CFPA)

The pollination behavior of blossoming plants served as the inspiration for the Flower Pollination Algorithm (FPA), a meta-heuristic algorithm. Yang created FPA to solve global optimization problems [7]. This section provides a detailed overview of FPA. A flower's primary function is to reproduce through the act of pollination. The process of pollination involves moving pollen from one area to another using pollinators, including insects, butterflies, birds, bees, bats, wind, and water. This type of pollination is known as biotic pollination if the pollen is spread by insects or animals. Abiotic pollination occurs when pollen is transferred by non-animal means like wind or water. Additionally, pollination can occur from the same bloom (self-pollination) or from a different flower (cross-pollination) [8]. According to the aforementioned guidelines, FPA may be mathematically divided into two components: the local pollination phase and the global pollination step. Global pollination is the process by which pollinators use lengthy flights to transport pollen over enormous distances.

$$x_i^{(t+1)} = x_i^{(t)} + \gamma L\acute{e}vy(\lambda)\left(gbest_t - x_i^{(t)}\right). \quad (1)$$

Where γ is the scaling parameter that controls the step size of the Lévy flight, $\gamma > 0$. $L\acute{e}vy\,(\lambda)$ is a function to produce step size, which is essential to the strength of the pollination. Lévy (λ) refers to the flight behaviour of pollinators based on the Lévy distribution:

$$L\acute{e}vy(\lambda) = \frac{\lambda\Gamma(\lambda)\sin\left(\frac{\pi\lambda}{2}\right)}{\pi}\frac{1}{s^{1+\lambda}}, (s \gg s_0 > 0). \quad (2)$$

$\Gamma(\lambda)$ is the standard gamma function. The recommended value of distribution factor λ is selected from 0.3 to 1.99 [9]. This distribution is valid for large steps s > 0. Local pollination is formulated by the following equation:

$$x_i^{(t+1)} = x_i^{(t)} + \epsilon(x_j^{(t)} - x_k^{(t)}). \quad (3)$$

Where $x_j^{(t)}$ and $x_k^{(t)}$ are random, selected pollens, ϵ is a uniform distribution in [0, 1]. In this context, Equation 3 simulates the characteristics of abiotic pollination and self-pollination, focusing on flower constancy. A switch condition based on random probability p is used to alternate between global pollination and local pollination.

The proposed S-box generation framework leverages a 1-D discrete chaotic map based on Lehmer code permutations to govern the global and local pollination movements of the Flower Pollination Algorithm (FPA). In this approach, the evolution of the pollinator population is driven by the iterative map:

$$Z_{i+1} = Z_i \; o \; l^{-1}(|l(C \; o \; Z_i) - l((C \; o \; Z)^r)|), \quad (4)$$

where the composition of permutations and the Lehmer bijective function $l: S_m \rightarrow \{0,1,2, \ldots, m! - 1\}$ provides a complex, non-linear trajectory. By correlating the discrete chaotic states with the S-box candidate space, the technique leverages the map's intrinsic ergodicity and sensitivity, enabling the FPA to navigate the extensive 256! search space more efficiently than conventional random walks. This distinct chaotic impact is essential for preserving population variation and averting stagnation of the fitness function during optimization for nonlinearity and differential uniformity. By replacing the conventional switch probability and step size with values obtained from this permutation-based chaos, the resultant S-boxes demonstrate improved cryptographic strength and structural intricacy. The standard nonlinearity of each generated S-box, calculated as follows, is the fitness function used in this work to evaluate each flower within the pollinator population:

$$N_g = 2^{n-1}(1 - 2^{-n} \max_{w \in GF(2^n)} |WS \prec g \succ (w)|). \quad (5)$$

Table 1: S-box produced by CFPA.

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

Table 2: Nonlinearity score of the proposed method.

S-box	L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8	Min.	Avg.
NL	108	106	106	106	110	110	108	108	106	107.75

The Walsh spectrum of $g(x)$ can be described as:

$$WS < g > (w) = \sum_{\lambda \in GF(2^n)} (-1)^{g(x) \oplus x.w}, \quad (6)$$

Where $w \in GF(2^n)$ and $\lambda . w$ signifies the dot product of λ and w written as:

$$error = 112 - NL(f_i). \quad (7)$$

Where the Advanced Encryption Standard's (AES) optimal nonlinearity value is 112 [10]. NL is a representation of the floral individual's nonlinearity function. The population's minimum error value for the current iteration determines the ideal flower worldwide.

2.1 Adjustment

Each pollen gamete functions as a possible 8x8 S-box in the Flower Pollination Algorithm (FPA), arranged in a string of 256 unique elements to guarantee bijectivity. The normal mathematical updates frequently cause the values to become out of alignment during the global and local pollination processes, which is where the problem occurs. In the range of 0 to 255, this often leads to repeated numbers or missing integers, which effectively destroys the one-to-one mapping required for a secure cypher. A repair mechanism handles these duplicates and fills in the gaps to maintain the validity of the S-box. As a result, the following procedures are used to apply a repair mechanism to every flower in the population:

1) To find redundant values, every S-box sequence is thoroughly inspected. The location of the duplicate element is noted in a temporary sequence V when a duplication is found. Additionally, this scanning procedure determines whether particular integers from the set $\{0,1,\ldots,255\}$ are missing.
2) Sequence V_2 is the collection of possible unique values that results from compiling the missing numbers into a sorted set and identifying the associated unoccupied locations.
3) In order to guarantee that the final flower individual reflects a legitimate, bijective S-box, the places noted in sequence V are then randomly populated using the available values from sequence V_2.

3 PERFORMANCE ANALYSIS OF THE PROPOSED S-BOX

This section presents descriptions of S-box design issues; the parameter configuration for the suggested method was established as follows: Population size equals 50 flowers, number of iterations equals 100, and switch probability p equals 0.8. Table 1 presents the S-box created in this investigation.

To evaluate the cryptographic strength of the S-box developed in this study; we employed various contemporary benchmarks created by security researchers to verify newly designed substitution components. The fundamental notion of differential uniformity was introduced by [11] through the differential cryptanalysis of DES, laying the groundwork for computing differential probability via input/output XOR distributions. Similarly, the work of [12] on linear cryptanalysis highlighted the critical role of linear approximation probability in determining cipher resilience. Furthermore, Dawson and Tavares [13] integrated information-theoretic principles into the design requirements for substitution layers. Consequently, the structural integrity of the proposed S-box is appraised using six primary criteria: the bijective property, nonlinearity, the strict avalanche criterion (SAC), the bit independence criterion (BIC), maximum expected linear probability (MELP), and differential uniformity. The efficacy of the resultant S-box in this investigation was juxtaposed with many S-boxes produced using metaheuristic-based techniques.

Table 3: SAC for the proposed S-box.

0.5625	0.5313	0.5156	0.5781	0.5000	0.5938	0.5156	0.5000
0.4844	0.4844	0.5000	0.5313	0.4844	0.4688	0.5156	0.5469
0.5781	0.4531	0.5469	0.5313	0.4531	0.5469	0.4375	0.5000
0.4531	0.5156	0.5156	0.4844	0.4844	0.4375	0.4688	0.4844
0.4844	0.5625	0.4688	0.5000	0.5000	0.4688	0.4375	0.4531
0.4688	0.5156	0.5156	0.5156	0.5000	0.4531	0.5625	0.5000
0.5625	0.4688	0.4844	0.5156	0.5156	0.5469	0.4844	0.5156
0.4688	0.4375	0.4688	0.5156	0.4219	0.4844	0.5156	0.5156

Table 4: BIC-SAC for the produced S-box.

–	0.4866	0.5000	0.5045	0.5201	0.5156	0.4911	0.5000
0.5134	–	0.4911	0.5112	0.5156	0.5000	0.4955	0.5268
0.5000	0.5223	–	0.5000	0.5179	0.5201	0.529	0.5067
0.4978	0.5067	0.5089	–	0.5223	0.4978	0.4911	0.5379
0.5022	0.4978	0.5022	0.4888	–	0.4911	0.5067	0.4866
0.5000	0.5045	0.4911	0.5313	0.5223	–	0.5246	0.5156
0.4754	0.5223	0.4933	0.4888	0.4777	0.5112	–	0.4978
0.4866	0.4978	0.4665	0.4799	0.5000	0.5022	0.4978	–

Table 5: BIC-nonlinearity for generated S-box.

–	102	104	106	104	104	106	106
102	–	104	104	102	108	102	102
104	104	–	106	106	100	106	104
106	104	106	–	104	100	104	104
104	102	106	104	–	106	104	104
104	108	100	100	106	–	106	106
106	102	106	104	104	106	–	100
106	102	104	104	104	106	100	–

Table 6: Comparative analysis for optimization algorithms with chaos-based S-boxes.

S-box Methods	Nonlinearity			SAC	BIC-NL		BIC-SAC	DP	LP
	Min.	Max.	Avg.	Avg.	Min.	Avg.	Avg.		
Proposed	106	110	107.75	0.5004	100	104.07	0.50343	10	0.1172
Firefly algorithm [14]	106	108	107.00	0.4963	102	104.64	0.4974	10	0.1250
Ant Colony optimization [15]	106	108	107.00	0.5015	98	104.21	0.5016	10	0.1172
Teaching learning [16]	104	110	106.50	0.4995	98	104.57	0.4983	10	0.1172
Bacterial Foraging [17]	106	110	107.50	0.5093	94	103.07	0.5029	10	0.1015
Jaya Algorithm [18]	104	108	106.25	0.5002	96	103.64	0.4996	10	0.1172
Particle swarm optimization [19]	104	108	106.50	0.5036	96	102.85	0.4995	10	0.1328
Nomadic people optimizer [20]	106	108	107.25	0.5034	98	103.00	0.5045	10	0.0706

3.1 Bijection

In an 8×8 S-box, the criterion for bijectivity is fulfilled when the produced S-box has a unique output value within the range [0, 255]. All distinct output values of the created S-boxes fall inside the interval [0, 255], so ensuring that the S-boxes produced by CFPA techniques meet the criteria of bijectivity.

3.2 Nonlinearity

High nonlinearity is an important trait for making sure that plaintext is confused and for making block ciphers more resistant to linear cryptanalysis. In the case of Boolean functions, this metric measures the minimum Hamming distance to the set of all affine functions, which is found by using the Walsh-Hadamard transform as defined in Eq. 5. The nonlinearity results for the S-box synthesized via the chaotic flower pollination algorithm are detailed in Table 2. The scores are clearly between 106 and 110, with an average nonlinearity of 107.75. This shows that the proposed S-box has the right level of cryptographic strength to protect against linear-based attacks.

3.3 Strict Avalanche Criteria

The Strict Avalanche Criterion (SAC) was initially introduced by [21]. his criterion specifies that the likelihood of all output bits changing is fifty percent when a single input bit is altered. They proposed an efficient method for verifying if the S-box meets the criteria for Strict Avalanche Criterion (SAC). The S-box's Strict Avalanche Criterion (SAC) is characterized by the dependence matrix; specifically, if each element in the dependence matrix approaches the optimal value of 0.5, the S-box nearly fulfills the SAC. The specifics of this computation are located in [21]. The SAC value of the suggested S-box is displayed in Table 3, with an average of 0.500495, which approximates the recommended value of 0.5.

3.4 Bit Independence Criteria

The pairwise independence of all avalanche vector sequences generated from a single plaintext complementation was first defined by [21] using the Output Bits Independence Criterion (BIC). The correlation between each pair's constituent parts can be used to evaluate the pairwise independence of pairs. Consider an S-box characterized by the Boolean functions $h_1, h_2, \dots, h_{n,}$; an S-box that fulfil the BIC, $h_{j \oplus h_k (j \neq k, 1 \leq j,k \leq n)}$, has been previously said to comply with the avalanche criterion and is expected to exhibit strong nonlinearity. Tables 4 and 5 represent the average BIC-SAC and BIC-nonlinearity values, respectively, for the S-box generated in this study.

3.5 Differential Probability

The S-box is a nonlinear element of an encryption procedure. Ideally, the S-box should exhibit differential uniformity; nevertheless, to guarantee a uniform mapping, each input differential must correspond uniquely to an output differential. These characteristics guarantee the likelihood of a consistent mapping for each input bit i. The differential uniformity of an S-box, when assessed using the differential approximation probability approach, may be mathematically expressed as:

$$DP(\Delta x \rightarrow \Delta y) = \left[\frac{\#\{x \in X | s(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^n} \right] \quad (5)$$

Where Δx and Δy are the input and output differentials, respectively. The highest achieved DP value was 0.039. This serves as more evidence that the suggested S-box can endure differential cryptanalysis.

3.6 Melp

Generally, the maximum imbalance value of an event can only be assessed using the maximal expected linear probability (MELP). It is a valuable metric for ascertaining the maximum. An imbalance influences the value of an event's result. Γx and Γy indicate two masks applied on the parity of the input and output bits, respectively. The MELP of bias for a certain S-box is delineated in [12]:

$$DP(\Delta x \rightarrow \Delta y) = \left[\frac{\#\{x \in X | s(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^n} \right]. \quad (8)$$

The set X encompasses all potential inputs, whereas 2^n denotes the quantity of its elements. According to standard design standards, the major objective is to maintain the bijectivity of the S-box while optimizing its minimal nonlinearity value.

4 COMPARISON ANALYSIS

Recently, many S-box designs have shifted toward using optimization algorithms. Current research often combines chaos theory with these optimization

methods [14]-[20]. Table 6 compares our proposed method with existing S-boxes, leading to several key observations summarized below.

- The suggested S-box in this study produced exceptional outcomes, achieving the highest nonlinearity among methods [16], [18]-[20] and the best average nonlinearity in comparison to all other methods. The results show that the suggested method works well to create S-boxes that are cryptographically strong and can withstand linear cryptanalysis.
- In the SAC test, all of the S-boxes that were compared did well, with their values coming very close to the ideal theoretical value of 0.5.
- The S-box created in this study demonstrated BIC-SAC results comparable to those of the other designs examined. The proposed S-box had a minimum BIC-nonlinearity value that was slightly lower than what was reported in [18], but it outperformed all the other substitution boxes that were compared.
- The proposed S-box reached a maximum DP value of 10, which is the same as the performance of the other substitution boxes in Table 6.
- The LP values in Table 6 indicate that the S-box created in this study gave the same results as those in [15], [16], [18], and performed better than the S-boxes in [18], [19]. The values were slightly lower than those in [17], [20], but the results indicate that the proposed method works well to create S-boxes that are difficult to break with linear cryptanalysis.

5 CONCLUSIONS

This paper presents a novel approach for constructing high-performance cryptographic S-boxes by integrating the Flower Pollination Algorithm (FPA) with a one-dimensional discrete chaotic map. The proposed Chaotic Flower Pollination Algorithm (CFPA) enhances the optimization process by introducing chaotic characteristics and employing Lehmer-coded permutations to achieve a more effective exploration of the cryptographic search space.

The generated S-box was comprehensively evaluated using several widely accepted security metrics, including bijectivity, nonlinearity, Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), Differential Probability (DP), and Linear Probability (LP). The experimental findings confirm that the proposed S-box fulfills the essential requirements of a secure cryptographic substitution component.

The achieved high nonlinearity values demonstrate strong resistance against linear cryptanalysis, while the SAC and BIC results confirm excellent diffusion capability and statistical independence among output bits. In addition, the low DP and LP values indicate that the generated S-box provides enhanced resistance against differential and linear cryptanalytic attacks.

A comparative analysis with existing S-box construction techniques shows that the proposed CFPA approach achieves competitive and, in several cases, superior performance across important cryptographic criteria. These results validate the effectiveness of combining chaotic systems with evolutionary optimization algorithms for generating secure and efficient substitution boxes.

Overall, the proposed CFPA-based S-box design provides a reliable and robust solution for modern cryptographic applications, including secure communication systems, lightweight cryptography, and advanced block cipher architectures requiring highly nonlinear and resilient substitution mechanisms.

REFERENCES

[1] F. Özkaynak and S. Yavuz, “Designing chaotic S-boxes based on time-delay chaotic system,” Nonlinear Dynamics, vol. 74, no. 3, pp. 551-557, 2013.

[2] C. E. Shannon, “Communication theory of secrecy systems,” Bell Labs Technical Journal, vol. 28, no. 4, pp. 656-715, 1949.

[3] Y. Tian and Z. Lu, “S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm,” Journal of Systems Engineering and Electronics, vol. 27, no. 1, pp. 232-241, 2016.

[4] C. Carlet, “On highly nonlinear S-boxes and their inability to thwart DPA attacks,” in INDOCRYPT 2005, Springer, 2005, pp. 49-62.

[5] S. Picek, E. Marchiori, L. Batina, and D. Jakobovic, “Combining evolutionary computation and algebraic constructions to find cryptography-relevant Boolean functions,” in International Conference on Parallel Problem Solving from Nature, Springer, 2014, pp. 822-831.

[6] C. Carlet, “On the higher order nonlinearities of Boolean functions and S-boxes, and their generalizations,” in International Conference on Sequences and Their Applications, Springer, 2008, pp. 345-367.

[7] X.-S. Yang, “Flower pollination algorithm for global optimization,” in International Conference on Unconventional Computing and Natural Computation, Springer, 2012, pp. 240-249.

[8] Z. A. A. Alyasseri, A. T. Khader, M. A. Al-Betar, M. A. Awadallah, and X.-S. Yang, “Variants of the

flower pollination algorithm: a review," Nature-Inspired Algorithms and Applied Optimization, pp. 91-118, 2017.

[9] I. Pavlyukevich, "Lévy flights, non-local search and simulated annealing," Journal of Computational Physics, vol. 226, no. 2, pp. 1830-1844, 2007.

[10] J. Daemen, "AES Proposal: Rijndael," AES Algorithm Submission, 1999, [Online]. Available: http://csrc.nist.gov/encryption/aes/Rijndael.pdf.

[11] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," in Advances in Cryptology-CRYPTO 1990, Springer, 1991, pp. 2-21.

[12] M. Matsui, "Linear cryptanalysis method for DES cipher," in Workshop on the Theory and Application of Cryptographic Techniques, 1993, pp. 386-397.

[13] M. Dawson and S. E. Tavares, "An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks," in Workshop on the Theory and Application of Cryptographic Techniques, 1991, pp. 352-367.

[14] H. A. Ahmed, M. F. Zolkipli, and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," Neural Computing and Applications, pp. 1-10, 2018.

[15] M. Ahmad, D. Bhatia, and Y. Hassan, "A novel ant colony optimization based scheme for substitution box design," Procedia Computer Science, vol. 57, pp. 572-580, 2015.

[16] T. Farah, R. Rhouma, and S. Belghith, "A novel method for designing S-box based on chaotic map and Teaching-Learning-Based Optimization," Nonlinear Dynamics, vol. 88, no. 2, pp. 1059-1074, 2017.

[17] Y. Tian and Z. Lu, "Chaotic S-Box: Intertwining Logistic Map and Bacterial Foraging Optimization," Mathematical Problems in Engineering, 2017.

[18] M. 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.

[19] H. S. Alhadawi, S. Q. Salih, and Y. D. Salman, "Chaotic particle swarm optimization based on meeting room approach for designing bijective S-boxes," in International Conference on Emerging Technologies and Intelligent Systems, Springer, 2021, pp. 331-341.

[20] H. S. Alhadawi, M. Ahmad, and S. Q. Salih, "A novel bijective substitution box design based on nomadic people optimizer and discrete chaotic map," Knowledge-Based Systems, vol. 325, p. 113977, 2025.

[21] A. Webster and S. E. Tavares, "On the design of S-boxes," in Conference on the Theory and Application of Cryptographic Techniques, Springer, 1985, pp. 523-534.