INSTITUTE OF INFORMATION
AND COMMUNICATION TECHNOLOGIES
BULGARIAN ACADEMY OF SCIENCES
CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **26**, No 2
Sofia • 2026
Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2026-0018

A Chaotic-Initiated Discrete Optimization Framework for Cryptographically Strong AES S-Box Generation

Sameeh Abdulghafour Jassim[1], *Alyaa Hasan Zwiad*[2], *Zena Mohammad Saadi Al-Beder*[3]

[1]*Department of Computer Sciences, College of Science, University of Al Maarif, Al Anbar, 31001, Iraq*
[2]*University of Technology, Iraq*
[3]*Computer Science College, University of Technology, Iraq*
E-mails: sameeh@uoa.edu.iq Alyaa.H.Zwiad@uotechnology.edu.iq
cs.22.15@grad.uotechnology.edu.iq

***Abstract*:** *Advanced Encryption Standard* (*AES*) *security relies on the Substitution box* (*S-Box*)*, which provides nonlinearity and confusion. Because this algebraic form is fixed, the cipher can be attacked with algebraic and structural cryptanalysis. To address this shortcoming, we proposed generating AES-compatible S-Boxes utilising chaotic Fisher-Yates initialization and metaheuristic optimization. A multi-objective fitness function, including the Average NonLinearity* (*AvgNL*)*, Minimum NonLinearity* (*MinNL*)*, and Differential Uniformity* (*DU*)*, is used to select the optimal S-Box. The experimental results show that the constructed S-Box has a considerable average nonlinearity of about 112, and average Strict Avalanche Criterion* (*SAC*) *and Bit Independence Criterion* (*BIC*) *Non-linearity values of 0.50048 and 104.285, respectively. Also, its NPCR and UACI are approximately 99.5924 and 33.3214, respectively. Moreover, histogram, correlation, and entropy analyses of images encrypted by the proposed system indicate that the proposed S-Box provides stronger security and greater flexibility for image encryption.*

***Keywords*:** *Security, Chaos theory, Logistic map, Nonlinearity, Metaheuristic optimization.*

1. Introduction

Currently, the Advanced Encryption Standard (AES) algorithm is considered the most popular symmetric cryptographic algorithm, favored for its robust resistance to attacks and its high efficiency [1]. Furthermore, the AES security relies heavily on the strength of its Substitution box (S-Box). Therefore, the heart of an AES encryption is the S-Box, which provides the nonlinearity and confusion of the block cipher [2, 3]. The classical method of designing an AES S-Box relies on algebraic inversion in a finite field, combined with an affine transformation, and thus yields a

highly structured S-Box. While still extremely secure in practice, the algebraic regularity of this S-Box may make it vulnerable to the most feared algebraic and structural cryptanalyses [4].

In the last few years, the growing need for light-weight, dynamic, and dedicated cryptographic primitives, especially for image encryption, IoT, and multimedia security applications, has pushed researchers to investigate other S-Box construction methods. Chaotic systems have proved to be a good solution due to their basic characteristics, such as sensitivity to initial conditions, pseudorandomness, and ergodicity [5, 6]. Moreover, there is hope that metaheuristic optimization algorithms will show notable potential for improving cryptographic properties by efficiently exploring large permutation spaces [7].

The Swarm Space Hopping Algorithm (SSHA) is a metaheuristic search algorithm that uses three complementary search strategies: (i) directed search toward the current best global solution, to increase exploitation; (ii) directed search toward the current local best or away from a randomly selected individual, to increase exploration and reduce the convergence; (iii) a space hopping strategy based on the arithmetic crossover operation, that lets the individuals adaptively jump across the search space by moving between the two halves of the search space when the individuals are stagnating [8].

In our proposed scheme, the methodology is built on the key concepts of the SSHA [8], specifically the multi-reference-guided search and its space-hopping exploration mechanism. However, the proposed method introduces a problem-specific reformulation tailored to discrete permutation optimization, which is used to design S-Boxes. Unlike the original SSHA algorithm, the adaptation algorithm would operate strictly within the permutation space via a bijection-preserving representation, thereby preserving valid structures as much as possible during the search process. It is important to clarify that, since position copying and crossover-based operators are utilised, the lightweight and deterministic repair methods are applied when required to ensure the bijectivity again. These operations are not an independent repair optimization, but they are a part of maintaining the permutation feasibility.

To manipulate the constraints in the chaos initialization, the chaotic Fisher–Yates shuffle is utilised rather than the rounding-based map in order to generate initial populations, thereby preventing bias in the initial permutations and achieving a decent statistical distribution from the first iteration. Additionally, search dynamics are modified by using a hybrid update strategy that integrates multi-agent leading, stochastic swap-based perturbations, and half-space chaos hopping. To guarantee an improved balance among exploration and stable convergence behavior.

Compared with conventional approaches, which depend on one fixed best solution, the developed approach utilises a distribution-based reference approach. Several high-quality agents guide the search trajectory to the optimal solutions. This design will efficiently avoid premature convergence in the search, minimize algorithmic bias, and enhance diversity and entropy levels within the designed substitution boxes.

A well-defined multi-objective fitness function acts as the core mechanism of the optimization procedure. It integrates Average NonLinearity (AvgNL), Minimum NonLinearity (MinNL), and Differential Uniformity (DU). Ultimately, the effectiveness and reliability of the proposed framework are verified through 30 independent runs, supported by convergence analysis, statistical evaluation, boxplot visualization, and additional performance metrics. The findings reveal improved cryptographic robustness, along with stable performance across multiple runs, which addresses concerns regarding experimental rigor and the credibility of the results. Also, the produced S-Box is embedded into an enhanced AES image encryption scheme to analyze its confusion and diffusion performance. The security analysis, covering nonlinearity, differential uniformity, avalanche performance, histogram sensitivity, correlation coefficient, entropy, NPCR, and UACI, has been extensively conducted to verify the proposed scheme against various cryptanalytic attacks.

The remaining part of this paper is organized as follows. The related works are described in section two. The S-Box problem is discussed in section three. The proposed approach is explained in section four. The evaluation of the proposed algorithms is described in section five. The most important results and the conclusion are introduced in section six.

2. Related works

The cryptographic strength of a block cipher fundamentally depends on its Sboxes, as they are the only nonlinear components that introduce Shannon's property of confusion. Therefore, it remains an ongoing research problem to generate S-Boxes that achieve superior cryptographic properties, such as high NL, robust Strict Avalanche Criterion (SAC), optimal Bit Independence Criterion (BIC), and minimal Differential Probabilities (DP) and Linear Probabilities (LP). The known methods for generating S-Boxes can be divided into three categories: algebraic design, chaos-based strategies, and metaheuristic approaches. Different benefits and drawbacks of these approaches, especially concerning dynamism, efficiency, and the depth of permutation-space exploration.

Algebraic and Structured Mathematical Constructions: This approach relies on well-understood algebraic structures and problems to generate S-Boxes with good properties deterministically. One of the most popular techniques uses groups over the residue classes of algebraic integers in a number field (e.g., the Gaussian Integers [9] or Eisenstein integers [10]). By carefully choosing a generator with a certain norm (floating point arithmetic), constructing a cyclic group, separating the real and imaginary parts (modular reduction), and extracting most or all of the bits in the generator output, a couple of pairs of bijective S-Boxes can be generated [9, 10]. These algebraic techniques provide fairly elegant and efficient construction schemes with good S-Box properties (nonlinearity up to 108, satisfactory SAC and BIC scores [9, 10]). Nonetheless, they are also rigorously static; their constructions provide S-Boxes that are permanent (fixed by the modulus, generator, etc.). They lack any inherent mechanism for key-dependent variability or dynamic

regeneration, making them susceptible to cryptanalysis that exploits a fixed nonlinear layer [11].

Chaos-based S-Box generation. Based on the inherent hierarchy, pseudo-randomness, and ergodicity of nonlinear dynamical systems, chaos-based algorithms extract entropy from chaotic maps to construct cryptographic S-Boxes. Commonly, the typical algorithm involves iterating a discrete [12] or continuous [13] time chaotic map, followed by normalization of its trajectory and direct mapping to a one-to-one permutation using the modulo operator, for instance. More recent variations utilize increasingly complex sets of maps, such as 2D hyperchaotic maps [14], time-delay systems, or combinations of systems integrated with quantum random walks to generate S-Boxes of similar cryptographic strength [15]. While chaos-based S-Box algorithms are capable of generating S-Boxes that exhibit well-known cryptographic attributes [12-15], in a dissenting critique of the rationale, Ozkaynak [16] suggested that robust S-Box structures can be achieved through non-chaotic frameworks. Ultimately, this study undermines the core premise that "complex chaos leads to cryptographically strong output," placing greater emphasis on the implementation of the algorithmic permutation logic. In addition, while chaos is used in image encryption schemes that dynamically select certain S-Boxes [14], the actual S-Boxes remain static, precomputed tables, and there are no algorithms that propose a further S-Box optimization phase to increase the cryptographic permutation space.

Metaheuristic optimization driven design. To directly explore the enormous space of 256! permutations to find optimized S-Boxes, the research groups treat S-Box formation as an optimization problem, mostly optimizing NL as the fitness value. Population-optimization metaheuristics based on biological models, such as the Globalized Firefly Algorithm (GFA) [17] and African Buffalo Optimization (ABO) [18], are used. These algorithms take as inputs random or chaos-seeded [17] candidate solutions and iteratively improve them using biologically motivated search strategies to produce S-Boxes with NL values above 108 110 [17, 18]. The advantage of this paradigm is that it can explicitly optimize a property like NL. However, there are major shortcomings: (i) in many cases, only a single objective optimization function is used, where the fitness values of the other properties like SAC or BIC are ignored; (ii) it is computationally expensive and not appropriate for dynamic, real time generation of S boxes; (iii) it standardly results in a single static S-Box for each run, that is not necessarily embedded with the strong criteria of the AES design.

Hybrid metaheuristic methods. Nowadays, the study of S-Box design has focused on the combination of chaotic systems with metaheuristic optimization in order to improve the cryptographic robustness. In spite of the notable progress, existing approaches still have limitations in their structure, which motivate further methodological refinement. A first hybrid metaheuristic approach considers multi-objective evolutionary optimizers, is illustrated in [19] when Davalos et al propose SBMO to jointly optimize the NL and the SAC by using Pareto-based evolutionary algorithms and chaotic initialisation; Despite this proposal has good performance (NL about 111.5), but also it has limited by restricted objective coverage (excluding

differential uniformity and bit independence), high dependence on the number of iterations (up to 5000 generations) and limited exploration diversity due to the fixed set of evolutionary operators without using adaptive search mechanisms. Another hybrid metaheuristic and chaos-based optimization study is given in [20], where Akyol presents a hybrid CSBA algorithm by combining the cuckoo search and bee algorithms, then initializes them using high-dimensional chaotic sets. Despite this, the proposal has good performance (NL about 109.75), and it improves population diversity, but it has also suffered from single-objective bias (optimization is mainly informed by NL), risk of getting stuck in premature convergence in a discrete permutation space, and lack of structured control over exploration–exploitation balance. The third study [21] involved general chaos-based optimizations with integrated the Particle Swarm Optimization (PSO) and Grey Wolf Optimizer (GWO), where higher-dimensional chaotic maps improve initial entropy and randomness, leading to higher quality initializations (with NL about 106.1); however, these approaches suffer from the weak refinement after initialization, limited stability across runs, and limited ability to control statistical correlation, resulting in variability in cryptographic performance. Another interesting study, X i and F a n [22] apply hash-driven chaotic sequences integrated with Simulated Annealing and an existing masking system to guarantee against side-channel attacks; Despite of this scheme has satisfactory levels of nonlinearity (NL about 111) and near-ideal SAC values, but it suffers from computational expensiveness, used single objective optimization function, and a design that is mainly dependent on the context of hardware masking, hence limiting its general applicability.

Fully integrated chaotic cryptosystems. Where chaotic S-Boxes are integrated into complete encryption algorithms, often targeted at images [11, 23]. As in the isolated S-Box case, improved security through dynamism is readily achieved, but this is often limited to the diffusion layer (chaotic pixel scrambling, etc.) or to selecting from several pre-synthesized S-Boxes [14]. The essential S-Box synthesis step is, in fact, often a simple chaotic map [11, 23] and does not benefit from the advanced permutation space search methods that produce the top-level cryptographic strength. Thus, highlights a disconnect between employing chaos for dynamism and systematically optimizing the core confusion element.

Identified research gaps and proposed contribution. The synthesis of the related work reveals several unresolved challenges that motivate the present work: (1) the static nature of algebraic and most chaos-based S-Boxes versus the need for key-dependent dynamism; (2) the overemphasis on chaotic source complexity over the optimization of the transformation process from chaos to cryptographically robust permutations; (3) the computational inefficiency and single-objective focus of most metaheuristic approaches, rendering them impractical for dynamic generation; (4) a lack of methods that simultaneously ensure AES compatibility while exploring the permutation space dynamically and efficiently.

Our combination initially uses a chaotic Fisher-Yates map to generate a high-entropy, bijective initial S-Box. Subsequently, we adapted the Swarm Space-Hopping Algorithm (SSHA) [8] to overcome the limitations mentioned above. It combines the advantages of the previous paradigms mentioned: utilizes a logistic

chaotic Fisher-Yates system for fast, key dependent initialization to move to a desirable point in the permutation space, thus satisfying the need for a dynamic scheme and exploiting chaos as a formidable pseudo random generator; then introduces a light-weight, guided optimization algorithm in the S-Box permutation space which, unlike classical algorithms, optimizes the most important criteria at once (AvgNL, MinNL, DU), finding superior solutions than the general best one while satisfying the specific AES criteria. This hybrid strategy generates high-strength S-Boxes structured for AES.

3. Problem description

The construction of cryptographically strong substitution boxes is an ongoing challenge in contemporary symmetric cryptography. S-Boxes are the primary source of nonlinearity and confusion within the composition of block ciphers, as well as the key determinant of a cipher's resistance to conventional forms of cryptanalysis (linear cryptanalysis, differential cryptanalysis, algebraic cryptanalysis, statistical cryptanalysis). However, the construction of strong S-Boxes involves meeting several stringent mathematical and statistical criteria [18].

Until recently, there had been concerns about the "secret" design process for the Data Encryption Standard S-Boxes (DES S-Boxes), and to foil possible suspicion of the existence of trapdoors, the NSA published security and design criteria for robust S-Boxes, stating that they should be resistant to differential and linear cryptanalysis, and also balanced and ideally nonlinear Boolean transformations [24].

Based on a comprehensive review of the modern cryptography literature, there is a set of criteria currently accepted by the community as the basic design requirements, i.e., a set to assess the security strength of the substitution used. Among the most accepted cryptographic characteristics are [25-27]:

i) *Nonlinearity*. Measure the nonlinearity of the Boolean function to all affine functions. Non-linearity must be as large as possible in order to be resistant to linear cryptanalysis. For the 8×8 output S-Box used in the experiment, high average and minimum component non-linearity could be an important design feature. Moreover, the Walsh spectrum can also be used to provide a measure of nonlinearity for a Boolean function $g(x)$. The Walsh transform is defined as [28]:

$$N_f = 2^{n-1} - \frac{1}{2}\max_{w\in \mathrm{GF}(2^n)}\left|S_f(w)\right|, \tag{1}$$

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

where $S_f(w)$ represented $g(x)$ walsh spectrum, and $x.w$ represented the x and w dot product, i.e., $x.w=x_1 \oplus w_1+\ldots+x_n \oplus w_n$.

ii) *Bijection*. In block cipher applications such as AES, the S-Box must be bijective so it can be inverted during decryption. A bijective S-Box has a one-to-one mapping between its input bits and its output bits, thus guaranteeing no information is lost and the data can be decrypted correctly. In this study, an (8×8) S-Box is required to produce various output values over the range [0, 255].

iii) *Differential Approximation Probability* (*DAP*). If *S*: $F_2^n \to F_2^m$ is an S-Box, then the DAP is expressed mathematically in the next equation [29, 25]:

(3) $$\mathrm{DAP}(S) = \max_{\Delta x \in F_2^n \{0\},\ \Delta y \in F_2^m} \frac{D_S(\Delta x,\ \Delta y)}{2^n},$$

where the entry of the Differential Distribution Table (DDT) is defined as

(4) $$D_S(\Delta x, \Delta y) = [\#\{x \in F_2^n \mid S(x) \oplus S(x \oplus \Delta x) = \Delta y\}].$$

In this way, DAP(*S*) measures the highest probability over each nonzero input difference Δx and output difference Δy, where

(5) $$\frac{1}{2^m} \leq \mathrm{DAP}(S) \leq \frac{\mathrm{DU}(S)}{2},$$

and the differential uniformity ($\mathrm{DU}(S)$) is defined by

(6) $$\mathrm{DU}(S) = \max_{\Delta x \neq 0} \max_{\Delta y} D_S(\Delta x, \Delta y).$$

Large DAP(*S*) implies less resistance to differential cryptanalysis. DAP values range from 0 to 1, where 0 represents the ideal state. Usage of DAP helps in the analysis of the resistance of a given S-Box to differential analysis. Whereas DU used to measure the maximum frequency of output differences for a given input difference in the DDT. The small value of the DU means a more uniform distribution, which is relevant to cryptographic security against differential cryptanalysis [30].

iv) *Strict Avalanche Criteria* (*SAC*). In 1985, AF Webster and SE Tavares proposed SAC. It is a requirement that flipping a single bit of one input should flip every output bit with probability 0.5 in the S-Box. This ensures strong diffusion and contributes to the overall cipher randomness [31, 27].

v) *Output Bits Independence Criteria* (*BIC*). The BIC criterion was realized by AF Webster and SE Tavares and is among the three most notable properties of an S-Box. It shows that the output bits provide a high independence degree for each corresponding plaintext bit when one bit of the ciphertext is complemented. Consequently, a strong BIC behaviour blocks statisticalities which an attacker could exploit [28].

vi) *BIC-NonLinearity* (*BIC-NL*). To evaluate the bit independence property, the BIC-NL is utilized. For any given two distinct output Boolean functions (f_i) and (f_j), if ($f_i \oplus f_j$) is highly non-linear, which means the absence of linear correlation between any two output bits [32].

vii) *Additional statistical and structural indicators*. Significant additional measures are the dynamic distance, the balancedness, the algebraic complexity, properties of the dependence matrix, the avalanche criterion percentage, the differential branch number, etc. These collectively test the diffusion, confusion, and statistical randomness properties of the S-Box [33, 34].

4. Proposed methodology

The suggested scheme is composed of two main phases: chaotic Fisher-Yates initialization and metaheuristic optimization.

4.1. Chaotic Fisher-Yates initialization

To ensure that the initial population of candidate S-Boxes is sufficiently diverse and well distributed, the proposed implementation uses a chaotic Fisher-Yates permutation [35] that employs the logistic map as a random generator.

Chaotic theory is concerned with the behaviour of the dynamical system. It is said to be totally random and is very sensitive to the control parameter and initial value of the system. Some properties of a chaotic system are loops of feedback, repetition, auto-organization, pattern, fractals, and dependency on the programming of the initial values [36, 37]. In our study, a logistic map is used to generate initial random permutation values for the proposed S-Box. The next equation represents a recurrent function X_{t+1} which is directly obtained based on the value of X_t and on a scale factor R [38, 39]:

(7) $$X_{t+1} = R \times X_t \times (1 - X_t),$$

where R =4.0 and $X_0 = (0.2171828)$. The pseudorandom sequence of chaos is used to extract the 256 elements of a bijective S-Box. Logistic maps are preferred because they are simple, demonstrate robust chaotic behavior, and are effective for cryptosystems [40]. Fig. 1 shows the Logistic maps with 100 iterations and 1000 iterations.

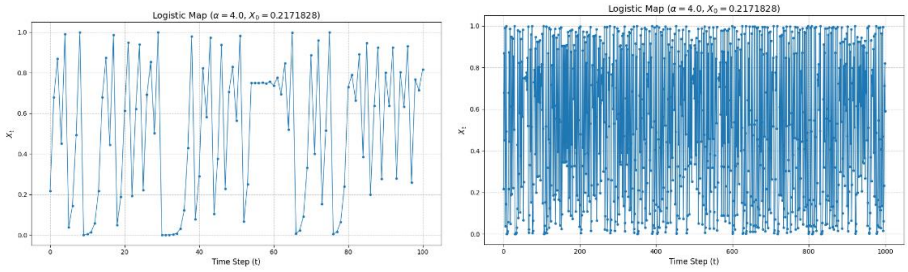

Fig. 1. Logistic maps (with 100 iterations and 1000 iterations)

In our proposal, we set the parameter R =4, which corresponds to a completely chaotic regime. Under this configuration, the generated sequence exhibits robust pseudo-random features appropriate for stochastic search and cryptographic applications. The initialization procedure begins with an ordered permutation representing the candidate S-Box: P = [0, 1, 2,…, 255].

We then apply a Fisher-Yates shuffle to convert this ordered sequence into a random permutation. Although the classical Fisher-Yates shuffle uses uniform random numbers, we take the values produced by the logistic map to decide swap positions. At iteration i, the swap index is found to be

(8) $$j = [x_t(i + 1)] \bmod (i + 1),$$

wherein x_t is the current chaotic value yielded by the Logistic map. At this stage, the factors at positions i and j are then exchanged in step with $P[i] \leftrightarrow P[j]$.

The procedure is reiterated from i=255 all the way down to i=1, resulting in a permutation having good randomness properties.

One of the great advantages of this method is that the Fisher-Yates shuffle can always generate a correct permutation, which means it guarantees the resulting

sequence is a bijective S-Box from the initial generation. Therefore, there is no need to repair the operation or de-duplicate removing operation during the initial population. Furthermore, applying chaotic dynamics will make the initial population more diverse, and the search algorithm would be more likely to discover varying regions of the search space, thus preventing premature convergence [41].

Through the combination of Fisher-Yates permutation mechanism with chaos-based sequence generation, the proposed initialization method offers a computationally efficient approach along with a reliable statistical framework for producing high-quality initial S-Box candidates used as input for the subsequent optimization stage.

Regarding the first S-Box result, only the application of the logistic chaos map with Fisher-Yates permutation is used, which already represents an efficient searching initial solution to enhance using Metaheuristic Optimization Algorithm than "from scratch" using less memory and decreasing time for ideal solutions. The starting values for the S-Box of metaheuristic optimization (shown in Table 1) are generated by logistic chaos maps and Fisher-Yates permutation with Average Nonlinearity AN = 104.75 and DU = 10. The next step will be to perform some manipulation of this S-Box by using a hybrid chaotic-SSHA search framework and obtain a strong and safe S-Box for cryptography.

Table 1. S-Box initial values generated by logistic chaos maps and Fisher-Yates permutation with AN =104.75 and DU = 10

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	25	43	55	40	31	20	71	72	60	20	23	49	70	56	24	99
1	10	21	20	14	14	20	22	39	11	98	24	53	15	15	37	16
2	19	12	11	91	23	97	12	64	17	18	18	13	18	10	21	16
3	18	14	19	10	21	14	54	26	67	10	11	10	95	13	38	17
4	16	89	17	20	28	11	12	65	82	58	24	21	22	87	69	25
5	25	80	47	24	81	96	10	85	25	24	29	83	18	84	32	86
6	17	88	19	90	34	92	35	25	17	17	57	18	13	15	61	18
7	16	16	16	19	24	11	73	14	6	12	68	20	11	76	23	13
8	78	18	17	30	8	13	59	16	18	13	63	12	23	12	24	15
9	14	75	15	5	19	19	18	20	77	21	16	93	12	11	12	41
A	19	10	13	23	19	10	13	46	15	10	33	16	66	15	11	13
B	12	42	23	2	22	18	23	22	21	74	16	21	21	4	22	19
C	10	24	13	20	23	14	14	20	15	15	15	50	13	20	11	17
D	14	48	19	79	22	20	12	17	62	17	21	94	27	7	1	23
E	22	22	24	22	25	19	15	51	21	23	45	22	14	44	11	23
F	10	21	16	52	14	3	24	0	24	12	36	9	25	11	22	17

4.2. Hybrid chaotic-SSHA optimization strategy

Once the initial population of candidate S-Boxes is produced by applying the chaotic Fisher-Yates initialization, the optimization process is accomplished in a hybrid chaotic-SSHA search framework [8]. This allows the cryptographic strength of the candidate S-Boxes to be maximized as much as possible by increasing

nonlinearity and decreasing differential uniformity. As shown in Fig. 2, the optimization process combines chaotic Fisher-Yates initialization with swarm space hopping optimization and local refinement to guarantee the bijective property and generate high-quality cryptographic S-Boxes with high nonlinearity and low differential uniformity. Therefore, the fitness function is driven by multiple criteria and defined by

(9) $$\text{Fitness} = \alpha \cdot \times \text{MinNL} + \beta \cdot \times \text{AvgNL} - \gamma \cdot \times \text{DU},$$

where: MinNL is the measure of minimum component nonlinearity; AvgNL is the measure of average nonlinearity; DU is the differential uniformity coefficient. In the proposed algorithm, the coefficient weights are set to α=40, β=10, and γ=8. With this form of decision criteria, an increase in one criterion (e.g., nonlinearity) is not achieved by a reduction in another (e.g., diffusion or differential resistance). Additionally, this approach focuses on improving the minimum nonlinearity, which guarantees a high level of nonlinearity in every component Boolean function, consequently achieving high resistance to linear cryptanalysis.

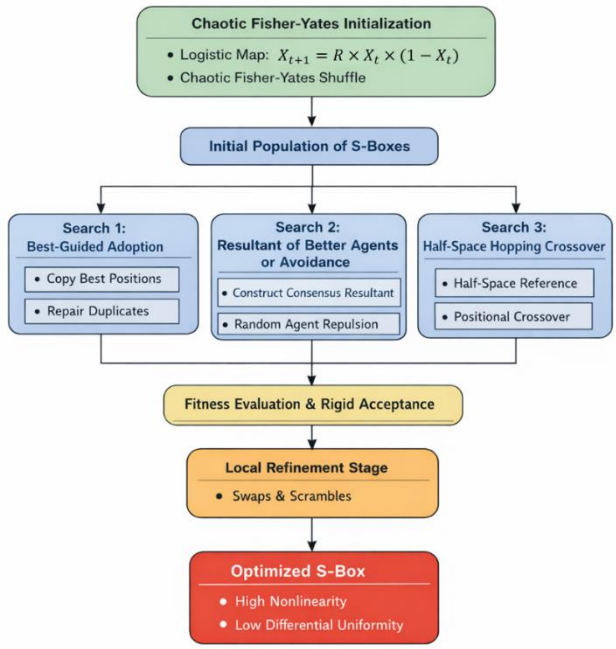

Fig. 2. Flowchart of the proposed Chaotic Fisher-Yates and Discrete Swarm Space Hopping S-Box generation method (CFY-DSSHA)

The adapted SSHA performs three complementary searches and uses rigid acceptance: Search Toward Best Agent, Resultant Solution from Better Agents, and Half-Space Chaotic Hop.

4.2.1. Search Toward Best Agent (exploitation)

This operator accelerates the convergence by guiding the agents to the current global best solution S_{best}. A subset of k positions K is updated as

(10) $$S_i(p_j) = S_{\text{best}}(p_j),\ p_j \in K.$$

To maintain a permutation, the repair operator replaces the result of duplicated values with the value that was missing from the set {0, ..., 255}.

4.2.2. Resultant solution from Better Agents (consensus-based search)

To increase the search robustness, the algorithm aggregates information from the set of superior agents $B_i = \{S_i | F(S_j) > F(S_i)\}$. The resulting S-Box ($B_i$) is generated on the most frequent values of each position *P*:

(11) $$S_r(p) = \arg_v^{\max \text{freq}_v},$$

where freq_v is the frequency of value *v* appearing at position *p* in B_i. If B_i is empty, a stochastic move (for example, a pairwise swap) is made to avoid stagnation.

4.2.3 Half-Space Chaotic Hop (diversification)

To avoid the local optima, this scheme relies on a large structural change. It divides the search space into two halves (h_1=[0.127] and h_2=[128.255]). After that, it selects a random subset of positions P_h in the S-Box (about 50% of the S-Box) to be updated by using a Fisher-Yates chaotic reference permutation S_{ref}:

(12) $$S_i(p) = S_{\text{ref}}(p), \ \ p \in P_h,$$

such a "hopping" mechanism will keep the population with sufficient diversity to explore uncharted territories of the permutation space.

4.2.4. Local refinement and stagnation handling

Every modified agent undergoes the Local Refinement Stage using the following operators: swap, multi-swap, and segment scrambling. Monotonicity improvement is enforced where the candidate succeeds the incumbent only when $F(S_{\text{new}}) \geq F(S_{\text{old}})$. If the global best fitness remains unchanged for a certain number of iterations (threshold), then a Partial Restart occurs. A portion of the population is re-initialized with a series of chaotic sequences, so as to reintroduce entropy into the system and overcome stagnation. The proposed S-Box generation and optimization process is presented in Algorithm 1.

Algorithm 1. Proposed CFY-DSSHA-S-Box

Input: The population size (*N*), maximum number of iterations (*T*).

Output: best S-Box (S_{b}).

Step 1. Apply the Chaotic Fisher-Yates method to generate *N* initial permutations.

Step 2. Evaluate each permutation using fitness by the equation (9)

Step 3. Set $S_{\text{b}} = \arg\max F(S)$.

Step 4. for *t*= 1 to *T*:

Step 4.1. For each agent S_i:

Search 1: best-guided adoption

Step 4.1.1. Copy k_1 random positions from S_{b} into S_i.

Step 4.1.2. Repair duplicates.

Step 4.1.3. Accept only if fitness improves.

Search 2: resultant / avoidance

Step 4.1.4. Build B_i.

Step 4.1.5. if $B_i \neq \emptyset$ compute resultant R_i and copy k_2 from it.

Step 4.1.6. Else apply disagreement-based repulsion from a random agent.
Step 4.1.7. Repair duplicates.
Step 4.1.8. Accept only if fitness improves.
Search 3: half-space hopping
Step 4.1.9. Determine whether improvement occurred after Search 1 and 2.
Step 4.1.10. Generate half-space reference H_i.
Step 4.1.11. Perform balanced positional crossover with H_i.
Step 4.1.12. Repair duplicates.
Step 4.1.13. Accept only if fitness improves.
Local refinement
Step 4.1.14. Apply swap, multi-swap, and segment scrambling local search.
Step 4.1.15. Keep the best local candidate.
Step 4.2. Update the global best S_{b}.
Step 5. Return S_{b}.

This process ensures the bijectivity during optimization, while cryptographic strength is improved systematically. Hence, Table 2 displays the S-Box values generation depending on the proposed chaotic Fisher-Yates and Swarm Space Hopping S-Box generation method.

Table 2. S-Box generation based on the proposed chaotic Fisher-Yates and Swarm Space Hopping S-Box generation method with AN = 112.0 and DU = 10

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

5. Evaluation of the proposed S-Box

In this section, the cryptographic security of the AES S-Box is thoroughly analyzed using several well-established security criteria. The objective is to show that the

proposed S-Box is resistant to linear, differential, and algebraic cryptanalysis and withstands statistical and structural cryptanalyses.

5.1. Computational complexity

The time complexity of the proposed CFY-DSSHA-S-Box algorithm is primarily based on the repetitive computation of the evaluation of candidate (8×8) S-Boxes. The time complexity is firstly decided by the computation of the DU (i.e., for testing all the input differences) and the NonLinear (NL) calculation (i.e., Walsh-Hadamard Transform (WHT).

The asymptotic complexity for a population of size (N), maximum number of iterations (T), and S-Box dimension (n) (where n=256 for an 8×8 S-Box), the complexity of evaluating DU is $O(n^2)$ [42]. Consequently, the total asymptotic complexity of the optimization framework is defined as

(13) $$O(T.N.n^2).$$

Since n is a fixed value 2^8 the complexity scales will be linear according to population size and number of generations.

In order to guarantee reproducing the experiments, we have used the parameters and hardware environment reported in Table 3.

Table 3. Experimental configuration and environment summary

Category	Parameter / Component	Specification
Optimization settings	Population size (N)	30
	Maximum iterations (T)	500
Search mechanisms	Elite population size	4
	Local refinement rounds	20
Hardware resources	Processor (CPU)	Intel Core i7-8565U @ 3.79 GHz
	Memory (RAM)	8 GB
Software platform	Operating system	Windows 11 (64-bit)
	Programming language	Python 3.10

Analysis of the empirical execution logs confirms that the search algorithm exhibits a high level of speed in navigating the 256! search space. On average, each iteration consumed about 24.1 s on the machine used, leading to a total runtime of about 3.35 h for a complete 500-iteration cycle.

Even with the heavy $O(n^2)$ the cost requirement for DU computation, the integrated use of optimized numerical libraries with the stochastic nature of SSHA can allow the system to converge on high-quality S-Boxes (for example: $\mathrm{NL} \geq 110$, $\mathrm{DU} \leq 10$) with acceptable computing time, maintaining a superior balance between exploration depth and computational cost [43].

5.2. Performance analysis of the generated S-Boxes

To guarantee the robustness of the proposed S-Box, the Nonlinearity property, Bijective property, SAC, and BIC will be discussed in the following subsections.

5.2.1. The property of NL

The generated S-Boxes nonlinearities values of the eight Boolean functions compared with other S-Boxes nonlinearities values obtained by different methods,

were calculated using Equation (1) and presented in Table 4. The S-Box obtained by using chaotic Fisher-Yates and adapted discrete SSHA-inspired optimization has nonlinearity of [112, 112, 112, 112, 112, 112, 112, 112] with an average of (112.0). The proposed CFY-DSSHA is regarded as appropriate and acceptable in achieving high non-linearity compared to the other methods.

Table 4. S-Boxes analysis nonlinearity

Reference	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	Avg	Min	Max
[9]	108	108	108	108	108	108	106	106	107.50	106	108
[16]	104	106	108	106	102	104	106	106	105.25	102	108
[18]	108	108	106	106	108	106	106	108	107.00	106	108
[11]	102	104	106	106	108	108	106	104	105.50	102	108
[12]	108	108	106	106	106	106	106	106	106.50	106	108
[14]	106	108	104	104	104	106	106	104	105.25	104	108
[13]	102	102	100	106	102	100	104	98	101.75	98	106
[44]	108	108	106	108	106	106	108	106	107.00	106	108
[10]	108	108	108	108	102	108	108	106	107.00	102	108
[15]	104	106	106	104	110	106	112	104	106.50	104	112
[23]	106	106	108	108	106	108	108	104	106.75	104	108
[17]	108	108	108	108	108	108	110	110	108.5	108	110
[20]	110	110	110	110	110	108	110	110	109.75	108	110
[19]	-	-	-	-	-	-	-	-	111.5	-	-
[21]	-	-	-	-	-	-	-	-	106.1	-	-
[22]	-	-	-	-	-	-	-	-	111	-	-
[45]	108	108	108	110	110	108	108	108	108.5	108	110
Proposed	112	112	112	112	112	112	112	112	112.0	112	112

5.2.2. Bijective property

A secure AES S-Box must be bijective to ensure invertibility during decryption. The obtained S-Box satisfies the bijectivity condition since all the S-Box values in period [0, 255]. Also, all Boolean functions' Hamming weight values are: 128, 128, 128, 128, 128, 128, 128, 128.

5.2.3. Strict Avalanche Criteria (SAC)

As shown in Table 5, the dependency matrix is used to describe the SAC of the proposed S-Box. The generated S-Box has an average SAC value of 0.50048. It's close to the optimal value (0.5). Table 7 shows a comparison of the SAC of the proposed S-Box in this study. The adapted Discrete SSHA-Inspired Optimization has demonstrated that its outputs have SAC values within an acceptable range.

Table 5. Proposed S-Box dependency matrix

0.4531	0.6250	0.5000	0.5938	0.4688	0.5469	0.5469	0.4688
0.4531	0.5156	0.5156	0.5156	0.4688	0.4844	0.5156	0.4062
0.5312	0.4531	0.5000	0.4844	0.4844	0.4688	0.4688	0.4531
0.5312	0.5000	0.5312	0.5469	0.4375	0.5000	0.5312	0.4688
0.5312	0.5156	0.5312	0.5156	0.4531	0.4219	0.5156	0.5000
0.5156	0.5156	0.5000	0.5312	0.4062	0.5156	0.5156	0.5000
0.4688	0.5000	0.5156	0.5156	0.4844	0.5312	0.5312	0.4688
0.5156	0.4844	0.5000	0.4688	0.5156	0.5312	0.5312	0.5156

5.2.4. Bits Independence Criteria (BIC)

Table 6 gives the results of the suggested S-Boxes. These results suggest that the predicted S-Box fully satisfies the BIC criterion [46]. Table 7 also provides a BIC average comparison of the suggested S-Box. As we observe, the mean BIC Nl value of the proposed S-Box was 104.285, which satisfies the BIC criteria of the AES S-Box.

Table 6. Proposed S-Box BIC-NL criterion

-	104	102	108	104	104	108	100
104	-	106	106	104	102	102	104
102	106	-	102	106	104	106	104
108	106	102	-	108	106	106	106
104	104	106	108	-	104	104	92
104	102	104	106	104	-	106	106
108	102	106	106	104	106	-	104
100	104	104	106	92	106	104	-

Table 7. Results of the comparison of BIC and SAC values

Reference	BIC Avg	SAC Avg
[9]	-	0.5093
[16]	103.57	0.4994
[18]	103.14	0.4980
[11]	103.29	0.4980
[12]	104.07	0.5001
[14]	102.72	0.5070
[13]	102.64	0.5017
[44]	-	0.5000
[10]	-	0.4970
[15]	104.60	0.4980
[23]	103.25	0.4989
[17]	103.78	0.4910
[20]	103.678	0.5000
[19]	-	0.5012
[21]	-	0.501
[22]	-	0.4998
[45]	103.25	0.496
Proposed S-Box	104.285	0.50048

5.3. Statistical stability and robustness analysis

In order to examine the robustness and stability of the suggested chaotic Fisher-Yates and adapted discrete SSHA, we have conducted a statistical analysis across 30 independent runs. The cryptographic results are listed in Table 8 (average NL and DU), in terms of minimum, median, maximum, average, and standard deviation. The results in Table 8 are indicative of high stability; the average NL values are tightly packed between 110.50 and 112.00 with a low standard deviation of 0.33. At the same time, the average of the DU is still kept at a low level from 8-10, with a mean of 9.27, which indicates a robust resistance against differential attacks.

Table 8. Statistical summary of 30 runs (Mean, Median, Std, Min, Max)

Metric	Min	Median	Max	Mean	Std
Average NL	110.5	111.25	112	111.16	0.33
DU	8	10	10	9.27	0.98

Moreover, the distribution of the metrics is displayed by the boxplots in Fig. 3. Hence, the average NL in Fig. 3a shows the narrow interquartile range of average NL, which means the proposed algorithm has a stable convergence toward high-quality S-Boxes. As for the DU distribution, Fig. 3b demonstrates that it remains within a limited interval, which proves the reliable differential performance of the proposed framework across repeated runs. Such statistics prove that our proposed optimization framework is initial condition independent and also reliably produces cryptography strongly S-Boxes.

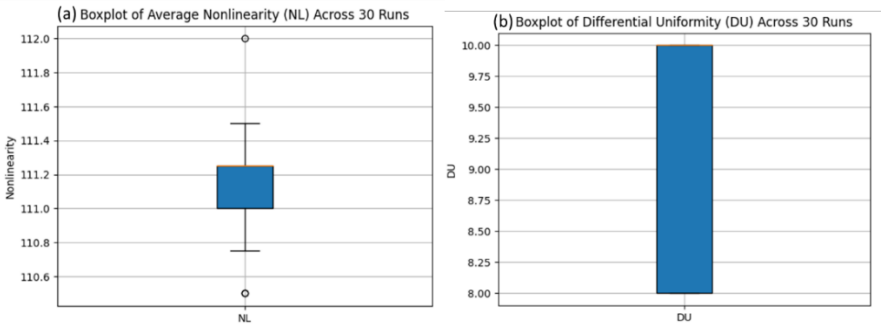

Fig. 3. Statistical distribution of: Average NL (a); DU over 30 independent runs (b)

In addition, Fig. 4 shows the convergence behavior of the proposed CFY-DSSHA in terms of average and minimum NonLinearity (NL) across iterations. It is evident that the proposed algorithm also improves quickly at the early stages (0-20 iterations), where the NL increases significantly from about 105 to over 110. After iteration 30, convergence stabilizes, indicating that the exploitation of high-quality regions in the search space has occurred. Also, the proposed algorithm consistently converges and tends toward very high NL values (about 111-112), providing a robust and stable solution across different rounds.

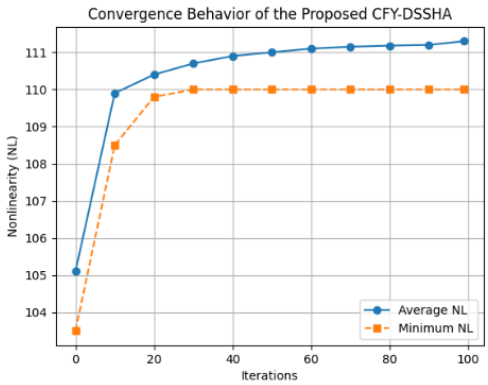

Fig. 4. Convergence Behavior of the Proposed CFY-DSSHA

5.4. The analysis of resistance against differential attack

Differential attack is also one of the most widely used attacks. The attacker selects a comparatively simple image and carries out small variations through differential cryptanalysis (for instance, changing a bit, [one bit]) and then performs encryption on the two images using the cipher method and attempts to recognize the scheme by tracking the change [47]. Usually, two metrics are used to measure the differential attack as follows: Unified Averaged Changed Intensity (UACI) and Number of Pixels Change Rate (NPCR). The formulas used to obtain these two metrics are as follows [48, 49]:

(14) $$\text{UACI} = \frac{1}{W \times H} \sum_{i=0}^{W-1} \sum_{j=0}^{H-1} \frac{|C_1(i,\ j) - C_2(i,\ j)|}{255} \times 100\%,$$

C_1 and C_2 represented the output of the cipher images of the proposed method,

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

where $D(i,j) = \begin{cases} 1 \text{ if } (C_1(i,\ j) \neq C_2(i,\ j), \\ 0 \text{ if } (C_1(i,\ j) = C_2(i,\ j). \end{cases}$

Experimental results show that by using a key-dependent XOR operation and feedback between two rounds, the NPCR value of the encrypted image is very close to the ideal value 99.5693%, and that for the UACI value is near the ideal value 33.2255% [48]. The overall findings of the suggested method were 99.5924% for NPCR and 33.3214% for UACI. The results prove that the proposed methods have perfect confusion and diffusion properties and also have high security for resisting differential attacks.

5.5. Histogram analysis

In this work, histogram analysis is used to examine the intrusion ability of the image encryption scheme [36]. As the histogram analysis may be attacked by an eavesdropper for the encryption image [50]. As can be seen from the experimental results in Fig. 5, the histograms of the original images have a very non-uniform distribution and present the statistical properties inherent to natural images [51]. On the contrary, the histograms of the encrypted images are almost uniformly distributed in all gray levels for input images, regardless of the content of the original images. This indicates that the proposed Sbox, together with the AES operations like ShiftRows, MixColumns, and key-dependent operations, is quite capable of providing a good disguise to the statistical property of the plaintext images. As a result, the encrypted images don't show any meaningful information in the histogram analysis, confirming strong resistance against statistical and histogram-based attacks.

5.6. Correlation coefficient analysis

Correlation coefficient analysis is performed to verify the proposed encryption scheme's effectiveness in eradicating the high correlation between adjacent pixels of natural images. Normally, natural images exhibit a strong correlation among neighboring pixels. On the other hand, an ideal encryption algorithm should have the lowest possible correlation to optimize security. Correlation coefficients between the plain images and their corresponding cipher images were acquired

using the equation (16). From the empirical results, we have that the correlation coefficient is very close to zero, which is evidence that the proposed scheme can successfully compromise the correlation of the ciphertext images [52]:

$$C_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{16}$$

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

where x_i, y_i represented the gray image values, N represented the total pixels, and $E(x)$, $E(y)$ are x_i and y_i mean values, respectively. It is concluded that the correlation results between pixels of plain image and pixels of cipher image are very poor (hard to near zero) (see Table 9). So the proposed method will work out effectively for preventing statistical analysis attacks.

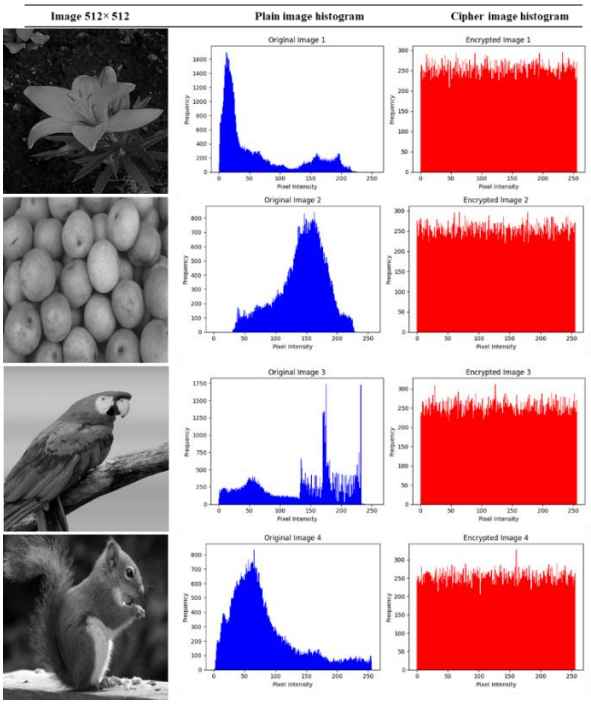

Fig. 5. Histogram of images

5.7. Shannon entropy analysis

Shannon entropy is used to evaluate the randomness and unpredictability of the cipher images. In the case of an 8-bit gray image, the entropy value should be 8. From the simulation results in Table 9, we observe that the entropy values of cipher images are very close to the ideal value 8, and the entropy of the original images is at an appreciably low value. The higher value of entropy shows that the proposed encryption scheme generates more random cipher images with uniform pixel distribution. So the information hidden in the image is well protected, and the encryption scheme is robust against entropy analysis and brute force cryptanalytic attacks [53].

Table 9. Various images, entropy, and correlation coefficient values

(Image 512×512)	Plain image entropy	Cipher image entropy	Correlation score
	6.99096	7.9969	0.00528
	7.24941	7.9970	0.00129
	7.53579	7.9969	0.00446
	7.49633	7.9973	0.005372

6. Conclusion

This study proposed a powerful and flexible scheme for the construction of cryptographically strong AES-compatible S-Boxes based on a chaotic Fisher-Yates initialization and metaheuristic optimization. With its utilization of a widespread chaotic system to derive the initial S-Box (thus ensuring randomness and sensitivity) and an adaptive discrete method to optimize the S-Box, the suggested scheme excellently avoids the structural restriction in traditional algebraic-S-Box design. The experimental results show that the generated S-Box used in the image encryption scheme exhibits strong cryptographic properties. The generated S-Box used in the proposed image encryption scheme has high average Nonlinearity and excellent Avalanche. The experimental results for the image encryption scheme indicate that the obtained NPCR values approach the ideal value of 99.5924% and the UACI approaches the ideal value of 33.3214, respectively. In addition, the generated image has a uniform histogram, a near-zero correlation coefficient, and almost the maximum entropy value of 8. Despite the strong security and effectiveness of this proposed approach, future research may extend the proposed approach by designing a key-dependent and dynamic S-Box generation method based on the key-dependent static S-Box generation approach to improve the resistance against the known plaintext and chosen plaintext attack.

References

1. Abd Al-Rahman, S. Q., S. A. Jassim, A. M. Sagheer. Design a Mobile Application for Managing Vehicles in a Transportation Issue. – Bull. Electr. Eng. Informatics, Vol. **10**, 2021, No 4.
2. Curlin, P. S., J. Heiges, C. Chan, T. S. Lehman. A Survey of Hardware-Based AES Sboxes: Area, Performance, and Security. – ACM Comput. Surv., Vol. **57**, 2025, No 9, pp. 1-37.
3. Kanshi, A., R. Soundrapandiyan, V. S. A. Sofia, V. R. Rajasekar. Hybridized Cryptographic Encryption and Decryption Using Advanced Encryption Standard and Data Encryption Standard. – Cybernetics and Information Technologies, Vol. **23**, 2023, No 4, pp. 63-78.
4. Tito-Corrioso, O. Generalization of the Class Elimination Attack to Block Ciphers. – In: Cryptol. ePrint Arch., 2026.
5. Li, F., H. Jing, Y. Su. Physical Layer Encryption Scheme Based on Human Biometric Keys and Five-Dimensional Hyperchaotic Systems. – Phys. Scr., 2026.
6. Yong, D., W. Chuansheng, G. Haimin. Particle Swarm Optimization Algorithm with Adaptive Chaos Perturbation. – Cybernetics and Information Technologies, Vol. **15**, 2015, No 6, pp. 70-80.
7. Zhang, H., H. Cheng, X. Wang, L. Zhu, D. Jiao, Z. Qiu. Improved Secretary Bird Optimization Algorithm for UAV Path Planning. – Algorithms, Vol. **19**, 2026, No 1, 64.
8. Kusuma, P. D., M. Kallista. Swarm Space Hopping Algorithm: A Swarm-Based Stochastic Optimizer Enriched with Half Space Hopping Search. – Int. J. Intell. Eng. Syst., Vol. **17**, 2024, No 2.
9. Sajjad, M., T. Shah, R. J. Serna. Designing a Pair of Nonlinear Components of a Block Cipher over Gaussian Integers. – Comput. Mater. Contin., Vol. **75**, 2023, No 3.
10. Hazzazi, M., M. Sajjad, Z. Bassfar, T. Shah, A. Albakri. Nonlinear Components of a Block Cipher over Eisenstein Integers. – Comput. Mater. Contin., Vol. **77**, 2023, No 3.
11. Özpolat, E., V. Çelik, A. Gülten. Hyperchaotic System-Based PRNG and S-Box Design for a Novel Secure Image Encryption. – Entropy, Vol. **27**, 2025, No 3, 299.
12. Lambić, D. A New Discrete-Space Chaotic Map Based on the Multiplication of Integer Numbers and Its Application in S-Box Design. – Nonlinear Dyn., Vol. **100**, 2020, No 1, pp. 699-711.
13. Muhammad, Z. M. Z., F. Özkaynak. A Cryptographic Confusion Primitive Based on Lotka-Volterra Chaotic System and Its Practical Applications in Image Encryption. – In: Proc. of 15th IEEE International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET'20), IEEE, 2020, pp. 694-698.
14. Zhou, S., Y. Qiu, X. Wang, Y. Zhang. Novel Image Cryptosystem Based on New 2D Hyperchaotic Map and Dynamical Chaotic S-Box. – Nonlinear Dyn., Vol. **111**, 2023, No 10, pp. 9571-9589.
15. Zhang, L., C. Ma, Y. Zhao, W. Zhao. A Novel Dynamic S-Box Generation Scheme Based on Quantum Random Walks Controlled by a Hyper-Chaotic Map. – Mathematics, Vol. **12**, 2023, No 1, 84.
16. Özkaynak, F. On the Effect of Chaotic Systems in Performance Characteristics of Chaos-Based S-Box Designs. – Phys. A Stat. Mech. Its Appl., Vol. **550**, 2020, 124072.
17. Alhadawi, H. S., D. Lambić, M. F. Zolkipli, M. Ahmad. Globalized Firefly Algorithm and Chaos for Designing Substitution Box. – J. Inf. Secur. Appl., Vol. **55**, 2020, 102671.
18. Jassim, S. A. Enhancing S-Box Generation Using African Buffalo Optimization Algorithm Techniques. – Int. J. Intell. Eng. Syst., Vol. **18**, 2025, No 3.
19. Dávalos, E., A. Salas, J. Benítez, C. Von Lücken. Multi-Objective Generation of S-Boxes Using Evolutionary Algorithms. – Eng. Proc., Vol. **123**, 2026, No 1, 9.
20. Akyol, S. Hybrid Cuckoo Search-Bees Algorithm with Memristive Chaotic Initialization for Cryptographically Strong S-Box Generation. – Biomimetics, Vol. **10**, 2025, No 9, 610.

21. Rasheed, A. M., R. M. S. Kumar, A. Ajayan. PSO-GWO Optimized Encryption Algorithm for Secure Medical Image Transmission in IoT-Cloud Healthcare Systems. – KSII Trans. Internet Inf. Syst., Vol. **20**, 2026, No 2.
22. Xi, J., C. Fan. Design of Dynamic S-Boxes Based on Simulated Annealing Algorithm and Its Application in Chaotic Masking Protection. – Int. J. Bifurc. Chaos, Vol. **35**, 2025, No 16, 2550190.
23. Ahmad Khan, N., A. Banga, T. M. Ghazal, B. Alabdullah, N. Iqbal, A. Alshamayleh, A. Ikram, H. Diab. Unveiling a Novel S-Box Strategy: The Dynamic 3D Scrambling Approach. – PLoS One, Vol. **20**, 2025, No 9, e0329024.
24. Adams, C. M., S. E. Tavares. The Structured Design of Cryptographically Good S-Boxes. – J. Cryptol., Vol. **3**, 1990, pp. 27-41 (Online).
https://api.semanticscholar.org/CorpusID:17832096
25. Said, L., M. Khan, M. Amin. An Efficient Recurrent Neural Network Based Confusion Component Construction and Its Application in Protection of Saliency in Digital Information. – Nonlinear Eng., Vol. **15**, 2026, No 1, 20250188.
26. Duong, P.-P., C.-K. Pham. Constructing 8×8 S-Boxes with Optimal Boolean Function Nonlinearity. – Cryptography, Vol. **9**, 2025, No 4, 67.
27. Sajjad, M., M. K. Abdalrahem, E. E. Elsayed, M.-D. Junjua, S. A. Al Qahtani. Cryptographic Protection of RGB Images Using SPN over Eisenstein Integer Ring Modulo Eisenstein Prime. – Sci. Rep., Vol. **15**, 2025, No 1, 37782.
28. Akhtar, T., N. Din, J. Uddin. Substitution Box Design Based on Chaotic Maps and Cuckoo Search Algorithm. – In: International Conference on Advanced Communication Technologies and Networking (CommNet'19), IEEE, 2019, pp. 1-7.
29. Xu, C., Y. Shang, Y. Yang, C. Zou. An Encryption Algorithm for Multiple Medical Images Based on a Novel Chaotic System and an Odd-Even Separation Strategy. – Sci. Rep., Vol. **15**, 2025, No 1, 2863.
30. Razaq, A., L. A. Maghrabi, M. Ahmad, F. Aslam, W. Feng. Fuzzy Logic-Based Substitution-Box for Robust Medical Image Encryption in Telemedicine. – IEEE Access, Vol. **12**, 2024, pp. 7584-7608 (online).
https://api.semanticscholar.org/CorpusID:266922162
31. Alhudhaif, A., M. Ahmad, A. Alkhayyat, N. Tsafack, A. K. Farhan, R. Ahmed. Block Cipher Nonlinear Confusion Components Based on New 5-D Hyperchaotic System. – In: IEEE Access, 2021.
32. Ozpolat, E., V. Çelik, A. Gülten. Hyperchaotic System-Based PRNG and S-Box Design for a Novel Secure Image Encryption. – Entropy, Vol. **27**, 2025 (online).
https://api.semanticscholar.org/CorpusID:277014010
33. Karpinski, M., et al. Development of High-Quality Cryptographic Constructions Based on Many-Valued Logic Affine Transformations. – Electronics, Vol. **14**, 2025, No 10, 2094.
34. Hosseini, K., S. Sadeghi. Differential Cryptanalysis of an Optimized Novel Light-Weight Block Cipher for Image Encryption. – In: Cryptol. ePrint Arch., 2025.
35. Lawnik, M., M. Berezowski. New Chaotic System: M-Map and Its Application in Chaos-Based Cryptography. – Symmetry (Basel), Vol. **14**, 2022, 895 (online).
https://api.semanticscholar.org/CorpusID:248445410
36. Jassim, S. A., A. A. Jihad, M. I. Khalaf. Enhanced Image Encryption through Combined Arnold and Three Other Chaos Techniques. – J. Cybersecurity Inf. Manag., Vol. **16**, 2025, No 2.
37. Fadhil, M. S., A. K. Farhan, M. N. Fadhil. Designing Substitution Box Based on the 1D Logistic Map Chaotic System. – In: Proc. of IOP Conference Series: Materials Science and Engineering, IOP Publishing, 2021, 12041.
38. Jassim, S. A., A. K. Farhan, A. H. Radie. Using a Hybrid Pseudo-Random Number Generator for Cryptography in the Internet of Things. – In: Proc. of 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA'21), IEEE, 2021, pp. 264-269.
39. Chen, W., X. Wu, Y. Lu. An Improved Path Planning Method Based on Artificial Potential Field for a Mobile Robot. – Cybernetics and Information Technologies, Vol. **15**, 2015, No 2, pp. 181-191.

40. Gabr, M., H. Younis, M. Ibrahim, S. Alajmy, I. Khalid, E. Azab, R. Elias, W. Alexan. Application of DNA Coding, the Lorenz Differential Equations and a Variation of the Logistic Map in a Multi-Stage Cryptosystem. – Symmetry (Basel), Vol. **14**, 2022, No 12, 2559.
41. Zheng, J., T. Bao. An Image Encryption Algorithm Using Cascade Chaotic Map and S-Box. – Entropy, Vol. **24**, 2022 (online).
https://api.semanticscholar.org/CorpusID:254778099
42. Azam, N. A., U. Hayat, I. Ullah. An Injective S-Box Design Scheme over an Ordered Isomorphic Elliptic Curve and Its Characterization. – Secur. Commun. Networks, Vol. **2018**, 2018, pp. 3421725:1-3421725:9 (online).
https://api.semanticscholar.org/CorpusID:56169308
43. Isa, H., S. A. Junid, A. S. Z'aba, M. R. Endut, R. Bin, S. M. Ammar, N. Ali. Enhancement of Non-Permutation Binomial Power Functions to Construct Cryptographically Strong S-Boxes. – Mathematics, 2023 (online).
https://api.semanticscholar.org/CorpusID:256171300
44. Sajjad, M., T. Shah, H. Alsaud, M. Alammari. Designing a Pair of Nonlinear Components of a Block Cipher over Quaternion Integers. – AIMS Math, Vol. **8**, 2023, No 9, pp. 21089-21105.
45. Saboncchi, A. K. S. Hybrid Metaheuristic Lion and Firefly Optimization Algorithm with Chaotic Map for Substitution S-Box Design. – J. Inf. Hiding Priv. Prot., Vol. **6**, 2024, 21.
46. Mahboob, A., M. Nadeem, M. W. Rasheed. A Study of Text-Theoretical Approach to S-Box Construction with Image Encryption Applications. – Sci. Rep., Vol. **13**, 2023, No 1, 21081.
47. Liu, Y., Z. Qin, X. Liao, J. Wu. A Chaotic Image Encryption Scheme Based on Hénon-Chebyshev Modulation Map and Genetic Operations. – Int. J. Bifurc. Chaos, Vol. **30**, 2020, No 06, 2050090.
48. Yavuz, E. A Novel Chaotic Image Encryption Algorithm Based on Content-Sensitive Dynamic Function Switching Scheme. – Opt. Laser Technol., Vol. **114**, 2019, pp. 224-239.
49. Nag, A., S. Biswas, D. Sarkar, P. P. Sarka. Secret Image Sharing Scheme Based on a Boolean Operation. – Cybernetics and Information Technologies, Vol. **14**, 2014, No 2, pp. 98-113.
50. Shah, A. A., S. A. Parah, M. Rashid, M. Elhoseny. Efficient Image Encryption Scheme Based on Generalized Logistic Map for Real-Time Image Processing. – J. Real-Time Image Process., Vol. **17**, 2020, No 6, pp. 2139-2151.
51. Cherukuri, A. K., S. Sannuthi, N. Elagandula, R. Gadamsetty, N. Singh, A. Jain, I. S. Thaseen, V. Priya, A. Jonnalagadda, F. Kamalov. A Secure Peer-to-Peer Image Sharing Using Rubik's Cube Algorithm and Key Distribution Centre. – Cybernetics and Information Technologies, Vol. **23**, 2023, No 3, pp. 126-144.
52. Xu, C., J. Sun, C. Wang. An Image Encryption Algorithm Based on Random Walk and Hyperchaotic Systems. – Int. J. Bifurc. Chaos, Vol. **30**, 2020, No 4, 2050060.
53. Cholewa, M., B. Płaczek. Application of Positional Entropy to Fast Shannon Entropy Estimation for Samples of Digital Signals. – Entropy, Vol. **22**, 2020, No 10, 1173.

Fast-track. Received: 25.02.2026, First revision: 20.03.2026, Second revision: 12.04.2026, Accepted: 18.04.2026