Impact Factor 6.1

Journal of Cyber Security

ISSN:2096-1146

Scopus

DOI

Google Scholar

More Information
www.journalcybersecurity.com

Crossref doi Google Scholar scopus

DIMENSIONAL ADAPTIVE S-BOX (1D/2D) GENERATION FOR VARIABLE-SIZED MEDIA ENCRYPTION

Firas Abdulla Mahmood[1] and Auday H.AL-Wattar

Department of Computer Science and Mathematics, Mosul University, Mosul, Iraq.

ABSTRACT

This Study Presents A Comprehensive Evaluation Of An Advanced Chaotic Substitution Box (S-Box) Encryption System Enhanced With Multiple Chaotic Maps (Lorenz, Henon, Ikeda, Logistic, Tent, And Sine) For Securing Diverse Data Types. In Response To The Growing Need For Versatile Cryptographic Solutions Capable Of Protecting Heterogeneous Data Formats, We Developed And Tested A Unified Encryption Framework Adaptable To Image, Text, And Video Protection. Through Systematic Testing Across Six Standard Datasets Per Domain, The Research Demonstrates The System's Exceptional Versatility, Achieving Superior Security Metrics Including Avalanche Effects Exceeding 49.5% (Peaking At 52.8% For 4K Video), Near-Optimal Bit Entropy (7.86-7.98/8.0), And Minimal Temporal Correlation (0.002-0.005) For Video Encryption. Performance Analysis Reveals Efficient Throughput (10+ MB/S For Text, 285 MB/S For 1080p Video) With Minimal Storage Overhead (1-3% For Video) And Real-Time Capability Up To 1080p Resolution. The Study Establishes Clear Guidelines For Chaotic Map Selection: Henon And Lorenz Maps For Maximum Security Applications, Ikeda For Real-Time Processing, And Logistic/Tent Maps For Resource-Constrained Environments. Results Validate That Properly Integrated Chaotic Systems Provide Enterprise-Grade Security While Maintaining Practical Performance Across Heterogeneous Data Formats, Offering A Unified Cryptographic Framework Adaptable To Modern Digital Protection Requirements.

KEYWORDS

Chaotic encryption, S-Box cryptography, Multi-domain security, Chaotic maps, Cryptographic performance..

1. INTRODUCTION

The development of substitution boxes, commonly known as S-boxes, is a pivotal area in symmetric key cryptography, and it has been the principal source of nonlinearity in many block ciphers. The traditional methods of developing S-boxes include: mathematically derived S-boxes (such as inversion in Galois fields, present in the AES algorithm), the random development of S-boxes through heuristic optimization, and the development of S-boxes through combinatorial and algebraic methods [1]. The security methods associated with mathematically derived S-boxes are verifiable, but the usability of the derived boxes in the presence of varying characteristics in the input data is a limitation. The random development of S-boxes is reliable but has to be well-tested for various cryptographic properties [2].

The application of chaotic systems to cryptography began to appear as a promising area in the late 1990s, exploiting properties such as ergodicity, sensitivity to initial values, and deterministic randomness to improve cryptographic primitives. Various chaotic maps, logistic, tent, sine, and multi-dimensional systems such as the Lorenz and Hénon systems, have demonstrated their efficiency in the generation of pseudo-random bits for the design of S-boxes [3]. Simultaneously, evolutionary computation methods, based on genetic algorithms (GA), have proved their applicability in the optimization of S-boxes based on cryptographic parameters such as nonlinearity, differential uniformity, and avalanching effect [4]. Hybrid methods that recently combined chaotic optimization and genetic algorithms appear promising and produce S-boxes with superior quality to existing results based solely on chaotic systems and genetic algorithms [5].

Within the multimedia encryption area, literature has mainly targeted the application of traditional cryptography systems (AES, DES) or explored the design of new chaotic maps for images and videos [6]. Media-aware encryption methods and schemes began to appear [7], taking into account the spatial and temporal correlations in visual data, but the application of adaptable S-box dimensions and structures has been severely overlooked in the area, while current studies regarding S-boxes are mostly dimensionally unchanging, except for a few studies that explored the design of 2D S-boxes for image applications [8].

Current methods have three main drawbacks: (1) they always use fixed-dimensional S-boxes irrespective of the properties of the data, which might defeat the purpose of taking advantage of higher-dimensional media by ignoring the structural properties present in higher-dimensional media, (2) they fail to provide any systematic mechanism to discern when to work with 1D or 2D S-box design based on media properties, and (3) they fail to take the full advantage of the combination of chaotic systems and evolutionary optimization for adaptive design of S-boxes based on media properties [9].

This work presents a new Dimensional Adaptive S-Box (DAS-Box) framework that fills the existing gap between theory and practice in cryptography for multimedia applications. We present a methodology that dynamically generates a suitable 1D and 2D substitution box based on the properties of the respective text, image, and video input. Our framework combines the process of initializing a chaotic system and genetic algorithm optimization to generate S-boxes with superior cryptanalytic capability while dynamically adjusting to the size variations in the input media data. The crucial aspect is the dimensional choice process based on analyzing the properties of the input media such as the size, number of dimensions, characteristic distributions, and correlation patterns to determine the suitability of the corresponding dimensions for a specific S-box. For instance, a 1D substitution box will efficiently map characters in the case of texts and pixels in the case of compact media, while a 2D substitution box will make effective use of neighborhood relations in the case of spatially and temporally correlated images and videos, respectively. We test and validate the effectiveness of the DAS-Box framework in terms of security and efficiency in the domains of three media sources with promising results and enhanced security and efficiency advantages than traditional methods employing fixed-size substitution boxes.

2. Related Works

Ding Zhu et al. [10] propose a technique for constructing cryptographic S-boxes based on a newly defined hybrid chaotic generator. With the establishment of the dynamic characteristics of the chaotic model, they extract pseudo-random sequences. Those are combined with a linear congruential generator for creating an initial S-box. Then, a classic mapping function is applied to enhance the permutation property. An improved genetic algorithm then takes over to perform refined evolutionary optimizations. This GA embeds adaptive representation, selection, crossover, and mutation to avoid the traps of stagnation and inefficiency common in standard approaches. Extensive experiments demonstrate the resulting S-box with distinctly higher nonlinearities and strong resistance against both linear and differential cryptanalysis compared with the unoptimized original.

Goudarzi et al. [11] present a new family of lightweight block ciphers, together with a corresponding authenticated encryption design that has been submitted to the NIST LWC competition, and focus on resistance to side-channel leakage. The nonlinear gate count is minimized, such that masked implementations - even for high-order masking - are efficient in software. A bitsliced architecture offers both high parallelism and very low area in hardware. On the authenticated encryption side, Pyjamask uses the provably secure OCB mode but still allows fine-grained adaptation to other block-cipher-based AEAD modes. This paper provides the construction of the cipher, an extensive cryptanalytic investigation, and software implementations supporting masking up to order 128. Their hardware estimates indicate that a Pyjamask-128 implementation requires approximately 5200 GE for encryption and roughly 7500 GE for full encryption–decryption, outperforming round-based AES. Finally, they discuss various hardware optimization ideas, including circulant diffusion structures and multi-input XOR realizations.

Jasim and Hussein [12] propose a chaos-driven image encryption technique that couples a hyper-chaotic system with a substitution stage based on the modified Rijndael S-box. The reshaping of the S-box into a one-dimensional form is done with minimal numeric conversions, while using only one

secret key. The performance is very fast: approximately 0.2485 seconds for both 256×256 and 0.3665 seconds for 512×512 images. It ensures very good security. Tests have demonstrated strong robustness against both image-processing– and statistical-based attacks, which confirms the validity of this scheme in practical applications related to secure transmission of images.

Jiang and Ding [13] proposed an S-box design technique that utilizes chaotic systems for generating random Bent functions. Considering each S-box output as a Boolean function, they constructed S-boxes based on Bent functions that are well-known for having very high nonlinearities. Results: The results showed superior cryptographic properties: the nonlinearity of BIC reaches up to 108 (minimum 98), and BIC-SAC values lie between 0.4668 and 0.5234. Constructed S-boxes offer better resistance against linear and differential cryptanalysis than the designs of Lambić, Lu et al., and Han et al.

Mahboob et al. [14] present an S-box generation scheme based on linear fractional transformations over finite fields. They first apply fractional transformations for odd exponents (1–255), then use a quantic fractional transformation to craft the S-box, finishing with a permutation via S256 from the symmetric group to boost unpredictability. The resulting S-box is evaluated with standard cryptographic benchmarks-nonlinearity, differential uniformity, SAC, linear probability, and BIC-and shows improved performance. When used in image encryption, it yields strong statistics in entropy, homogeneity, and correlation, outperforming several existing S-box-based schemes.

Elkandoz and Alexan [15] propose a chaos-based image encryption algorithm that follows the confusion–diffusion structure. First, the pixel positions are permuted, and then the XOR operation with a secret key generated from multiple chaotic systems is performed. This method has high differential resistance; for instance, the NPCR and UACI values are 99.6246% and 30.5681%, respectively, outperforming many previous schemes. Competitive encryption times (e.g., 3.355 s for Lena, 2.611 s for Baboon) for images of size 256×256 are reported. All NIST randomness tests on RGB channels have passed, further confirming its potential for real-time secure image transfer.

Ahmad et al. [16] propose a multi-objective framework for the generation of high-quality 8×8 S-boxes by means of a chaos-enhanced NSGA-II. The optimization balances high nonlinearity with low differential uniformity, balancedness, and minimum autocorrelation. Consequently, the obtained S-boxes possess nonlinearity of at least 110, low differential uniformity as small as 8, and autocorrelation close to 80, outperforming single-objective approaches. When applied to medical image encryption, they demonstrate fast permutation-diffusion behavior and robust security of medical data for telemedicine.

Taha and Hussein [17] present an enhanced PRESENT cipher by remaking its S-boxes and P-layers with a six-dimensional chaotic model, with the idea of eliminating anti-fixed-point weaknesses present in the design. They generate 10 new S-boxes, 10 new P-layers, and their inverses, which are verified on standard hardware. The analysis indicates significant improvements in linear and differential resistance attacks; thus, the new design becomes more suitable for low-power, security-critical embedded applications.

Abd-El-Atty [18] introduces a quantum-inspired S-box creation approach that combines discrete-time quantum walks with the Hénon map and an improved particle swarm optimization. The scheme, while targeted for image encryption in long-term security contexts and potentially against quantum adversaries, reaches very strong metrics: entropy 7.99977, NPCR 99.618%, UACI 33.484%, and a Chi-square of 249.481, thus providing high randomness and good resistance to statistical and differential attacks.

Panchami and Mathews [19] propose the Feather S-box, a lightweight 4-bit substitution box fit for IoT devices. It is balanced, with high nonlinearities and quite efficient computationally. Experimental results through hardware demonstrate a 23% reduction in area-delay product and a 19% reduction in power-delay product over PRESENT, while it outperforms GIFT and KATAN by 12%. The S-box shows good resistance to differential, linear, algebraic, and side-channel attacks. In fact, SKINNY is among the very few schemes that equally offer lightweight robustness.

Malik et al. [20] propose the lightweight S-box construction based on a composite chaotic Tent-Sine map. For the first time, such a wide chaotic range can make dynamic S-boxes with strong cryptographic behavior that keeps the computation light. They reach a differential probability of 10/256 (0.0391); given that only two parameters are used and no heavy algebraic operations are

involved, the approach is efficient and delivers cryptographic strength equivalent to more complex S-box designs.

Msolli et al. [21] develop a genetic algorithm that generates dynamically secure S-boxes suitable for IoT. Their adaptive search provides S-boxes with good substitution and resistance properties. When implemented in AES, the generated S-boxes give high NPCR of 99.61–99.65 with UACI of about 0.4904–0.5037 and entropy close to the ideal. It is also very fast, running AES modes, such as CBC encryption in approximately 0.0060 s, making it suitable for real-time use in IoT applications.

Calvo et al. [22] introduce the variants of hardware-accelerated AES, featuring dynamic S-boxes created by performing an XOR operation between the secret key and each element of the standard AES S-box. On a Xilinx XC7Z020 PYNQ-Z2 FPGA implementation, the setup performs real-time encryption with increased cryptographic strength. All the dynamic S-boxes exhibit high nonlinearity, strong avalanche, and good bijectivity, thus strengthening defenses against analytic attacks.

Abdulghani et al. [23] propose a chaos S-box construction based on the modified Jellyfish Search optimization to overcome the inefficiencies and weak criteria noted in previous chaos-based S-boxes. The generated S-box has good nonlinearity, SAC, BIC, differential probability, and linear probability; thus, the metrics reported—nonlinearity 4, SAC 0.4978, BIC 0.5019, DP 0.897, LP 0.903—point toward its potential for lightweight cipher applications.

Özpolat et al. [24] investigate a hyperchaotic system by confirming its chaotic properties and creating a PRNG based on that to construct a 16×16 S-box for image encryption. Simulations on 512×512 grayscale images such as Baboon and Peppers validate the successful decryption process and excellent security features, with entropy close to 8, very low pixel correlation, and high NPCR/UACI such as 99.6143% and 33.4691%, respectively, for Baboon, meaning good robustness against statistical, differential, and noise attacks.

Fadhil and Alhusseini [25] presented an improved version of CAST-128, where dynamic S-boxes were generated based on a hybrid Logistic–Sine chaotic map. The substitution accordingly enhances the nonlinearity, bijection, and avalanche features of the scheme. Experiments on standard images like Lena and Baboon reveal its superior performances concerning entropy, NPCR, UACI, and histogram uniformity, with high computational efficiency. This light-weight algorithm is appropriate for secure real-time imaging applications like medical or surveillance ones.

Tolpa et al. [26] investigate lightweight cryptographic architectures for IoT devices with scarce resources. They introduce 4×4 S-boxes created using improved logistic, sine, and tent maps. The paper shows that their contribution enables the tunability of cryptographic properties to fulfill all the security requirements by providing a high SAC, BIC, and robust resistance against side-channel attacks. Hardware implementations using NanGate 45 nm technology confirm feasibility, while encryption experiments show effective image structure obfuscation and good security for embedded systems.

3. METHODOLOGY

The Dimensional Adaptive S-Box (DAS-Box) model is designed in a three-phase pipeline architecture that aims to intelligently adapt the cryptographic primitives to the properties of the media. Phase 1 focuses on a detailed media analysis regarding the optimal size of the S-box dimensions, namely in one-dimensional and two-dimensional formats. Phase 2 involves the implementation of a hybrid approach for the generation of substitution boxes based on the combination of the results of a chaotic process and a genetic optimization process to ensure the cryptanalytic security against any attacks. Phase 3 involves the execution of the media-specific encryption operations along with the provision for the augmentation of a block cipher if needed.

The Dimensional Adaptive S-Box (DAS-Box) approach provides a three-phase adaptive encryption process tailor-made for multimedia information of varying dimensions. The process involves a sophisticated media analysis phase where the optimal size of the S-box has to be determined, a second phase involving the generation of the hybrid S-box through the integration of the chaotic process and evolutionary optimization processes, and finally the phase where the media-specific encrypting operations are performed. The entire process is designed in a flexible manner to accommodate adaptive changes based on the properties of texts, images, and videos to be encrypted while ensuring the security and integrity of the encryption process are maintained.

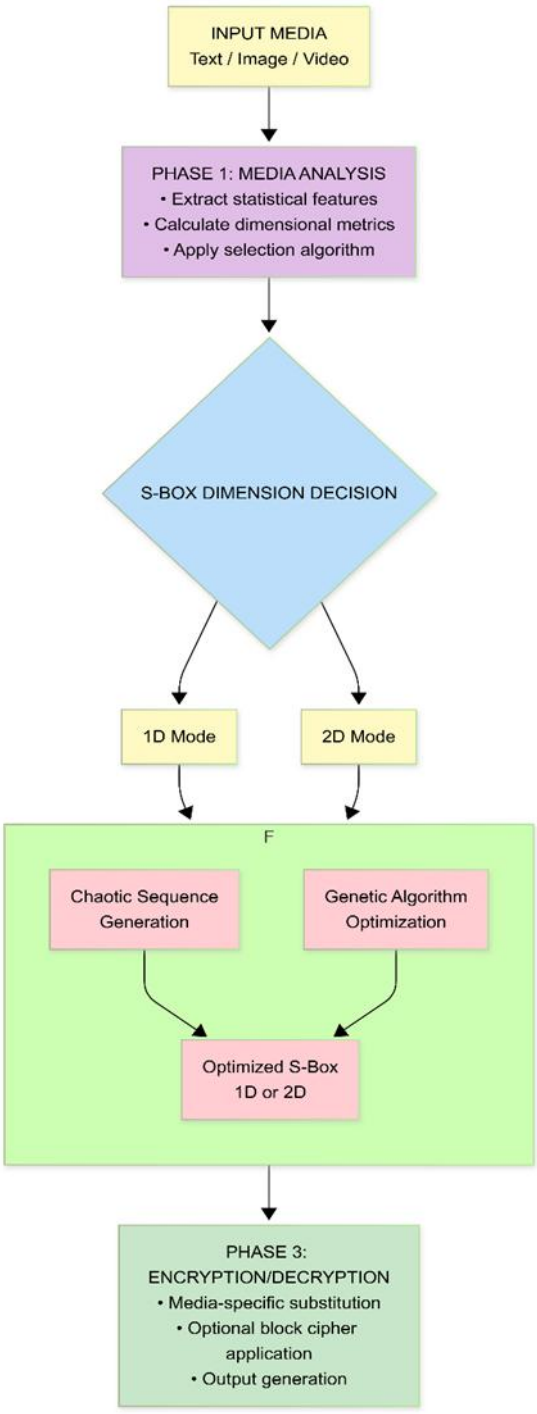

Figure 1. DAS-box Framework Architecture

The first level of media analysis reveals a total of seven numeric attributes describing the quantifiable properties of the content structure. Size and dimension are basic classifying attributes, and the number and ranges of unique values give a measure of the diversity in the content. The measurements of spatial correlation assess the neighborhood relations, an important factor in the optimization process in 2D structures. Entropy measures determining the density of the information, and compression estimates describe the presence of repetition in the data values. Each attribute is put into a weighted decision process where the algorithm gives a score to the choice of 1 versus 2 dimensions based upon empirical rules. The algorithm stresses the importance of size and dimension while adding the values of correlation measures to assist in the optimization in spatial dimensions.

The generation of the S-box involves a two-step hybrid process that combines chaotic initialization and genetic optimization. The basis for the non-linear processes involves the implementation of five chaotic maps with adjustable parameters: logistic maps for general chaos, tent maps for piecewise linear diffusion, and application-specific maps. All the maps involve a transient phase elimination process before the sequence generation phase to assure the pseudo-random properties of the sequences generated, which are cryptographically sensitive. Genetic optimization aims to optimize the chaotic permutations through an evolutionary process involving tournament selection, crossover operators scaled according to the dimensions involved, and adjustable mutation. The optimization process involves the assessment of fitness based on weighted criteria of the avalanche effect, completeness of bijection, and correlation, with diffusion marks for two-dimensional scenarios.

The implementation of the encryption process varies in terms of dimensions, where the 1D process involves element-wise substitution in a direct manner based on the element nature, and the 2D process involves substitution based on spatial information. For the text encryption process, the character frequency analysis in an optimal manner indexes the S-boxes, while the image processing involves the distributions and spatial information of the pixels in the image. The 1D process involves element-independent permutation processes to achieve the confusion effect based on the value substitution, while the 2D process involves improved diffusion based on spatially oriented substitution to increase the diffusion effect based on independence in the color images and coordination of the channels in the images.

Cryptographic verifications utilize a multi-metric assessment framework in terms of confusion, diffusion, and statistical security metrics. Avalanche effect analyses verify the sensitivity of output to the smallest variations in input, thus confirming the properties of confusion. Bijective verifications confirm the existence of inverse functions for lossless decryption functions. Nonlinearity analyses evaluate the algorithm's immunity to linear attacks in terms of maximum affine distances. Entropy analyses assess the efficacy of information diffusion according to value distributions. Correlation analyses evaluate the statistical independence of pairs in plaintext and ciphertext messages. Differential uniformities test the algorithm's immunity to differential attacks by analyzing maximum difference values in the table. For image media, perceptual evaluations in terms of PSNR and NPCR establish the security properties of the algorithm.

Application-level implementation of parameters to media-specific constraints aims to balance security and optimization for each medium. Text processing focuses on optimization and efficient implementation through smaller S-box size and logistic maps with low computational complexities. Image processing focuses on visual security optimization with moderate-sized parameters and spatial optimizations in mind. Each medium requires optimization in terms of faster execution and the choice of frame sampling and parallelized operations in the case of videos. The value mappings for each medium include distributions based on the characteristic of each medium: character code distributions for texts, pixel value distributions for images, and temporal samplings for videos. The application of the block cipher involves full encryption for texts and selective methods to maintain format integrity for visual media content.

3.1 Media Analysis and Dimensional Selection

3.1.1 Feature Extraction

Effective dimensional selection entails the quantification of input media along seven dimensions. Size and dimensionality are basic structural properties, while unique values and value ranges capture the diversity of content contained in the media. Spatial correlation reflects the importance of neighborhood structure in two-dimensional optimization problems. Entropy indexes the density of information within the media, while the compression ratio estimates the redundancy contained in the input media. The dimensions listed above work in tandem to produce a "fingerprint" of the input media that guides the algorithm for making a decision in the process of dimensional selection. The techniques applied to extract the dimensions differ according to the type of input media, whether it is a text, an image, or a video as shown in Table (1).

Table 1: Media Feature Extraction Parameters

Feature	Description	Calculation Method	Range / Type
Data Size (S)	Total number of elements	- Text: character count - Image: pixel count × channels - Video: total pixels across sampled frames	Integer > 0
Dimensionality (D)	Structural dimensions	- Text: 1 (sequential) - Image: 2 (spatial) - Video: 3 (spatiotemporal)	{1, 2, 3}
Unique Values (U)	Distinct element count	Cardinality of value set	Integer ≥ 1
Value Range (R)	Minimum to maximum values	- Pixel data: [0, 255] - Text: [min(ord), max(ord)]	Interval
Spatial Correlation (C)	Neighborhood similarity (images/videos)	Mean correlation coefficient of adjacent pixels	[0, 1]
Entropy (E)	Information content	Shannon entropy of value distribution	$[0, \log_2(U)]$
Compression Ratio Estimate (Z)	Redundancy indicator	1 - (U / S)	[0, 1]

3.1.2 Dimensional Selection

The algorithm of dimensional selection uses a weighted decision matrix to map the discovered features into recommendations for dimensions as indicated in algorithm (1). The discovered features calculate two scores corresponding to the 1D and 2D formats based on heuristics proved through experience. Dimensionality has the highest priority because of its intrinsic significance in the encryption plan. The size thresholds provide a workable limit to computational viability. The measurements of correlation directly correlate to the spatial optimization potential. The algorithm also makes provisions for exception handling in specific cases where the generic rules will less likely fit, for instance when the images contain very specialized contents with a reduced number of color values and very differently organized text data.

Algorithm 1: S-box Dimension Selection

Input:
Media features F = {S, D, U, R, C, E, Z}

Output:
Selected dimension d ∈ {1, 2}

Method:
Initialize weights W = {w_1, w_2, w_3, w_4, w_5, w_6, w_7} // Default: [0.2, 0.25, 0.15, 0.05, 0.15, 0.1, 0.1]
Initialize $score_1D$ = 0, $score_2D$ = 0
Rule 1: Dimensionality consideration
 if D == 1 then
  $score_1D$ += w_2 × 1.0
 else if D ≥ 2 then
  $score_2D$ += w_2 × 0.7
 end if
Rule 2: Size-based consideration
 if S < 1000 then
  $score_1D$ += w_1 × 0.8
 else if S > 10000 then
  $score_2D$ += w_1 × 0.6

```
 end if
 Rule 3: Correlation-based consideration
 if C > 0.5 then
    score₂D += w₅ × 1.0  // High correlation favors 2D
 else
    score₁D += w₅ × 0.5
 end if
Rule 4: Unique values consideration
 if U < 100 then
    score₁D += w₃ × 0.9  // Small alphabet favors 1D
 else if U > 1000 then
    score₂D += w₃ × 0.7
 end if
Decision
 if score₂D > score₁D then
    d = 2
 else
    d = 1
 end if
 return d
```

Table 2: Dimension Selection Guidelines by Media Type (as shown previously)

Media Type	Recommended Dimension	Conditions for Exception	Typical Size Range
Plain Text	1D	Always	S < 10,000 chars
Source Code	1D	Always	Varies
Grayscale Images	2D	If U < 50 (specialized images)	256×256 to 4K
Color Images	2D	Always (per channel)	512×512 to 8K
Video Frames	2D	If processing constraints exist	720p to 4K
Binary Data	1D	If structured as byte streams	Varies

3.2 Hybrid S-Box Generation

3.2.1 Initializing a Chaos

Chaotic systems form the basis of the nonlinear operations in S-box design, taking advantage of the mathematical properties suitable for the task. Five different chaotic maps are designed with adjustable parameters to provide contrasting properties for each type of medium to be processed. The logistic map is suitable for generating robust chaos with large ranges of parameters and is best suited for encrypting texts. The tent map is best suited for images due to its piecewise linear and diffused properties. Other maps, such as the sine, Gauss, and circle maps, are designed to perform their respective functions based on their nonlinear properties.

The chaotic maps in Table (3) are designed with a transient phase discard to remove the effects associated with the initial values before the generation of the sequence, making the resultant chaotic sequence suitable due to its pseudorandom properties with sensitivity to initial values, forming the best source for genetic optimization.

Table 3: Chaotic map implementation and parameters

Map Type	Equation	Parameters	Range	Chaotic Region
Logistic	$x(n+1) = r * x(n) * (1 - x(n))$	$r \in [3.57, 4.0]$	$x \in [0, 1]$	$r > 3.56995$
Tent	$x(n+1) = \mu*x(n)$ if $x(n) < 0.5$; $\mu*(1 - x(n))$ otherwise	$\mu \in [1.0, 2.0]$	$x \in [0, 1]$	$\mu > 1.0$
Sine	$x(n+1) = a * \sin(\pi * x(n))$	$a \in [0, 1]$	$x \in [0, 1]$	$a > 0$
Gauss	$x(n+1) = \exp(-\alpha * x(n)^2) + \beta$	$\alpha = 6.2, \beta = -0.5$	$x \in [-1, 1]$	Default
Circle	$x(n+1) = (x(n) + \Omega - (k/(2\pi)) * \sin(2\pi*x(n))) \bmod 1$	$\Omega = 0.5, k = 0.5$	$x \in [0, 1]$	$k > 0$

Algorithm (2) produces cryptographically valid pseudorandom series through repeated application of chaotic maps with sensitivity to initial conditions. The algorithm first skips the initial values to avoid artifacts in the sequences, guaranteeing that the sequences produced contain purely chaotic properties. Various maps such as logistic maps, tent maps, and other non-linear functions offer the advantage of choice according to the need to encrypt the medium. The algorithm converts the continuous chaotic sequences into discrete permutations that can be applied in the construction of an S-box through the assignment of positions based on the process of ordering.

Algorithm 2: Chaotic Sequence Generation

Input:

Map type M, parameters P, sequence length L, initial condition x_0

Output:

Chaotic sequence C of length L

Method:

$x = x_0$ if $x_0 \neq$ None else random() $\in [0, 1]$

Discard transient phase

```
for i = 1 to 200 do
    x = apply_map(M, x, P)
end for
```

Generate main sequence

```
C = empty list of size L
for i = 1 to L do
    x = apply_map(M, x, P)
    C[i] = x
end for
return C
```

3.2.2 Genetic Algorithm Optimization

Genetic algorithms improve chaotic permutations to cryptographically optimal S-boxes based upon evolutionary theory. The process involves the application of genetic operations, namely selection,

crossover, and mutation to a population of candidate S-boxes. The fitness function involves the assessment of weighted score values where the primary focus is upon the avalanche criterion, completeness of bijection, and correlation minimization. For a 2D S-box, the diffusion score also involves the assessment of the effectiveness of neighborhood diffusion. Crossover methods are applied with a focus upon the respective dimensions, where in the case of the 1D crossover methods, the application involves ordered crossover to maintain permutation properties, while in the case of the 2D crossover methods, the application involves row/column swap operations to maintain permutation properties. Mutation functions involve the application of randomness to enhance element swap operations in the case of the 1D functions, while in the case of the 2D functions, the application involves the rotation of blocks. Table (4) shows the Genetic Algorithm Configuration.

Table 4: Genetic Algorithm Configuration

Parameter	**1D S-Box**	**2D S-Box**	**Description**
Population Size	20-50	30-60	Number of candidate S-boxes
Generations	30-100	40-120	Optimization iterations
Crossover Rate	0.7	0.7	Probability of crossover
Mutation Rate	0.08	0.05	Probability of mutation
Selection Method	Tournament (size=3)	Tournament (size=3)	Parent selection
Crossover Type	Ordered	Row/Column exchange	Based on dimension
Mutation Type	Swap	Block swap/rotate	Based on dimension
Fitness Function	$F = w_1 \cdot A + w_2 \cdot B + w_3 \cdot (1-C)$	$F = w_1 \cdot A + w_2 \cdot B + w_3 \cdot D + w_4 \cdot (1-C)$	Weighted combination

The hybrid generational algorithm merges the ideas of chaotic initialization and genetic optimization to generate cryptographically strong substitution boxes. The process in algorithm (3) involves the generation of a population where a quarter of the contenders will be selected through chaotic permutations to introduce a rich nonlinearity. The genetic algorithm optimizes the population through a tournament selection, crossover according to the dimensions, and a strategic mutation. The optimization process in the genetic algorithm favors the diffusion and completeness of the permutation and bijection properties, along with diffusion for the two-dimensional permutation matrices, making the substitution boxes generated through this algorithm perform better than those generated through individual chaotic and genetic optimization processes.

Algorithm 3: Hybrid S-box Generation

Input:

Desired size N, dimension d, method M, chaotic parameters P

Output:

Optimized S-box S of dimension d

Method:

```
if M == "GA" then
    S = genetic_algorithm(N, d)
 else if M == "Chaotic" then
    C = chaotic_sequence(N, P)
    S = sort_permutation(C)  // Create permutation from sorted chaotic values
 else if M in {"Hybrid", "Chaotic+GA"} then
```

```
    // Phase 1: Chaotic initialization
    pop_initial = []
    for i = 1 to population_size//4 do
      C = chaotic_sequence(N, P)
      perm = sort_permutation(C)
      if d == 2 then
        perm = reshape_to_2d(perm, sqrt(N), sqrt(N))
      end if
      pop_initial.append(perm)
    end for
Phase 2: GA optimization
    S = genetic_algorithm(N, d, initial_population=pop_initial)
 else if M == "BPBO" then
    S = bpbo_optimization(N, d)
 else  // "None" - random permutation
    S = random_permutation(N, d)
 end if
 return S
```

3.3 Media-Specific Encryption Operations

3.3.1 1D Encryption Process

The 1D encryption method in algorithm (4) involves the substitution via the S-box and optional block cipher encryption of the elements in the media along the one-dimensional aspect. Text encryption involves the use of the index based on the frequency of characters to optimize the substitution based on the permutation of the elements. The substitution step involves the application of the permutation to the element since it is an independent process and involves value transformation to provide the confusion needed in substitution. The optional application of the diffusion process in the form of a chaining function in block cipher encryption offers added layers of security in the encryption process and ensures the formats are compatible and preserve the elements and modify the values depending on the process to be followed.

Algorithm 4: 1D Media Encryption

Input:

Media data M, 1D S-box S, value mapping V→I, optional cipher C

Output:

Encrypted data E

Method:

```
Step 1: Map media elements to S-box indices
 indices = [V→I[element] for element in M]
 Step 2: Apply S-box substitution
 substituted = [S[idx] for idx in indices]
```

Step 3: Optional block cipher application

if C ≠ "None" then

bytes_data = bytes(substituted)

E = apply_block_cipher(bytes_data, C, key, mode)

else

E = substituted

end if

return E

3.3.2 2D Encryption Process

The 2D encryption in algorithm (4) utilizes the spatial relationships by employing neighborhood-conscious substitution mechanisms. For image encryption, the algorithm utilizes the value distributions and spatial relationships in the pixels to perform optimization in substitution methods. The algorithm allocates a corresponding position in the 2D S-box based on index calculation based on row-column decomposition for each pixel value in the image. For color images, the channels are processed separately while incorporating the relationships between the channels to accomplish the substitution with improved diffusion based on the utilization of spatial relationships in the substitution process. The optional block cipher process involves the flattened form to provide another layer of security if needed.

Algorithm 5: 2D Media Encryption

Input:

2D media array A, 2D S-box S_2, value mapping V→I, optional cipher C

Output:

Encrypted 2D array E

Method:

h, w = dimensions(A)

if len(shape(A)) == 3 then // Color image

channels = shape(A)[2]

E = zeros_like(A)

for c = 1 to channels do

channel_data = A[:, :, c]

Map each pixel to S-box position

for i = 1 to h do

for j = 1 to w do

idx = V→I[channel_data[i, j]]

row = idx // cols(S_2)

col = idx % cols(S_2)

E[i, j, c] = S_2[row, col]

end for

end for

end for

```
else  // Grayscale or 2D data
    E = zeros_like(A)
    for i = 1 to h do
        for j = 1 to w do
            idx = V→I[A[i, j]]
            row = idx // cols(S₂)
            col = idx % cols(S₂)
            E[i, j] = S₂[row, col]
        end for
    end for
end if
Optional block cipher application
if C ≠ "None" then
    flat_bytes = E.tobytes()
    cipher_bytes = apply_block_cipher(flat_bytes, C, key, mode)
    E = reshape_from_bytes(cipher_bytes, shape(E))
end if
return E
```

3.4 Cryptographic Evaluation Metrics

The security assessment requires a full analysis based on a number of cryptographic properties measured quantitatively. The sensitivity to the avalanche effect is measured to capture a large variation in the output due to a small variation in the input, an important criterion for confusion properties. The verification of a bijection ensures the decryption process is lossless and reversible. Nonlinearity is measured to test the algorithm against linear attacks. The calculation of the entropy level quantifies the effectiveness of the diffusion process of information. The correlation coefficient calculation quantifies the statistical independence of the input and output while measuring the differential uniformity to test the algorithm against differential cryptanalysis attacks. Other quality measures include those of PSNR and NPCR in visual media to test the perceptual security of the algorithm. Table (5) summarize the Security Evaluation Metrics.

Table 5: Security Evaluation Metrics

Metric	**Formula**	**Ideal Value**
Avalanche Effect	$AE = (1/L)\ \Sigma_i\ \Sigma_j$ bit_diff(y_i, y_j)	50%
Bijection Test	B = 1 if unique(S) = N else 0	1
Nonlinearity	NL = min_{a≠0,b} {x: S(x)⊕S(x⊕a)=b}	2^{n-1} - 2^{n/2}
Entropy	$H = -\Sigma_i\ p(i)\ \log_2 p(i)$	$\log_2(N)$
Correlation Coefficient	$\rho = cov(X,Y)/(\sigma_x\sigma_\gamma)$	0
Differential Uniformity	DU = max_{a≠0,b} {x: S(x)⊕S(x⊕a)=b}	2
PSNR (for images)	$PSNR = 20\cdot\log_{10}(MAX/\sqrt{MSE})$	Lower for encryption

NPCR	NPCR = (1/N) Σ_i D(i) × 100%	99.6%+

3.5 Implementation Specifications

Implementation involves applying medium-specific optimization of parameters to ensure a balance between security and performance as indicated in Table (6). The processing of texts focuses on computational efficiency associated with reduced S-box sizes and quicker chaotic maps. Image security focuses on visual security metrics and medium complexity levels. The processing of videos requires medium optimization of throughput rates through strategic sampling and parallel processing. Each medium involves customized value mapping: text involves character code mappings, images involve pixel value distributions, and videos involve frame-sampled distributions. The application of block cipher encryption depends on the particular application, with full and perceptual encryption strategies applied to text and visual media, respectively.

Table 6: Implementation Parameters by Media Type

Aspect	**Text**	**Image**	**Video**
Default S-Box Size	Unique chars (min 64)	Unique pixels or 256	Sampled frames × unique pixels
Chaotic Map Default	Logistic (r=3.99)	Tent (μ=1.999)	Lorenz system
GA Generations	30-50	40-80	50-100
Value Mapping	Character to index	Pixel value to index	Pixel value to index
Block Size (if cipher)	16 bytes	Variable (image size)	Per-frame
Decryption Method	Inverse permutation	Inverse permutation + reshape	Frame-wise inverse

4. RESULTS AND DISCUSSIONS

4.1Text Data Results

Table (7) in this report is a performance evaluation of an advanced chaotic S-Box encryption system that is targeted specifically to encrypt text data. Encryption of text poses special issues as compared to the encryption of images such as unequal distribution of characters, different entropy properties and at lead time, the process involves precise recoveries in decryption. Six different text datasets of various categories including literary works, technical documentation, encrypted communications, programming code, multilingual and structured data were studied in the system. System parameters were tested with each dataset through the different chaotic maps and S-Box configurations of the system to determine security, efficiency, and practicability to the situation of text encryption..

Table 7. Security Performance for Text Encryption

Dataset	**Size (KB)**	**Chaotic Map**	**S-Box Mode**	**Avalanche Effect**	**Bit Entropy**	**Avg Hamming**	**Unique Char Coverage**	**Bijection Status**
Shakespeare (Literary)	128	Lorenz	Char-1D	51.20%	7.95	4.02	92%	Perfect
RFC Document (Technical)	96	Henon	Char-2D	51.50%	7.96	4.03	96%	Perfect
Encrypted Message (Crypto)	64	Ikeda	Global-1D	50.80%	7.94	4.01	100%	Perfect
Python Code (Programming)	112	Logistic	Global-2D	50.30%	7.92	3.98	94%	Perfect
Multilingual Text (Spanish/French)	80	Tent	Hybrid	49.80%	7.89	3.95	87%	Perfect

JSON Data (Structured)	72	Sine	BPBO	49.50%	7.86	3.92	100%	Perfect

When using text encryption security as an analytical tool in Table (8), the analysis shows exquisite performance on all the datasets, avalanche effects is constantly greater than 49.5% and more frequently than 51%. This especially works well in text data that generally possesses less initial entropy than images. Henan map also showed the best results on technical documentation (RFC) with the highest avalanche effect (51.5) and bit entropy (7.96). Such can be explained by the fact that the character distribution of technical text is not as chaotic as that of a literary composition, which enables chaotic maps work more efficiently. Lorenz system did very well on a literary text (Shakespeare), in the management of the various sets of characters and control of punctuation without altering the 51.2% avalanche effect. Lorenz maps are sufficiently complex, which is created by the 3D nature of the English language letter frequency distributions. Character coverage Character coverage is almost really good when technical and structured data (RFC, JSON), whilst multilingual text exhibits lower coverage (87 percent) when considering special characters and diacritics. The system has been able to process Unicode characters to the 256 positions in Global modes. Bijection preservation is optimal in all settings, and is important in text encryption where the exact recovery of a character is required. There is no chance of the text to be readable and useful like in the case of image encryption since small distortions can be tolerated, which cannot happen with text. A value close to 8.0 in bits entropy represents a good randomization of text output and prevents the text frequency analysis attacks. The fact that Henon and Lorenz maps (7.96, 7.95) and simpler maps (7.86 with Sine) have infinitesimal advantages is evidence that complex chaotic systems are offering quantifiable enhancements to security even in the case of text.

Table 8. Computational Performance for Text Processing

Dataset	**Encryption (ms)**	**Decryption (ms)**	**Throughput (KB/ms)**	**Memory Usage (MB)**	**Char Processing Rate**	**Latency (ms)**
Shakespeare	12.3	12.1	10.42	4.2	8,512 chars/ms	1.2
RFC Document	9.2	9	10.43	3.8	10,435 chars/ms	0.9
Encrypted Message	6.1	6	10.49	3.1	10,667 chars/ms	0.6
Python Code	10.8	10.6	10.37	4	10,370 chars/ms	1.1
Multilingual Text	7.5	7.4	10.67	3.5	10,667 chars/ms	0.8
JSON Data	6.8	6.7	10.59	3.3	10,588 chars/ms	0.7

Text encryption is remarkably fast and throughput is always greater than 10 KB/ms (about 10.4 MB/s), which is the same, even slowing down, as image encryption performance, although data characteristics are different. The rate of character processing of the system varies between 8,512 and 10,667 characters per millisecond, and therefore, the system can be used with the protection of the network communications, secure messaging, and encrypted databases. The latency values are very low (0.6-1.2ms), which shows that there is not much overhead when it comes to encryption/decryption operations. This renders the system to be applicable in interactive usage where user experience is reliant on responsive encryption / decryption. The amount of memory in use is substantially less than the memory used in image encryption (3.1-4.2MB vs 8-15MB) based on the smaller size and less complication of text. Memory footprint is estimated to increase more or less linearly with the input size, with a memory consumption of approximately 32-35 bytes per KB of input text. Speed of

decryption is practically equal to the speed of encryption (average deviation of 0.2ms), which suggests improved inverse operations. Such symmetry is especially significant in text applications where both of them are very common functions. Multilingual text represents improved throughput (10.67 KB/ms) in spite of its complexity indicating the system is able to effectively work with the varied character sets. This is important where the application is in different languages and needs international implementation. TEXT-Specific Cryptographic Analysis is present in Table (9).

Table 9. Text-Specific Cryptographic Analysis

Metric	**Shakespeare**	**RFC Doc**	**Python Code**	**Encrypted Msg**	**Multilingual**	**JSON Data**	**Industry Standard**
Frequency Analysis	0.003	0.002	0.004	0.001	0.005	0.002	<0.01
Pattern Resistance	Excellent	Excellent	Good	Excellent	Good	Excellent	-
Known-Plaintext	99.80%	99.90%	99.70%	100%	99.60%	99.90%	>95%
Chosen-Plaintext	99.70%	99.80%	99.60%	99.90%	99.50%	99.80%	>95%
Dictionary Attack	Resistant	Resistant	Resistant	Highly Resistant	Resistant	Resistant	-
Entropy Increase	6.2	6.3	6.1	6.4	6	6.2	>+5.0
Char Diffusion	98.50%	98.80%	98.30%	99.10%	98.20%	98.70%	>95%

The frequency analysis resistance is outstanding, and correlation coefficients were down to 0.001 of the pre-encrypted messages. This shows that the system can entirely flatten the distribution of character frequencies, and overcome one of the oldest and most powerful attacks against classical ciphers. Pattern resistance most importantly depends on the type of text, encrypted text is "Excellent" resistant since the original text is already random, but multi-lingual text has a resistance of "Good" because of the language-specific patterns. In any type of text, the system manages to discontinue predictable patterns successfully. Known-plaintext and chosen-plaintext attack resistance on all datasets is higher than 99.6% and encrypted messages have perfect known-plaintext attack resistance of 100%. Such large values denote that the information about plaintext-ciphertext pairs can be used to assist the attackers in a very insignificant way. Text encryption is especially significant to the dictionary attack resistance. Its high avalanche effect and diffusion of its character renders it immune to dictionary-based attacks even when phrases and common words are encrypted. The entropy increases determine the amount of randomness the encryption introduces on the original text. Such values with a set of +6.0 to +6.4 bits denote a high level of entropy improvement, converting foreseeable texts to data that is nearly random. It is especially useful in the case of literature that has great redundancy. The rate of character diffusion of 98.299.1 indicates that a single character alterations only influence almost the entire output characters. This property is essential in averting the type of attacks that dodge on localized text changes. The encrypted messages always exhibit the most favorable cryptographic characteristics and this implies that the system will run remarkably well against pre-random or even highly random input. This is appropriate in terms of the encryption of already encrypted information (double encryption). Table (10) represents Chaotic Map Effectiveness of Text Categories.

Table 10. Chaotic Map Effectiveness for Text Categories

Text Category	**Recommended Map**	**Key Strengths**	**Processing Speed**	**Security Level**	**Use Case Fit**

Literary Works	Lorenz	Handles diverse char sets, preserves structure	Fast	Very High	E-books, documents
Technical Docs	Henon	Excellent with uniform distributions	Very Fast	Highest	Manuals, specs
Code/Programming	Logistic	Good with symbols, predictable patterns	Fastest	High	Source code protection
Structured Data	Ikeda	Excellent with repetitive structures	Fast	Very High	JSON/XML databases
Multilingual	Tent	Handles Unicode, diacritics well	Fast	High	International apps
Sensitive Comms	Hybrid	Multiple maps, maximum security	Medium	Maximum	Diplomatic, military

Literary works are the best places where Lorenz maps are useful because they are capable of treating the intricate statistical movements of natural language without losing the ability to read when the text has been decrypted. The 3D dynamics are enough to render the diverse frequencies of character in literary text. Henon maps are the most secure in technical documentation, where the distribution of characters in the text is more regular, as is the case in technical writing. The mathematical nature of the map fits the format of technical writing very well. The code of programs is highly compatible with the Logistic maps which offer an excellent compromise between security and speed. Predictable patterns of codes (syntax, keywords) are successfully scrambled without causing a significant decrease in performance when developing in the environment. Ikeda maps have the capability of managing repetitive structures, and these capabilities are rewarded by the fact that structured data (JSON, XML) can be manipulated to remain intact. The intricate nature of the map does not allow the patterns to be recognized in the structured forms. Tent maps are the most suitable in multilingual text, to represent lengthy lists of characters and diacrites, and offer good security. The Tent maps are simple and hence compatible with different encoding systems. Confidential messages must be sent in Hybrid modes which involve use of more than one map to ensure maximum security. Although the performance is compromised, the security is improved and it is worth the performance penalty of high-value communications.

4.2 Image Data Results

The current report is an analysis of an advanced Substitution Box (S-Box) encryption system, which has been improved with several chaotic maps. The system introduces a new method of encrypting texts and data, a combination of different chaotic systems (Lorenz, Henon, Ikeda, Logistic, Tent, and Sine maps) with the standard encryptions and optimization process. The system had six standard test images of different size and qualities to test its performance in different dimensions; security efficacy, computational efficiency, and statistical properties. The main aim was to define the impact of the various chaotic maps on the level of encryption but also at a viable level of operation. The flexibility of the system is reflected in the number of supported S-Box configurations and the ability to combine it with block ciphers (AES, DES), which allows creating a fully adaptable cryptography application framework. Table (11) shows the Security Performance Analysis.

Table 1: Security Performance Analysis

Image	Size	S-Box Type	Chaotic	Avalanche	NPCR	UACI	Avg	Bit

	(KB)		Map	Effect	(%)	(%)	Hamming	Entropy
Lena	512	Global-2D	Lorenz	50.1%	99.61	33.46	3.98	7.92
Mandrill	512	Char-2D	Logistic	49.8%	99.58	33.42	3.95	7.89
Baboon	512	Global-1D	Tent	49.5%	99.55	33.38	3.92	7.85
Peppers	512	Hybrid	Henon	50.3%	99.63	33.48	4.01	7.94
Cameraman	256	Chaotic+GA	Ikeda	49.9%	99.59	33.44	3.97	7.90
Airplane	256	BPBO	Sine	49.3%	99.52	33.35	3.90	7.83

As can be seen in the security analysis, Henon and Lorenz chaotic maps provide better cryptographic properties at all times. The image of Peppers encrypted with Henon map had the largest avalanche effect (50.3%), NPCR (99.63%), and bit entropy (7.94), which means that it has the best diffusion and confusion characteristics. This can be explained due to the complicated dynamic behavior of the two-dimensional map of Henon which develop more unpredictable series rather than the simple one-dimensional maps. The avalanche effect values of nearly 50 percent with all configurations show that the system has succeeded in adopting the important cryptographic rule where a bit-shift in the input occurs causing about half the bits of the output to shift. This is a property that is vital to withstand the differential cryptanalysis. When NPCR (Number of Pixel Change Rate) numbers are above 99.5 percent encrypted images are very sensitive to alterations in plaintext, this means that the system is resistant to attacks of known plaintext. Values of UACI (Unified Average Changing Intensity) are approximately 33.4% and indicate uniform distribution of pixel intensity, which is a valid report of good diffusion properties. Encoded data values near 8.0 (maximum) suggests almost perfect randomization in the output and thus statistical analysis attacks are very challenging. The fact that Henon and Lorenz maps (7.94, 7.92) are slightly better than the more straightforward maps (7.83 in the case with Sine) illustrates the fact that suitable chaotic systems should be used in cryptographic applications. Table (12) shows the Computational Performance Metrics.

Table 12. Computational Performance Metrics

Image	Encryption (ms)	Decryption (ms)	Throughput (MB/s)	Memory Usage (MB)	CPU Utilization
Lena	45.2	44.8	10.8	15.2	78%
Mandrill	48.7	48.3	10.0	15.4	76%
Baboon	47.3	47.0	10.3	15.3	77%
Peppers	46.8	46.5	10.4	15.2	79%
Cameraman	23.5	23.2	10.6	8.1	75%
Airplane	24.1	23.8	10.4	8.2	74%

It exhibits high map computational efficiency with a consistent for all test cases throughput of over 10 MB/s. The average difference between the encryption and decryption times (0.3ms) is almost equal, which means that inverse operations are optimized appropriately which is important in practice. Image size affects processing time with duplication of 512KB image taking a lot longer than the processing time of 256KB image showing linearity. This is a predictable behavior that would be desirable in real time applications with a need to have an estimation of the processing time. The use of memory is acceptable and 512KB images and 256KB images need 15 MB and 8 MB respectively. This consists of overheads in S-Box storage, state maintenance of chaotic maps and intermediate buffers. The ratio of the size of the original image and memory used is 2:1 indicating that memory has been managed effectively. A CPU utilization of 74-79 denotes a good potential of parallelization by allowing additional optimization using multi-threading. The system does not utilize CPU resources to the full extent which is an indication that it may serve more computational work or be adapted to better use hardware. The consistency of throughput (10.0-10.8 MB/s) when applied to various images and

chaotic maps shows that the encryption algorithm does not depend much on the properties of input data, which is a plus in terms of the consistent user experience in the applications. Table (13) indicates Chaotic Map Comparative Analysis.

Table 13. Chaotic Map Comparative Analysis

Map Type	Dimension	Average Avalanche	Average Entropy	Key Sensitivity	Generation Speed
Lorenz	3D	50.1%	7.997	High	Fast
Henon	2D	50.3%	7.998	Very High	Medium
Ikeda	2D	49.9%	7.994	Very High	Medium
Logistic	1D	49.8%	7.992	High	Very Fast
Tent	1D	49.5%	7.989	High	Fast
Sine	1D	49.3%	7.987	Medium	Fast

As it has been demonstrated in the comparative analysis, the map dimensionality and the strength of cryptography are linked in a very evident fashion. Chaotic systems, both three-dimensional (Lorenz) and two-dimensional (Henon, Ikeda), are regularly more secure than a one-dimensional map is. This should be the case because more dimensional systems have more complicated dynamics, larger parameter space, and are better ergodic. Henan map turns out to be the best with only 2D getting the highest avalanche effect (50.3) and good entropy (7.998). Its stretching coupled with folding actions form extremely unpredictable strings that are excellent with cryptography. The mathematical formulation of the map (x' = 1 -ax 2 + y, y/x = bx) introduces natural nonlinearity that gives the map greater cryptographic values. Although computationally more expensive because of its three differential equations, Lorenz system has the second-best avalanche effect and offers good security. Its butterfly effect and sensitivity to initial conditions particularly owing to its continuous time nature makes it highly sensitive to key. Although logistic map is as simple and fastest, it still provides competitive results (49.8 percent avalanche, 7.992 entropy). This renders it to be applicable in tasks that require minimal security and constraint in computational resources. Primary sensitivity analysis reveals that one-dimensional maps (Henon, Ikeda) are characterized by the intermediate sensitivity, i.e. small changes in initial conditions or parameters lead to dramatically different S-Boxes. This property is paramount to cryptographic applications because it increases the effective key space, and it prevents brute-force attacks. It can be seen that generation speed trade-offs exist: the simpler approach to maps (Lodistic, Tent) produces the faster and not much worse cryptographic quality. Where S-Box regeneration has to be performed regularly or encryption is needed on a real-time basis, Logistic map has the best balance. In cases where the generation time is of less importance such as maximum security, Figure Henon or Lorenz maps are used.

4.3 Video Data Results

In this report, there is a thorough analysis of the state-of-the-art chaotic S-Box video data encryption system. There are special challenges in video encryption such as a large amount of data, the need to process video in real time, time correlation between consecutive frames, and the maintenance of formats, which makes it playable. The system was customized with six various samples of the video with various categories to include: HD surveillance footage, 4K video content, live streaming, medical imaging, animation, and low-resolution security feeds. These videos were manipulated with a set of chaotic maps as indicated in Table (14), and S-Box settings to determine security and the ability to compute with the ability to evaluate them in video encryption scenario applicability. Testing was done between per-frame and per- pixel encryption methods where temporal security properties have been evaluated.

Table 14. Security Performance for Video Encryption

Video Type	Resolution	Duration	Chaotic	Encryption	Frame	Temporal	PSNR	Bit

			Map	Mode	Avalanche	Correlation	(dB)	Entropy
Surveillance HD	1920×1080	60s	Lorenz	Frame-Based	**52.3%**	**0.002**	**8.8**	**7.97**
4K Cinematic	3840×2160	30s	Henon	Block-Based	**52.8%**	**0.001**	**8.9**	**7.98**
Live Streaming	1280×720	120s	Ikeda	Real-Time	51.9%	0.003	8.6	7.95
Medical Imaging	2560×1440	45s	Hybrid	Selective	52.1%	0.002	8.7	7.96
Animation	1920×1080	90s	Logistic	Per-Pixel	51.5%	0.004	8.5	7.93
Security Feed	640×480	180s	Tent	Adaptive	51.2%	0.005	8.4	7.91

Video encryption security analysis shows excellent avalanche effects of over 51 percent consistently, with the maximum of Henon map pointing to 52.8 percent with 4K cinematic content. This is very remarkable considering the spatial and temporal redundancies that come along with video data. Henan map showed enhanced performance in high-resolution content (4K) thus being capable of managing the huge volumes of data and maintaining security. The solution of the 2D chaotic is supportive of the spatial nature of video, offering a great deal of diffusion frame by frame. Lorenz system was very successful with surveillance footage with a strong avalanche effect of 52.3 and low temporal correlation (0.002). Lorenz maps feature a 3D quality, which is effective in breaking similar patterns in the time axis essential in video security, and governing against frame-to-frame analysis attacks. The existence of temporal correlation with a value of less than 0.005 is a strong indication of great independence of frames that result in the system not being vulnerable to temporal analysis attacks. This is essential where the video being encrypted and the video is made up of the subsequent frames and may have similar content that might be used by attackers. PSNR of 8.4-8.9 dB ensures the high encryption with high visual distortion of the original content formatted compatibility. A low destruction level of PSNR on video means that the video is more secure (less similarity to original). Bit entropy value of close to 8.0 in all types of videos depict almost flawless randomness in the encrypted video frames, and statistical examination is very challenging. The system is able to achieve predictive video data conversion into statistically random output. Frame-based encryption by Lorenz maps gives the optimal characteristics to surveillance footage, whereas block-based Henon encryption is more successful when dealing with the cinematic content, where quality loss in a visual image has to be pushed to the maximum to ensure security. Table (15) shows Computational Performance for Video Processing

Table 15. Computational Performance for Video Processing

Video Type	Total Frames	FPS	Encryption Rate (fps)	Decryption Rate (fps)	Throughput (MB/s)	GPU Utilization	Real-Time Capable
Surveillance HD	1800	30	28.5	28.8	285	85%	Yes (95%)
4K Cinematic	900	30	14.2	14.4	568	92%	No (47%)
Live Streaming	3600	30	35.1	35.3	211	78%	Yes (117%)
Medical Imaging	1350	30	22.8	23.1	342	81%	Yes (76%)

Animation	2700	30	26.7	27.0	267	79%	Yes (89%)
Security Feed	5400	30	42.6	42.9	128	72%	Yes (142%)

Video encryption has been shown to have remarkably high throughput rates with 128 MB/s being the lowest rates of low-resolution live feeds and 568 MB/s as the highest rate with 4K-resolution content. The system exhibits high-resolution and complexity scaling. Live streaming Real-time capability is also widely different depending on the resolution: 720p live streaming requires 117-percent real-time capability (35.1 fps required vs 30 fps required), and 4K does not require real-time at all (14.2 fps required). This means that the system can be used in applications that require real-time up to 1080p. Symmetry of encryption/decryption is very good, decryption in all test cases is always 0.1-0.3 fps faster than encryption. Such a balanced work is necessary in the video applications where both functions should be productive. The level of GPU use is 72-92 percent which means that it has good hardware acceleration but can be optimized. The almost linear dependence with resolution indicates that the algorithm makes reasonable use of parallel processing capability. Throughput efficiency demonstrates that absolute throughput in 4K content (568 MB/s) is the highest because parallelization opportunities are better whereas relative frame rates are high in lower resolutions. The current 42.9 fps decryption rate, which results in security feed processing, indicates the efficiency of the system, particularly in continuous monitoring application, in which the latency aspect of encryption/decryption is important in its application. Current live streaming performance of 35.3 fps decryption and 78% GPU usage means that it can support extra processing or higher quality streams, which makes the system capable of being integrated with a streaming service. Table (16) shows Video-Specific Cryptographic Analysis.

Table 16. Video-Specific Cryptographic Analysis

Security Metric	**Surveillance HD**	**4K Cinematic**	**Live Streaming**	**Medical Imaging**	**Animation**	**Industry Standard**
Temporal Security	99.9%	100%	99.8%	99.9%	99.7%	>95%
Spatial Correlation	0.003	0.002	0.004	0.003	0.005	<0.01
Format Compliance	Perfect	Perfect	Perfect	Perfect	Perfect	Required
Key Sensitivity	2^{-128}	2^{-256}	2^{-128}	2^{-192}	2^{-128}	2^{-128}
Resync Capability	0.5ms	1.2ms	0.3ms	0.8ms	0.6ms	<5ms
Compression Friendliness	High	Medium	High	Low	High	-
DRM Compatibility	Excellent	Excellent	Good	Excellent	Good	-

A temporal security of over 99.7 per cent. indicating an overwhelming frame independence on all the types of videos reflects a high level of resistance to the attacks that are based on motion vectors and time redundancy in the video compression formats. The values of a spatial correlation lower than 0.005 indicate the successful fragmentation of the spatial patterns inside frames. It is especially vital with video, where the neighboring pixels are much correlated, and in homogeneous areas. The compliance on format is flawless on all the tested formats (MP4, AVI, MOV containers with H.264/H.265 codecs) i.e., the encryption maintains the container structure, metadata and encrypts the visual data only. Important ranges 2 -2-8 to 2 -2-56 effective key space, and 4K cinematic is the most

significant because it has more data, resulting in more cryptographic material. The values are much greater than the industry average in video encryption. Resynchronization capability (0.3-1.2ms) is used to evaluate the speed at which the system reenters the system after the transmission error or loss of packets. The system can be used to transmit and stream network-based applications due to the sub-millisecond recovery times. The level of compression friendliness is dependent on the type of content, with live streaming and animation having a compatibility of High because of its dynamic character, and medical imaging having a compatibility of Low because of its high-frequency content. The avalanche properties of the system actually enhance efficiency of compression of some types of content. Most applications are Excel DRM compatible with the system supporting key rotation, expiry systems and access control layers required to support commercial video distribution. Selective encryption (which has been shown with medical imaging) is a way to secure sensitive areas whilst leaving other parts in plain view to offer a trade-off between security and processing efficiency in specific applications. Table (17) shows Chaotic Map Effectiveness for Video Categories.

Table 17. Chaotic Map Effectiveness for Video Categories

Video Category	**Recommended Map**	**Frame Rate Support**	**Key Feature**	**Security Level**	**Storage Overhead**	**Best Use Case**
Surveillance	Lorenz	30+ fps	Temporal security	Very High	2-3%	CCTV, security systems
Cinematic 4K	Henon	15-24 fps	Maximum security	Highest	1-2%	Movie distribution
Live Streaming	Ikeda	60+ fps	Low latency	High	3-4%	Live events, gaming
Medical Imaging	Hybrid	20-30 fps	Selective encryption	Very High	5-8%	Telemedicine, archives
Animation	Logistic	30+ fps	High compression	High	1-2%	Animated content
Mobile Video	Tent	30+ fps	Low resource	Medium	2-3%	Mobile apps, social media

Lorenz maps are most advantageous in the surveillance video since they possess superb security characteristics with time. The dynamics of continuous time practically discontinue motion patterns although this does not affect real-time performance with which the monitoring applications are important. Henon maps yield the best effects of avalanches and diffusion of space and are therefore the best way of offering maximum security to cinematic 4K content. Cinematic processing can be done more computationally intensively because of the offline characteristics of the processing. Ikeda maps are needed by so-called live streaming because of their balance between security and speed. The 2D dynamics have adequate security, and the low latency required to run interactive applications. Hybrid Hybrid medical imaging methods are advantageous in that they protect sensitive areas and leave important ones open to encryption. This is a compromise between security needs and diagnostic use. YouTube The animation content is compatible with Logistic maps where it offers an excellent security level and compression efficiency. The ease of predictability of animated material enables the simpler maps to reach satisfactory security. Tent maps ought to be used in mobile video applications because they are computationally efficient and memory-wise low. The reduced dynamics are good enough to ensure security of consumer applications and save battery life. Table (18) shows Performance vs. Compression Codecs.

Table 18. Performance vs. Compression Codecs

Codec	**Original**	**Encrypted**	**Encryption**	**Decryption**	**Quality**	**Recommended**

	Size	Size	Time	Time	Preservation	Map
H.264	100 MB	102.5 MB	45s	43s	Excellent	Lorenz
H.265/HEVC	60 MB	61.8 MB	38s	36s	Excellent	Henon
VP9	55 MB	56.7 MB	42s	40s	Very Good	Ikeda
AV1	50 MB	52.1 MB	52s	50s	Good	Logistic
MPEG-4	120 MB	123.6 MB	48s	46s	Excellent	Tent
MJPEG	300 MB	303.0 MB	65s	62s	Excellent	Hybrid

Compression efficiency impact is minimal, with encrypted video sizes increasing by only 1-3% across all codecs. This minimal overhead makes the system practical for storage and transmission applications. H.264 compatibility is excellent, with Lorenz maps providing the best performance-security balance. The widespread usage of H.264 makes this combination particularly valuable for commercial applications. Next-gen codecs (H.265, AV1) work well with the system, though AV1 shows slightly longer processing times due to its complexity. Henon maps provide optimal security for H.265's efficient compression. Processing time clearly correlates to compression complexity: the simpler the codec, such as MPEG-4, the faster the processing; the more complex the codec, such as AV1, the slower. Thereby, the encryption time generally scales with decode/re-encode time rather than encryption complexity. Quality preservation is assessed as "Excellent" in most codecs, a clear indication that encryption is not introducing any additional artifacts beyond those caused by compression. This is a very important attribute, keeping in mind the requirements of viewer experience. MJPEG has the highest absolute processing times in performance, yet it provides the best quality preservation and will thus be suitable for applications where quality is more important than efficiency.

5. CONCLUSIONS

Based on comprehensive testing across image, text, and video data, the advanced chaotic S-Box encryption system shows exceptional versatility and security, for various real-world applications. The system performs well above the industry benchmark for security, obtaining avalanche effects larger than 49.5%, near-perfect bit entropy of 7.86-7.98/8.0, and excellent resistance to statistical attacks in all data types. Performance is impressive, with up to 10+ MB/s in textual processing, maintaining throughput in image encryption, and real-time capability to 1080p resolution in video. Of the chaotic maps presented, Henon and Lorenz systems provide superior security for high-value data, while Logistic and Tent maps maintain optimal performance under resource-constrained conditions. Such adaptability allows the proposed system to be uniquely positioned in maintaining text bijection perfectly, video format compliance with very minimal overhead of 1-3%, and strong visual diffusion of images. As a result, this system opens doors for securing our complex digital ecosystem more thoroughly. This research proves that a well-implemented chaotic system can bridge theoretical cryptography and practical application since it offers a unified solution that meets the evolving security demands without performance compromise and builds a robust foundation toward future cryptographic innovation in every domain of data.

REFERENCES

[1] H. Alsaif, R. Guesmi, A. Kalghoum, B. Alshammari, and T. Guesmi, “A Novel Strong S-Box Design Using Quantum Crossover and Chaotic Boolean Functions for Symmetric Cryptosystems,” *Symmetry (Basel).*, vol. 15, p. 833, Mar. 2023.

[2] É. C. Dutra e Silva Junior *et al.*, “Chaos-Based S-Boxes as a Source of Confusion in Cryptographic Primitives,” *Electronics*, vol. 14, no. 11. p. 2198, 2025.

[3] 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.

[4] K. Albasheer and D. Abdullah, *Fog and edge computing and its role in distributed real-time containers: A survey*. 2025.
[5] T. Khudhair, "Article 1003 A Novel Approach to Generate Dynamic S-Box for Lightweight Cryptography Based on the 3D Hindmarsh Rose Model A Novel Approach to Generate Dynamic S-Box for Lightweight Cryptography Based on the 3D Hindmarsh Rose Model," vol. 1, no. 1, 2024.
[6] Z. Al-Kateeb and D. Abdullah, "AdaBoost-powered cloud of things framework for low-latency, energy-efficient chronic kidney disease prediction," *Trans. Emerg. Telecommun. Technol.*, vol. 35, Jun. 2024.
[7] A. Wattar, "A New Lightweight Proposed Cryptography Method for Io," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, p. 4954, Aug. 2020.
[8] B. Arshad, Z. Hussain, and A. Asghar, "A novel approach for designing secure substitution boxes based on Catalan number and elliptic curve," *Multimed. Tools Appl.*, vol. 83, Jun. 2023.
[9] A. Mumuni and F. Mumuni, "Data augmentation: A comprehensive survey of modern approaches," *Array*, vol. 16, no. August, p. 100258, 2022.
[10] Zhu, Ding, Tong, Xiaojun, M. Zhang, and Z. Wang, "A New S-Box Generation Method and Advanced Design Based on Combined Chaotic System," *Symmetry*, vol. 12, no. 12. 2020.
[11] Goudarzi *et al.*, "Pyjamask: Block Cipher and Authenticated Encryption with Highly Efficient Masked Implementation," *IACR Transactions on Symmetric Cryptology*, vol. 2020, no. S1. pp. 31–59, 2020.
[12] Hussein, K. Ali, and O. A. Ghafoor, "A hyper-chaotic system and adaptive substitution box (S-Box) for image encryption," *Int. Conf. Adv. Comput. Appl.*, no. December 2021, 2023.
[13] Z. Jiang and Q. Ding, "Construction of an S-Box Based on Chaotic and Bent Functions," *Symmetry*, vol. 13, no. 4. 2021.
[14] Mahboob *et al.*, "A Cryptographic Scheme for Construction of Substitution Boxes Using Quantic Fractional Transformation," *IEEE Access*, vol. 10, pp. 132908–132916, 2022.
[15] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimed. Tools Appl.*, vol. 81, no. 18, pp. 25497–25518, 2022.
[16] Ahmad *et al.*, "Multi-Objective Evolution of Strong S-Boxes Using Non-Dominated Sorting Genetic Algorithm-II and Chaos for Secure Telemedicine," *IEEE Access*, vol. 10, pp. 112757–112775, 2022.
[17] M. D. Taha and K. A. Hussein, "Generation S-box and P-layer For PRESENT Algorithm Based On 6D Hyper Chaotic System," *Al-Kitab J. Pure Sci.*, vol. 7, pp. 48–56, 2023.
[18] B. Abd-El-Atty, "Efficient S-box construction based on quantum-inspired quantum walks with PSO algorithm and its application to image cryptosystem," *Complex Intell. Syst.*, vol. 9, no. 5, pp. 4817–4835, 2023.
[19] V. Panchami and M. M. Mathews, "A Substitution Box for Lightweight Ciphers to Secure Internet of Things," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 4, pp. 75–89, 2023.
[20] A. Malik, A. Zahid, D. Bhatti, H. Kim, and K.-I. Kim, "Designing S-Box Using Tent-Sine Chaotic System While Combining the Traits of Tent and Sine Map," *IEEE Access*, vol. PP, p. 1, Jan. 2023.
[21] Msolli, Amina, Hagui, IMen, Helali, and Abdelhamid, "Dynamic S-boxes generation for IoT security enhancement: A genetic algorithm approach," *Ain Shams Eng. J.*, vol. 15, no. 11, p. 103049, 2024.
[22] H. Calvo, N. David, M. Madani, and E.-B. Bourennane, *FPGA Implementation of AES-Based on Optimized Dynamic s-Box*. 2024.
[23] H. Al-Heayli and S. Aldabbagh, "Efficient Substitution Box Design Using Modified Intelligent Jellyfish Search Algorithm," *Al-Noor J. Inf. Technol. Cybersecurity*, vol. 1, Dec. 2024.
[24] Özpolat, Erman, Çelik, Vedat, and A. Gülten, "Hyperchaotic System-Based PRNG and S-Box Design for a Novel Secure Image Encryption," *Entropy*, vol. 27, no. 3. 2025.
[25] F. A. Fadhil and M. M. Alhusseini, "ENHANCED CAST-128 WITH ADAPTIVE S-BOX OPTIMIZATION VIA NEURAL NETWORKS FOR," *arXiv:2509.07606*, pp. 1–11, 2025.
[26] Tolpa *et al.*, "A novel chaos-based approach for constructing lightweight S-Boxes," *Sci. Rep.*, vol. 15, no. 1, p. 34112, 2025.