Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.078078

ARTICLE

Brownian-Perturbed Hénon Map for Image Encryption: Application in Biomedical Images

Walaa Alayed[1], Asad Ur Rehman[2], M.Awais Ehsan[3], Waqar Ul Hassan[4] and Ahmed Zeeshan[5,6,*]

[1]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia
[2]Department of Mathematics, Capital University of Science & Technology (CUST), Islamabad, Pakistan
[3]School of Natural Sciences, National University of Science and Technology, Islamabad, Pakistan
[4]Department of Mathematics, Government College University, Lahore, Pakistan
[5]Department of Mathematics & Statistics, Faculty of Science, International Islamic University Islamabad, H-10, Islamabad, Pakistan
[6]Department of Mathematics, College of Science, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul, Republic of Korea

*Corresponding Author: Ahmed Zeeshan. Email: ahmad.zeeshan@iiu.edu.pk

Received: 23 December 2025; Accepted: 26 February 2026; Published: 08 May 2026

ABSTRACT: The rapid growth in the field of data and cloud computing has made it essential to ensure information security. Encryption consists of multiple layers, among which a critical component is the Substitution box (S-box). The S-box provides nonlinearity and confusion between the original and cipher forms, and its performance directly determines the security of the cipher against cryptanalysis. Chaotic systems have been widely used for image encryption, however, they suffer from well known limitations such as deterministic periodicity and reduced unpredictability in finite field digital environments. To address these issues, we propose a new S-box generation scheme based on an improved chaotic map, which combines the Hénon chaotic map with Brownian motion, concept in thermodynamics. In the proposed method, the initial keys used in the permutation and diffusion stages interact with each other, thereby enhancing the complexity of the system. We leverage the sensitivity and periodicity of the Hénon map and inject a zigzag Brownian motion sequence into its iteration process to overcome limitations of standalone chaotic maps. The extended scheme is implemented, and a comprehensive security analysis is performed on various cipher images obtained through the modified design. The results of the analysis demonstrate strong security properties, while the running time of the proposed scheme is comparatively better. The proposed scheme is both novel and adaptable, making it suitable for enhancing resistance against differential and algebraic attacks. Hénon-map S-box with Brownian perturbation secures biomedical images (MRI/CT, ultrasound and Xrays) and biofluid sequences (micro-PIV/microfluidics). High unpredictability enables real-time encryption which preserves privacy of patient data/IP.

KEYWORDS: Substitution boxes; cryptography; encryption; Hénon chaotic map; biomedical; biofluid; Brownian motion

1 Introduction

Cryptography is the practice and study of techniques for secure communication in the presence of adversaries. It is all about protecting and encrypting data so that if someone intercepts it during transmission, they are unable to read or understand the message [1]. The process of securing data in a certain way is called encryption [2]. Throughout history, encryption techniques have evolved from ancient methods like the Caesar cipher, key used method to today's highly advanced systems [3]. As computational power and

mathematical understanding have grown, old methods became easier to crack, making it essential to develop stronger and more sophisticated algorithms in order to stay one step ahead and keep communication safer.

A key theoretical leap was Kerckhoffs's principle, which states that a cryptosystem should remain secure even if everything about the system except the secret key is publicly known [4], subsequently formulated by Claude Shannon as "The enemy knows the system" by which the approach to encryption can be publicly known, but not the key. From this, Shannon in 1945–1949 developed the basis of modern cryptography with his information theoretic analysis of secrecy systems [5]. Shannon defined the principles of confusion and diffusion, fundamental principles for block cipher design. Confusion hides relationships between key and cipher text, while diffusion disseminates the plain text structure throughout the output to prevent statistical attacks. Shannon also demonstrated that perfect secrecy, such that cipher text never provides any information on plain text, is attainable only with a key length equivalent to that of the message, as with the one time pad. In the contemporary age, cryptography divides into symmetric and asymmetric techniques, symmetric encryption employs one and the same key for decryption and encryption [2]. Block ciphers such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard) employ substitution–permutation networks, where S-boxes introduce confusion and permutation layers provide diffusion. Asymmetric encryption is based on pairs of keys, one public and another private, to encrypt and decrypt communication [6]. Such schemes usually rely on difficult mathematical problems such as integer factorization or discrete logarithms. Elliptic Curve Cryptography (ECC) is a new, compact scheme for safe key exchange.

S-boxes play a pivotal role in symmetric key cryptography as the primary source of nonlinearity and confusion in block cipher algorithms [7]. A cryptographically secure S-box should exhibit certain properties [8], it must be a bijective mapping (permutation) to prevent cipher degeneracies, and it should have high Nonlinearity (NL) to resist linear cryptanalysis [9]. It should also satisfy the Strict Avalanche Criterion (SAC), a single-bit change in input flips about 50 percent of output bits, and the Bit Independence Criterion (BIC), output bit changes should be statistically independent [10]. Furthermore, a good S-box has low Differential Uniformity (DU) (minimizing the probability that a given input difference leads to a particular output difference), thereby resisting differential cryptanalysis [11]. Low maximum linear approximation probability (LAP) is desired for resistance to linear cryptanalysis, and high algebraic complexity (e.g., high algebraic degree) helps resist algebraic attacks [12]. Achieving all these properties simultaneously in an S-box is challenging, especially for larger S-box sizes (8×8), which motivates continued research into new design methods. Chaos theory has emerged as a promising approach for S-box construction due to the inherent randomness and sensitivity of chaotic maps [13]. Chaotic systems are deterministic but exhibit pseudo random behavior, a tiny perturbation in the initial state yields vastly different trajectories [14], akin to the avalanche effect in cryptography. These properties can be harnessed to generate S-boxes with good confusion properties. Indeed, numerous works have explored chaos-based S-box generation using maps like the logistic map, tent map, Lorenz system, etc., S-boxes with competitive cryptographic properties. Chaotic S-boxes offer flexibility and often satisfy bijectivity and NL requirements. However, using chaotic maps in digital cryptography also presents challenges [15]. Finite precision effects in digital implementations cause chaotic sequences to eventually repeat (entering periodic orbits) [16], potentially undermining unpredictability. Many 1D maps (e.g. logistic map) have limited chaotic ranges or smaller Lyapunov exponents, reducing entropy and making sequences more predictable or unevenly distributed [17]. Consequently, naive use of a single chaotic map may produce S-boxes with hidden weaknesses such as short cycle lengths, biases, or insufficient randomness. To overcome these limitations, researchers have combined multiple sources of chaos or introduced perturbations to enrich chaotic behavior [18]. Reference [19] proposed a discrete memristive conservative chaotic map for secure communication. Recently, several chaos based image

encryption schemes have been proposed for biomedical applications, focusing on improved diffusion and resistance against statistical attacks [20–24].

In this work, we propose an enhanced chaos-based S-box generation method that synergistically combines the 2D Hénon map with Brownian motion. The Hénon map is a well known discrete time chaotic system with proven chaotic dynamics and a two dimensional state that provides more complexity than 1D maps. Brownian motion, on the other hand, is a stochastic process characterized by random, continuous movements, intuitively, the irregular zigzag movement of particles suspended in fluid (also known as a Wiener process in mathematical terms). By injecting a Brownian motion component into the iterative process of the Hénon map, we effectively introduce an external source of randomness that perturbs the chaotic trajectory in a controlled manner. This hybrid approach yields a composite chaotic system with improved unpredictability, reduced periodicity, and greater entropy compared to the use of the Hénon map alone. In essence, the Brownian perturbation continually perturbs the deterministic chaos, preventing it from settling into short cycles and ensuring a broader exploration of state space. We leverage this enhanced chaos to generate S-boxes that are highly random yet reproducible (with a secret key seed) and that fulfill the strict criteria for cryptographic substitution components. The Brownian perturbed Hénon (BPH) map is ideal for privacy safe encryption of biomedical and biofluid imaging in real time, without degrading diagnostic quality. The main contributions of the paper are:

1. A hybrid Brownian perturbed Hénon chaotic map is proposed to mitigate finite-precision degradation in chaos based S-box generation.
2. A deterministic, key dependent S-box construction framework is developed using rank order mapping, guaranteeing bijectivity and cryptographic soundness.
3. The proposed hybrid map enhances robustness by combining deterministic chaos with controlled stochastic perturbations, resulting in increased unpredictability and improved statistical complexity compared with conventional chaotic maps.
4. The controlled Brownian perturbations in the proposed map are specifically designed to suppress periodicity inherent in finite precision implementations while preserving determinism and key dependence.

The remainder of the paper is organized as follows. In Section 2, we review existing S-box design approaches and their limitations. Section 3 introduces the necessary preliminaries, including the Hénon chaotic map and discrete Brownian motion. Section 4 presents the proposed S-box generation method in detail. In Section 5, we evaluate the cryptographic properties of the proposed S-box and compare them with existing state-of-the-art designs. Section 6 demonstrates the effectiveness of the proposed S-box in image encryption through statistical and graphical analysis. Finally, Section 7 concludes the paper and outlines directions for future research.

2 Related Work

Over the past few decades, diverse approaches have been developed for constructing S-boxes, each with its own philosophy and trade-offs. We categorize them into a few broad categories, algebraic constructions, chaos-based methods, heuristic techniques and cipher derived S-boxes, and discuss how our work relates to and improves upon these.

Many classical ciphers use S-boxes designed with algebraic structures or human crafted criteria. The AES S-box, for example, is constructed by inverting elements in the finite field GF (2^8) and then applying an affine transformation [25]. This design gives the AES S-box excellent properties, it is bijective with an algebraic degree of 7, a DU of 4, and NL of 112 [26]. It is considered one of the best 8×8 S-boxes in terms of cryptographic strength. Similarly, the older DES cipher uses 4-bit S-boxes that were carefully constructed

to satisfy known criteria [27]. Algebraic S-box design often involves ensuring that there are no simple mathematical relations, for example, AES is an affine equivalent of an almost perfect NL (APN) function, thus optimally resistant to differential attacks [28]. Chaos theory has inspired numerous S-box design methods, leveraging the complex dynamics of chaotic maps. Many works in this vein took simple 1D maps to produce pseudo random sequences that are then mapped to S-box permutations. For instance, an S-box pattern generation using an enhanced logistic map is proposed by El Gaabouri et al. (2024) [29], where the chaotic map's output is used to shuffle values. Two dimensional chaotic maps and higher dimensional systems have also been used to achieve better randomness and avoid the limited chaos of 1D maps [30]. A notable challenge addressed in recent chaos-based designs is the problem of finite precision and short periodicity. When chaotic maps are implemented with finite bits, they can fall into short cycles. Some researchers have proposed perturbation or switching techniques to extend the effective period [31]. For example, Li et al. (2020) introduced an anterior perturbation to the logistic map to form an Enhanced Logistic Map with infinite chaotic length [32]. Similarly, composite systems that switch between multiple maps or use multiple chaotic variables have been explored [33]. Another vein of research treats S-box design as an optimization problem. Since metrics like NL, DU, SAC, etc., can be computed for a given S-box, one can attempt to search the space of all permutations (which is huge for 8-bit) for those with good properties. Direct brute force is infeasible, but heuristic search algorithms have been successful in finding S-boxes with excellent properties. Techniques include genetic algorithms, particle swarm optimization, hill-climbing, simulated annealing, and more recently, deep learning models (e.g., using generative adversarial networks to produce candidate S-boxes) [34]. For example, Wang et al. (2020) evolved S-boxes and achieved NL around 104–106 and DU 4–6. A 2023 study by Thakor et al. used a multi objective evolutionary approach to optimize boomerang and algebraic immunity along with standard criteria. A final category is the reuse or adaptation of S-boxes from existing cryptosystems. For lightweight cryptography, 4×4 S-boxes like that of the PRESENT cipher or GIFT cipher are often used as they are small and efficient. The PRESENT S-box, for instance, was designed to have no fixed points or opposite fixed points and to achieve DU 4 and relatively high NL ~4 or 6. It has an affine algebraic representation which can be used in cryptanalysis, but overall is strong for its size. Researchers sometimes adapt such S-boxes to create new designs. While this approach benefits from known security of existing S-boxes, it lacks novelty and the flexibility of generating brand new S-boxes.

The literature shows a trade-off between structured approaches (algebraic, manual design) that give provable optimality in some criteria, and automated or chaotic approaches that can generate many alternative S-boxes but require careful analysis to ensure no weaknesses.

There are various ways to counter the shortcomings in chaotic systems. Chaos anti control methods are aimed at producing and improving chaotic phenomena by the application of control inputs, and they were applied in the study of chaotic encryption algorithms [35]. Stochastic perturbation approaches add random or noising perturbations to modify trajectories in the system, which helps affecting the escape rates and fractal properties found in chaotic systems [36]. Hybrid perturbation delay methods involve periodically disturbing system parameters to account for the digital precision effect and to achieve ergodicity [37]. Even these methods can be used for increasing the complexity of a system, however, they involve either increased structural complexity or parameter adjustments. Brownian motion, on the other hand, is a well known stochastic process for diffusion, which can be coupled with a pre-existing chaotic map for controlled randomness, efficient trajectory diffusion within phase space, and compensation for finite precision without incurring too much computational expense. The use of Brownian motion in chaos based cryptographic systems has proven useful for improving pseudo random sequence statistical properties and encrypting performance [38].

Our work combines two different sources, Hénon and Brownian, to form a composite chaotic system. A closely related prior effort is the work by Harmouch and El Kouch (2018) on using Brownian motion to generate 8 × 8 S-boxes [39]. They argued that Brownian motion's random nature increases the complexity for attackers. However, Brownian motion alone is not deterministic or key driven in the same way chaotic maps are, and using it directly can complicate reproducibility of the S-box. We improve on this by using Brownian motion in a controlled manner, as a perturbation to a deterministic chaotic map. Thereby ensuring the S-box generation is both pseudo-random and deterministically reproducible given the secret key (which seeds both the chaotic map and the pseudo Brownian sequence). The Hénon map provides structure and reproducibility, while Brownian motion injects entropy and irregularity. Addition of controlled Brownian perturbation in the Hénon map can counteract the effect of finite precision problems in digital chaotic systems, making it more unpredictable and less cyclic in the produced sequences. When compared to traditional chaotic mappings, this unique property of being more irregular adds to other cryptographic desirable characteristics of higher nonlinearity in produced S-boxes [40].

3 Preliminaries

This section introduces the basic concepts and mathematical tools used to construct cryptographically robust S-boxes. We cover the Hénon chaotic map, discrete Brownian motion, and rank order mapping for generating bijective permutations.

3.1 Hénon Chaotic Map

The Hénon map is a two dimensional discrete time dynamical system introduced by Michel Hénon [41]. It exhibits chaotic behavior for certain parameter values and is defined as:

$$\begin{cases} x_{n+1} = 1 - a\,x_n^2 + y_n, \\ y_{n+1} = b\,x_n, \end{cases} \qquad n = 0, 1, 2, \ldots \tag{1}$$

where $(x_0, y_0) \in \mathbb{R}^2$ is the initial condition and $(a, b) \in \mathbb{R}^2$ are parameters. For the canonical values $a = 1.4$ and $b = 0.3$, the map exhibits sensitive dependence on initial conditions, generating the famous Hénon attractor, a fractal strange attractor. The Jacobian matrix is:

$$J = \begin{bmatrix} -2ax & 1 \\ b & 0 \end{bmatrix} \tag{2}$$

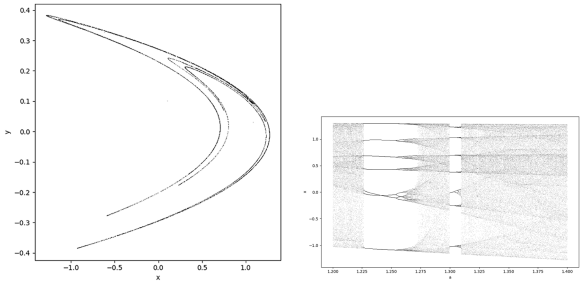
which shows that the map is area preserving. An area preserving chaotic map is a conservative dynamical system whose Jacobian determinant equals unity, ensuring that phase-space area remains invariant under iteration. This property is fundamental to its chaotic dynamics. The Hénon attractor is presented in Fig. 1a and Orbit diagram for the Hénon map, keeping b = 0.3 and varying a is shown in Fig. 1b. The plot shows the classic period doubling route to chaos.

3.2 Discrete Brownian Motion

Brownian motion is a continuous time stochastic process with independent Gaussian increments. In digital implementations, it is commonly approximated in discrete time as a cumulative sum of zero mean random increments, referred to as discrete Brownian motion [42].

$$X_n = \Delta X_1 + \Delta X_2 + \cdots + \Delta X_n \tag{3}$$

where $\Delta X_i \sim \mathcal{N}(0, \sigma^2)$ are i.i.d. Gaussian variables. In a cryptographic setting, a key dependent pseudo random generator produces these increments to ensure deterministic reproducibility. As shown in Fig. 2, the simulated discrete Brownian motion path exhibits the characteristic zigzag behavior, illustrating how the particle undergoes random, small scale displacements at each time step [43].



(a) Hénon attractor (a = 1.4, b = 0.3) **(b)** Orbit diagram varying a

Figure 1: Hénon map results: (**a**) Attractor and (**b**) Orbit diagram.

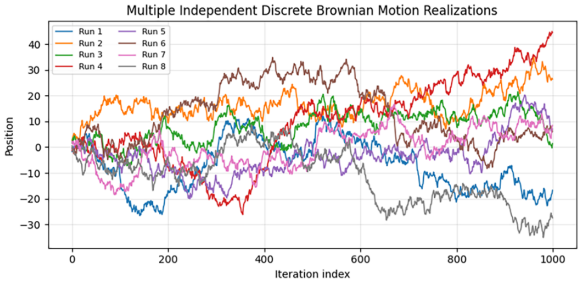


Figure 2: Multiple independent realizations of discrete Brownian motion.

3.3 Rank Order Mapping: Generating Permutations

Rank-order mapping is a mathematical technique to transform a real-valued sequence into a unique permutation of integers [44]. This is particularly useful when a continuous sequence, such as one generated by a chaotic map or a discrete Brownian motion needs to be converted into a discrete bijective sequence. Let $N = 2^n$ denote the length of the sequence. Given a real-valued sequence

$$H = [H_0, H_1, \ldots, H_{N-1}] \tag{4}$$

the rank-order mapping produces a permutation P of $\{0, 1, \ldots, N-1\}$ as follows:

1. Sort H in ascending order and record the original indices $\mathsf{idx}(j)$ of the j-th smallest element.
2. Define the permutation P: $\{0, \ldots, N-1\} \to \{0, \ldots, N-1\}$ by

$$P(\mathsf{idx}(j)) = j, \quad j = 0, 1, \ldots, N-1 \tag{5}$$

This procedure ensures that each element of the original sequence is assigned a unique rank, which will help us yielding a bijective mapping suitable for later use in constructions of S-boxes.

4 Proposed S-Box Generation Method

This section presents our method for constructing cryptographically strong S-boxes by combining a hybrid Hénon chaotic map with key dependent Brownian perturbations and applying deterministic rank-order mapping [44]. The procedure ensures sensitive dependence on the secret key while mitigating finite precision artifacts inherent to digital chaotic systems.

4.1 Hybrid Hénon-Brownian Chaotic Source

To enhance the unpredictability of the Hénon map in finite precision computations, we inject small key dependent Brownian perturbations into the system. Let $\varepsilon_1, \varepsilon_2 > 0$ denote small perturbation scales, and let $\Delta X_n, \Delta Y_n$ be Gaussian increments with mean 0 and variance σ^2, generated from a cryptographically secure PRNG seeded by the secret key K. The hybrid system is defined as:

$$x'_n = x_n + \varepsilon_1 \Delta X_n, \tag{6}$$

$$y'_n = y_n + \varepsilon_2 \Delta Y_n, \tag{7}$$

$$x_{n+1} = 1 - a(x'_n)^2 + y'_n, \tag{8}$$

$$y_{n+1} = b x'_n, \tag{9}$$

where a and b are the standard Hénon parameters, and (x_0, y_0) are the initial states derived from the secret key. The perturbations $\varepsilon_1 \Delta X_n$ and $\varepsilon_2 \Delta Y_n$ reduce latent periodic cycles while preserving the map's chaotic properties.

Fig. 3 illustrates the phase space trajectories of the Hénon map after introducing controlled Brownian perturbations into its iterative process. Each trajectory corresponds to an independent realization generated using different pseudo random seeds while keeping the chaotic parameters fixed. Compared with the classical Hénon attractor under finite precision arithmetic, the perturbed system exhibits increased trajectory dispersion and reduced recurrence of short periodic orbits. This behavior indicates that the Brownian perturbation disrupts deterministic numerical artifacts and mitigates degradation effects commonly observed in digital chaotic implementations.

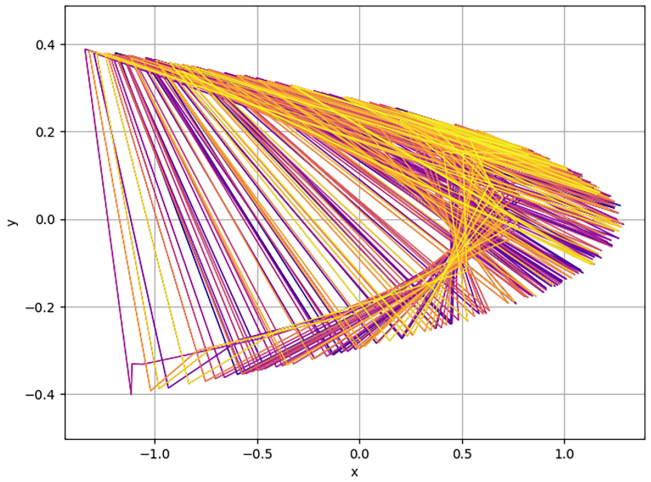


Figure 3: Trajectory of the Hénon map with Brownian perturbations applied at each step.

4.2 Key Dependent Initialization

The secret key K initializes the system as follows:

1. Apply a key derivation function (KDF) to K.
2. Extract the initial states (x_0, y_0), Hénon parameters (a, b), and perturbation scales $(\varepsilon_1, \varepsilon_2)$ from the KDF output.
3. Seed the PRNG for generating Gaussian increments $\Delta X_n, \Delta Y_n$.

Each key produces a unique chaotic trajectory, ensuring that the resulting S-box is key-dependent and distinct.

4.3 Optional 3D Brownian Perturbation

While the Hénon map is two-dimensional, the principle of Brownian perturbation can be extended to three dimensions for applications such as image encryption. 3D Brownian perturbation introduces multi-dimensional (x, y, z) random variations into the Hénon map iterations to further enhance unpredictability and diffusion. This perturbation can be enabled or disabled depending on the required security level. For S-box generation, 2D perturbations suffice, but this extension demonstrates the method's flexibility.

4.4 S-Box Construction via Rank-Order Mapping

Using the chaotic trajectory generated by the hybrid system, a bijective S-box is obtained through rank order mapping. Let $N = 2^n$ denote the S-box size (e.g., $N = 256$ for an 8×8 S-box).

1. Discard the first N_0 iterations of x_n as transient to avoid initialization bias (e.g., $N_0 = 1000$).
2. Collect the next N values $H_0, H_1, \ldots, H_{N-1}$ from the x-coordinate.
3. Sort H in ascending order and record the original indices $\mathsf{idx}(j)$ of the j-th smallest element.
4. Define the S-box permutation $S : \{0, \ldots, N-1\} \to \{0, \ldots, N-1\}$:

$$S(\mathsf{idx}(j)) = j, \quad j = 0, 1, \ldots, N-1.$$

This method guarantees a bijective, key dependent S-box with strong diffusion properties while mitigating finite precision artifacts in the chaotic system.

4.5 Hénon–Brownian S-Box Generator Algorithm

Algorithm 1 describes the step-by-step procedure employed to construct the Hénon–Brownian S-box generator.

Algorithm 1: Hénon–Brownian S-box generator

```
Input: Secret key K, S-box size N = 256, transient length N_0
Derive initial state (x_0, y_0), system parameters (a, b), perturbation scales (ε_1, ε_2), and PRNG seed from K.
for i = 0 to N_0 − 1 do
    Generate perturbations (ΔX_i, ΔY_i) from PRNG
    Update (x_{i+1}, y_{i+1}) via (6)–(9)
end for
for i = 0 to N − 1 do
    Generate perturbations (ΔX_i, ΔY_i) from PRNG
```

(Continued)

Algorithm 1 (continued)

Update (x_{i+1}, y_{i+1})
Record $H_i \leftarrow x_{i+1}$
end for
Sort $H = \{H_0, \ldots, H_{N-1}\}$ in ascending order to obtain index array idx
Define $S[\text{idx}[j]] \leftarrow j$ for $j = 0, \ldots, N-1$
return S-box S

4.6 Toy Example: 4 × 4 S-Box (16 Elements)

To illustrate the procedure of Algorithm 1, we consider a small-scale example with $N = 16$:

$$(x_0, y_0) = (0.10, 0.30), \quad a = 1.4, \quad b = 0.3,$$
$$\varepsilon_1 = \varepsilon_2 = 10^{-2}, \quad N_0 = 2, \quad N = 16$$

After discarding N_0 transient iterations, the Hénon Brownian system produces the following x-sequence:

$$H = [\, 0.72, -0.34, 0.11, 0.93, -0.15, 0.58, 0.46, -0.09,$$
$$0.67, -0.44, 0.25, 0.81, 0.39, 0.12, 0.56, 0.05\,].$$

Applying rank-order mapping, we obtain the permutation index array:

$$\mathsf{idx} = [9, 1, 4, 7, 15, 2, 13, 10, 12, 6, 14, 5, 8, 0, 11, 3].$$

Finally, the resulting 4 × 4 S-box is:

$$S = [13, 1, 5, 15, 2, 11, 9, 3, 12, 0, 7, 14, 8, 6, 10, 4].$$

This example demonstrates the same procedure as Algorithm 1, but on a smaller scale for clarity. The full 8 × 8 S-box is obtained by following identical steps with $N = 256$.

4.7 Discussion on Proposed Method

We now discuss how parameters are chosen in practice and why these choices contribute to both functionality and security of our Proposed method.

4.7.1 Parameter Selection

Each stage of the construction is governed by parameters that balance chaotic richness with numerical stability:

1. **Hénon map parameters (a, b):** The canonical values $a = 1.4$ and $b = 0.3$ keep the map within a strongly chaotic regime. Minor variations may be derived from the secret key, provided the system remains chaotic.
2. **Perturbation scales $(\varepsilon_1, \varepsilon_2)$:** Small perturbations (10^{-3}–10^{-2}) preserve the geometry of the Hénon attractor while introducing stochastic "zigzag" deviations, thereby reducing the risk of short cycles in finite-precision computations.
3. **Transient length N_0:** Discarding the first $N_0 = 50{,}000$ iterations (for an 8 × 8 S-box) eliminates bias from initial conditions and ensures that the system samples the attractor's invariant distribution.

4. **Sequence length *N*:** For an n-bit S-box, $N = 2^n$ outputs are drawn from the perturbed trajectory. Applying rank-order mapping to this sequence yields a bijective permutation of integers.
5. **PRNG seeding:** The Gaussian increments used in perturbation are generated from a pseudo random number generator seeded with the secret key, ensuring both reproducibility and key dependence.

4.7.2 Remarks and Implementation Guideline

The proposed framework admits several natural extensions and practical considerations. Larger S-boxes can be generated by increasing the sequence length N, while multiple S-boxes may be obtained by exploiting different chaotic coordinates. Furthermore, the perturbation principle is not restricted to two dimensions; its extension into three dimensions enables stronger shuffling mechanisms in multimedia and image encryption applications. In all such cases, parameter values must be tuned to preserve both chaotic behavior and the small perturbation scales that underpin security.

From an implementation perspective, double-precision floating point arithmetic is recommended in order to maximize the effective state space and reduce numerical artifacts arising from finite precision. When applying rank-order mapping, a stable sorting procedure should be used to ensure consistency in the presence of potential ties. Finally, if the S-box is intended for high-assurance scenarios where secrecy is critical, the Gaussian increments driving perturbations should be generated by a cryptographically secure PRNG, ensuring resistance against adversarial reconstruction attempts.

4.7.3 S-Boxes Generated Using Proposed Scheme

In the proposed scheme, we present generated S-boxes. These S-Boxes provide better resistance against cryptanalytic attacks. The constructed S-Boxes are presented in Tables 1 and 2.

Table 1: α S-Box generated using the proposed method.

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

Table 2: β S-Box generated using the proposed method.

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

5 Results and Comparisons

We generated a number of 8×8 S-boxes using the proposed HénonBrownian methodology with different random keys and computed their cryptographic properties. In this section, we present the results for one representative S-box instance generated by a particular key. Furthermore, we compare these metrics with those of well-known existing S-boxes to highlight the effectiveness of the proposed construction.

5.1 S-Box Generation Time Analysis

The computational efficiency of our proposed Hénon Brownian S-box generation method was evaluated by measuring the time taken to generate each S-box for a set of different keys. Fig. 4 shows the generation times for 20 representative keys. The Fig. 4 indicates that the time remains fairly consistent across different keys, with minor variations due to the random initialization in the Hénon Brownian process. The average generation time per S-box is approximately 0.01 s, demonstrating that our method is computationally efficient and suitable for practical cryptographic applications.

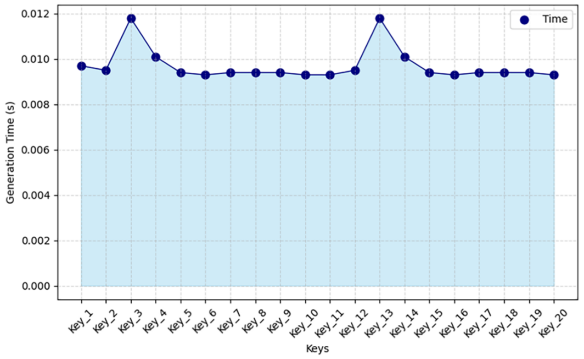


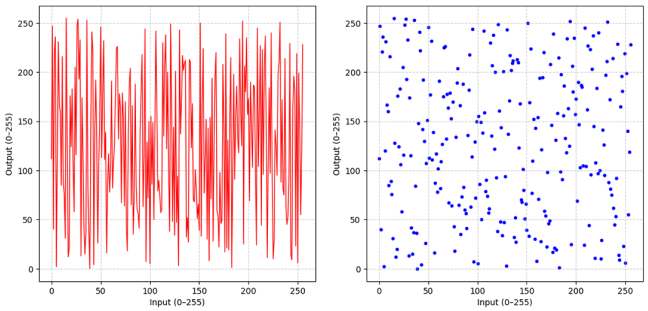
Figure 4: Generation time for Hénon Brownian S-boxes across 20 different keys.

5.2 Cryptographic Properties of the Proposed S-Box

The strength of any S-box is determined by its ability to withstand cryptanalytic attacks. To this end, the proposed S-box has been evaluated against the standard set of cryptographic properties that ensure confusion, diffusion, and resistance to both linear and differential attacks.

Bijectivity:

By construction, the S-box is a permutation of 0–255, hence bijective (one-to-one and onto). It can be seen in Fig. 5 that all 256 output values are unique and every input maps to a unique output. There were no fixed points in our S-box (i.e., no input x such that $S(x) = x$) and no opposite fixed points ($S(x) = \bar{x}$) either, which eliminates certain weak linear structures.



(a) Input vs. output mapping **(b)** Bijectivity visualization

Figure 5: Bijectivity analysis of the proposed S-box.

Nonlinearity:

The nonlinearity of an S-box is measured as the minimum Hamming distance of its output Boolean functions from all affine functions [9]. For an 8 × 8 S-box, there are 8 Boolean output functions. We computed the Walsh–Hadamard spectrum of each output bit to find its nonlinearity. Our S-box's minimum nonlinearity among the 8 bits is 106, and the average nonlinearity is 110.5. This is good enough, the theoretical maximum for 8-bit S-boxes is 112, achieved by AES. Achieving 106 means the S-box's outputs are highly nonlinear and well balanced. This strong NL directly indicates resistance to linear cryptanalysis, since any linear approximation holds only slightly better than random guessing. The Walsh–Hadamard spectrum of an output bit is illustrated in Fig. 6.

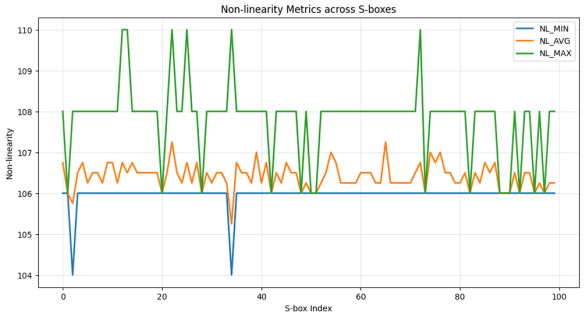


Figure 6: Walsh–Hadamard spectrum of an output bit.

Strict Avalanche Criterion (SAC):

We tested SAC by flipping each input bit and observing the change in output. The average number of output bits that change was 3.994 out of 8 (49.925 percent), which is essentially the ideal 50 percent [45]. Each of the 8 input bits individually showed close to 50 percent avalanche effect, with no weak input bit. Satisfying SAC means a one-bit difference in input leads to a completely different output, ensuring strong diffusion as shown in Fig. 7.

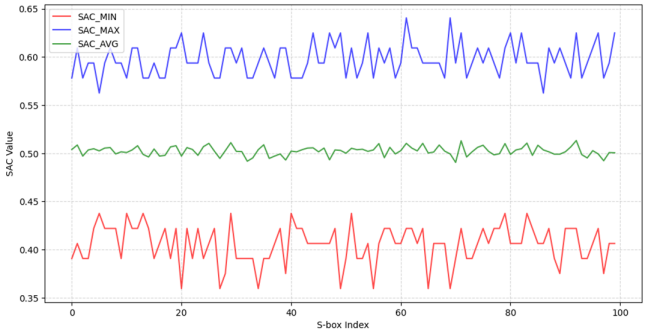


Figure 7: Strict Avalanche Criterion (SAC) results of the proposed S-box.

Bit Independence Criterion (BIC):

BIC refines the SAC by additionally testing whether output bits change independently when a single input bit is flipped [46]. We evaluated the BIC–SAC values by computing correlations between the avalanche patterns of different output bits. All correlation values were found to be very close to zero ($|\rho| < 0.05$), which indicates excellent statistical independence among output bits. This ensures that no exploitable linear or multi-bit dependencies exist, thereby strengthening resistance against advanced differential and linear cryptanalysis techniques as shown in (Fig. 8).

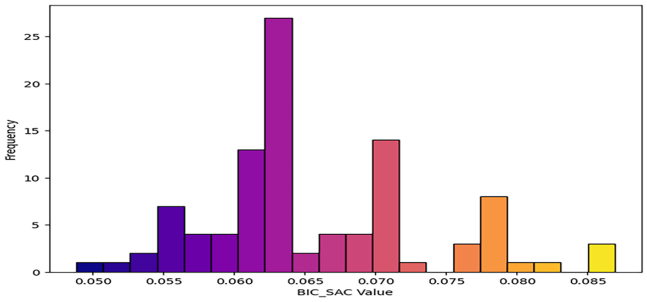


Figure 8: BIC–SAC analysis of the proposed S-box.

Comparison

To validate the effectiveness of the proposed S-boxes, we compared their cryptographic performance with several state-of-the-art S-boxes reported in recent literature. Table 3 presents a comprehensive comparison in terms of NL, SAC, BIC, and DU. The proposed S-boxes achieve high average nonlinearity (around 106–106.5) and well-balanced SAC values close to the ideal 0.5, while maintaining a low maximum differential probability of 0.0469. These results demonstrate that our S-boxes not only provide strong confusion and diffusion properties but also surpass many existing constructions, highlighting their robustness against classical cryptanalytic attacks.

Table 3: Comparison of the proposed S-boxes with existing works.

S-box	Year	NL Min	NL Max	NL Avg.	SAC Min	SAC Max	SAC Avg.	DP Max
α (Proposed)	2025	106	106	106	0.4063	0.6094	0.5085	0.0469
β (Proposed)	2025	106	108	106.5	0.3906	0.5938	0.5034	0.0469
Garipcan et al. (2025b) [47]	2025	106	110	108.5	0.4063	0.6094	0.5125	0.148
Garipcan et al. (2025a) [48]	2025	106	110	107.25	0.3750	0.5938	0.4961	0.125
Aydin et al. [49]	2024	104	110	106.75	0.4063	0.5781	0.4995	0.125
Wu & Kong [50]	2024	106	108	107.25	0.3906	0.6250	0.5006	0.117
Savadkouhi & Tootkaboni [51]	2024	104	108	105.75	0.4063	0.5938	0.4939	0.117
Haider et al. [52]	2024	106	108	107.0	0.4219	0.5938	0.4995	0.102
Corona-Bermúdez et al. [53]	2023	98	106	104.25	0.3750	0.6094	0.5029	0.125
Khan et al. [54]	2023	106	106	106	0.3906	0.6094	0.474	–
Hayat et al. [55]	2022	106	106	106	0.4063	0.5938	0.468	–
Murtaza and Azam [56]	2021	106	106	106	0.4219	0.5938	0.471	–
Farah et al. [57]	2020	104	108	106.25	0.3594	0.6094	0.5003	0.133

6 Application in Image Encryption

To demonstrate the practical utility of the proposed S-box, we apply it to image encryption. Digital images contain a high degree of correlation among adjacent pixels, which makes them vulnerable to statistical attacks if not sufficiently diffused and confused. The nonlinearity and key-dependence of our S-box design provide an effective mechanism for breaking this correlation and achieving secure encryption.

Let $D = [d_{ij}]$ represent a grayscale image with a rows and b columns, where each pixel d_{ij} is represented over the symbol set $\{0, 1, \ldots, 2^m - 1\}$. The encryption procedure using the proposed S-box generator is as follows:

1. **S-box generation:** Generate a collection S of $m \times m$ S-boxes using the proposed Hénon Brownian method. Let ρ_k denote the k-th S-box in the set S.
2. **Selection matrix:** Construct an $(a \times b)$ matrix $R = [r_{ij}]$ such that each r_{ij} is an integer in the range $[1, |S|]$, chosen via a key-dependent pseudo-random generator.
3. **Pixel substitution:** For each pixel d_{ij} in the plain image, compute the corresponding encrypted pixel:

$$e_{ij} = \rho_{r_{ij}}(d_{ij}),$$

thereby obtaining the ciphertext image $E = [e_{ij}]$.

The decryption process follows the same procedure in reverse using the identical secret key. Since each S-box in the set S is bijective, its inverse ρ_k^{-1} exists and can be efficiently computed. For each encrypted pixel e_{ij}, the original pixel is recovered as

$$d_{ij} = \rho_{r_{ij}}^{-1}(e_{ij}),$$

Fig. 9 illustrates the plain, encrypted, and decrypted images, demonstrating that the proposed scheme produces noise-like ciphertext while allowing exact recovery of the original image without any loss of visual information.

Figure 9: Visual comparison of plain, encrypted and decrypted images using the proposed S-box.

In addition to visual inspection, a quantitative analysis was carried out to evaluate the correlation and entropy of the encrypted images. Table 4 reports the correlation coefficients of adjacent pixels in horizontal, vertical, and diagonal directions, along with entropy values, for both plain and encrypted images. The plain images exhibit high pixel correlation, which is expected due to the natural redundancy in images. However, after encryption, the correlation drops close to zero in all directions, indicating effective removal of statistical dependencies. Furthermore, the entropy values of the encrypted images approach the ideal value of 8, confirming that the proposed scheme produces cipher texts with high randomness and resistance against statistical attacks.

Table 4: Correlation and entropy analysis of plain and encrypted images using the proposed S-box. where H-Corr, D-Corr, and V-Corr denote horizontal, diagonal, and vertical correlation coefficients, respectively, and (P/C) represents plain image/cipher image values.

Image #	Dimension	H-Corr (P/C)	D-Corr (P/C)	V-Corr (P/C)	Entropy (P/C)
1	(256, 256)	0.8985/0.0062	0.8302/0.0079	0.8899/0.0001	6.5915/6.5915
2	(256, 256)	0.8425/0.0183	0.7122/−0.0018	0.7978/0.0083	7.3338/7.3338
3	(256, 256)	0.9736/0.0028	0.9494/0.0000	0.9721/0.0028	7.3841/7.3841
4	(256, 256)	0.8960/0.0160	0.7905/−0.0016	0.8724/−0.0031	7.4175/7.4175
5	(256, 256)	0.9248/0.0016	0.8500/−0.0045	0.9182/0.0024	7.5560/7.5560

7 Conclusion and Future Work

In this work, we presented a novel methodology for constructing S-boxes with strong cryptographic properties. The proposed S-boxes were thoroughly evaluated using well established criteria such as Bijectivity, NL, SAC and BIC. In addition, their practical effectiveness was demonstrated through image encryption experiments. The visual inspection of encrypted images, together with correlation and entropy analysis, confirmed that the proposed scheme achieves high confusion and diffusion, produces cipher texts with noise like statistical distributions, and effectively removes redundancy from plain images. These results highlight the robustness of the proposed design against classical cryptanalytic and statistical attacks. Additionally, the high key sensitivity ensures that minimal variations in the secret key yield completely different S-boxes and encrypted outputs, further strengthening resilience against key related attacks.

Although the proposed approach shows promising results, there remain several interesting directions for future research. One avenue is to investigate adaptive or key-dependent S-box generation mechanisms, which can dynamically modify substitution layers to resist structural attacks more effectively. Another direction is to explore the integration of the proposed S-boxes into full fledged block and stream cipher architectures, evaluating performance metrics such as throughput, latency, and energy consumption in practical implementations. Moreover, a systematic study on the robustness of the proposed S-boxes against emerging attack paradigms, including algebraic attacks, and machine learning assisted cryptanalysis, can provide additional confidence in their security. Finally, extending the methodology to lightweight and resource constrained environments can ensure that strong cryptographic properties are achieved without compromising efficiency.

Acknowledgement: The authors gratefully acknowledge the support provided by Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding Statement: This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project Number PNURSP2026R500, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Author Contributions: Walaa Alayed: conceptualization, validation, writing—review and editing, funding acquisition. Asad Ur Rehman: methodology, formal analysis. M. Awais Ehsan: methodology, software, investigation, writing—original draft preparation. Waqar Ul Hassan: validation, visualization, writing. Ahmed Zeeshan: conceptualization, formal analysis, supervision, writing—review and editing. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Data will be available on request. Ahmed Zeeshan (ahmad.zeeshan@iiu.edu.pk). Datasets used are publicly available.

Ethics Approval: This study does not involve human participants, animals, or any clinical trials. All image data used in the experiments are publicly available benchmark images; therefore, ethical approval was not required.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Paar C, Pelzl J. Understanding cryptography. Vol. 1. Cham, Switzerland: Springer; 2010.
2. Bellare M, Desai A, Jokipii E, Rogaway P. A concrete security treatment of symmetric encryption. In: Proceedings 38th Annual Symposium on Foundations of Computer Science. Piscataway, NJ, USA: IEEE; 1997. p. 394–403.
3. Davies D. A brief history of cryptography. Inf Secur Tech Report. 1997;2(2):14–7.
4. Stallings W. Network and internetwork security: principles and practice. Saddle River, NJ, USA: Prentice-Hall, Inc.; 1995 [cited 2026 Feb 2]. Available from: https://dl.acm.org/doi/abs/10.5555/193189.

5. Shannon CE, Weaver W. The mathematical theory of communication. Champsaign, IL, USA: University of Illinois Press; 1998.
6. Farah S, Javed Y, Shamim A, Nawaz T. An experimental study on performance evaluation of asymmetric encryption algorithms. In: Recent Advances in Information Science, Proceeding of the 3rd European Conference of Computer Science,(EECS-12). Athens, Greece: WSEAS; 2012. p. 121–4.
7. Buchmann J, Buchamann J. Introduction to cryptography. Vol. 335. Cham, Switzerland: Springer; 2004.
8. Mohamed K, Pauzi MNM, Ali FHHM, Ariffin S, Zulkipli NHN. Study of s-box properties in block cipher. In: 2014 International Conference on Computer, Communications, and Control Technology (I4CT). Piscataway, NJ, USA: IEEE; 2014. p. 362–6.
9. Nyberg K. Perfect nonlinear s-boxes. In: Workshop on the Theory and Application of of Cryptographic Techniques. Cham, Switzerland: Springer; 1991. p. 378–86. doi: 10.1007/3-540-46416-6_32.
10. VERGİLİ I, Yücel MD. Avalanche and bit independence properties for the ensembles of randomly chosen n\times n s-boxes. Turkish J Electr Eng Comput Sci. 2001;9(2):137–46.
11. Blondeau C, Canteaut A, Charpin P. Differential properties of $x \mapsto x^{2^t-1}$. IEEE Trans Inf Theory. 2011;57(12):8127–37. doi:10.1109/tit.2011.2169129.
12. Courtois NT, Meier W. Algebraic attacks on stream ciphers with linear feedback. In: International Conference on the Theory and Applications of Cryptographic Techniques. Cham, Switzerland: Springer; 2003. p. 345–59.
13. Sankpal PR, Vijaya P. Image encryption using chaotic maps: a survey. In: 2014 Fifth International Conference on Signal and Image Processing. Piscataway, NJ, USA: IEEE; 2014. p. 102–7.
14. De Micco L, Antonelli M, Rosso OA. From continuous-time chaotic systems to pseudo random number generators: analysis and generalized methodology. Entropy. 2021;23(6):2021–671. doi:10.3390/e23060671.
15. Beirami A, Nejati H, Callegari S. Fundamental performance limits of chaotic-map random number generators. In: 2014 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton). Piscataway, NJ, USA: IEEE; 2014. p. 1126–31.
16. Klöwer M, Coveney PV, Paxton EA, Palmer TN. Periodic orbits in chaotic systems simulated at low precision. Sci Rep. 2022;13(1):2023–11410. doi:10.21203/rs.3.rs-2223046/v1.
17. Li S, Chen G, Mou X. On the dynamical degradation of digital piecewise linear chaotic maps. Int J Bifurcat Chaos. 2005;15(10):3119–51. doi:10.1142/s0218127405014052.
18. Ahmad M, Alkanhel RI, Soliman NF, Algarni AD, El-Samie FEA, El-Shafai W. Securing healthcare data in iomt network using enhanced chaos based substitution and diffusion. Comput Syst Sci Eng. 2023;47(2):2361–80. doi:10.32604/csse.2023.038439.
19. Deng Q, Wang C, Sun Y, Yang G. Discrete memristive conservative chaotic map: dynamics, hardware implementation, and application in secure communication. IEEE Trans Cybern. 2025;55(8):3926–34. doi:10.1109/tcyb.2025.3565333.
20. Abba A, Teh JS, Alawida M. Towards accurate keyspace analysis of chaos-based image ciphers. Multimed Tools Appl. 2024;83(33):79047–66. doi:10.1007/s11042-024-18628-8.
21. Zhang B, Liu L. Chaos-based image encryption: review, application, and challenges. Mathematics. 2023;11(11):2585.
22. Gao J, Shen Y, Li S, Zhang J. An enhanced hybrid chaotic system and its application in image encryption. J King Saud Univ Comput Inf Sci. 2025;37(9):295. doi:10.1007/s44443-025-00320-y.
23. Andreatos AS, Leros AP. Secure chaotic cryptosystem for 3D medical images. Mathematics. 2025;13(20):3310. doi:10.3390/math13203310.
24. Song K, Imran N, Chen JY, Dobbins AC. A hybrid chaos-based cryptographic framework for post-quantum secure communications. arXiv:2504.08618. 2025. doi:10.48084/etasr.12471.
25. Daemen J, Rijmen V. AES proposal: Rijndael, Tech. rep., NIST AES candidate submission, version 2. 1999 [cited 2026 Feb 2]. Available from: https://www.cs.miami.edu/home/burt/learning/Csc688.012/rijndael/rijndael_doc_V2.pdf.
26. Parikh C, Patel P. Performance evaluation of AES algorithm on various development platforms. In: 2007 IEEE International Symposium on Consumer Electronics. Piscataway, NJ, USA: IEEE; 2007. p. 1–6.

27. IBM. Data encryption standard. Federal Information Processing Standards Publication. 1999 [cited 2026 Feb 2]. Available from: https://academickids.com/encyclopedia/index.php/Data_Encryption_Standard.
28. Sakallı MT, Aslan B, Buluş E, Mesut AŞ, Büyüksaraçoğlu F, Karaahmetoğlu O. On the algebraic expression of the AES s-box like s-boxes. In: International Conference on Networked Digital Technologies. Cham, Switzerland: Springer; 2010. p. 213–27.
29. Gaabouri IEl, Senhadji M, Belkasmi M, Bhiri BEl. A new s-box pattern generation based on chaotic enhanced logistic map: case of 5-bit s-box. Cybersecurity. 2024;7(1):2024–59. doi:10.1186/s42400-024-00254-4.
30. James D, Priya TL. An innovative approach for dynamic key dependent s-box to enhance security of IoT systems. Measurement: Sensors. 2023;30:100923. doi:10.1016/j.measen.2023.100923.
31. Nagaraj N, Shastry MC, Vaidya PG. Increasing average period lengths by switching of robust chaos maps in finite precision. Eur Phys J Spec Top. 2008;165(1):73–83. doi:10.1140/epjst/e2008-00850-4.
32. Nazish M, Javid M, Banday MT. Enhanced logistic map with infinite chaos and its applicability in lightweight and high-speed pseudo-random bit generation. Cybersecurity. 2025;8(1):24. doi:10.1186/s42400-024-00319-4.
33. Namuq J. S-box design utilizing 3D chaotic maps for cryptographic application. Magalla Al-Basra Al-Ulūm Al-Handasiyya. 2024;24(2):68–73.
34. Zhang R, Shu R, Wei Y, Zhang H, Wu X. A novel s-box generation methodology based on the optimized gan model. Comput Mater Contin. 2023;76(2):1911–27. doi:10.32604/cmc.2023.041187.
35. Wang S, He J. Design of chaotic systems with multiple scrolls via anti-control method and its encryption application. IAENG Intl J Appl Math. 2024;54(12):2636–44.
36. Liu T, Wan X-J, Zhou Z. Novel two-stage uncertainty optimization design of a compliant finger based on stochastic perturbation approach. Appl Math Model. 2025;142(11):115952. doi:10.1016/j.apm.2025.115952.
37. Xiang H, Liu L. A new perturbation-feedback hybrid control method for reducing the dynamic degradation of digital chaotic systems and its application in image encryption. Multimed Tools Appl. 2021;80(13):19237–61. doi:10.1007/s11042-021-10680-y.
38. Premkumar R, Mahdal M, Elangovan M. An efficient chaos-based image encryption technique using bitplane decay and genetic operators. Sensors. 2022;22(20):8044. doi:10.3390/s22208044.
39. Harmouch Y, Kouch REl. Brownian techniques for constructing high-strong cryptographic s-boxes. In: Proceedings of the 2nd International Conference on Smart Digital Environment; 2018 Oct 18–20; Rabat, Morocco. p. 19–26.
40. Nazish M, Bandy MT. e-cm: a novel approach to advancing chaotic dynamics in discrete one-dimensional maps for secure IoT applications. Cybersecurity. 2025;8(1):71.
41. Hénon M. A two-dimensional mapping with a strange attractor. Commun Math Phys. 1976;50(1):69–77. doi:10.1007/bf01608556.
42. Zainalabideen A, Suwais K, El-Bakry H, Abdelmaksoud I. Brownian motion models: cryptographic applications, capabilities, and limitations. Frontiers Comput Sci. 2025;7:1649256. doi:10.3389/fcomp.2025.1649256.
43. Coeurjolly J-F. Estimating the parameters of a fractional brownian motion by discrete variations of its sample paths. Stat Inference Stoch Process. 2001;4(2):199–227. doi:10.1023/a:1017507306245.
44. Gnedin A. Coherent random permutations with record statistics. In: 2007 Conference on Analysis of Algorithms, AofA 07. Nancy, France: Discrete Mathematics & Theoretical Computer Science; 2007. p. 157–70.
45. Kim K, Matsumoto T, Imai H. A recursive construction method of s-boxes satisfying strict avalanche criterion. In: Conference on the Theory and Application of Cryptography. Cham, Switzerland: Springer; 1990. p. 565–74.
46. Levinskas M, Mihalkovich A. Avalanche effect and bit independence criterion of perfectly secure shannon cipher based on matrix power. Math Models Eng. 2021;7(3):50–3.
47. Garipcan AM, Aydin Y, Özkaynak F. An efficient 2D hyper chaos and DNA encoding-based S-box generation method using chaotic evolutionary improvement algorithm for nonlinearity. Chaos Soliton Fract. 2025;191(9):115952. doi:10.1016/j.chaos.2024.115952.
48. Garipcan AM, Aydın Y, Özkaynak F. A novel S-box generation method based on metastable inducing over FPGA for block ciphers. Knowl Based Syst. 2025;310:112968.

49. Aydin Y, Garipcan AM, Özkaynak F. A novel secure S-box design methodology based on FPGA and SHA-256 hash algorithm for block cipher algorithms. Arab J Sci Eng. 2025;50(2):1247–60. doi:10.1007/s13369-024-09251-8.
50. Wu W, Kong L. Image encryption algorithm based on a new 2D polynomial chaotic map and dynamic S-box. Signal Image Video Processing. 2024;18(4):3213–28. doi:10.1007/s11760-023-02984-3.
51. Savadkouhi MB, Tootkaboni MA. S-boxes design based on the Lu-Chen system and their application in image encryption. Soft Comput. 2024;28(20):12119–40. doi:10.1007/s00500-024-09912-8.
52. Haider T, Azam NA, Hayat U. A novel image encryption scheme based on ABC algorithm and elliptic curves. Arab J Sci Eng. 2023;48(8):9827–47. doi:10.1007/s13369-022-07383-3.
53. Corona-Bermúdez E, Chimal-Eguía JC, Corona-Bermúdez U, Rivero-Ángeles ME. Chaos meets cryptography: developing an S-box design with the Rössler attractor. Mathematics. 2023;11(22):4575.
54. Khan H, Hazzazi MM, Jamal SS, Hussain I, Khan M. New color image encryption technique based on three-dimensional logistic map and grey wolf optimization based generated substitution boxes. Multimed Tools Appl. 2023;82(5):6943–64.
55. Hayat U, Ullah I, Murtaza G, Azam NA, Bustamante MD. Enumerating discrete resonant rossby/drift wave triads and their application in information security. Mathematics. 2022;10(23):4395. doi:10.3390/math10234395.
56. Murtaza G, Azam NA, Hayat U. Designing an efficient and highly dynamic substitution-box generator for block ciphers based on finite elliptic curves. Secur Commun Netw. 2021;2021:3367521. doi:10.1155/2021/3367521.
57. Farah MB, Farah A, Farah T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dyn. 2020;99(4):3041–64. doi:10.1007/s11071-019-05413-8.