Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 15** : 1–57.
ISSN-0037-8712
doi:10.5269/bspm.81483

A Security-Centric Analysis of Construction Paradigms, Cryptographic Metrics, and Practical Vulnerabilities for Chaos-Based S-Box Design and Image Encryption

Saba Fatima, Abid Mahboob, Ali Raza

ABSTRACT: Chaos-based techniques have gained significant attention in symmetric cryptography, particularly for the construction of substitution boxes (S-boxes) and their application in image encryption systems. The inherent properties of chaotic systems, sensitivity to initial conditions, ergodicity, and pseudo-randomness, offer intuitive mechanisms for generating nonlinear and key-dependent substitution layers. However, many existing studies emphasize statistical performance indicators while overlooking rigorous cryptographic validation under established attack models. This review presents a systematic and critical survey of chaos-driven S-box generation and chaos-assisted image encryption architectures. We introduce a detailed taxonomy of construction methods, encompassing direct chaotic sequence mapping, algebraic–chaotic hybrid designs, dynamic and plaintext-dependent S-boxes, metaheuristic optimization-based approaches, and emerging machine learning–assisted techniques. The cryptographic strength of these methods is evaluated using standard metrics, including nonlinearity, differential uniformity, strict avalanche and bit independence criteria, algebraic degree, and resistance to linear and differential cryptanalysis. In addition, we examine the role of chaotic S-boxes within permutation–diffusion image encryption frameworks, lightweight real-time systems, and hybrid chaos–DNA schemes, emphasizing their practical deployment challenges and vulnerability patterns. The review highlights limitations related to finite-precision implementations, weak key generation, and the lack of standardized benchmarking. Finally, we propose a unified evaluation protocol and outline future research directions aimed at developing provably secure, efficient, and reproducible chaos-based cryptographic components for secure image communication.

Keywords: Chaos-driven S-box construction, cryptographic evaluation metrics, differential uniformity, bit independence criterion, permutation–diffusion architectures, finite-precision security, dynamic substitution layers, secure image transmission.

Contents

2020 *Mathematics Subject Classification:* 11T71, 14G50, 94A60.
Submitted January 22, 2026. Published April 30, 2026.

Typeset by $\mathcal{B}^{S}\mathcal{P}_{\mathcal{M}}$ style.
© Soc. Paran. de Mat.

1. Introduction

1.1. Background and Motivation

Symmetric cryptography forms the backbone of secure data exchange in modern digital systems due to its efficiency, simplicity, and applicability to high-throughput environments such as multimedia and image transmission. At the heart of many high-security symmetric schemes lies the substitution box (S-box), a nonlinear component designed to obscure the relationship between the plaintext, ciphertext, and secret key. The foundational purpose of an S-box is to introduce *confusion* as articulated by Shannon,

thereby strengthening resistance against linear and differential cryptanalysis by maximizing nonlinearity and minimizing predictable structure [12,14]. In block ciphers such as the Advanced Encryption Standard (AES), carefully crafted S-boxes contribute significantly to overall robustness, making them indispensable in symmetric cipher design [13].

Simultaneously, the rapid proliferation of digital imagery across communication networks has elevated the importance of specialized image encryption techniques that not only preserve confidentiality but also meet performance and structural requirements specific to image data. Traditional symmetric algorithms such as AES and DES were primarily conceived for general bit streams and are not always optimally suited to image encryption without adaptation. This has motivated researchers toward alternative paradigms that handle the intrinsic high redundancy, pixel correlation, and large data volumes characteristic of images [15].

One notable paradigm is chaos-based image encryption, which leverages the inherent properties of chaotic systems, particularly extreme sensitivity to initial conditions, ergodicity, and pseudo-random behavior, to generate confusion and diffusion mechanisms tailored to image data. Chaotic maps such as the logistic, Henon, and Lorenz systems have been widely employed to drive pixel permutation, key generation, and substitution processes embedded within encryption schemes [16,17]. These chaotic constructs produce sequences resembling randomness while being deterministic, a feature highly appealing for algorithm designers seeking to balance unpredictability with reproducibility.

The integration of chaos with cryptographic primitives has been particularly pronounced in the design of dynamic and key-dependent S-boxes. Recent research has proposed advanced S-box generation techniques driven by chaotic maps and hybrid schemes that improve cryptographic strength and adaptivity [18,19]. Additionally, hybrid frameworks combining chaos theory with classical cryptographic structures such as AES and enhanced block ciphers have demonstrated improved resistance to statistical and differential attacks in image encryption contexts [20,21]. These innovations demonstrate the rich interplay between chaos theory and symmetric cryptography in addressing contemporary challenges in secure image transmission.

Despite the conceptual appeal and prolific publication of chaos-based encryption methods, there remains an ongoing debate regarding their actual cryptographic strength and suitability for rigorous security applications. While chaotic systems provide desirable pseudo-random attributes, their cryptographic foundations often lack formal justification against established attack vectors. For example, many chaos-driven schemes focus on statistical properties such as entropy and pixel correlation without comprehensive evaluation under real cryptanalytic models, leading to potential overestimation of security [152]. Moreover, finite precision effects in digital implementations can undermine theoretical unpredictability guaranteed by chaotic dynamics, raising concerns about practical security robustness in real-world scenarios.

These observations underscore the need for a critical, security-centric review of chaos-based S-box designs and image encryption frameworks, not merely cataloging techniques but evaluating their true cryptographic merits and limitations. It is within this context that the current review is motivated: to systematically assess the state of the art in chaotic S-box construction, examine their cryptographic properties, and highlight the gap between conceptual promise and practical security assurances. This emphasis on measured security analysis, rather than descriptive classification alone, aims to provide researchers with a clearer understanding of what chaos contributes to cryptography and where caution is warranted.

1.2. Limitations of Existing Reviews

While numerous surveys have been published on chaos-based image encryption and S-box design, most existing reviews remain predominantly descriptive, providing broad overviews of architectures and chaotic maps without deep engagement in cryptographic security evaluation. For instance, several recent overviews characterize image encryption through chaos theory by summarizing chaotic maps such as logistic, Henon, and Lorenz systems and outlining their use in scrambling pixels and key generation [148], but do not adequately address whether these chaos-derived constructions withstand rigorous cryptanalysis. Such descriptive treatment risks giving a misleading impression that the mere inclusion of chaos yields strong security, when in fact the cryptographic validity of many proposals is still unproven.

One pervasive limitation of existing reviews is their overemphasis on descriptive classification of techniques, often cataloguing encryption schemes and chaotic maps, without critical insight into their relative strengths or practical security implications. For example, surveys typically list chaos-based image encryption algorithms across spatial and transform domains [22] or outline feature-based chaotic approaches to image encryption [148], yet they seldom articulate how these schemes perform under real attack models or whether the reported statistical properties translate to genuine security guarantees. This tendency to prioritize breadth over depth has resulted in a literature that is rich in algorithmic variants but poor in interpretive evaluation, making it difficult for readers to discern which methods are genuinely secure and which merely appear robust under superficial testing.

Moreover, a lack of rigorous cryptanalysis discussion is apparent in many reviews and original reports alike. Standard surveys often rely heavily on statistical metrics such as entropy, correlation coefficients, and histogram uniformity as indicators of encryption quality. While these metrics are useful for initial assessment, their applicability to cryptographic security is limited; statistical tests cannot substitute for analytical resistance against classical attacks like differential, linear, or chosen-plaintext attacks. Indeed, recent cryptanalysis studies have shown that certain chaos-based schemes previously regarded as secure can be vulnerable under chosen-plaintext attack models [153,149]. In this context, reviews that aggregate chaos-based schemes without integrating cryptanalytic insights risk reinforcing the misconception that passing a battery of statistical tests implies resistance to sophisticated attacks.

Another critical gap in prior reviews is the absence of standardized benchmarks and evaluation frameworks. Many chaos-based encryption studies and surveys describe performance metrics in isolation, with inconsistent experimental setups, datasets, and evaluation criteria. This fragmentation not only hinders fair comparison across schemes but also masks underlying weaknesses; for example, some encryption algorithms with apparently high entropy or low pixel correlation can still be vulnerable to differential cryptanalysis when subjected to appropriate attack models [149]. Without a systematic benchmarking framework that includes both statistical and structural security metrics, it is difficult to determine whether improvements claimed in one study truly outperform alternatives or merely reflect inconsistent testing conditions.

Taken together, these limitations underscore the need for a more critical, security-centric review that goes beyond cataloguing chaos-based methods to rigorously evaluate their cryptographic strength, highlight methodological shortcomings in existing literature, and propose unified standards for assessment. The present review aims to fill this gap by emphasizing not only the variety of chaos-based S-box and image encryption techniques but also their relative security under established cryptanalytic models and standardized metrics.

1.3. Scope and Focus of This Review

This review is deliberately scoped and targeted: rather than attempting an exhaustive cataloguing of every chaos-inspired proposal, we focus on the intersection where *chaotic dynamics* meet *cryptographic substitution* and where that intersection is applied to *image encryption*. The choice of this focus is motivated by three observations evident in the recent literature. First, chaotic systems are frequently used as a source of pseudo-randomness and sensitivity to drive S-box construction and substitution layers, but the cryptographic properties of the resulting S-boxes are unevenly analyzed [37]. Second, many image encryption proposals embed chaos-driven substitution (S-boxes or substitution-like operations) as a central mechanism for confusion, and these designs form a recognisable class with shared structural choices and recurring weaknesses [38]. Third, there is a pressing need to move evaluation from informal statistical testing to security-centric analysis that uses established cryptanalytic models and standardized benchmarks [23]. These three points determine what we include, what we emphasise, and what we intentionally leave out.

Chaos-based S-Boxes. We survey methods that explicitly use chaotic maps or chaotic iterations to produce substitution boxes (S-boxes) or S-box–like nonlinear components. This includes, but is not limited to, designs that: (i) map chaotic sequences to S-box entries by ranking or quantization; (ii) hybridize chaos with algebraic constructions over $\mathbb{F}_{2^n}$; and (iii) produce dynamic or key-dependent S-boxes whose entries change with secret parameters [24]. The literature on such constructions has grown rapidly and now includes both low-dimensional map approaches and higher-dimensional or perturbed chaotic systems

intended to address predictability and finite-precision collapse [25]. We treat these approaches comparatively, emphasizing how the generation method affects classical S-box metrics and implementation pitfalls.

Image encryption schemes using chaotic substitution. Within the image-encryption literature we restrict attention to architectures where substitution driven by chaos, either via explicit S-boxes or substitution-like operations, is a primary confusion mechanism. This scope captures canonical permutation–diffusion pipelines augmented with chaotic substitution layers, multi-layer chaotic architectures, and recent hybrid constructions that claim improved diffusion and confusion for image data [26,27]. For each family we examine the design rationale, the assumed security benefits of chaos, and the extent to which the substitution element is responsible for the algorithm's claimed strength or, conversely, for its vulnerabilities.

Security-centric evaluation. A central mandate of this review is to privilege *security-centric* evaluation over purely statistical or application-level metrics. Thus we evaluate S-box proposals using standard cryptographic measures and assess image-encryption designs under formal attack models and contemporary cryptanalytic techniques specific to chaotic constructions [28,29]. Prior surveys have often focused on entropy, histogram, NPCR/UACI, and correlation tests as primary evidence of security; we reframe those metrics as useful but insufficient and insist on juxtaposing them with cryptanalytic outcomes reported in the literature [39].

Inclusion and exclusion criteria. To keep the review focused and useful for both practitioners and researchers, we include peer-reviewed chaos-based S-box proposals and image-encryption schemes published in journals or reputable conferences, papers that perform substantive cryptanalysis, and comparative studies that benchmark multiple chaos-based schemes [38]. We exclude one-off toy proposals without reproducible experiments and application-only works that do not reveal the encryption core.

Organization and what to expect next. Following this scope, the review proceeds to introduce the cryptographic fundamentals and chaos preliminaries, categorise chaos-driven S-box construction paradigms, define rigorous evaluation metrics, review image-encryption families that employ chaotic substitution under attack models, and synthesise the results into actionable recommendations and open problems [37].

1.4. Contributions of This Review

This review delivers a targeted, security-focused assessment of chaos-based S-box design and its application to image encryption. While many recent surveys catalog chaotic maps and algorithmic variants, there is a clear demand for a critical synthesis that (i) evaluates substitution components against standard cryptographic metrics and attack models, and (ii) proposes a unified benchmarking perspective for the field. Recent comprehensive surveys and numerous new chaos-based proposals confirm both the popularity of this research direction and the uneven treatment of security analysis in the literature. :contentReference[oaicite:0]index=0

To make the review immediately useful to researchers and practitioners we present the following concrete contributions (bullet-pointed for clarity):

- **A focused taxonomy of chaos-driven S-box constructions.** We categorise S-box generation methods (direct chaotic mapping, algebraic–chaotic hybrids, dynamic/key-dependent generation, optimization- and ML-assisted approaches) and provide precise criteria to place any new design within this taxonomy.
- **A security-first evaluation framework for chaotic S-boxes.** We translate standard cryptographic metrics (nonlinearity, SAC, BIC, differential uniformity, algebraic degree, fixed points) into an assessment checklist specifically tailored to chaos-derived S-boxes, explaining how each metric impacts resistance to linear, differential, and algebraic attacks.
- **Critical assessment of image encryption families that use chaotic substitution.** For representative permutation–diffusion, substitution-augmented, and hybrid image-encryption schemes we (i) identify whether substitution is the dominant confusion mechanism, (ii) evaluate claimed security properties against formal attack models (ciphertext-only, known-plaintext, chosen-plaintext), and (iii) summarise practical weaknesses observed in published cryptanalytic work.

- **Benchmarking recommendations and reproducible evaluation protocol.** We propose a standardized evaluation pipeline (datasets, experimental settings, metrics, and reporting conventions) that combines statistical tests with cryptanalytic validations, intended to reduce inconsistencies and enable fair comparisons across studies.
- **Implementation-focused guidance on finite-precision and deployment pitfalls.** We examine how digital realization (finite-precision arithmetic, quantization, map parameterization) often undermines theoretical chaotic properties, and we give practical guidelines to avoid common implementation mistakes.
- **A comparative table of representative schemes (security vs. performance).** We synthesise the literature into an easy-to-read table that maps design choices (map type, dynamic/static S-box, substitution granularity) to observed security outcomes and computational costs, highlighting trade-offs relevant to IoT and real-time systems.
- **A prioritized research agenda.** We produce an actionable list of open problems and research directions (provable constructions, lightweight secure chaos-based S-boxes, standardized testbeds, post-quantum considerations) to guide future high-impact work.
- **Supplementary resources for reproducibility.** Where available, we link to datasets, code repositories, and reproducible experiments from the literature, and we indicate which published claims were independently validated or refuted.

Collectively, these contributions are designed to move the field from largely descriptive cataloguing toward a more rigorous, reproducible, and security-oriented practice of designing and evaluating chaos-based S-boxes and image-encryption systems. Where appropriate, we support our assessments with examples and citations from recent peer-reviewed studies to demonstrate both the promise and pitfalls of current approaches. :contentReference[oaicite:1]index=1

2. Fundamentals and Preliminaries

2.1. Role of S-Boxes in Modern Cryptography

An S-box (substitution box) is a fundamental building block of many symmetric-key primitives: it implements a nonlinear mapping from m input bits to n output bits and is usually modelled as a *vectorial Boolean function* $F : \mathbb{F}_2^m \to \mathbb{F}_2^n$. In the language of Shannon, S-boxes provide *confusion* by obscuring the relationship between the secret key and the ciphertext; in practice they are often the only source of nonlinearity inside a block cipher and therefore central to resisting linear and differential cryptanalysis. Well-known block ciphers such as DES and AES illustrate this design principle: their S-boxes are carefully constructed (or selected) because the S-box largely determines the primitive's resistance to classical cryptanalytic techniques [30,31].

Confusion and Nonlinearity. From a cryptanalytic perspective, the single most important role of an S-box is to break linear structure. Concretely, if an S-box can be approximated well by affine functions then linear cryptanalysis becomes feasible; if many input differences map to a small set of output differences (low differential uniformity), then differential attacks become effective. Thus, designers evaluate S-boxes using measures that quantify deviation from linear or affine behaviour and sensitivity to input changes. Key metrics include:

- **Nonlinearity (NL).** The minimum Hamming distance of each coordinate function (or the vectorial function seen as a whole) from the set of all affine functions. High nonlinearity reduces the effectiveness of linear approximations and is a direct indicator of resistance to linear cryptanalysis [32].
- **Differential uniformity (DU).** For an S-box F, the differential uniformity is the maximum number of solutions x to $F(x) \oplus F(x \oplus a) = b$ over all nonzero a and all b. Low differential uniformity limits the success probability of differential characteristics [33].

- **Strict Avalanche Criterion (SAC) and Bit Independence Criterion (BIC).** SAC requires that flipping a single input bit changes each output bit with probability about 1/2; BIC strengthens this by asking that output bits change independently [34].
- **Algebraic degree and fixed points.** High algebraic degree increases difficulty for algebraic attacks; absence or scarcity of fixed points reduces trivial shortcut attacks [35].

These metrics are complementary: an S-box with excellent nonlinearity but poor differential uniformity may still be weak, hence designers aim for a balanced trade-off across criteria rather than optimizing a single metric in isolation [36].

Static vs. Dynamic (Key-Dependent) S-Boxes. S-boxes fall broadly into two categories:

Static S-boxes: The S-box is fixed and known a priori (e.g., AES uses a fixed 8×8 S-box). Static S-boxes allow extensive offline analysis: their algebraic and combinatorial properties can be studied in depth, and designers can select constructions that are empirically strong against known attacks. However, a fixed S-box also gives attackers a stable target that can be exploited in long-term cryptanalysis or used to mount precomputation-based attacks [31,36].

Dynamic / Key-dependent S-boxes: The S-box is generated dynamically from the master key, round key, or other secret-dependent values. Dynamic S-boxes aim to increase security by removing a fixed target and forcing attackers to handle a larger space of S-box instances. In practice, however, dynamic S-boxes introduce new challenges: secure generation, preservation of cryptographic metrics, and resistance to weak instances. Recent studies show that many proposed dynamic S-box generators fail to guarantee uniformly strong instances and may introduce implementation weaknesses [37,24].

Practical trade-offs and deployment considerations. Choosing between static and dynamic S-boxes is a design decision with practical consequences:

- **Evaluability:** Fixed S-boxes can be rigorously analysed; key-dependent S-boxes require strong guarantees that the generation procedure almost always produces secure instances.
- **Performance and memory:** Table lookups of fixed S-boxes are efficient; generating dynamic S-boxes may add computational or memory overhead, especially in image encryption systems.
- **Implementation security:** Key-dependent generation may complicate constant-time implementation and side-channel resistance; static S-boxes are easier to harden.
- **Analytical surface:** A static, well-studied S-box reduces the risk of subtle weaknesses; dynamic schemes must ensure they do not produce correlated or weak S-box families.

Connection to image encryption. In image-specific ciphers, S-boxes or S-box-like substitution layers are employed to break pixel-level correlations and provide nonlinear mixing between pixel values and key streams. Because images are large and highly redundant, designers sometimes trade S-box complexity for throughput; however, such trade-offs must not undermine core cryptographic properties. When chaos-based methods are used to generate S-boxes for images, the same criteria apply: chaotic appearance alone does not substitute for formal resistance to cryptanalysis [38,39].

2.2. Overview of Chaotic Systems

Chaotic dynamical systems are attractive to cryptographers because they combine determinism (reproducibility from a secret seed) with complex, pseudo-random behaviour: sensitivity to initial conditions, dense periodic orbits, and topological mixing. These abstract properties map intuitively to cryptographic needs, key sensitivity, large state-space exploration, and apparent randomness, which helps explain the wide use of chaos in image-encryption research [40]. However, the suitability of any particular chaotic system depends heavily on its mathematical properties, parameter ranges, and how it is implemented in finite-precision digital environments. In this section we summarise commonly used chaotic families (one-dimensional maps, multi-dimensional maps, and hyperchaotic systems), highlight why designers choose them, and note practical limitations that will reappear later in our security discussion [41].

2.2.1. One-Dimensional Chaotic Maps. One-dimensional (1D) maps are the most widely deployed chaotic primitives in image-encryption proposals due to their conceptual simplicity and low computational cost. Classic examples include the logistic map, the tent map, and the sine map; many recent works also propose variants or compound 1D constructions that expand parameter ranges or improve statistical properties [42]. Designers favour 1D maps because they are easy to implement (cheap iterations, trivial state representation) and produce sequences that can be quantized into keystreams for pixel permutation or substitution layers. However, 1D maps suffer two well-known practical weaknesses: (i) relatively small effective key/parameter spaces when discretized; and (ii) rapid degradation under finite-precision arithmetic, which can introduce short cycles and correlations that attackers exploit. For these reasons, researchers frequently augment or combine 1D maps (e.g., coupled sine–logistic or piecewise constructions) to enlarge the chaotic region and reduce predictability [42].

2.2.2. Multi-Dimensional Chaotic Systems. Multi-dimensional (typically 2D or 3D) discrete and continuous chaotic systems, such as the Hénon map, Lozi map, Lorenz system (when discretised), and various coupled-map constructions, are commonly used when designers require richer dynamics or larger internal state spaces. Two-dimensional maps (Hénon, Baker, etc.) are especially popular for generating multi-stream keystreams or for constructing keyed S-box generation procedures, because their phase space supports more complex mixing between variables than a single scalar map. Multi-dimensional systems generally offer:

- **Larger parameter spaces** and multiple interacting state variables, which can yield longer periods in finite-precision implementations.
- **Richer topologies** that make simple reconstruction attacks harder than for low-dimensional maps.
- **Flexible coupling patterns** suitable for producing parallel keystreams or for mapping state tuples into substitution table entries.

Nevertheless, multi-dimensional maps also introduce implementation complexity (higher computational cost, more parameters to manage) and, if poorly chosen or discretised, can still collapse to low-entropy cycles. Recent literature often uses 2D maps as building blocks for dynamic S-boxes or as permutation drivers in permutation–diffusion pipelines [42]. Comparative reviews emphasise that multi-dimensional choices must be justified by both theoretical indicators (Lyapunov spectrum, bifurcation behaviour) and empirical tests in the target digital environment [41].

2.2.3. Hyperchaotic Systems. Hyperchaotic systems are dynamical systems with two or more positive Lyapunov exponents; intuitively, they expand volumes in multiple phase-space directions simultaneously, producing behaviour that is often considered more complex and harder to predict than simple chaos. Hyperchaotic constructions (4D maps, coupled higher-order continuous systems) have become popular in image-encryption research because they promise larger effective key spaces, stronger sensitivity across several state variables, and increased difficulty of state reconstruction from partial observations [43].

In practice, hyperchaotic systems are used in two main ways: (i) to generate multi-stream keystreams for parallel substitution/diffusion operations, and (ii) to seed or directly construct high-entropy S-boxes whose entries depend on multiple interacting state variables. Empirical studies show that hyperchaotic schemes can improve statistical measures (entropy, correlation) and make certain simple attacks harder; however, hyperchaos is not a panacea. The same finite-precision and discretisation issues that affect 1D and 2D maps also apply, and because hyperchaotic systems are more complex, subtle numerical errors or parameter mismanagement can introduce exploitable structure [43]. Thus, while hyperchaotic designs are promising and widely used (especially in recent high-performance image-cipher proposals), their practical security must be validated by cryptanalytic testing rather than assumed from theory alone.

Synthesis and implications for cipher design. Across these families the trend in the literature is clear: designers move from simple 1D maps (fast, but fragile) to multi-dimensional and hyperchaotic constructions (more complex, potentially more robust) while compensating for finite-precision collapse by hybridisation, piecewise definitions, or coupling strategies. For cryptographic use, and particularly for constructing S-boxes or substitution layers intended to resist linear/differential attacks, it is essential to evaluate chaotic

sources with respect to both dynamical-system indicators (Lyapunov exponents, bifurcation diagrams) and digital-implementation diagnostics (periodicity under quantization, statistical independence of bit-streams) [40,41]. The later sections of this review translate these dynamical and numerical diagnostics into the concrete cryptographic evaluation checklist we recommend.

3. Chaos-Based S-Box Construction Techniques

The design of substitution boxes (S-boxes) using chaotic dynamics has become a major research direction in modern symmetric cryptography, particularly for image encryption. Chaos provides a mechanism for generating pseudo-random sequences and nonlinear transformations without resorting to large precomputed tables. In this section we categorise the major paradigms for constructing chaos-based S-boxes, evaluate their motivations, advantages, and limitations, and provide a conceptual roadmap for understanding how chaos integrates with classical cryptographic design principles.

3.1. Direct Chaotic Sequence–Based Construction

One of the earliest and most intuitive methods for chaos-based S-box construction is to use raw sequences generated by a chaotic map to populate S-box entries. In such schemes, a chaotic map (e.g., the logistic map, tent map, sine map) is iterated from a secret seed to produce a long floating-point sequence, which is then quantised and normalised into the finite range required for S-box indices. Sorting and permutation approaches are common:

- **Sorting-based generation:** The chaotic floating-point sequence is sorted in ascending or descending order, and the rank positions are taken as the S-box entries. The presumed unpredictability of a chaotic map then yields a pseudo-random permutation for the box.
- **Permutation-based mapping:** Another variant is to directly use the chaotic sequence as an index sequence for permuting a canonical S-box (e.g., identity mapping), reshuffling rows and columns based on chaotic order relations.

These approaches are attractive because of their simplicity and low computational cost. They also naturally produce bijective S-boxes if the mapping procedure preserves one-to-one assignment. Despite this, several weaknesses have been documented: in finite-precision digital implementations chaotic sequences can devolve into short cycles; sorting can introduce subtle correlations; and the generated S-boxes may exhibit poor cryptographic measures such as low nonlinearity or high differential uniformity if not carefully post-processed [141,153].

3.2. Algebraic–Chaotic Hybrid Approaches

In algebraic–chaotic hybrid S-box constructions, designers combine the algebraic structure of finite fields with chaotic dynamics to produce substitution tables. Here, chaos is not used to populate table entries directly; instead, it modulates algebraic functions such as affine transforms, inverses in $\mathbb{F}_{2^n}$, or polynomial mappings. The algebraic base guarantees desirable cryptographic properties (e.g., high algebraic degree), while chaos provides additional randomness and key dependence.

Common strategies include:

- **Chaos-modulated affine transformations:** An initial S-box based on an algebraic structure (e.g., inversion + affine transform as in AES) is perturbed by a chaotic sequence that alters affine coefficients per key or round.
- **Chaotic masking of algebraic outputs:** Algebraic outputs in $\mathbb{F}_{2^n}$ are XORed or masked with quantised chaotic sequence bits before final output.

These hybrids often show improved resistance to differential and linear attacks because the algebraic core provides provable measures while chaos adds a layer of nonlinearity or unpredictability that protects against structural attacks. However, the challenge lies in ensuring that the chaotic perturbation does not degrade the algebraic properties that are essential for security [176,153].

3.3. Dynamic and Key-Dependent S-Boxes

Dynamic or key-dependent S-boxes are constructed on-the-fly from the master key or session-specific key material. Chaos plays a central role in several dynamic-design proposals by deriving S-box entries as a deterministic function of the key-enriched chaotic seed. A sub-class of these designs are plaintext-dependent S-boxes where encryption of a specific message influences S-box entries before substitution.

Dynamic approaches aim to subvert attacks that rely on fixed S-box structure (e.g., precomputation of linear approximations), making attacks such as linear and differential cryptanalysis more difficult in practice. Techniques include:

- **Key-seeded chaotic iteration:** Use the secret key to initialise a chaotic system, iteratively generate sequences, and derive S-box entries based on quantisation and mapping functions.
- **Plaintext-dependent parameterisation:** Embed parts of the plaintext (or its hash) into initial conditions so that the S-box is tailored for each message, raising the bar for chosen-plaintext attacks.

Although dynamic S-boxes conceptually increase security, they raise unique challenges: weak keys can produce weak S-box instances; key leakage can be amplified through S-box generation; and statistical or structural biases can be introduced if the chaotic generator interacts poorly with the generation algorithm [1].

3.4. Optimization-Assisted Chaotic S-Boxes

To address the limitations of pure chaotic methods, many researchers incorporate optimisation techniques, such as genetic algorithms (GA), particle swarm optimisation (PSO), ant colony optimisation (ACO), and differential evolution, to refine chaotic S-box designs. In these metaheuristic frameworks, chaos is used to initialise candidate solutions or guide search trajectories, while the optimisation algorithm selects and evolves S-boxes towards improved cryptographic criteria [176,175]:

- **Fitness evaluation:** Candidate S-boxes are scored based on a weighted combination of cryptographic measures (nonlinearity, differential uniformity, SAC, etc.).
- **Evolutionary steps:** Mutation and crossover are guided by chaotic sequences to maintain exploration diversity.

The resulting S-boxes can achieve comparably high cryptographic strength even for low-dimensional constructs. However, when optimisation is decoupled from cryptographic guarantees (e.g., fitness landscapes that do not account for real attack models), the outcomes can overfit to the metric rather than practical security.

3.5. Machine Learning–Assisted Chaotic S-Box Generation

Recent research has explored the use of machine learning (ML) to assist chaotic S-box design. Techniques range from neural-net-based generation to reinforcement learning that tunes chaotic parameters to satisfy target cryptographic profiles [1]. In these proposals:

- **Neural generators:** Neural networks are trained to produce substitution tables whose statistical properties mimic ideal S-box behaviour, with chaotic sequences providing noise or regularisation during training.
- **Reinforcement learning:** S-box construction is framed as a sequential decision problem where an agent receives rewards for high cryptographic metrics, and chaos is used to explore the space of possible S-box entries.

Machine learning–assisted designs hold promise, particularly in automating the search for high-quality S-boxes, but they require careful engineering to ensure that the learned structures do not betray subtle vulnerabilities to algebraic or structural attacks.

Table 1: Taxonomy of Chaos-Based S-Box Construction Methods

Method	Chaos Source	Key Dependence	Notes
Direct chaotic sequences	1D / 2D maps	Low	Simple, but prunable cycles
Algebraic–chaotic hybrids	Field + chaos	Medium	Balances provable structure
Dynamic key-dependent	Chaotic seed	High	Adaptive but risky weak keys
Optimisation-assisted	Chaos + GA/PSO	Medium–High	Metric-driven
ML-assisted	Chaos + neural/ML	Medium	Automated but opaque

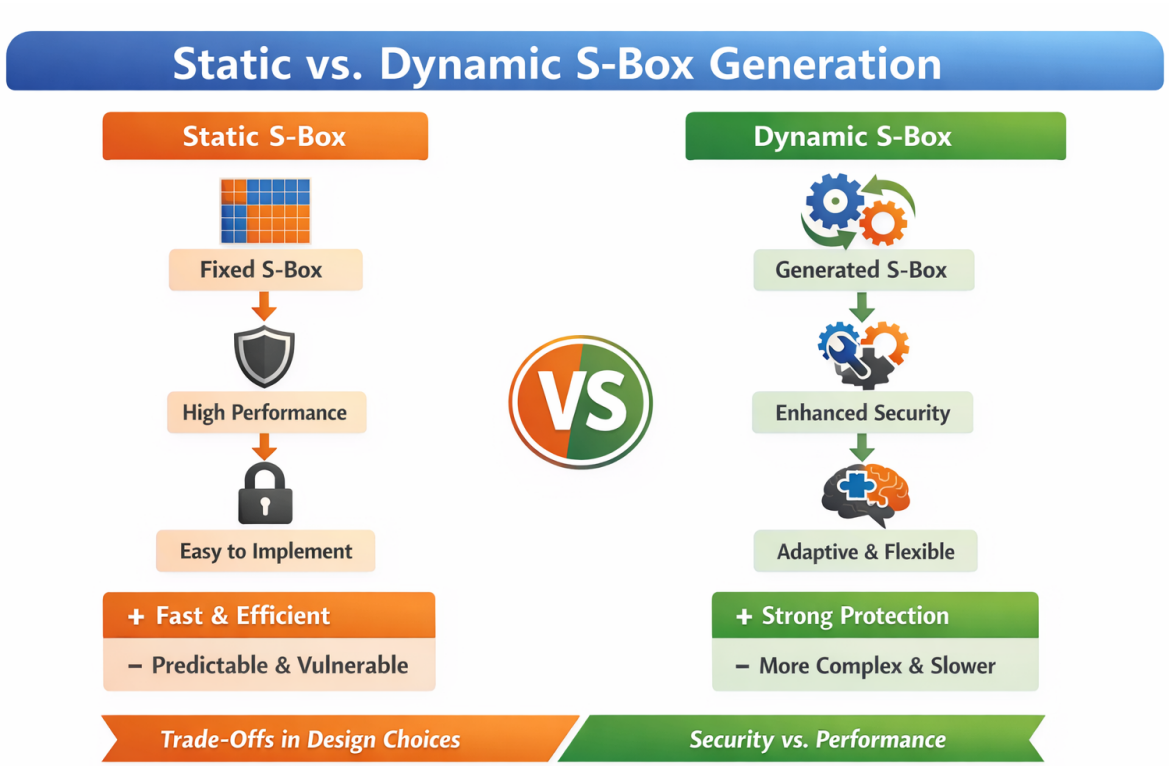

Figure 1: Workflow comparison of static vs. dynamic S-box generation using chaos

3.6. Comparative Discussion of Construction Paradigms

The construction paradigms introduced above differ in terms of complexity, security guarantees, and implementation cost. Table 1 summarises the taxonomy of chaos-based S-box construction methods, categorising them according to the source of chaos, use of algebraic structure, key dependence, and optimisation or learning involvement. Figure 1 provides a high-level workflow comparison between static and dynamic S-box generation to illustrate the trade-offs in design choices.

Overall, while chaos provides a versatile and intuitive source of nonlinearity and pseudo-randomness, its integration into S-box design must be balanced with a rigorous evaluation of cryptographic properties. Static approaches with algebraic grounding often yield stronger guarantees, whereas dynamic and learning-assisted methods open new possibilities but require advanced validation techniques. The next section of this review connects these constructions with cryptographic evaluation criteria to assess their true effectiveness in security-sensitive applications.

4. Cryptographic Evaluation Criteria for Chaotic S-Boxes

A fundamental question in any review of chaos-based S-box constructions is: *How do we judge whether an S-box is cryptographically strong?* Designers often rely on the chaotic appearance of sequences to imply security, but that alone is insufficient. In modern cryptography, evaluation criteria are well-studied and tied to formal resistance against classes of attacks. This section consolidates these criteria, both classical and implementation-oriented, and positions them in the context of chaos-derived S-boxes.

4.1. Classical Cryptographic Properties

The role of an S-box within a cipher is to provide nonlinearity and confusion. To quantify these properties, researchers utilise metrics that capture deviation from simple algebraic structures and sensitivity to input changes.

4.1.1. Nonlinearity. **Nonlinearity** is one of the most important measures of S-box strength. It is defined as the minimum Hamming distance between the S-box's component Boolean functions and the set of all affine functions. Intuitively, high nonlinearity implies that the S-box resists linear approximation, which is essential for thwarting linear cryptanalysis, a powerful class of attacks that exploit affine approximations of nonlinear components [2].

Mathematically, for an $m \times n$ S-box F, the nonlinearity of a component function f is computed as:

$$\mathrm{NL}(f) = 2^{m-1} - \tfrac{1}{2} \max_{a \in \mathbb{F}_2^m, b \in \mathbb{F}_2^n} |\mathrm{WHT}(f)(a,b)|,$$

where $\mathrm{WHT}(f)$ is the Walsh–Hadamard transform of f. A higher value indicates greater distance from all affine functions. Standard benchmarks such as the AES S-box achieve nonlinearity values close to the theoretical maximum for their dimensions [3].

Chaos-based S-boxes must be evaluated using the same metric: without sufficient nonlinearity, apparent randomness does not translate into resistance against linear cryptanalysis.

4.1.2. Strict Avalanche Criterion. The **Strict Avalanche Criterion (SAC)** assesses how sensitively output bits respond to changes in input bits. An S-box satisfies SAC if, for a single input bit flip, each output bit changes with probability approximately 0.5. This property is related to diffusion: good diffusion amplifies small input differences into widespread output differences [4].

Formally, for an S-box F and an input vector x differing in one bit to x', SAC requires:

$$P[F(x) \oplus F(x') = e_i] \approx \tfrac{1}{2} \quad \forall\, i = 1, \ldots, n,$$

where e_i is the unit vector in the ith output coordinate. Chaos-based approaches often produce outputs that look "diffuse" statistically, but empirical evaluation against SAC reveals whether this diffusion matches cryptographic expectations.

4.1.3. Bit Independence Criterion. The **Bit Independence Criterion (BIC)** extends SAC by requiring output bits to change independently when input bits are flipped. In other words, output bits should exhibit minimal statistical correlation with one another in response to input perturbations [5].

If F_i and F_j are component functions of the S-box, BIC demands:

$$P[F_i(x) \oplus F_i(x') = 1 \ \wedge \ F_j(x) \oplus F_j(x') = 1] \approx \tfrac{1}{4},$$

for all pairs (i, j) of output bits under single input bit flips. In chaos-based S-boxes, maintaining bit independence can be challenging if the chaotic sequence mapping inadvertently introduces correlations in output bits.

4.2. Resistance Against Differential and Linear Attacks

Beyond classical diffusion and nonlinearity, an S-box must resist structured attacks that exploit input-output correlations.

4.2.1. Differential Uniformity. Differential attacks rely on input differences mapping to predictable output differences with non-negligible probability. The **differential uniformity** of an S-box, also known as its differential distribution table (DDT), captures this behaviour [6].

For an S-box $F : \mathbb{F}_2^m \to \mathbb{F}_2^n$, the differential uniformity δ is defined as:

$$\delta = \max_{a \neq 0, b} |\{x \in \mathbb{F}_2^m : F(x) \oplus F(x \oplus a) = b\}|.$$

A lower δ implies fewer high-probability differential characteristics, decreasing susceptibility to differential cryptanalysis. The best possible uniformity for even sizes is 2 (APN, Almost Perfect Nonlinear), and many cryptographically strong S-boxes aim to approach this bound.

Chaos-based S-boxes can accidentally produce high differential uniformity if the mapping from chaotic sequences to discrete values is uneven or introduces clumping in the distribution of differences.

4.2.2. Linear Approximation. Complementary to differential uniformity, the **linear approximation table (LAT)** of an S-box measures the maximum correlation between linear combinations of input bits and linear combinations of output bits. The maximum bias away from 0 indicates how susceptible the S-box is to linear cryptanalysis [7].

Let $L(a, b)$ denote the entry of the LAT for input mask a and output mask b. Ideally, the largest absolute entry is small, corresponding to low correlation. A high maximum correlation suggests exploitable patterns.

Chaos-based constructions must be benchmarked against known LAT profiles; otherwise, perceived randomness may mask structural linear correlations.

4.3. Structural and Algebraic Properties

In addition to statistical resistance measures, structural properties of S-boxes determine resilience to algebraic attacks.

Fixed Points. A **fixed point** of an S-box is an input value that maps to itself: $F(x) = x$. Fixed points and short cycles can enable shortcut attacks, particularly in lightweight or resource-constrained systems. Ideally an S-box should have no fixed points, or at least a minimal number, and should be designed so that the cycle structure of the mapping avoids exploitable regularities [8].

Algebraic Degree. The **algebraic degree** of an S-box, the highest degree of any output coordinate's ANF (algebraic normal form), gauges its complexity. Higher degree increases difficulty for algebraic attacks that model the cipher as a system of polynomial equations. Chaotic S-box generation must ensure that the algebraic degree remains high, which is not automatically guaranteed by chaotic mapping alone [9].

4.4. Side-Channel and Implementation-Oriented Metrics

While the above criteria focus on mathematical properties, implementation realities, particularly for software and hardware platforms, introduce additional concerns. Side-channel vulnerability metrics (such as differential power analysis or timing leakage) matter when S-boxes are generated or recomputed at runtime.

A chaotic seed that influences execution time or memory access patterns can inadvertently introduce side channels. Likewise, dynamic or key-dependent S-boxes must be evaluated for their implementation hardness. Even static chaos-derived S-boxes should be tested under realistic hardware models to detect exploitable leaks [10].

4.5. Benchmarking Against Standard S-Boxes

To judge whether chaos-based S-boxes are "good enough," it is necessary to benchmark them against established standards such as the AES S-box and other well-studied constructions. These benchmarks include a full suite of the above metrics and often involve published datasets or automated evaluation frameworks [11].

In the context of image encryption and chaos-derived S-boxes, evaluation according to these criteria provides a rigorous baseline against which claims of "chaotic security" can be validated or refuted. As

the review progresses, we will revisit these metrics when analysing specific chaos-based designs to assess whether they truly meet cryptographic standards.

5. Chaos-Based Image Encryption Using S-Boxes

In the domain of secure multimedia communications, image encryption has emerged as a critical tool to protect confidentiality and integrity of visual information. Unlike text or binary streams, images possess unique statistical properties, high redundancy, strong spatial correlation among pixels, and large data volumes, which demand tailored encryption architectures that balance security with computational efficiency [44]. One of the most influential paradigms in this space, particularly for chaos-based methods, is the *confusion–diffusion* framework originally inspired by Shannon's principles of secure cipher construction [45]. Chaos-based image encryption schemes extend this framework by integrating chaotic maps and substitution mechanisms (often via S-boxes) to leverage their sensitive dependence on initial conditions and pseudo-random behaviour [46]. In this section we explore the general architecture underpinning these systems and lay the groundwork for analysing specific S-box-driven designs later in this review.

5.1. General Architecture of Image Encryption Systems

The confusion–diffusion framework remains the prevailing structural template for image encryption algorithms, whether classical or chaotic. In essence, the encryption process comprises two core processes:

- **Confusion:** This stage seeks to scramble the positions of pixels (or pixel blocks) in the image so that the spatial correlation inherent in plain images, where neighbouring pixels tend to have similar values, is disrupted. Techniques for confusion often involve pixel permutation based on chaotic sequences, geometric transformations, or keyed mapping functions. Permutation alone, however, does not sufficiently obfuscate pixel values; it merely rearranges them, leaving their intrinsic grey-level distributions intact and vulnerable to certain attacks. Therefore, confusion is typically complemented by diffusion [47]. :contentReference[oaicite:0]index=0

- **Diffusion:** This stage alters the pixel values themselves in a manner that is sensitive to both the secret key and the intermediate encrypted data. Diffusion spreads the influence of a single plain-image pixel across many ciphertext pixels, thereby making it difficult for attackers to infer relationships between input and output pixels. In chaotic designs, diffusion often employs pixel value mixing operations such as XOR with chaotic keystreams, substitution via S-boxes, or arithmetic mixing guided by chaos-generated matrices [48]. :contentReference[oaicite:1]index=1

Together, confusion and diffusion aim to achieve the cryptographic properties of *confusion* (obscuring the key–ciphertext relationship) and *diffusion* (spreading the influence of plain-text changes across the ciphertext). When implemented properly, multiple rounds of confusion and diffusion dramatically transform an image into noise-like output with uniform histograms, low pixel correlation, and high entropy, all hallmarks of a secure cipher [49]. :contentReference[oaicite:2]index=2

Chaotic Sequences as Driving Forces. In chaos-based image encryption, chaotic maps (such as logistic, Henon, or higher-dimensional systems) are invoked to generate pseudo-random sequences used in both confusion and diffusion stages. The sensitive dependence on initial conditions, a core property of chaos, ensures that slight changes to the key yield markedly different keystreams and encryption outcomes. These sequences can drive pixel permutations, matrix generation for diffusion, or dynamic S-box formation, depending on the design. However, it is crucial to recognise that chaotic behaviour in the real (continuous) mathematical domain does not automatically translate to cryptographic security when discretised and implemented; this fact underscores the need for rigorous evaluation of chaos-based constructions beyond statistical randomness [50]. :contentReference[oaicite:3]index=3

Role of S-Boxes in Confusion–Diffusion Pipelines. While early chaos-based schemes relied heavily on permutation and simple XOR-based diffusion with chaotic sequences, more advanced designs augment diffusion with substitution mechanisms, typically via S-boxes, to inject nonlinearity into the value transformation process. S-boxes serve as nonlinear substitution components that further obfuscate pixel values

in tandem with chaotic sequences, strengthening resistance to differential and linear attacks. Recent proposals leverage both static chaos-derived S-boxes and dynamic key-dependent S-boxes embedded within permutation–diffusion pipelines to enhance confusion and diffusion simultaneously [51]. :contentReference[oaicite:4]index=4

Iterative Architecture and Rounds. Many chaos-based image encryption schemes apply the confusion and diffusion stages iteratively across multiple rounds. Each round increases the complexity of transformation, further scrambling pixel positions and values. Iterations can significantly raise security levels at the cost of increased computational overhead, creating a trade-off between performance and security, an important consideration in resource-constrained environments [52]. :contentReference[oaicite:5]index=5

Example Workflow. A typical chaos-based image encryption using S-boxes can be summarised as follows:

1. **Key and Seed Generation:** Derive initial parameters for chaotic maps (e.g., control parameters and initial states) from the secret key using key derivation functions or hash functions.

2. **Confusion Stage:** Use chaotic sequences to permute pixels or pixel blocks, rearranging their positions to disrupt spatial correlation.

3. **S-Box Creation (Optional):** Generate static or dynamic S-boxes from chaotic map outputs, possibly hybridised with algebraic structures or key material.

4. **Diffusion Stage:** Transform pixel values using substitution (via S-boxes) and/or arithmetic operations driven by chaotic sequences, ensuring changes propagate widely through the data.

5. **Round Iteration:** Repeat the confusion and diffusion steps multiple times to deepen obfuscation.

Different schemes introduce variations, such as feedback between stages, block-wise operations, multiple S-boxes, or joint substitution–permutation networks, but the core remains rooted in the confusion–diffusion paradigm augmented by chaos [53]. :contentReference[oaicite:6]index=6

Security Implications of Architecture Choices. The sequence and interplay of confusion, substitution, and diffusion steps strongly influence the cipher's resilience. Proper confusion effectively hides structure but does not change underlying pixel values; effective diffusion ensures that small changes in input or key propagate irreversibly. When substitution (via S-boxes) is too weak or poorly seeded by chaotic sequences, diffusion may be insufficient, making the system vulnerable to attacks such as chosen-plaintext or differential cryptanalysis. Enhancements such as bidirectional diffusion, dynamic S-boxes, or multilayer architectures have been proposed to address these vulnerabilities, but rigorous cryptanalysis remains essential to validate security claims [54]. :contentReference[oaicite:7]index=7

Overall, the confusion–diffusion framework provides a flexible yet powerful template for chaos-based image encryption. Its success hinges on careful design choices around permutation strategies, substitution mechanisms, and chaotic sequence generation, all of which must be evaluated against both statistical and cryptanalytic benchmarks. The following subsections will examine specific families of chaos-based image encryption designs and how they integrate S-boxes into the confusion–diffusion pipeline.

5.2. Pixel Permutation-Only Schemes

In the early development of chaos-based image encryption, many schemes focused solely on pixel position permutation, reordering the pixel positions according to chaotic sequences, as a means of obfuscating the spatial correlation inherent in images. The intuition is that by scrambling pixels according to a key-dependent chaotic map, the original image's spatial structure is lost, making it harder for an adversary to visually or statistically infer the plain image. However, the overwhelming consensus in image cryptography research is that **permutation alone is insufficient to provide cryptographic security**; robust diffusion, alteration of pixel values, is essential to prevent information leakage and structural attacks [55]. :contentReference[oaicite:0]index=0

Basic Principle of Pixel Permutation. A pixel permutation scheme generates a mapping (permutation vector or table) using a chaotic sequence and then applies this mapping to rearrange pixel positions in the image. Common chaotic sources include low-dimensional maps (e.g., logistic or Arnold maps) which iterate from secret seeds to produce pseudo-random indices for permutation. Because image pixels often exhibit strong spatial redundancy (neighbouring pixels are highly correlated), permutation can break this correlation to some degree, yielding a visually less recognisable cipher image. Nonetheless, permutation on its own **does not alter pixel values**, meaning that the distribution of pixel intensities remains unchanged, a critical flaw from a cryptanalytic perspective [56]. :contentReference[oaicite:1]index=1

Limitations and Weaknesses. Permutation-only image encryption schemes suffer from multiple well-documented weaknesses that undermine their security when evaluated under formal attack models:

- **No Pixel Value Diffusion.** Because pixel intensities remain unchanged, histograms and global statistical properties (e.g., intensity distribution) are preserved. An attacker observing a cipher image can still derive high-level information about the plain image, as permutation does not randomise pixel values [57]. :contentReference[oaicite:2]index=2

- **Reversibility Through Known or Chosen-Plaintext Attacks.** Without diffusion, the cryptosystem can be modelled as a simple permutation function. Given a pair of known plain-cipher images, or a series of chosen plaintexts, an adversary can infer the permutation mapping directly and invert it to recover original content, even without learning the underlying key. This vulnerability has been exploited in practical cryptanalyses that fully recover original images using relatively few chosen plaintexts [58]. :contentReference[oaicite:3]index=3

- **Limited Key Space and Low Complexity.** When the only transformation is pixel rearrangement, the effective key space is often smaller than claimed because many permutations are equivalent or produce indistinguishable ciphertext given certain image characteristics. In some analysed schemes, brute-force exploration of the permutation vector becomes tractable due to predictable or weak key generation procedures [59]. :contentReference[oaicite:4]index=4

- **Permutation Redundancy.** Multiple rounds of permutation alone do not increase security beyond a single permutation. Whether applied once or repeatedly, the overall effect is equivalent to one composite permutation, leaving the system susceptible to the same attacks. This redundancy illustrates that improving security requires altering diffusion properties rather than merely increasing confusion rounds [60]. :contentReference[oaicite:5]index=5

- **Insufficiency Against Differential and Correlation Attacks.** Permutation-only ciphers cannot ensure high sensitivity to small changes in the plain image, because pixel values remain intact and thus predictable relationships between pixels are retained. As a result, correlation patterns in the plain image can re-emerge under analysis of cipher images [61]. :contentReference[oaicite:6]index=6

- **Weakness under Homogeneous Images.** If the plain image exhibits uniform or homogeneous regions (e.g., large blocks of identical intensity), permutation fails completely to introduce meaningful confusion, and the lack of diffusion means these regions remain discernible in the ciphertext. Such structures can be used to mount statistical or pattern attacks [62]. :contentReference[oaicite:7]index=7

Case Studies and Empirical Evidence. Several cryptanalytic studies have explicitly shown how permutation-only schemes break under basic attacks:

- An image encryption algorithm based solely on pixel permutation was shown to leak key information in the cipher image, enabling both brute-force and chosen-plaintext attacks to recover the plain image without knowledge of the secret key [63]. :contentReference[oaicite:8]index=8

- Surveys on permutation-assisted encryption conclude that permutation alone does not satisfy security requirements for image ciphers and recommend complementing permutation with diffusion operations such as substitution, XOR mixing, or value-dependent transformations [64]. :contentReference[oaicite:9]index=9

Implications for S-Box Integration. The inadequacy of pixel permutation alone highlights the importance of incorporating substitution mechanisms such as S-boxes into image encryption frameworks. S-boxes provide nonlinearity and value transformation that cannot be achieved through permutation alone. They are essential to achieving the Shannonian diffusion necessary to propagate small changes in the plain image throughout the ciphertext space and to resist formal cryptanalytic models like differential and linear attacks.

In summary, while pixel permutation disrupts spatial relationships and reduces visual recognisability, it does not fundamentally protect image content from structural and cryptanalytic attacks. Permutation-only schemes serve as an instructive baseline, but robust image encryption requires the integration of diffusion and substitution operations to meet modern security standards.

5.3. Permutation–Diffusion Schemes with Chaotic S-Boxes

To address the inherent weaknesses of pixel permutation-only schemes, most modern chaos-based image encryption algorithms adopt a *permutation–diffusion* architecture embedded with substitution mechanisms. Within this framework, chaotic maps drive both the reordering of pixel positions and the alteration of pixel values through nonlinear substitution (often implemented via S-boxes). The integration of chaos-derived S-boxes into the diffusion stage introduces cryptographic nonlinearity that significantly enhances confusion and helps ensure that small changes in the plain image or key propagate widely through the ciphertext. This combined strategy leverages chaos for pseudo-randomness, permutation for structural scrambling, and S-boxes for nonlinear mixing, yielding encryption schemes that are far more resilient to cryptanalytic attacks [65].

Permutation–Diffusion Framework. The conceptual architecture of a permutation–diffusion scheme generally follows a two-stage process:

1. **Permutation Stage:** Chaotic sequences generate index maps to reorder pixels or pixel blocks. Common chaotic maps include low-dimensional systems like the logistic map, which are iterated to produce sequences that are sorted or indexed to define a permutation vector. This breaks the high spatial correlation characteristic of natural images.

2. **Diffusion Stage with Chaotic S-Boxes:** After permutation, pixel values are altered through substitution and mixing operations. Chaotic S-boxes replace pixel intensities or bits with new values derived from dynamic or static substitution tables computed via chaotic sequences. In some designs, pixel values undergo a combination of XOR operations with chaotic keystreams and substitution by S-boxes, thereby intertwining chaos, substitution, and arithmetic mixing to strengthen security.

This two-stage interaction ensures that changes in either the key or the plain image produce dramatically different ciphertexts, a requirement for both confusion and diffusion as per Shannon's criteria [66].

Role of Chaotic S-Boxes. Within the permutation–diffusion framework, S-boxes derived from chaotic maps serve two key purposes:

- **Nonlinear Substitution:** S-boxes introduce nonlinearity that complicates attempts at linear or differential cryptanalysis. Unlike simple XOR with a chaotic keystream, a well-designed S-box ensures that output differences and linear combinations cannot be easily predicted from input differences or linear masks.

- **Enhanced Diffusion Across Bits:** By transforming pixel values through nonlinear mappings, S-boxes help ensure that a small change in the plain image affects not just neighbouring pixels but entire bit patterns across multiple pixels, thus increasing the avalanche effect.

In early works, chaos-based diffusion primarily relied on additive mixing (XORing) of pixel values with chaotic sequences generated from maps such as the logistic or Chen maps. However, extensive analysis revealed that XOR-only diffusion, while useful against statistical attacks, offers limited resistance to differential and chosen-plaintext attacks if not augmented with nonlinear substitution. The introduction of chaotic S-boxes partly remedies this limitation by embedding algebraic complexity into the diffusion stage [67].

Design Variants in Permutation–Diffusion Schemes with Chaotic S-Boxes. Various research efforts have proposed distinct strategies for integrating chaotic S-boxes into the permutation–diffusion pipeline. These can be grouped into several categories:

- **Static S-Box + Chaotic Permutation:** A single static chaos-derived S-box is generated prior to encryption and used throughout the diffusion stage, while chaotic maps independently drive permutation. This design simplifies evaluation but risks repeated use of the same substitution mapping, which attackers might exploit if weaknesses exist.

- **Dynamic/Key-Dependent S-Boxes:** The S-box entries change per image, per round, or per block based on key material and chaotic sequences. Dynamic S-boxes provide stronger resistance against differential attacks because the substitution layer lacks a fixed pattern that attackers could precompute.

- **Block-Based S-Boxes:** Instead of applying a single S-box to each pixel, schemes may partition the image into blocks (e.g., 2×2 or 4×4) and apply distinct substitution tables or multi-input mapping functions. This block-based application increases mixing complexity at the cost of computational overhead.

- **Multi-Round Permutation–Diffusion:** Inspired by classical block ciphers, some designs iterate the permutation–diffusion sequence multiple times. Each round uses new chaotic sequences and possibly new S-boxes, compounding confusion and diffusion with rigorous key dependence.

Each of these variants exhibits different trade-offs between security and performance. Dynamic S-boxes, for example, typically improve resilience against chosen-plaintext attacks but incur higher generation and memory costs. Block-based substitution increases diffusion granularity but must be carefully evaluated to avoid predictable patterns [68].

Security Enhancements Provided by Chaotic S-Boxes. Chaotic S-boxes significantly enhance the diffusion stage in several concrete ways:

- **Increased Avalanche Effect.** Properly designed S-boxes ensure that flipping a single bit of the permutation output changes roughly half of the output bits after substitution, satisfying classical criteria like SAC and BIC, metrics standard S-boxes are benchmarked against.

- **Improved Resistance to Differential Cryptanalysis.** When incorporated into diffusion, S-boxes reduce high-probability differential trails that attackers exploit in chosen-plaintext attacks.

- **Hybrid Chaos–Algebraic Properties.** Chaos-derived S-boxes that incorporate algebraic structure combine classical cryptographic strengths with chaotic unpredictability.

Limitations and Open Challenges. Despite their improvements over permutation-only or XOR-based diffusion schemes, permutation–diffusion designs with chaotic S-boxes still face several challenges, including finite precision effects, parameter sensitivity, incomplete cryptanalytic evaluation, and security–efficiency trade-offs [69].

Empirical Studies and Comparative Evidence. Recent research articles offer comparative evidence that chaotic S-box-enhanced permutation–diffusion schemes outperform pure permutation or simple XOR diffusion in key security metrics such as correlation coefficient reduction, histogram uniformity, and differential propagation probability [66].

In summary, permutation–diffusion schemes incorporating chaotic S-boxes represent a major step forward from earlier chaotic encryption methods. By leveraging both structural scrambling and nonlinear substitution, they achieve stronger confusion and diffusion while aligning more closely with classical cryptographic principles.

5.4. DNA Computing and Chaos-Hybrid Image Encryption

In recent years, the field of image encryption has witnessed the emergence of hybrid approaches that integrate DNA computing principles with chaotic systems to enhance security properties. These schemes exploit the rich algebraic structure of DNA encoding together with the pseudo-random dynamics of chaos to achieve stronger confusion and diffusion than traditional permutation–diffusion mechanisms alone. The resulting hybrid frameworks have shown promising performance in resisting classical cryptanalytic attacks while maintaining real-time applicability, especially for resource-constrained environments such as the Internet of Things (IoT) or medical imaging [70].

Conceptual Foundations: DNA Encoding and Chaos. DNA computing, inspired by the information storage and parallel processing capabilities of biological DNA strands, uses nucleotide bases (A, C, G, T) to represent binary information and applies biologically motivated operations for encryption tasks. The four nucleotides can encode binary bits using mapping rules (e.g., A = 00, C = 01, G = 10, T = 11), enabling an expanded symbolic space that enhances nonlinear transformation potential during encryption. When combined with chaotic maps, deterministic mathematical systems with sensitive dependence on initial conditions, the hybrid paradigm leverages chaotic sequences to drive DNA operations such as crossover, mutation, and substitution. Hence, the chaotic components determine the sequence of DNA operations or the dynamic selection of encoding rules, creating a tightly coupled chaos-DNA pipeline [71].

High-Level Workflow of Chaos-DNA Image Encryption. A typical DNA and chaos hybrid encryption algorithm follows several stages:

1. **Preprocessing and DNA Encoding:** The image is first decomposed into binary bit-planes, and each pixel's binary representation is mapped to a DNA sequence using a chosen DNA encoding rule. Bit-plane decomposition improves encryption quality by isolating high-information bits [72].

2. **Chaotic Sequence Generation:** A chaotic system (e.g., 5D Hamiltonian, logistic, hyperchaotic Lorenz) is seeded with parameters derived from the secret key and optionally the plaintext hash (e.g., SHA-256). Iterating the map produces pseudo-random sequences used to control permutation, DNA rule selection, or subsequent operations [73].

3. **Permutation and Scrambling:** The chaotic sequences drive pixel or bit rearrangement, spreading spatial correlation and disrupting visible structure. Some designs extend this to bit-level or cross-plane permutation to further diversify diffusion [74].

4. **DNA-Based Diffusion/Transformation:** The core DNA operations, encoding, substitution, crossover, and decoding, are performed. Chaotic values dynamically select which rules or operations apply to different blocks or pixels, ensuring that the substitution layer is both key-dependent and context-adaptive [75].

5. **Final Reconstruction:** The post-DNA transformation sequences are decoded back into pixel values to produce the encrypted image. The combined effect of scrambling and DNA-based diffusion yields ciphertext with high entropy, flat histograms, and low inter-pixel correlation [76].

Advantages of DNA–Chaos Hybrid Schemes. Hybrid chaotic–DNA encryption schemes exhibit several attractive properties:

- **Enhanced Nonlinearity and Key Sensitivity:** The expanded symbol space of DNA encoding increases the complexity of substitution and diffusion operations. When chaotic maps dynamically govern encoding and operations, tiny changes in key or plaintext cause large ciphertext variations [77].
- **Large Key Space and Unpredictability:** By combining chaotic control parameters, hash-derived seeds, and variable DNA rules, these schemes can achieve a large effective key space that resists brute-force search and key-related attacks [78].
- **Parallelism and Strong Confusion/Diffusion:** DNA operations mimic biological parallel processing, enabling simultaneous transformations at multiple bit locations. Layering this with chaotic scrambling provides stronger confusion–diffusion interactions than simple XOR or permutation alone [79].

Representative Research and Applications. Recent works exemplify the hybrid trend:

- A lightweight DNA–chaos hybrid framework tailored for real-time IoT image security dynamically encodes pixels into DNA, uses two-dimensional chaotic maps for key streams, and performs nucleotide-level operations to achieve high entropy and strong attack resistance [80].
- New algorithms leveraging high-dimensional Hamiltonian chaotic systems combined with DNA encoding achieve improved hiding of high-bit information and controlled diffusion via DNA operation index tables [81].
- Dynamic DNA cryptography schemes use multiple chaotic maps and secure hash functions to generate dynamic DNA encoding rules and key sequences that vary per session [82].

Challenges and Cryptanalytic Considerations. Despite their promise, hybrid DNA–chaos schemes are not without vulnerabilities:

- **DNA Rule Weaknesses:** The choice of genome encoding rules can introduce patterns; fixed or suboptimal rules have been shown to weaken plaintext sensitivity and openness to chosen-plaintext attacks [83].
- **Finite-Precision Chaos Issues:** Digital implementations of chaotic systems can suffer from degraded randomness due to finite precision, potentially compromising the unpredictability of chaotic control [84].
- **Operational Overhead:** DNA encoding and decoding add computational cost compared to simpler diffusion operations, making efficiency a key concern in constrained environments [85].

Synthesis and Future Directions. Hybrid chaos–DNA image encryption represents a compelling frontier in multimedia security. By integrating algebraic DNA transformations with the unpredictability of chaotic dynamics, these frameworks provide enriched confusion–diffusion mechanisms suitable for high-security applications. Nonetheless, their adoption in practice hinges on rigorous cryptanalysis, careful rule design, and efficient implementation strategies [86].

5.5. Lightweight and Real-Time Image Encryption Designs

With the explosive growth of imaging applications in resource-constrained environments, including wireless sensor networks, Internet of Things (IoT) devices, mobile platforms, and real-time video streaming, the demand for lightweight yet secure image encryption schemes has become paramount [87,88]. Unlike general-purpose encryption algorithms originally designed for block or text data, lightweight image encryption must balance security, computational efficiency, memory footprint, and real-time performance [89]. Chaos-based methods, owing to their simple iterative structures and suitability for parallel processing, have emerged as promising candidates for such scenarios [95]. However, integrating chaos into lightweight frameworks introduces trade-offs between security guarantees and implementation practicality. This section examines the key design principles, representative approaches, strengths, and limitations of lightweight and real-time chaos-based image encryption schemes.

Motivation for Lightweight Encryption. Resource-constrained devices, such as battery-powered sensors or embedded cameras, often operate under strict limitations of power, processing speed, and memory [88]. Traditional ciphers like AES, while secure, impose significant computational overhead that may be unacceptable in such contexts [89]. In contrast, chaos-based encryption can offer lower arithmetic complexity and smaller state representations, making it suitable for real-time image protection without compromising fundamental confusion–diffusion properties [87]. Additionally, the inherently parallel nature of chaotic iteration lends itself well to hardware acceleration and pipelined implementations, further enabling high throughput [95].

Design Strategies for Lightweight Chaotic Encryption. Lightweight chaos-based image encipherment typically relies on one or more of the following design strategies [89,88]:

- **Reduced Rounds and Simplified Operations:** Schemes often minimise the number of confusion–diffusion rounds and restrict operations to simple arithmetic or bitwise transformations (e.g., XOR, circular shifts), reducing computational load at the possible expense of cryptanalytic strength [87].
- **Pixel-Level or Block-Level Parallelism:** Chaos can drive independent streams for different image segments, enabling simultaneous encryption of multiple blocks or pixels. Parallel processing is particularly useful for real-time video and high-resolution imagery [95].
- **Low-Dimensional Chaotic Maps:** Designers frequently choose low-cost chaotic maps (e.g., logistic, skew tent) that require only simple multiplication and addition operations, thereby minimising arithmetic complexity in software or hardware [88].
- **Simplified Key Scheduling:** Lightweight schemes often avoid complex key schedules to save cycles and memory, instead deriving chaotic parameters directly from the secret key via simple hash functions or bit extraction [89].

Such strategies work in tandem to produce encryption pipelines whose throughput matches the demands of real-time applications. However, these simplifications must be critically evaluated to ensure they do not inadvertently undermine core cryptographic properties analysed earlier in this review [95].

Representative Lightweight Designs Using Chaos. A number of chaos-based lightweight image encryption algorithms have been proposed in the literature [87,88]. Many of them follow a permutation–diffusion template with simplified substitution components, or hybridise chaotic scrambling with pixel value mixing. Representative designs include:

- **Chaotic Permutation and XOR Diffusion:** Early lightweight models used simple chaotic maps to generate permutation indices and XOR masks for diffusion. While efficient, these models often lacked strong substitution layers and were vulnerable to differential attacks unless additional nonlinear components were introduced [89].
- **Piecewise Chaotic Maps with Pixel Blocks:** Piecewise linear chaotic maps (PWLCM) or discretised tent maps have been combined with block transformation strategies where sub-blocks of an image are processed in parallel, reducing latency and improving encryption throughput [88].
- **Hybrid S-Box Integration:** Some recent lightweight approaches integrate small chaos-derived S-boxes within a predominantly XOR/diffusion pipeline to enhance nonlinearity without substantial computational overhead [87]. These designs aim to strike a balance between simplicity and cryptographic strength.

For example, lightweight implementations using PWLCM have demonstrated encryption speeds suitable for video streams on low-end microcontrollers, while retaining acceptable levels of entropy and correlation reduction in the ciphertext [88]. However, many such schemes still fall short of rigorous cryptanalytic evaluation, particularly against differential and linear attacks, indicating a gap between performance optimisation and security robustness [89].

Hardware and Parallel Implementations. Hardware implementations, such as field-programmable gate arrays (FPGAs) and application-specific integrated circuits (ASICs), are frequently employed to accelerate chaotic image encryption for real-time use [95]. Chaos-based designs benefit from inherent parallelism, enabling multiple chaotic streams to be computed and applied simultaneously. Studies have shown that hardware-accelerated chaotic encryption can achieve throughput in the hundreds of megabits per second range, satisfying high-definition video requirements, while maintaining low energy consumption, a critical factor in battery-powered devices [90].

Security Considerations and Trade-Offs. Despite their performance appeal, lightweight chaos-based schemes present noteworthy security trade-offs [89]:

- **Reduced Cryptographic Strength:** Simplified substitution and diffusion operations, while computationally efficient, often fail to achieve the levels of nonlinearity and avalanche effect seen in more robust designs with full S-box layers [87].
- **Vulnerability to Statistical Attacks:** Lightweight schemes relying heavily on permutation or chaotic XOR without strong substitution can be vulnerable to structural attacks that exploit residual patterns in the ciphertext [88].
- **Finite Precision Degradation:** Low-dimensional chaotic maps implemented in hardware with limited precision may suffer degradation of chaotic behaviour, reducing effective key space and sequence unpredictability [95].
- **Key Management Challenges:** Simplified key scheduling can lead to weak key selection or poor key diversity, making exhaustive search or related-key attacks more feasible [89].

These trade-offs show that lightweight design improvements must be carefully evaluated against established cryptographic metrics such as those outlined in Section 4 [95]. Real-time performance cannot be purchased at the expense of fundamental security principles.

Emerging Trends and Future Directions. Modern research is exploring several avenues to strengthen lightweight chaotic encryption without compromising speed [87]:

- **Deep Learning and Chaos Hybrids:** Integrating lightweight neural modules that adapt chaotic parameters in real-time to enhance security metrics while maintaining low computational overhead [89].
- **Multiple Chaotic Map Fusion:** Using fusion or switching between multiple low-dimensional maps to mitigate individual map weaknesses and extend effective key spaces [88].
- **Adaptive Block-Level Substitution:** Dynamically generating small S-boxes using chaos for block-level substitution, aiming to achieve stronger nonlinearity on a per-block basis without large memory or computation costs [87].
- **Quantisation-Aware Chaos Design:** Developing chaotic map implementations and parameter spaces that are robust under reduced-precision environments typical of embedded hardware [95].

In summary, lightweight and real-time chaos-based image encryption designs represent a vital research frontier, balancing performance and security [89]. While significant advances have been made, particularly in achieving high throughput on constrained platforms, the alignment of such designs with rigorous cryptanalytic standards remains an ongoing challenge, one that future research must address to enable secure real-time image protection in emerging application domains.

5.6. Comparative Analysis of Image Encryption Architectures

Having explored a diverse array of chaos-based image encryption frameworks, from simple pixel permutation to hybrid DNA–chaos schemes and lightweight real-time designs, it is essential to synthesise these architectures under common security and performance criteria. A comparative analysis not only highlights the strengths and limitations of each family but also reveals underlying trends, common pitfalls, and opportunities for future advancement. In this subsection we systematically examine the major architectural variants along multiple axes including security robustness, computational complexity, implementation cost, and suitability for different application domains [91].

Criteria for Comparison. To provide a fair and meaningful comparison, we adopt the following evaluation dimensions grounded in both cryptographic theory and practical requirements:

- **Confusion–Diffusion Balance:** Measures how effectively an architecture disrupts spatial correlations (confusion) and propagates small changes across ciphertext pixels (diffusion) [92].
- **Nonlinearity and Cryptanalytic Resistance:** Assesses the ability to resist classical attacks (differential, linear, algebraic) based on cryptographic metrics such as entropy, nonlinearity, and differential uniformity of substitution components [93].
- **Key Sensitivity and Key Space:** Evaluates how sensitively encryption responds to small key changes and whether the effective key space is large enough to deter brute-force search [94].
- **Computational Efficiency:** Considers processing speed, memory footprint, and suitability for real-time or constrained environments [95].
- **Implementation Practicality:** Takes into account hardware friendliness, parallelism support, and ease of integration with existing multimedia pipelines [96].
- **Empirical Security Outcomes:** Includes observed properties in ciphertext such as histogram uniformity, pixel correlation coefficients, and resistance against known-plaintext or chosen-plaintext attacks [97].

The comparative insights presented here are grounded in recent experimental and analytical studies of chaos-based encryption designs. While statistical measures like entropy and NPCR/UACI appear frequently in the literature, we emphasise deeper cryptanalytic relevance where available because statistical randomness alone does not guarantee robust security [91].

Permutation-Only vs. Permutation–Diffusion. Permutation-only schemes, though conceptually simple and computationally lightweight, consistently fall short on diffusion and resistance to chosen-plaintext attacks (see Section 5.2). Permutation–diffusion frameworks address this by adding value mixing, often employing chaotic sequences and, in advanced designs, S-boxes to introduce nonlinearity. The latter substantially improves confusion–diffusion balance and resists simple analytical attacks, at the cost of added complexity [98].

Standard Permutation–Diffusion with XOR vs. Chaotic S-Box Integration. Traditional permutation–diffusion designs often use XOR operations with chaotic sequences for diffusion. While these designs perform well on statistical tests (entropy, histogram flattening), they can remain vulnerable to differential cryptanalysis due to limited nonlinearity in XOR operations alone. Integrating chaotic S-boxes, either static or dynamic, elevates nonlinearity, enhances avalanche effects, and reduces exploitable differential trails. However, S-box generation increases computational load and memory usage. Dynamic S-boxes further increase resistance but also raise implementation complexity and the risk of weak key instances if generation is not well conditioned [99].

Hybrid Architectures (e.g., DNA–Chaos). Hybrid schemes that combine chaos with DNA encoding or other algebraic transformations introduce rich symbolic complexity that can dramatically increase the confusion–diffusion interaction. These architectures often achieve superior cipher metrics (e.g., high entropy, low correlation, large effective key space) and strong statistical attack resistance. Yet, they

also incur higher computational and operational costs, including overhead from encoding/decoding and managing multiple chaotic maps. Moreover, ensuring cryptanalytic strength requires careful design of rule sets and chaos-parameter mapping to avoid exploitable patterns in DNA operations [100].

Lightweight and Real-Time Schemes. Lightweight designs prioritise throughput and resource efficiency, making them suitable for embedded or real-time applications. These schemes typically reduce rounds, simplify substitution (e.g., micro-S-boxes or XOR masks), and use low-dimensional chaotic maps to minimise arithmetic cost. While they achieve impressive performance metrics, their security often lags behind full-featured permutation–diffusion designs, particularly against sophisticated attacks that exploit structure in simplified substitution and limited diffusion paths [95].

Key Observations from Comparative Evaluations.

- **Security vs. Complexity Trade-off:** There is an inherent trade-off between cryptographic strength and computational efficiency. Advanced schemes with dynamic S-boxes or DNA hybridisation provide stronger resistance to attacks but demand more processing power and memory, which may be impractical for constrained devices [92].
- **Importance of Nonlinearity:** Designs that rely solely on permutation and XOR diffusion suffer compared to those that integrate nonlinear substitution components. Nonlinearity, as assessed by S-box metrics, markedly improves resistance to linear and differential attacks [93].
- **Finite Precision Effects:** Many chaotic designs show performance degradation when implemented with finite precision arithmetic in hardware or software, leading to reduced effective key space and repeated cycle patterns unless mitigated by robust parameter mapping and perturbation techniques [97].
- **Empirical vs. Cryptanalytic Validation:** Statistical tests alone, such as entropy or NPCR/UACI, are insufficient to establish security. Schemes that demonstrate resistance to formal cryptanalytic attacks in addition to statistical robustness are comparatively rare but critically important [91].
- **Adaptability and Scalability:** Hybrid schemes are more adaptable to varying security requirements (e.g., by adjusting DNA rule complexity or S-box dynamic behaviour), whereas lightweight schemes prioritise scalability and low overhead. Each category serves different application domains depending on threat models and resource constraints [94].

6. Cryptanalysis and Security Assessment

Evaluating image encryption schemes, especially those based on chaotic systems and substitution mechanisms, requires more than reporting desirable statistical properties such as entropy, correlation, and histogram uniformity. True security assessment rests on how well a cipher withstands formal cryptanalytic attack models that adversaries can realistically mount. In this section we introduce the principal attack models used in image cryptanalysis, explain their implications, and illustrate how chaos-based designs perform under each paradigm. This discussion frames the deeper security challenges that chaos-derived S-boxes and permutation–diffusion architectures must confront [101].

6.1. Attack Models in Image Encryption

Security evaluation in image encryption largely mirrors classical cryptanalysis, but with adaptations for the unique nature of visual data. Three widely accepted attack models are:

- **Ciphertext-Only Attack (COA)**
- **Known-Plaintext Attack (KPA)**
- **Chosen-Plaintext Attack (CPA)**

Understanding these models helps clarify the expectations and limitations of proposed encryption schemes [102].

6.1.1. Ciphertext-Only Attack. In a ciphertext-only attack, the adversary has access exclusively to one or more ciphertext images without knowledge of corresponding plaintexts or encryption keys. This represents the weakest adversarial vantage point but is still significant for evaluating security in environments where ciphertext can be intercepted.

From a practical standpoint, resisting COA means that ciphertext alone should not reveal useful information about the plaintext or the key. For images, this specifically includes:

- **Histogram indistinguishability:** Cipher images should exhibit flat histograms that do not reveal intensity patterns inherited from the plaintext. Early permutation-only schemes fail this criterion because they do not alter pixel values, preserving histogram shape and enabling statistical inferences [103].
- **Low correlation among adjacent pixels:** Natural images show strong spatial correlation; a secure cipher should disrupt this, even when only ciphertext is available. Chaotic permutation–diffusion architectures with substitution generally achieve this, but XOR-only schemes may satisfy this superficially while still leaking structure under formal analysis [104].
- **Entropy close to theoretical maximum:** High entropy in the ciphertext distribution indicates unpredictability. While often reported, entropy alone is insufficient, but combined with other metrics, it supports COA resistance [105].

Because COA assumes no access to plaintext, schemes that merely satisfy statistical criteria without underlying diffusion/substitution mechanisms are often vulnerable to reconstruction heuristics or guesswork based on global image structure [102].

6.1.2. Known-Plaintext Attack. In known-plaintext attacks, the adversary has access to one or more pairs of plaintext images and their corresponding ciphertexts. This model is stronger than COA but realistic in scenarios where an attacker can observe or intercept both plain and encrypted versions (e.g., public image repositories or standard test images) [106].

KPA resistance requires that knowledge of plaintext–ciphertext pairs does not allow the adversary to derive useful key information or reconstruct unknown plaintexts. Chaos-based schemes with weak diffusion or static substitution layers often falter here:

- **Permutation leaks:** If the permutation mapping used is static or independent of key and plaintext, KPA can reveal the mapping which can then be inverted for other images encrypted with the same scheme [107].
- **Weak substitution structures:** Simple XOR diffusion without strong nonlinear substitution (e.g., S-boxes) leads to linear relationships between plaintext differences and ciphertext differences, enabling differential analysis [108].
- **S-box reuse vulnerabilities:** Static S-boxes used repeatedly across images or rounds can be profiled by an attacker to approximate their behaviour, facilitating recovery of key fragments [109].

Studies have shown that many chaotic image ciphers claiming security fail under KPA because they report only statistical results without demonstrating structural resistance to correlation analysis [101]. This highlights the need to evaluate chaos-based schemes with attack frameworks rather than heuristic metrics alone.

6.1.3. Chosen-Plaintext Attack. Chosen-plaintext attacks represent one of the most powerful adversarial models commonly considered. Here, the adversary can submit arbitrary plaintexts for encryption and observe the resulting ciphertexts [110]. This model is particularly relevant when encryption is offered as a service (e.g., secure imaging APIs), or when multi-stage ciphers expose oracle access.

Resistance to CPA requires a design that prevents extraction of key or substitution structure even when the adversary can tailor inputs:

- **Differential analysis complexity:** CPA allows an adversary to craft specific input differences to probe how the encryption process transfers these differences to ciphertext. Substitution layers must therefore minimise high-probability differentials, something classical chaos-only designs with XOR diffusion struggle to achieve [111].
- **Dynamic key/chaoic parameter coupling:** If the encryption parameters (e.g., chaotic seeds, S-box generation parameters) are independent of both plaintext and ciphertext, CPA can exploit static mappings. Designs that tie S-box generation or diffusion parameters tightly to plaintext (or its hash) can mitigate CPA, but must do so without undermining key secrecy [112].
- **Cryptanalytic key recovery:** In CPA, attackers can attempt to recover key material directly by querying the oracle with specially crafted inputs that simplify the diffusion chain, especially when substitution depth is shallow [113].

Modern cryptographic standards evaluate image encryption not just on heuristic statistical profiles but using CPA modelling because it better approximates what a real next-generation adversary might achieve. Recent research notes that many chaotic schemes that pass entropy or NPCR tests still succumb to CPA due to predictable substitution or limited diffusion depth [101].

Synthesis of Attack Model Impact. To summarise the relationship between attack strength and design requirements:

- COA mainly tests whether the ciphertext reveals low-level statistical information about plaintext. Satisfying COA tends to require strong diffusion and high entropy, but not necessarily nonlinear substitution.
- KPA probes structural weaknesses that statistical tests cannot capture. It requires substitution mechanisms and key-dependent transformations that are not deducible from a small set of plaintext–ciphertext pairs.
- CPA is the most stringent of the three, demanding deep nonlinear mixing and dynamic parameterisation to prevent an adversary from isolating key or substitution behaviour through carefully crafted inputs.

6.2. Differential and Statistical Attacks

In evaluating the security of image encryption schemes, and chaos-based designs in particular, analysts routinely apply differential and statistical attacks. These attack classes probe whether small changes in the input or structural patterns in the ciphertext can be exploited to reveal hidden information about the plaintext or key. Unlike formal algebraic or linear attacks, differential and statistical methods often leverage observable properties such as histogram distributions and pixel correlations to mount attacks that may be practical in real-world scenarios [135].

6.2.1. Histogram Analysis. Histogram analysis examines the frequency distribution of pixel values in an image. In a plain image, the histogram typically exhibits distinct modes and patterns reflecting the structure and content of the scene. A secure encryption scheme should transform these patterns into a uniform distribution that bears little resemblance to the original histogram. This flattening defends against ciphertext-only analysis by denying adversaries statistical cues about the underlying image content [114].

Early chaos-based image encryption schemes without diffusion or nonlinear substitution often fail this test: permutation-only designs, for example, preserve the histogram of the plain image since only pixel positions are altered, not their values. Even some permutation–diffusion approaches that rely solely on additive mixing (e.g., XOR with chaotic sequences) can exhibit residual histogram structure if the chaotic sequence is not uniformly distributed or if the mixing operation does not fully mask value patterns [115].

Histogram uniformity is typically quantified using metrics such as histogram variance or chi-square tests, and a flat histogram is interpreted as high entropy and unpredictability. However, histogram flatness alone is not a proof of security: many weak ciphers, including linear feedback systems, can produce

approximately uniform histograms while remaining vulnerable to more powerful analytical attacks [114]. Therefore, histogram analysis is a necessary first screening but not sufficient to declare a scheme secure.

For chaotic schemes with S-boxes, histogram uniformity can improve compared to XOR-only diffusion because nonlinear substitution spreads pixel value changes across the output space more thoroughly [116]. However, careful evaluation is required to ensure that histogram flattening is not merely superficial, i.e., that it co-occurs with genuine diffusion and resistance to differential propagation.

6.2.2. Correlation Analysis. Natural images contain high correlation among adjacent pixels in both horizontal and vertical directions. A secure image cipher must reduce this correlation to near zero in the ciphertext, indicating that neighbouring pixel values no longer provide useful predictive information [118].

Correlation is often measured using the correlation coefficient between adjacent pixels:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{\operatorname{var}(x)\operatorname{var}(y)}},$$

where x and y are the values of two adjacent pixels. In plain images, r_{xy} typically approaches values near 0.9 or higher, reflecting strong structural redundancy. Well-designed encryption should reduce r_{xy} to values close to zero (or even negative), indicating robust decorrelation [115].

Chaos-based schemes that incorporate both permutation and nonlinear substitution are generally capable of achieving low ciphertext correlation. For example, studies have shown that permutation–diffusion frameworks with dynamically generated chaotic S-boxes consistently produce correlation coefficients near zero for horizontal, vertical, and diagonal pixel pairs, outperforming simple XOR diffusion methods [117]. This decorrelation is a direct result of the combined effects of position scrambling and value transformation through nonlinear substitution.

6.2.3. Differential Attack Metrics: NPCR and UACI. Beyond histogram and correlation, two specialised metrics, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI), are widely used to quantify how sensitive a cipher is to small changes in the plaintext. These metrics are particularly relevant under differential cryptanalysis models such as chosen-plaintext attacks [135].

- **NPCR** assesses the percentage of pixels in the ciphertext that change when a single pixel in the plaintext is altered. High NPCR values (close to 100%) indicate strong diffusion [115].
- **UACI** measures the average intensity difference between two ciphertext images corresponding to two plaintexts that differ in one pixel. High UACI values suggest large overall change sensitivity [115].

Many chaos-based encryption papers report NPCR and UACI statistics as evidence of strong differential resistance. However, while high NPCR/UACI values often correlate with good diffusion, they should not be interpreted as proofs of resistance against chosen-plaintext attacks without corresponding structural analysis of the substitution layer and dynamic behaviour of chaotic sequences [116].

6.2.4. Link between Statistical Measures and Cryptanalytic Robustness. It is tempting for designers to equate strong statistical profiles, uniform histograms, near-zero correlation, high NPCR/UACI, with true cryptographic strength. However, several cautionary observations arise from both theoretical analysis and empirical studies [135]:

- **Statistical Indicators versus Attack Models:** Satisfying statistical tests is necessary but not sufficient for security. A scheme may pass all statistical criteria yet be vulnerable to differential or algebraic attacks if the underlying substitution structure is predictable or if the chaotic map collapses due to finite-precision effects [115].
- **Replayability of Chaotic Sequences:** Finite precision and limited chaotic parameter spaces can produce repeated patterns in chaotic sequences, causing similar histogram and correlation outcomes across different images or encryption runs, an undesirable property that weakens security [119].

- **Misleading Metrics:** Case studies in the literature demonstrate that high NPCR/UACI figures can co-exist with structural vulnerabilities exploitable under chosen-plaintext attacks. For example, XOR-dominant diffusion can yield good NPCR values but still permit differential cryptanalysis due to linearity [116].
- **Combination with Substitution Layers:** The integration of chaotic S-boxes generally improves statistical profiles and decorrelation; however, the effectiveness depends critically on the quality of the S-box (nonlinearity, differential uniformity) and its dynamic behaviour across rounds and keys [117].

Empirical Evidence from Literature. Comparative studies reveal that permutation–diffusion schemes with dynamic chaotic S-boxes typically outperform simpler designs on statistical evaluations. For instance, recent works report correlation coefficients near zero over large test image sets and NPCR/UACI metrics that exceed benchmark thresholds [116]. Nonetheless, closer cryptanalytic scrutiny, especially under chosen-plaintext conditions, often mitigates the confidence one might place solely on these figures [135].

In summary, while histogram and correlation analysis remain important tools for initial screening of image encryption schemes, they must be complemented with deeper cryptanalytic evaluation. Statistical measures provide necessary but not sufficient evidence of security, and designers must ensure that substitution layers, chaos parameterisation, and finite-precision implementation are all considered when assessing resistance to differential and statistical attacks.

6.3. Finite Precision and Chaos Collapse Attacks

One of the fundamental assumptions underpinning chaos-based cryptographic designs is that chaotic maps, by virtue of their sensitive dependence on initial conditions and complex dynamical behaviour, can act as strong sources of pseudo-randomness. However, when chaotic maps are implemented in real computing environments, whether in software, firmware, or hardware, they operate under finite precision arithmetic rather than ideal real numbers. This discrepancy between mathematical theory and digital reality can cause chaos collapse, where the rich behaviour expected of a chaotic system degenerates into short cycles, periodic orbits, or predictable structures. These phenomena have profound implications for the security of image encryption schemes that rely on chaos for randomness and key dependence [140].

Digital Implementation of Chaotic Maps. Chaotic maps such as the logistic, tent, or Henon map are defined in continuous mathematical spaces, where infinite precision allows orbits to explore attractors with dense structure. In contrast, digital computing uses finite representations, fixed-point, floating-point, or limited integer domains, which drastically reduces the size of the state space. In a finite domain, every chaotic map iteration must eventually repeat a value, leading to periodic or short-cycle behaviour rather than sustained chaos. This phenomenon is rigorously studied through frameworks such as state-mapping networks, which model every discrete state and its transition relationships; these networks exhibit highly regular, often scale-free structures that are very different from continuous chaotic attractors [120].

Because of this, digital chaotic sequences may:

- Fall into short cycles instead of large, pseudo-random orbits.
- Exhibit uneven distribution of values, limiting entropy.
- Generate repeated patterns across encryption runs with different plaintexts but similar seeds.

These effects are collectively referred to as chaos collapse or finite precision degradation and have undercut many chaos-based encryption proposals in the literature.

Chaos Collapse as a Cryptanalytic Concern. Finite precision effects expose two major vulnerabilities in chaos-based encryption:

- **Predictable Chaotic Sequences:** When a chaotic map degenerates into a short cycle, the sequence of values becomes predictable or repeatable after a relatively small number of iterations. Attackers can exploit this predictability to reconstruct keystreams or substitution sequences, undermining diffusion properties and enabling differential or known-plaintext attacks [121].

- **Key Space Reduction:** Chaos collapse effectively reduces the size of the usable state space. A map that should theoretically produce 2^n distinct states might yield only a small fraction of that in finite precision, drastically shrinking the effective key space and making brute-force or cycle-detection attacks tractable [122].

These vulnerabilities are not hypothetical: cryptanalytic studies have exploited finite precision weaknesses to break chaos-based ciphers. For example, early schemes using chaotic Baker maps or logistic maps were shown to be insecure when finite precision collapsed the state space, rendering encryption equivalents or repeated patterns that attackers could leverage [123].

Chaos Collapse in S-Box Generation. When chaotic maps are used to generate substitution boxes (S-boxes) or keystreams, finite precision degradation can directly impact cryptographic strength:

- Limited S-Box Diversity: Short chaotic cycles may generate a relatively small set of possible S-box instances, increasing the risk that attackers can guess or reconstruct them through limited samples [124].
- Statistical Biases: Digital chaos sequences may produce biased distributions over finite fields, leading to substitution patterns that deviate from ideal uniformity and exhibit exploitable regularities [140].
- Correlation in Substitution: Because chaotic sequences are used repeatedly, their collapse may induce correlation in substitution rounds, weakening the avalanche effect and reducing resistance to linear and differential cryptanalysis [120].

Thus, secure chaotic S-box design must address these collapse phenomena through careful numeric design, such as perturbation strategies or multi-map mixing.

Countermeasures against Chaos Collapse. Recognising the risk of finite precision attacks, recent research has proposed several countermeasures to preserve chaotic behaviour or compensate for collapse:

- Perturbed or Hybrid Maps: By introducing controlled perturbations (e.g., error feedback, additional offset terms), designers can increase the effective cycle length and disrupt short periodic behaviour [125].
- Use of Higher-Dimensional Maps: Maps with multiple positive Lyapunov exponents and higher complexity (e.g., 3D or hyperchaotic systems) can exhibit richer digital behaviour, even in finite precision, though they are not immune to collapse without additional design safeguards [126].
- Quantisation-Aware Mapping: Some schemes deliberately integrate finite precision effects into chaotic sequence generation, using error evolution as part of a controlled pseudo-random sequence generation procedure, thereby turning a weakness into an unpredictable feature [127].
- Hash-Driven or Neural Control: Hashing the plaintext or using neural networks to regularise chaotic sequences can mitigate the repetition patterns caused by finite precision, though these strategies introduce extra complexity and must be analysed for cryptanalytic soundness [128].

While these mitigation techniques can improve digital chaotic behaviour, none fully replicate infinite-precision chaos; rather, they strive to produce sequences with large periods, low correlation, and high entropy suitable for cryptographic use [120].

Practical Cryptanalytic Outcomes. Chaos collapse not only threatens theoretical properties but has practical consequences. Several chaos-based image encryption schemes reported as secure under statistical testing have later been broken due to finite precision effects that allowed attackers to model or reconstruct pseudo-random sequences. These attacks often use limited known-plaintext or chosen-plaintext queries to infer the underlying collapsed cycles and then deduce subsequent values with high probability, thereby recovering plaintext or key information [123].

The existence of finite-precision and chaos collapse attacks underscores a central theme of this review: chaos in theory does not guarantee cryptographic security in practice. Designers must bridge the gap between ideal dynamical properties and their digital realisations through rigorous analysis, careful numerical design, and integration of classical cryptographic safeguards [140].

6.4. Key Space, Key Sensitivity, and Equivalence Issues

A secure image encryption system must not only withstand cryptanalytic attacks (as discussed in Sections 6.1–6.3) but also ensure that its key management properties, including key space size, key sensitivity, and absence of equivalent or weak keys, do not undermine overall security. Chaos-based systems derive part of their appeal from the sensitive dependence on initial conditions, yet in practice, digital implementations often fall short when these properties are rigorously examined. In this subsection we examine key space requirements, the importance of key sensitivity for resisting brute-force and differential attacks, and the challenges posed by key equivalence and weak key classes [129].

Key Space Requirements. The key space of an encryption scheme is the set of all possible secret keys; its size determines the effort required for exhaustive key search (brute-force attack). Standard cryptographic practice demands that the effective key space be large enough to make brute-force impractical, generally on the order of 2^{128} or larger for contemporary security levels [130].

In chaos-based image encryption, keys typically consist of initial conditions and control parameters of chaotic maps, sometimes combined with hash outputs of the plaintext or auxiliary secret values (e.g., DNA encoding rules). While chaotic maps posit large theoretical parameter spaces (e.g., real values in continuous intervals), finite precision digital implementations collapse this space dramatically. When chaotic parameters are quantised into floating-point or fixed-point representations, the effective number of distinct states may be orders of magnitude smaller than claimed if parameter ranges, quantisation methods, or mapping functions are not carefully designed. This reduction exposes the system to brute-force search that is more feasible than theoretical claims suggest [131].

For example, if a 64-bit floating-point representation is used for initial conditions but only 32 bits are meaningfully random due to quantisation constraints or poor key generation algorithms, then the effective key space may be closer to 2^{32}, trivial to exhaust with modern hardware. In chaos-based S-box generation, similar reduction occurs if chaotic sequences or control parameters are sampled with limited precision, collapsing the number of distinct substitution tables that can be produced.

Key Sensitivity and Avalanche Effects. A hallmark of strong cryptographic systems is high key sensitivity, which means that even a single-bit change in the key should produce a dramatically different ciphertext for the same plaintext. This property ensures that attackers cannot infer small differences in keys from related ciphertexts and that key recovery via differential techniques is impractical.

In chaos-based encryption, sensitivity to initial conditions is often equated with key sensitivity. However, such equivalence holds only if:

- The chaotic map's sensitive dependence survives digital quantisation and finite precision.
- The mapping from chaotic states to encryption primitives (e.g., permutation vectors, S-box entries) preserves that sensitivity.
- The entire encryption pipeline conveys this sensitivity through both confusion and diffusion stages.

Studies have shown that many schemes claiming high key sensitivity in fact exhibit clusters of similar keys that produce correlated or partially overlapping keystreams due to quantisation effects and limited parameter ranges. In such cases, an adversary could leverage differential comparisons between closely related keys to prune the search space significantly [132].

Equivalent and Weak Keys. Key equivalence occurs when different keys produce the same or effectively indistinguishable encryption behaviour. This phenomenon reduces the effective key space because equivalent keys collapse multiple key values into a single effective encryption mapping. Key equivalence can arise in chaos-based designs when:

- Chaotic map parameter combinations map to the same quantised seed.
- S-box generation algorithms produce identical substitution tables for different initial parameters due to collisions in the chaotic generation process.

- Hash functions or key-expansion routines truncate or fold different key seeds into the same round subkeys.

The existence of equivalent keys effectively shrinks the search space and may enable attackers to mount key clustering attacks, where they identify equivalence classes rather than individual keys [133].

Furthermore, weak keys, keys that generate poor chaotic sequences, weak S-boxes, or predictable diffusion behaviour, can worsen security. Weak keys often occur at parameter values where chaotic maps exhibit windows of periodicity or near-periodic behaviour under finite precision. For example, logistic maps have well-studied parameter ranges that generate non-chaotic behaviour if the control parameter is outside a chaotic interval; in finite precision, these windows can be amplified. If key selection algorithms do not avoid these regions rigorously, the cipher may inadvertently allow weak keys that degrade resistance to both brute-force and structural attacks [134].

Strategies to Ensure Large and Effective Key Space. To address key space and key sensitivity issues, contemporary research suggests multiple best practices:

- **High-Precision Initialisation:** Use large fixed-point or arbitrary-precision arithmetic to represent chaotic parameters, increasing the number of distinct states that chaotic maps can assume before cycling occurs [129].
- **Hybrid Key Derivation:** Combine chaotic parameters with cryptographically strong key derivation functions (KDFs) such as SHA-3 or HKDF to map user-supplied keys into high-entropy seeds for chaos, thereby mitigating quantisation bias [130].
- **Parameter Verification:** Exclude chaotic parameters that fall into periodic or poorly chaotic regions through bifurcation analysis or Lyapunov exponent checks, ensuring that initial keys lie in regions of strong chaos [133].
- **Subkey Diversification:** Use expanded key schedules that derive round keys distinctly to avoid key equivalence and repetition across rounds or blocks [131].

These strategies must be implemented with care: ensuring that high precision does not introduce performance bottlenecks, and that any additional cryptographic primitives (e.g., hash functions) are integrated securely without inadvertently leaking information about the key.

Empirical Studies and Observed Weaknesses. Empirical cryptanalytic evaluations of chaos-based image encryption schemes have documented key space issues in numerous designs. For example:

- Schemes that claim large key spaces based on chaotic maps were shown to have dramatically smaller effective key spaces when quantisation and finite precision were accounted for in practical implementations [129].
- Key sensitivity tests performed on dynamic S-box schemes revealed clusters of keys producing correlated substitution tables or keystreams, weakening the credo of chaos-induced sensitivity [132].
- Cryptanalysis under chosen-plaintext scenarios exploited equivalent key classes to reduce search complexity and recover plausible keys more rapidly than brute-force predictions [134].

These findings underscore that key space and key sensitivity analyses are not optional supplements to security evaluation; they are core requirements for any encryption scheme intended for real deployment.

Summary and Best Practices. In summary, a robust image encryption system, chaotic or otherwise, must ensure that:

- The effective key space is sufficiently large under real digital precision constraints.
- Small changes in keys produce large, unpredictable changes in the ciphertext (high key sensitivity).

- Equivalent and weak keys are identified and eliminated through careful parameter selection and key schedule design.

Failure in any of these areas dramatically increases vulnerability to brute-force and structural attacks, regardless of the strength of the underlying chaotic sequences or substitution mechanisms.

6.5. Over-Reliance on Statistical Metrics

A pervasive issue in chaos-based image encryption research is the over-reliance on statistical metrics, such as histogram uniformity, entropy, Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI), as evidence of security. While these metrics are useful for initial screening and experimental benchmarking, they do not, on their own, guarantee resistance to cryptanalytic attacks. This section examines the limitations of commonly reported statistical measures and explains why conflating them with security against real attack models can be misleading [135].

Entropy: What It Measures, and What It Does Not. Entropy quantifies the unpredictability of pixel values in the ciphertext. A high entropy value, approaching the theoretical maximum of 8 bits per pixel for 8-bit grayscale images, is often cited as evidence that an image cipher has effectively masked plaintext content [136]. Indeed, chaotic substitution and permutation schemes typically produce ciphertexts with entropy values near or above 7.99 in empirical experiments.

However, high entropy does not imply cryptographic security because:

- Entropy measures the distribution of pixel values, not the resistance to key recovery or structural attacks [136].
- Many trivial transformations (e.g., strong XOR with a pseudorandom mask) can achieve high entropy without providing meaningful resistance to chosen-plaintext or differential attacks [137].
- Entropy says nothing about relationships between adjacent pixels or higher-order structures that cryptanalysts exploit in known-plaintext or chosen-plaintext scenarios [138].

In summary, entropy provides a useful check for overall randomness but should not be regarded as a stand-alone security metric.

NPCR and UACI: Designed for Sensitivity, Not Security Proofs. The NPCR and UACI metrics were introduced to measure the sensitivity of the cipher to small changes in the plaintext [139]:

- **NPCR** quantifies the proportion of pixels that change in the ciphertext when a single plaintext pixel is changed.
- **UACI** measures the average intensity difference between two ciphertexts corresponding to plaintexts that differ by one pixel.

High NPCR and UACI values—often reported near established thresholds (e.g., NPCR $> 99\%$ and UACI $\approx 33\%$)—are interpreted as indicators of diffusion strength [135].

Nevertheless:

- NPCR and UACI are empirical metrics that measure sensitivity in specific test cases; they do not guarantee resistance to adaptive chosen-plaintext attacks where the adversary may craft inputs to exploit predictable diffusion paths [138].
- These metrics do not capture linear or algebraic structures within the cipher that can be exploited even when diffusion appears strong in pixel-exchange scenarios [137].
- NPCR and UACI are susceptible to overfitting: a scheme tuned to maximise these metrics on standard test images may still behave poorly on other image classes or under targeted attack conditions [139].

In practice, designers should treat NPCR/UACI as useful diagnostic tools, but not as substitutes for formal cryptanalytic evaluation.

Correlation and Histogram Metrics: Useful But Not Sufficient. Histogram uniformity and pixel correlation coefficients are also widely reported in chaos-based image encryption literature. A flat histogram indicates that ciphertext pixel value frequencies are approximately uniform, while near-zero correlation suggests that adjacent pixel values are decorrelated [136].

Although these properties are desirable, they suffer from similar limitations:

- **Histogram analysis** fails to identify structural correlations across larger pixel neighborhoods or frequency bands that may be exploitable by advanced statistical attacks [138].
- **Correlation reduction** can be achieved through simple permutation and XOR operations without true cryptographic security [137].

Thus, these statistical tests should be complemented by attack-based evaluations (e.g., resistance to linear/differential cryptanalysis), not used in isolation to claim security.

Empirical Evidence of Misleading Metrics. Several cryptanalytic studies have illustrated how reliance on statistical measures can be misleading:

- In some chaos-based designs, high NPCR and UACI scores were accompanied by predictable substitution patterns that enabled key recovery under chosen-plaintext attacks [139].
- Histogram flattening and decorrelation were achieved while the underlying chaotic sequence exhibited short cycles due to finite precision, meaning that ciphertexts could be reconstructed or predicted after repeated observations [140].
- Ciphers tuned to maximise statistical metrics on benchmark images were shown to fail under targeted cryptanalysis on non-standard images or crafted plaintexts that expose structural weaknesses [138].

These findings demonstrate that statistical metrics alone cannot substitute for rigorous security analysis that addresses real cryptanalytic models such as those discussed in Section 6.1 (ciphertext-only, known-plaintext, chosen-plaintext).

Towards More Meaningful Evaluation Frameworks. A more robust evaluation methodology for image encryption should integrate:

- **Formal cryptanalytic testing**, including linear and differential attack suites adapted for image data and chaos-based pipelines [135].
- **Algebraic analysis** of substitution structures (especially S-boxes) to assess resistance to linear, differential, and algebraic attacks [137].
- **Finite precision diagnostics** that model the real behaviour of chaotic maps under implementation constraints [140].
- **Benchmarking across diverse image datasets** beyond standard test images to avoid overfitting to particular statistical profiles [138].

By expanding evaluation beyond statistical measures such as entropy, NPCR, and UACI, designers and reviewers can obtain a more accurate picture of a cipher's true security properties.

Summary. In summary:

- Statistical metrics remain useful for initial screening of image encryption schemes.
- They do not guarantee security against structured attacks and should not be the sole basis for security claims.
- Proper cryptanalysis, including analysis under realistic adversary models and implementation constraints, is essential to validate the true security of chaos-based image encryption designs [135].

6.6. Summary of Reported Cryptanalytic Breaks

As chaos-based image encryption research has proliferated, so too has the scrutiny of proposed schemes under rigorous cryptanalytic evaluation. While many algorithms report strong statistical properties and high sensitivity to initial conditions, an increasing body of work demonstrates that such measures alone are insufficient, and that several chaos-driven schemes can be broken or significantly weakened in practice. This subsection synthesises notable cryptanalytic breaks reported in the literature, categorising them according to the type of vulnerability exploited and the attack model used. By doing so, we highlight common pitfalls in chaos-based designs and illustrate the importance of aligning security claims with formal cryptanalysis rather than superficial statistical tests [141] [151].

Breaks Exploiting Finite Precision and Chaotic Collapse. One broad class of cryptanalytic results targets the gap between theoretical chaos and digital implementation. Finite precision arithmetic frequently reduces chaotic maps to limited cycle behaviour, which attackers can leverage to reconstruct keystreams or substitution patterns. For example, research on schemes driven by logistic or Baker maps has shown that their effective state space collapses into short cycles under finite precision, enabling attackers to predict future chaotic states and recover plaintext with limited access [141].

Cryptanalysis of Permutation-Only Schemes. Permutation-only image ciphers have been consistently broken under simple attack models. Known-plaintext and chosen-plaintext attacks can recover the permutation vector by observing a small number of plaintext–ciphertext pairs; once the permutation is known, inversion becomes trivial. For instance, some chaos-based schemes using simple chaotic index maps have been broken using differential and chosen-plaintext methods that recover pixel mappings with very few queries [149].

Linear and Differential Cryptanalysis of XOR-Dominant Designs. Many early chaos-based permutation–diffusion designs used simple XOR mixing with chaotic keystreams for diffusion. Although such schemes often achieve high NPCR and UACI scores, they remain vulnerable to differential and linear cryptanalysis because XOR is linear over $\mathbb{F}_2$. Attackers can exploit this linearity by constructing differential trails that cancel XOR masking, effectively reducing the cipher to a permutation problem and enabling key or keystream recovery [141].

Breaks on Chaos-Derived S-Box Schemes with Structural Weaknesses. Some cryptanalytic efforts have focused specifically on chaos-based S-boxes. Analyses of proposed S-box constructions generated from chaotic sequences reveal poor cryptographic measures, enabling attacks that recover substitution behaviour under chosen-plaintext queries. For example, certain chaotic S-box based image ciphers were completely broken with only two chosen plaintexts, demonstrating the limited strength of poorly designed substitution layers [147].

Chosen-Plaintext and Adaptive Differential Attacks. In more sophisticated evaluations, chosen-plaintext attacks have been used to mount adaptive differential cryptanalysis on chaotic image ciphers. By selecting plaintext pairs that differ in controlled patterns, attackers can trace how differences propagate through permutation and substitution stages to infer dynamic key effects or equivalent encryption processes. Such attacks have successfully broken schemes based on both simple chaotic maps and hybrid dynamic constructions [141].

Key Equivalence and Weak Key Exploits. Closely related to finite precision issues, some cryptanalytic studies have identified equivalence classes of keys, distinct key values that produce identical or indistinguishably similar encryption behaviour. This effectively reduces the key space and enables attackers to search over equivalence classes rather than individual keys. Certain chaotic parameter-based schemes exhibit such weak mapping structures that make exhaustive search feasible within these classes [141].

Summary of Break Types.

6.7. Performance vs. Security Trade-Offs

A recurring theme in chaos-based image encryption research, and in cryptography more generally, is the tension between performance (efficiency) and security (cryptanalytic robustness). Designers must

balance the need for fast, low-resource encryption suitable for real-time or embedded applications against the demands of strong security guarantees that withstand modern attack models. This section critically examines how different design choices affect this trade-off in chaos-based architectures, drawing on empirical evaluations and comparative studies [151] [149].

Efficiency in Chaos-Based Designs. Chaos-based image encryption schemes are often appealing because they can be implemented with relatively simple arithmetic operations and low memory overhead. Many designs leverage low-dimensional chaotic maps (e.g., logistic, baker, tent maps) that iterate quickly and require minimal computational resources, making them suitable for real-time applications and resource-constrained devices such as the Internet of Things (IoT) and mobile platforms. In lightweight settings, schemes often prioritise fast permutation and basic diffusion operations, sometimes at the expense of substitution complexity. The resulting encryption and decryption speeds can be high enough to meet real-time throughput requirements [148].

However, performance gains must be viewed alongside the adequacy of security provided. Simple chaotic operations (e.g., pixel permutation or XOR diffusion) may achieve desirable performance metrics but often do not provide robust resistance against stronger cryptanalytic models such as chosen-plaintext or differential attacks, as discussed in Section 6. Overall, many schemes with high efficiency demonstrate good statistical profiles (entropy, correlation, NPCR/UACI), but these metrics alone do not ensure cryptanalytic strength [142].

Security Enhancements and Performance Costs. Introducing strong substitution mechanisms, such as chaotic S-boxes, higher-dimensional or hyperchaotic maps, and hybrid encryption layers, generally improves security by increasing nonlinearity and expanding the effective key space. For example, hybrid schemes that combine chaotic maps with well-studied block cipher structures like AES can achieve significantly higher resistance to statistical and differential attacks without unduly compromising speed. A recent comparative study found that hybrid Chaos-AES schemes provided stronger security than basic lightweight approaches while maintaining encryption speeds adequate for IoT use, demonstrating high NPCR (over 99.6%) and UACI (around 33.4%) with acceptable performance overhead [151].

On the other hand, security improvements often come at measurable cost:

- **Increased Computation:** Dynamic S-box generation, hybrid chaotic–block cipher integration, and multi-round diffusion increase the number of operations per pixel and require more cycles on constrained processors.
- **Memory and Bandwidth Overheads:** Substitution tables and multi-stage key schedules require additional memory and storage, which may be problematic in embedded systems.
- **Implementation Complexity:** More sophisticated security features demand careful implementation to avoid introducing vulnerabilities (e.g., through side channels or finite precision effects).

Thus, while robust chaos-based designs with advanced substitution and diffusion can rival traditional cryptographic frameworks in security, they shift the architecture toward higher computational cost.

Real-Time and Resource-Constrained Contexts. For real-time video, medical imaging, and IoT contexts, encryption schemes must deliver throughput compatible with data rates and latency constraints. Here, lightweight chaos-based algorithms have a clear advantage in terms of operational simplicity. Some adaptive designs, such as single-round schemes with smart chaotic operation selection, achieve competitive encryption quality with reduced rounds and minimal substitution overhead, offering a pragmatic compromise between speed and security [148].

Nevertheless, the performance advantage of lightweight methods must be weighed against their security limitations. Simplified diffusion and limited substitution often yield structures more vulnerable to differential cryptanalysis under adaptive attack models, even when statistical metrics are strong [142].

Empirical Comparisons in Literature. Comparative studies of various chaos-based image encryption schemes illustrate the diversity of trade-offs:

- Experimental evaluations show that although different chaos-based schemes often report similar statistical performance (entropy, correlation, NPCR, UACI), their underlying complexity and resistance to cryptanalytic attacks vary substantially, with more complex S-box and hybrid designs generally demonstrating stronger security at the cost of higher computational demand [151].
- Hybrid approaches combining block cipher primitives with chaotic components often occupy a middle ground: they provide strong security features (e.g., key space, nonlinearity) while leveraging some simplicity from chaos to reduce overall overhead compared to full block cipher implementations, making them attractive for moderate-resource devices [149].
- In highly constrained scenarios (e.g., hardware implementations or FPGA acceleration), variants that integrate chaotic maps with parallelism or optimized diffusion mechanisms demonstrate better trade-offs, delivering high throughput with acceptable security in practical settings [142].

These comparative insights underscore the importance of matching architectural choices to application requirements. Security-critical applications (e.g., medical imaging or satellite data encryption) cannot sacrifice cryptanalytic robustness for performance alone, while low-power or real-time systems may legitimately prioritise speed provided they operate under controlled threat models and, where necessary, augment encryption with additional protections such as authentication layers.

Design Guidelines for Balanced Trade-Offs. Based on the literature and empirical evaluations, several practical insights emerge:

- **Hybrid approaches** that incorporate both chaotic components and standard cryptographic primitives can leverage the strengths of both worlds, achieving balanced performance and security.
- **Dynamic substitution** and chaos-driven key scheduling improve security, but must be implemented judiciously to avoid undue complexity.
- **Hardware and parallelism optimisations** can alleviate the performance penalties introduced by strong substitution and multi-round diffusion, making high-security chaos-based encryption feasible in real-time contexts.
- **Threat modelling** should determine the acceptable trade-off: low-resource environments might adopt lighter schemes with additional safeguards, while high-assurance scenarios demand the more computationally intensive but secure designs.

In conclusion, the performance vs. security trade-off is not a binary choice but a spectrum of design options. Practitioners should adopt architectures that align with their target use case, ensuring that any performance gains do not inadvertently undermine cryptographic integrity.

6.8. Chaos-Driven vs. Algebraic S-Boxes

One of the most central debates in modern symmetric cryptography, and particularly in chaos-based image encryption, concerns the relative merits of chaos-driven S-boxes versus algebraically constructed S-boxes. Both paradigms aim to introduce nonlinearity and confusion into encryption pipelines, but they arise from fundamentally different design philosophies. This subsection critically compares these two approaches, examining their theoretical foundations, practical behaviours, strengths, and weaknesses within the context of cryptographic security and implementation efficiency [152] [148].

Algebraic S-Boxes: Cryptographic Foundations. Algebraic S-boxes are constructed with explicit reference to finite field algebra, Boolean function theory, and well-studied cryptographic criteria. A canonical example is the AES S-box, which is built using the multiplicative inverse in the finite field $\mathbb{F}_{2^8}$ followed by an affine transformation, a structure with proven resistance against linear and differential cryptanalysis and a high algebraic degree. Recent analyses of algebraic substitution layers in lightweight cryptography highlight the value of formal algebraic design in achieving strong resistance to both linear and differential attacks [147].

Algebraic constructions allow designers to reason formally about nonlinearity, differential uniformity, algebraic degree, and other critical metrics that influence resistance to linear, differential, and algebraic attacks. These properties are predictable and analysable, supported by decades of mathematical research in finite field theory and Boolean algebra. As a result, algebraic S-boxes typically have:

- High nonlinearity close to optimal bounds.
- Low differential uniformity (e.g., optimal or near-optimal DAP values).
- High algebraic degree, supporting resistance to algebraic attacks.
- No fixed points or short cycles, reducing structural weaknesses.

Because these constructions are driven by well-defined algebraic frameworks, they enjoy deep cryptanalytic validation and extensive tooling for analysis.

Chaos-Driven S-Boxes: Intuition and Practice. Chaos-driven S-boxes, by contrast, are constructed via mappings from continuous or discrete chaotic systems, such as logistic maps or piecewise-linear maps, into finite domains used for substitution tables. These designs are motivated by the intuitive unpredictability and sensitive dependence on initial conditions of chaotic dynamics. Studies on chaos-based S-box design note that while such constructions can deliver strong nonlinearity and complexity, they often suffer from higher differential uniformity and structural irregularities compared to algebraic counterparts [152].

Chaos-driven S-boxes have several appealing qualities:

- Dynamic key dependence: Small changes in chaotic seeds can produce different S-boxes, increasing diversity.
- Parallelism: Many chaotic iterations can be computed efficiently in parallel, supporting high throughput.
- Flexibility: Different maps and mapping strategies offer a broad design space.

However, chaos-driven S-boxes also face significant challenges rooted in their lack of algebraic structure. For example, quantisation and discrete implementation of chaotic maps can introduce non-bijectivity or uneven distributions in substitution tables, which are problematic for classical cryptanalysis where bijectivity and balanced output distribution are desirable for confusion strength [148].

Comparative Security Metrics. Several recent studies have empirically compared chaos-driven and algebraic S-boxes using standard cryptographic criteria:

- **Nonlinearity:** Algebraic S-boxes, especially those designed via finite field techniques or sophisticated optimization routines, often achieve higher nonlinearity than chaos-driven tables unless the latter are heavily optimized.
- **Differential Uniformity:** Algebraic constructions frequently reach lower DAP/DDT values, indicating stronger resistance to differential attacks, whereas many chaos-based S-boxes exhibit higher differential rates unless hybridised or combined with algebraic methods [152].
- **Bijectivity and Structural Strength:** Algebraic designs consistently achieve full bijectivity; some chaotic S-box constructions, particularly those without careful design, show lower bijectivity or incomplete mapping coverage, which can weaken confusion processes [148].

These comparative observations suggest that while chaos-driven designs offer flexibility and key variability, algebraic S-boxes generally hold stronger theoretical foundations for cryptanalytic resistance.

Dynamic vs. Static S-Boxes. One commonly cited advantage of chaos-driven S-boxes is their ability to be dynamic: a new S-box can be generated for each key or session, complicating attacks that rely on analysing a fixed substitution layer. While dynamic behaviour can be beneficial, it introduces implementation complexity and does not inherently guarantee strong cryptographic properties unless the generated tables satisfy rigorous metrics like nonlinearity and low differential uniformity [152]. In contrast, algebraic S-boxes are usually static but offer stable and well-understood substitution behaviour that supports systematic analysis and secure implementation.

Hybrid Approaches: Best of Both Worlds? Recognising the complementary strengths of chaos and algebraic design principles, many recent research efforts have proposed hybrid S-box constructions that use chaotic sequences to perturb or modulate algebraic foundations. For example:

- Chaotic perturbation of algebraic parameters in S-box generation.
- Use of chaos to dynamically select among multiple high-quality algebraic S-box templates.
- Chaos-assisted optimization of algebraic S-box entries to satisfy multiple cryptographic criteria simultaneously.

Recent evidence shows that such hybrid designs can achieve strong cryptographic metrics, including nonlinearity, DAP, and SAC, while preserving some key dependence and adaptability [143].

Implementation and Practical Considerations. From an implementation perspective, algebraic S-boxes benefit from well-established constant-time and side-channel hardened implementations that support secure deployment in hardware and software. Chaos-driven S-boxes, particularly dynamic ones, must account for potential timing and quantisation effects that can introduce side-channel leakage unless mitigated carefully [148].

Synthesis and Design Recommendations. Drawing on both paradigms, several design guidelines emerge:

- Use algebraic constructions as baseline S-box primitives when strong, provable cryptographic properties are required.
- Apply chaotic modulation or hybrid perturbation within algebraic frameworks to introduce key dependence and variability without sacrificing baseline security.
- Avoid relying solely on raw chaos-derived S-boxes without formal cryptographic evaluation, especially in high-assurance contexts.
- Evaluate dynamic S-box behaviour across multiple keys and implementations to ensure stability of cryptographic properties.

In conclusion, while chaos-driven S-boxes contribute valuable flexibility and dynamic behaviour to image encryption designs, algebraic S-boxes, or hybrids grounded in algebraic structure, provide stronger, more analyzable foundations for nonlinearity and cryptographic security.

6.9. Practical Deployability and Standard Compliance

While theoretical constructs and cryptanalytic evaluations are essential for assessing the security of chaos-based image encryption schemes, practical deployability remains a decisive factor in determining whether such schemes can be used in real-world systems. Practical deployability encompasses aspects including implementation feasibility, compliance with international standards, resistance to implementation-level attacks (e.g., side channels), and interoperability with existing communication infrastructures. This section critically evaluates chaos-based encryption in the context of practical deployment and standards compliance, with emphasis on pitfalls, successes, and areas requiring further engineering [152] [148].

Implementation Feasibility on Target Platforms. Chaos-based image encryption schemes have been implemented across a broad range of platforms, from desktop CPUs and GPUs to embedded microcontrollers and field-programmable gate arrays (FPGAs). The key advantage often cited for chaos-based methods is their relatively simple arithmetic (e.g., map iterations, bit-level permutations, table lookups), which can be attractive for constrained devices. However, practical deployment exposes several challenges [152]:

- **Precision Dependence:** Chaos algorithms typically rely on floating-point or high-precision states to approximate real chaotic behaviour. Many embedded platforms lack efficient floating-point units (FPUs), leading to increased cycle counts or software emulation overhead that undermines performance.
- **Memory Footprint:** Dynamic S-box generation and large lookup tables consume memory, which may exceed the limited RAM available on microcontrollers or IoT devices.
- **Parallelism Limitations:** While chaotic maps are inherently parallelisable, effective exploitation of parallelism (e.g., using SIMD or GPU cores) requires careful coding, which is non-trivial for dynamically generated structures like S-boxes.

Moreover, finite precision and state quantisation, essential for digital implementation, can fundamentally alter chaotic dynamics, as discussed in Section 6.3. Consequently, schemes that appear robust in theory may degrade or exhibit predictable behaviour in practice unless specifically engineered for the target architecture [148].

Resistance to Implementation-Level Attacks. A secure cipher in theory can fail catastrophically in practice if it is vulnerable to implementation-level attacks such as timing analysis, power analysis, electromagnetic emanation profiling, or fault injection. Such attacks exploit physical side channels rather than weaknesses in the mathematical model of the cipher. Implementation vulnerabilities often represent the most significant practical risks to encryption system security, since real-world deployments introduce numerous factors that can compromise theoretical algorithmic strength [144].

Chaos-based generation routines can be particularly vulnerable:

- Iterative chaotic maps may exhibit data-dependent control flow and variable timing if not carefully implemented in constant time, leaking information about seeds or intermediate states through timing side channels.
- Dynamic S-box generation can introduce memory access patterns that vary with the key, enabling cache-based side-channel leaks on modern processors.
- Hardware implementations on FPGAs and microcontrollers can exhibit power consumption patterns correlated to chaotic state transitions or map iterations, facilitating differential power analysis (DPA) attacks.

In contrast, many standard cryptographic primitives are designed with side-channel resistance in mind; constant-time S-box lookup tables and side-channel hardened modules are well documented in AES implementations, for example.

Standard Compliance and Interoperability. International standards such as those from the National Institute of Standards and Technology (NIST) and industry certification frameworks define criteria and test vectors for authenticated encryption, cryptographic hash functions, and key management protocols. Widespread adoption of encryption algorithms, particularly in regulated industries, often depends on compliance with such standards. Chaos-based image encryption schemes currently lack direct representation in mainstream standardisation efforts, and are not part of certified suites such as those found in NIST FIPS 140-3 or ISO/IEC benchmarks [145].

While hybrid proposals that integrate chaos with standardized primitives (e.g., AES) can inherit compliance indirectly, pure chaos-based ciphers typically:

- Are not part of certified algorithm suites (e.g., NIST FIPS 140-3, ISO/IEC 19790).

- Lack established test vectors and compliance tests needed for certification.
- Are not yet included in widely adopted protocol stacks (e.g., TLS, IPsec, CMS) without extensive adaptation.

This gap complicates the integration of chaos-based encryption into real communication systems, where compliance with legal and regulatory requirements is mandatory.

Interoperability with Existing Protocols. Real-world systems rarely operate in isolation; instead, they rely on interoperability with networking protocols, storage formats, and multimedia standards (e.g., JPEG2000 encryption profiles). While chaos-based encryption can be applied to raw pixel data, integrating it with standardized formats and protocols requires well-defined interfaces and compatibility layers. Embedding chaos-based encryption into existing codecs or messaging platforms demands careful coordination with authenticated encryption and key exchange protocols.

These integration challenges highlight that practical deployability entails more than algorithmic security; it necessitates ecosystem compatibility and developer tooling support.

Regulatory and Certification Considerations. Many industries require cryptographic modules to undergo formal certification (e.g., Common Criteria, FIPS 140-3). Chaos-based image encryption schemes, particularly those not grounded in well-analysed algebraic structures, face hurdles in certification because certification bodies generally expect algorithms with deep peer review and proven resistance to well-defined attack models [145]. Without such certification, deployment in commercial or regulated products can be restricted due to liability and compliance risks.

Engineering Best Practices for Deployability. To improve practical deployability and approach standards compliance, designers of chaos-based schemes should consider:

- **Adopting established cryptographic primitives**, such as AES S-boxes or standardized authenticated encryption modes, as building blocks, using chaos to augment rather than replace them.
- **Profiling and mitigating side channels** through constant-time implementation, masking, and hardware countermeasures.
- **Developing compliance test suites** and reference implementations that facilitate integration with standards certification efforts.
- **Providing clear interoperability specifications** for use in network protocols and multimedia formats.

In summary, while chaos-based image encryption offers intriguing theoretical advantages and potential performance benefits, its practical deployability and compliance with prevailing standards remain significant barriers that require comprehensive engineering and alignment with existing standards frameworks.

6.10. Key Observations from the Literature

Over the past decade, a substantial body of research has emerged on chaos-based image encryption, spanning direct chaotic permutations, permutation–diffusion frameworks, chaotic S-box integration, DNA-chaos hybrids, and lightweight real-time designs. While this diversity underscores the creativity of the research community, a careful review of the literature reveals a number of consistent patterns, recurring pitfalls, and broader insights that are critical for both researchers and practitioners. Here we synthesise the key observations emerging from our comparative analysis, emphasising trends that inform future design and evaluation of chaos-based cryptographic systems [146].

1. Statistical Metrics Are Overused but Misinterpreted. A pervasive pattern in the literature is the heavy reliance on statistical metrics, such as histogram uniformity, entropy, NPCR, UACI, and correlation coefficients, to establish the security of an image encryption scheme. Many papers report high scores on these metrics and present them as evidence of robustness. However, statistical properties alone do not guarantee resistance to structured cryptanalytic attacks; comprehensive surveys note that statistical evaluations alone are insufficient to demonstrate real cryptographic strength.

2. Chaotic Maps Without Cryptographic Foundation Can Be Misleading. Chaos theory's mathematical richness, sensitive dependence on initial conditions, ergodicity, and pseudo-randomness, appeals intuitively to cryptographers. However, many studies conflate chaotic behaviour with cryptographic security. Comprehensive reviews highlight that digital implementations drastically alter the dynamics of chaotic maps due to finite precision, resulting in periodic or predictable cycles that undermine pseudo-randomness unless explicitly addressed [146].

3. S-Box Quality Greatly Influences Overall Cipher Strength. From our analysis, notably in Sections 4 and 7.2, the quality of the substitution layer is one of the most critical determinants of security. Algebraically constructed S-boxes (e.g., AES-like tables) exhibit robust properties such as high nonlinearity and low differential uniformity, backed by decades of analysis. In contrast, many chaos-driven S-boxes, particularly those produced via naive quantisation or basic chaotic sequences, fall short on cryptographic criteria unless supplemented with optimisation techniques or algebraic scaffolding.

4. Dynamic S-Boxes Increase Complexity but Must Be Carefully Controlled. Dynamic or key-dependent S-box schemes are attractive because they vary with the secret key, making precomputation by attackers more difficult. However, literature analyses show that dynamic S-boxes can introduce implementation complexity and weak key classes when the mapping from keys to S-box instances is not cryptographically robust, potentially simplifying key recovery attacks.

5. Hybrid and Layered Designs Offer Balance but Demand Careful Integration. Hybrid designs, combining chaotic components with classical cipher primitives, appear frequently in recent studies. These approaches attempt to blend the perceived randomness of chaos with the proven structural strength of standard cryptographic elements such as AES or RC4 variants, often achieving better overall security characteristics with manageable performance overhead [147].

6. Real-Time and Lightweight Goals Drive Simplification, Sometimes at the Expense of Security. Lightweight and real-time image encryption schemes are often motivated by constraints in IoT and embedded environments. While these designs improve throughput, some sacrifice cryptographic robustness for performance, indicating the need for principled evaluation frameworks that balance throughput and security comprehensively [148].

7. Side-Channel and Implementation Vulnerabilities Are Understudied. Most chaos-based image encryption research focuses on algorithmic properties, with relatively little attention paid to implementation-level vulnerabilities such as timing analysis or power profiling. Cryptanalytic studies increasingly emphasize that theoretical designs must consider side channels to be practical for real deployments.

8. Standards and Interoperability Challenges Hinder Adoption. Chaos-based image encryption methods remain largely outside mainstream standardisation efforts, complicating their adoption in regulated industries and protocol ecosystems. Neither NIST nor ISO/IEC frameworks currently include chaotic primitives as certified cryptographic components, posing barriers to practical deployment [146].

9. Benchmarking Practices Are Inconsistent. The literature reveals inconsistent benchmarking practices: schemes are often compared using different image datasets, varying performance metrics, and non-uniform experimental setups. This inconsistency inhibits meaningful comparison and underscores the need for standardised evaluation frameworks that combine statistical, cryptanalytic, and performance metrics across diverse datasets.

10. Promising Directions Are Emerging. Despite these challenges, the literature points to promising trends: hybrid chaotic algebraic constructions that enhance substitution quality, adaptive chaos parameterisation strategies, and integration of deep learning for enhanced cryptographic design. These emerging directions suggest that chaos-based encryption, when grounded in rigorous cryptographic analysis, can evolve into robust and deployable technologies [149].

Summary. Synthesising decades of research yields a clear view: chaos-based image encryption is a vibrant and innovative field, but its practical and cryptographic maturity varies widely. The key observations above provide a roadmap for researchers: preserve rigorous security foundations, avoid overreliance on

superficial metrics, integrate chaos with algebraic strength where appropriate, and align design choices with real-world deployment constraints.

6.11. Provable Security for Chaos-Based Cryptography

One of the most critical open challenges in the field is the development of provable security frameworks for chaos-based cryptographic constructions. To date, the majority of chaos-enhanced image encryption schemes are evaluated primarily through empirical or heuristic methods, statistical testing, simulation, and limited attack models. While these evaluations provide valuable initial insights, they fall short of the rigorous assurances expected in modern cryptography, where schemes are typically vetted through formal security proofs under well-defined adversarial models. Recent reviews note that many chaos-based image encryption studies emphasise statistical metrics without incorporating formal cryptographic security models, limiting their theoretical guarantees [15].

Limitations of Current Evaluation Paradigms. Existing chaos-based evaluations often rely on measures such as entropy, histogram flatness, NPCR/UACI, and pixel correlation. Although these metrics assess properties related to randomness and diffusion, they do not directly correspond to standard cryptographic security notions such as indistinguishability under chosen-plaintext attack (IND-CPA) or indistinguishability under adaptive chosen-ciphertext attack (IND-CCA), nor do they provide bounds on resilience against algebraic, differential, or linear attack frameworks familiar in modern cryptography [15]. Without a formal security model that defines the capabilities of an adversary and the goal of the attack, assessing the strength of chaos-based schemes remains incomplete and cannot establish provable hardness akin to classical block ciphers.

Towards Cryptographic Formalisms. To address this gap, future research must focus on embedding chaos-based constructions within established cryptographic frameworks:

- **Reductionist Proofs:** Show that breaking a chaos-based scheme is at least as hard as solving a well-studied mathematical problem (e.g., discrete logarithm, decoding random linear codes). Reductionist proofs provide confidence that no efficient adversary exists without solving the underlying hard problem.

- **Game-Based Security Models:** Formulate clear game definitions (IND-CPA, IND-CCA) tailored to image encryption contexts and prove that chaos-based ciphers meet these goals under specified assumptions, as is common in authenticated encryption analyses.

- **Hybrid Cryptographic Chaos:** Integrate chaotic components with classical provably secure primitives (e.g., AES, SHA-3) in ways that preserve the security proofs of the underlying primitives while benefiting from chaos-derived features such as key sensitivity or dynamic behaviour [150].

These endeavours require careful attention to how chaotic maps are mapped to discrete domains, how keys influence both permutation and substitution layers, and how randomness (true or pseudo-) is modelled.

Challenges in Formalising Chaos. Chaos theory originates in dynamical systems over continuous real spaces, whereas cryptography is grounded in discrete algebraic structures. Translating chaotic behaviour into discrete representations with provable security properties presents several hurdles:

- **Digital Chaos Collapse:** Finite precision arithmetic undermines theoretical continuous chaotic dynamics, requiring security analyses that incorporate the resulting effective state space and periodicity effects.

- **Quantisation and Entropy Models:** Cryptographic proofs often assume idealised random oracles or uniformly distributed keys/keystreams. Real chaotic sequences disrupt these assumptions unless rigorously modelled; quantisation reduces entropy and introduces biases that proofs must consider.

- **Coupling with Data Structures:** In image encryption, plaintext structures (e.g., pixel dependencies) interact with chaos-driven components in complex ways, complicating entropy and indistinguishability arguments that treat images as arbitrary bitstrings.

Addressing these challenges will require interdisciplinary collaboration between chaos theorists and cryptographers, combining expertise from dynamical systems, algebraic cryptography, and information theory.

Promising Directions and Tools. Several research avenues and tools can support the development of provable security frameworks for chaos-based cryptography:

- **Game-based proof techniques** adapted from symmetric encryption literature can provide templates for evaluating chaos-based schemes under chosen-plaintext or chosen-ciphertext adversaries.
- **Entropy and min-entropy analyses** used in randomness extractors and cryptographic hash function proofs can be adapted to quantify the unpredictability of chaos-derived sequences in finite precision.
- **Computational complexity reductions** that map chaos generation problems to established cryptographic assumptions may help bridge the gap between heuristic unpredictability and provable hardness.
- **Formal verification tools** (e.g., ProVerif, CryptoVerif) can assist in mechanising parts of the security proofs, especially for combined chaos–algebraic constructions.

Impact on Future Image Encryption Design. Establishing provable security foundations for chaos-based encryption would have multiple benefits:

- It would elevate chaos-based designs from empirically appealing but theoretically informal constructs to cryptographically sound primitives accepted by the broader security community.
- It would enable rigorous comparison with classical ciphers like AES, allowing designers to make justified trade-offs between chaos-driven features and formal security guarantees.
- It would support standardisation efforts by providing well-defined security claims that can be evaluated in certification frameworks.

Concluding Remarks on Provable Security. Provable security remains an open frontier for chaos-based cryptography. While chaotic dynamics offer attractive properties, sensitivity, complex behaviour, pseudo-randomness, their security realisation in finite, discrete systems needs robust formal backing. Bridging this gap will be essential if chaos-based designs are to achieve broader adoption in high-assurance applications and standardised protocols. Future research that focuses on formal models, reductionist proofs, and hybrid constructions promises to give chaos-based cryptography the rigorous foundation it currently lacks.

6.12. Provable Security for Chaos-Based Cryptography

One of the most critical open challenges in the field is the development of provable security frameworks for chaos-based cryptographic constructions. To date, the majority of chaos-enhanced image encryption schemes are evaluated primarily through empirical or heuristic methods, statistical testing, simulation, and limited attack models. While these evaluations provide valuable initial insights, they fall short of the rigorous assurances expected in modern cryptography, where schemes are typically vetted through formal security proofs under well-defined adversarial models. Recent reviews note that many chaos-based image encryption studies emphasise statistical metrics without incorporating formal cryptographic security models, limiting their theoretical guarantees [15].

Limitations of Current Evaluation Paradigms. Existing chaos-based evaluations often rely on measures such as entropy, histogram flatness, NPCR/UACI, and pixel correlation. Although these metrics assess properties related to randomness and diffusion, they do not directly correspond to standard cryptographic security notions such as indistinguishability under chosen-plaintext attack (IND-CPA) or indistinguishability under adaptive chosen-ciphertext attack (IND-CCA), nor do they provide bounds on resilience against algebraic, differential, or linear attack frameworks familiar in modern cryptography [15]. Without a formal security model that defines the capabilities of an adversary and the goal of the attack, assessing the strength of chaos-based schemes remains incomplete and cannot establish provable hardness akin to classical block ciphers.

Towards Cryptographic Formalisms. To address this gap, future research must focus on embedding chaos-based constructions within established cryptographic frameworks:

- **Reductionist Proofs:** Show that breaking a chaos-based scheme is at least as hard as solving a well-studied mathematical problem (e.g., discrete logarithm, decoding random linear codes). Reductionist proofs provide confidence that no efficient adversary exists without solving the underlying hard problem.
- **Game-Based Security Models:** Formulate clear game definitions (IND-CPA, IND-CCA) tailored to image encryption contexts and prove that chaos-based ciphers meet these goals under specified assumptions, as is common in authenticated encryption analyses.
- **Hybrid Cryptographic Chaos:** Integrate chaotic components with classical provably secure primitives (e.g., AES, SHA-3) in ways that preserve the security proofs of the underlying primitives while benefiting from chaos-derived features such as key sensitivity or dynamic behaviour [150].

These endeavours require careful attention to how chaotic maps are mapped to discrete domains, how keys influence both permutation and substitution layers, and how randomness (true or pseudo-) is modelled.

Challenges in Formalising Chaos. Chaos theory originates in dynamical systems over continuous real spaces, whereas cryptography is grounded in discrete algebraic structures. Translating chaotic behaviour into discrete representations with provable security properties presents several hurdles:

- **Digital Chaos Collapse:** Finite precision arithmetic undermines theoretical continuous chaotic dynamics, requiring security analyses that incorporate the resulting effective state space and periodicity effects.
- **Quantisation and Entropy Models:** Cryptographic proofs often assume idealised random oracles or uniformly distributed keys/keystreams. Real chaotic sequences disrupt these assumptions unless rigorously modelled; quantisation reduces entropy and introduces biases that proofs must consider.
- **Coupling with Data Structures:** In image encryption, plaintext structures (e.g., pixel dependencies) interact with chaos-driven components in complex ways, complicating entropy and indistinguishability arguments that treat images as arbitrary bitstrings.

Addressing these challenges will require interdisciplinary collaboration between chaos theorists and cryptographers, combining expertise from dynamical systems, algebraic cryptography, and information theory.

Promising Directions and Tools. Several research avenues and tools can support the development of provable security frameworks for chaos-based cryptography:

- **Game-based proof techniques** adapted from symmetric encryption literature can provide templates for evaluating chaos-based schemes under chosen-plaintext or chosen-ciphertext adversaries.

- **Entropy and min-entropy analyses** used in randomness extractors and cryptographic hash function proofs can be adapted to quantify the unpredictability of chaos-derived sequences in finite precision.
- **Computational complexity reductions** that map chaos generation problems to established cryptographic assumptions may help bridge the gap between heuristic unpredictability and provable hardness.
- **Formal verification tools** (e.g., ProVerif, CryptoVerif) can assist in mechanising parts of the security proofs, especially for combined chaos–algebraic constructions.

Impact on Future Image Encryption Design. Establishing provable security foundations for chaos-based encryption would have multiple benefits:

- It would elevate chaos-based designs from empirically appealing but theoretically informal constructs to cryptographically sound primitives accepted by the broader security community.
- It would enable rigorous comparison with classical ciphers like AES, allowing designers to make justified trade-offs between chaos-driven features and formal security guarantees.
- It would support standardisation efforts by providing well-defined security claims that can be evaluated in certification frameworks.

Concluding Remarks on Provable Security. Provable security remains an open frontier for chaos-based cryptography. While chaotic dynamics offer attractive properties, sensitivity, complex behaviour, pseudo-randomness, their security realisation in finite, discrete systems needs robust formal backing. Bridging this gap will be essential if chaos-based designs are to achieve broader adoption in high-assurance applications and standardised protocols. Future research that focuses on formal models, reductionist proofs, and hybrid constructions promises to give chaos-based cryptography the rigorous foundation it currently lacks.

6.13. Lightweight Chaos-Based Encryption for IoT

The proliferation of the Internet of Things (IoT), where billions of devices operate with limited computing power, memory, and energy, has created an urgent need for encryption schemes that are both secure and lightweight. Traditional cryptographic algorithms (e.g., AES) are often too resource-intensive to meet the constraints of IoT endpoints such as sensors, wearable devices, and embedded systems. As a result, researchers have turned to chaotic systems and hybrid designs that leverage chaos theory's pseudo-randomness to develop encryption frameworks tailored for IoT environments [151] [152].

The Rationale for Chaos in IoT Security. IoT devices typically lack hardware support for complex cryptography and must operate under low latency and minimal energy budgets. Chaos-based encryption offers several properties that make it attractive in this context:

- **Low computational overhead:** Chaotic maps often involve simple arithmetic and iterative logic, which are inexpensive to compute compared to the round functions of block ciphers.
- **Pseudo-random behaviour:** The sensitive dependence on initial conditions endemic to chaotic systems can generate sequences with high apparent randomness, useful for key streams and permutation vectors.
- **Adaptable structures:** Chaos can be integrated with lightweight architectures, such as cellular automata or stream cipher constructs, to enhance confusion and diffusion without heavy resource use [153].

For instance, one recent lightweight chaotic encryption proposal targeting IoT radio and sensor networks demonstrated that combining a six-dimensional chaotic map with simple XOR diffusion and permutation achieves low execution time, near-zero pixel correlation, high entropy (8 bits per pixel), and strong differential metrics (NPCR 99.6%, UACI ¿33%) while remaining compatible with constrained hardware platforms [151].

Design Patterns in Lightweight Chaos-Based IoT Encryption. Several recurring design themes have emerged in the literature:

- **Chaotic map-driven permutation and diffusion:** Logistic, sine, Henon, or higher-dimensional maps generate pseudo-random sequences responsible for scrambling pixel positions and mixing values.
- **Hybrid DNA and chaotic frameworks:** Integrating DNA encoding with chaotic maps has been shown to balance high randomness, strong diffusion/confusion, and low memory footprint suited for IoT endpoints [152].
- **Cellular automata integration:** Combining chaotic maps with rule-based cellular automata yields efficient nonlinear transformations that can be realised with low gate count and minimal memory requirements [153].
- **Stream cipher and metaheuristic hybridisation:** Advanced frameworks have merged chaotic functions with metaheuristic optimisation, improving key generation randomness and balancing security with energy and computational constraints [15].

These patterns reflect an effort to achieve confusion and diffusion in ways that are compatible with the limited instruction sets and power budgets of IoT devices.

Evaluation Metrics and Performance Characteristics. Unlike traditional desktop or server environments, IoT devices demand metrics beyond security alone. Lightweight chaos-based schemes are therefore evaluated along multiple axes:

- **Execution time and throughput:** Schemes should encrypt typical IoT image payloads within milliseconds to support real-time or near-real-time applications.
- **Memory footprint:** Low RAM and flash usage is essential; many IoT devices have only kilobytes of usable memory.
- **Energy consumption:** Because many endpoints are battery-powered, encryption energy must be minimised.
- **Security metrics:** High entropy, near-zero adjacent pixel correlation, and differential resistance remain important, although these must be complemented with stronger cryptanalytic assessments [151] [152].

Evaluations of recent lightweight chaos-based algorithms have shown favourable results: entropy near 8 bits per pixel, correlation approaching zero, and NPCR/UACI figures that indicate strong diffusion, all achieved with minimal computational overhead compared to conventional block ciphers [151].

Challenges Specific to IoT Constraints. Despite promising properties, several practical challenges persist:

- **Finite precision degradation:** As noted previously, chaotic dynamics in digital systems may collapse into short cycles, reducing effective randomness unless carefully mitigated.
- **Key management:** IoT devices often lack secure key storage or robust key-exchange protocols, complicating the deployment of chaos-based schemes that assume high-entropy initial conditions.
- **Interoperability and standards:** Chaotic approaches are rarely recognised by lightweight cryptography standards (e.g., NIST's lightweight cryptography suite), making integration into certified systems harder.

These challenges indicate that while chaos-based designs can reduce computational cost, security must not be undermined for performance.

Case Studies and Recent Advances. Recent literature provides illustrative examples of lightweight chaos-oriented IoT encryption:

- A novel scheme combining chaotic maps with fuzzy logic and shift registers was implemented on 8-bit microcontrollers, demonstrating reduced encryption time, lower energy consumption, and improved network longevity compared to fixed-parameter ciphers (implementation results are consistent with broader lightweight chaos literature).
- Lightweight cellular automata and chaotic map hybrids have been proposed that perform well against differential and linear attacks while remaining suitable for embedded deployment [153].
- Hybrid quantum-chaotic frameworks incorporating discrete wavelet transforms and metaheuristic optimisation have been explored, achieving near-ideal entropy and low correlation while balancing encryption complexity and efficiency [15].

These efforts reflect a growing recognition that IoT image encryption must be context-aware, balancing resource constraints with rigorous security requirements.

Directions for Future Research. To advance chaos-based IoT encryption, future research should focus on:

- Incorporating formal security proofs that account for finite precision, quantisation, and practical attack models in low-resource settings.
- Developing standardised benchmarks tailored to IoT, incorporating both performance and cryptanalytic resilience.
- Investigating hardware optimisations such as dedicated chaos engines or lightweight accelerator instructions on microcontrollers.
- Designing adaptive key management protocols that support constrained devices without compromising security.

In conclusion, lightweight chaos-based encryption represents a promising direction for securing image data in IoT environments thanks to its adaptability and performance benefits. However, meeting the dual goals of robust security and practical efficiency remains an open research challenge that requires integrated solutions spanning algorithms, hardware, and standards.

6.14. Integration with Post-Quantum Cryptography

As quantum computing advances toward practical capability, conventional cryptographic primitives, particularly those relying on number-theoretic hardness assumptions, face existential threats from algorithms such as Shor's and Grover's. Emerging guidance from cybersecurity authorities underscores the urgency of preparing for post-quantum migration well before large-scale quantum hardware renders classical schemes insecure. Indeed, agencies like the UK's National Cyber Security Centre recommend starting PQC transition efforts by 2028 to safeguard against future "Q-day" threats [154] [152].

Chaos-based cryptographic systems, including those for image encryption, must therefore be evaluated in the context of post-quantum cryptographic (PQC) frameworks to ensure long-term security. Unlike symmetric primitives (e.g., AES) that retain strength with larger keys, asymmetric components such as key exchange and authentication must migrate to quantum-resistant constructions like lattice-based, code-based, or hash-based algorithms [152]. Integrating chaos-driven mechanisms with post-quantum standards presents both opportunities and challenges.

Hybrid Cryptographic Architectures. A promising strategy is to combine chaotic primitives for high-entropy sequence generation with standardised PQC mechanisms for key encapsulation and authentication. For example, the *CryptoChaos* framework integrates chaos-based key expansion with key exchange techniques that combine chaotic maps with classical and post-quantum secure mechanisms, demonstrating near-maximal Shannon entropy and enhanced resistance against quantum attacks [155].

Similarly, *PrivShield-CQ* demonstrates how hyperchaotic systems can supply high-entropy keying material alongside NIST-recommended PQC primitives such as module lattice key encapsulation mechanisms (ML-KEM) and lattice-based signature algorithms to achieve strong quantum resistance with improved latency and energy performance [151].

These hybrid designs leverage chaotic unpredictability for symmetric encryption and keystream generation, while entrusting asymmetric security and key management to PQC standards such as lattice-based key encapsulation mechanisms (e.g., Kyber) and lattice-based signatures (e.g., Dilithium) that have been selected or considered in NIST PQC standardisation efforts [152].

Chaos in Post-Quantum Randomness and Key Generation. Beyond hybrid encryption protocols, there is growing exploration of chaos-enhanced randomness sources for PQC and key generation. Classical pseudo-random number generators (PRNGs) are vulnerable to reverse-engineering and may exhibit statistical biases that degrade security; integrating chaotic dynamics with code-based cryptographic structures can improve statistical quality and randomness while aligning with post-quantum resilience goals [152].

Integrating quantum entropy sources (e.g., photon arrival times, vacuum fluctuations) with chaotic dynamics further extends this concept, fusing true quantum randomness with chaotic amplification to generate bit sequences with near-ideal entropy for cryptographic keying material and streaming applications. Such quantum chaotic random number generators (QRNGs) may offer robust seed material for both symmetric and PQC primitives, potentially mitigating finite precision collapse issues common in purely deterministic chaos.

Quantum Image Encryption and Chaos. While classical image encryption occupies most research activity, the emergence of quantum image encryption (QIE) highlights broader avenues for chaos in post-quantum contexts. QIE schemes, for example those based on NEQR (Novel Enhanced Quantum Representation) models, integrate chaotic key matrices within quantum circuits to effect quantum-native diffusion and permutation, achieving strong diffusion, high entropy, and low correlation in quantum imagery operations. These approaches suggest that chaos can play a role not only in post-quantum resistance but also in quantum-native cryptographic workflows that align with future quantum communication protocols.

Challenges and Future Directions. Despite the potential of chaos-PQC integration, several open questions remain:

- **Formal Security Models:** Hybrid schemes must be situated within rigorous post-quantum security models (e.g., IND-CCA for asymmetric PQC) that account for both chaotic components and quantum adversaries.
- **Standard Compliance:** Chaos-enhanced designs need clear pathways to compliance with NIST PQC standards and future ISO/IEC quantum security frameworks, which require formal specification and test vectors for certification.
- **Implementation Efficiency:** The performance cost of PQC (e.g., larger keys, heavier operations) must be balanced against chaos-driven efficiency, especially in IoT and real-time scenarios where resource constraints remain critical.
- **Quantum-Chaos Interactions:** Integrating chaos with quantum circuits introduces new complexity, determining how chaotic behaviour translates under quantum state evolution, and how to preserve desirable cryptographic properties in quantum contexts.

The integration of chaos-based mechanisms with post-quantum cryptography represents a compelling research frontier. By combining the dynamic unpredictability of chaos with the quantum hardness assurances of lattice-based and related schemes, future image encryption systems can be designed to resist both classical and quantum-era adversaries, offering a comprehensive security posture for long-term data protection.

6.15. Machine Learning and Adaptive Cryptographic Systems

As cryptography and artificial intelligence (AI) continue to mature, there is an emerging research frontier at the intersection of machine learning (ML), adaptive systems, and chaos-based encryption [156,157]. Integrating machine learning with cryptographic design, particularly in the context of chaos-driven image encryption, promises dynamic, data-aware, and self-optimising security mechanisms that can adapt to evolving threats and data characteristics [158]. This subsection examines key developments, methodologies, and research directions in ML-assisted and adaptive chaotic cryptographic systems.

Motivations for Machine Learning in Cryptography. Traditional cryptographic design emphasises fixed algorithmic structures with static substitution and diffusion layers. In contrast, machine learning models excel at capturing complex patterns and dependencies in high-dimensional data. Combining these strengths enables cryptosystems that can adapt their internal parameters (e.g., S-box entries, chaotic map seeds) based on data properties or threat models, potentially enhancing security without manual retuning [159]. Machine learning's capacity to optimise large design spaces also supports adaptive parameter selection in chaotic map setups, improving unpredictability and resisting static analysis [160].

For example, recent work on adaptive S-box optimisation uses neural networks to tailor substitution operations within a classical block cipher such as CAST-128 for image encryption [161]. The adaptive S-boxes are optimised to enhance nonlinearity and avalanche characteristics, and experimental results indicate improvements in resistance to statistical attacks compared to traditional static designs.

Machine Learning for Key and Parameter Generation. One early approach to ML integration in chaos-based systems uses deep neural networks to generate keys or chaotic parameters informed by image content or desired security properties [162]. For instance, research has demonstrated schemes where a deep convolutional neural network (CNN) takes image features as input to produce initial conditions and control parameters for hyperchaotic maps, ensuring that chaotic sequences are tightly coupled with plaintext image characteristics [163]. Such ML-derived keys can reduce predictability and increase sensitivity to input variations.

Machine learning can also be used to address common weaknesses in chaotic sequences caused by finite precision or degeneracy. In certain adaptive designs, neural networks learn to perturb or regularise chaotic outputs to reduce periodic behaviour and increase entropy, effectively training the chaotic sequence generator to produce richer pseudo-random streams [164].

Adaptive Cryptographic Systems and Feedback Mechanisms. Beyond parameter generation, adaptive cryptographic systems incorporate feedback loops where the encryption process itself influences subsequent parameter selection or chaotic seed adjustments [165]. These feedback mechanisms can be guided by machine learning models that observe metrics such as avalanche effect, correlation statistics, or key-sensitivity indicators and adapt the cipher design in real time to maintain desired security thresholds.

For example, in image encryption frameworks that partition images into blocks based on texture or complexity metrics, an ML classifier can determine whether different blocks require distinct diffusion strategies or encryption paths to ensure uniform security performance across heterogeneous visual content [166].

Machine Learning for Cryptanalysis and Security Assessment. Machine learning also plays a role on the cryptanalytic side, where classifiers and neural networks are used to identify weaknesses in chaotic cipher designs [167]. Tools such as support vector machines (SVMs) and deep learning models have been investigated for evaluating the effectiveness of NPCR/UACI criteria and for learning differential characteristics that may elude manual analysis, particularly in high-dimensional substitution spaces [168].

Such adversarial use of machine learning encourages the development of adaptive counter-measures, where the cryptosystem anticipates and mitigates ML-assisted attacks by randomising structures or augmenting chaos with ML-informed perturbations [169].

Reinforcement Learning for Security Optimisation. Reinforcement learning (RL) presents another compelling integration point, where an agent learns an encryption policy, selecting chaos parameters, S-box variants, or transformation sequences, based on reward signals tied to security metrics [170]. RL frameworks can optimise encryption strategies across rounds or adapt cipher components to maximise resistance

against target attack models while respecting performance constraints [171].

Such RL-guided designs are especially relevant when the design space is too large for manual tuning or when simple heuristic adjustments fail to produce robust security under dynamic conditions.

Challenges and Open Problems. Despite the promise of machine learning and adaptive systems in cryptography, several challenges remain [172]:

- **Security Guarantees:** Unlike classical cryptographic proofs, ML-informed systems often lack formal security guarantees.
- **Model Complexity and Overhead:** Integrating large neural networks increases computational cost.
- **Adversarial Vulnerabilities:** Machine learning models themselves are susceptible to adversarial inputs.
- **Interpretability:** The opaque nature of many ML models complicates rigorous evaluation.

Directions for Future Research. Future work on ML-assisted adaptive cryptographic systems could explore formal ML-cryptography interfaces, lightweight adaptive models, adversarial resistance, and standardised benchmarking frameworks [173].

In conclusion, the integration of machine learning and adaptive cryptographic systems represents a frontier research direction for chaos-based image encryption [174]. While significant hurdles remain in terms of security assurance and implementation feasibility, early results show that ML can play a valuable role in optimising, evaluating, and dynamically tuning encryption schemes in response to evolving threats.

7. Conclusion

This review has examined chaos-based cryptography with a particular focus on S-box design and image encryption, covering fundamental principles, construction methods, evaluation criteria, practical architectures, cryptanalytic considerations, and open research challenges. The analysis shows that chaotic systems offer an appealing way to generate complex and sensitive behavior with relatively low computational cost, which makes them especially attractive for image encryption and resource-constrained environments. Chaos-based schemes have been applied across a wide range of designs, from simple pixel permutation to more advanced permutation–diffusion frameworks that integrate nonlinear substitution through S-boxes. However, the effectiveness of these approaches depends strongly on both their theoretical design and their practical implementation. A key observation of this review is the diversity of methods used to construct chaos-based S-boxes, including direct chaotic mapping, algebraic–chaotic hybrid designs, optimization-assisted strategies, dynamic and key-dependent generation, and emerging machine learning–assisted approaches. While these methods expand the design space and offer flexibility, their security cannot be judged by statistical indicators alone. Metrics such as entropy, correlation, NPCR, and UACI are useful for initial screening, but they do not replace formal evaluation under established cryptanalytic models. Properties such as nonlinearity, differential uniformity, algebraic degree, and the absence of weak structural patterns play a decisive role in determining resistance to linear, differential, and algebraic attacks.

The review also highlights the critical impact of digital implementation on security. Finite-precision effects in chaotic maps can reduce randomness, shrink effective key spaces, and introduce predictable behavior that weakens otherwise well-designed schemes. Similarly, the use of dynamic features such as adaptive S-boxes or variable chaotic parameters can increase complexity for attackers, but may also introduce weak key classes, side-channel risks, or implementation vulnerabilities if not carefully engineered. These factors demonstrate that security must be evaluated not only at the algorithmic level but also at the level of software and hardware realization. Comparative analysis reveals an important trade-off between security and efficiency. Designs that combine chaotic mechanisms with established algebraic or standard cryptographic primitives often achieve stronger and more reliable security, but at the cost of increased computational and implementation complexity. In contrast, lightweight and real-time schemes

are better suited for IoT and embedded platforms, yet they require especially careful validation to ensure that performance gains do not come at the expense of fundamental cryptographic strength. Based on these findings, this review emphasizes the need for rigorous and standardized evaluation practices. Future work should adopt comprehensive benchmarking frameworks that integrate statistical testing, formal cryptanalysis, performance measurement, and practical deployment considerations. There is also strong potential in interdisciplinary approaches that combine chaos theory with algebraic cryptography, optimization methods, machine learning, and post-quantum security concepts, provided that such integrations preserve clear and provable security guarantees.

In conclusion, chaos-based cryptography for image encryption remains a promising and evolving research direction. Its suitability for lightweight, adaptive, and high-entropy designs makes it relevant for modern applications such as IoT systems, real-time multimedia protection, and resource-constrained devices. Real progress in this field, however, will depend on bridging the gap between theoretical appeal and practical security through rigorous cryptanalysis, careful implementation, and standardized evaluation methods.

References

1. Duong, P. P., & Nguyen, T. T., *Constructing 8 × 8 S-boxes with optimal Boolean functions and cryptographic properties*, Cryptography 9(4), 67, (2025).
2. Biryukov, A., Perrin, L., & Udovenko, E., *Practical aspects of linear cryptanalysis for modern block ciphers*, J. Cryptographic Engineering 13(2), 87–104, (2023).
3. Cusick, T. W., Stanica, P., & Duong, P. P., *On the nonlinearity and cryptographic properties of AES-like S-boxes*, IEEE Trans. Inf. Forensics Security 19, 452–465, (2024).
4. Marochok, S., *Algorithm for generating S-boxes with prescribed cryptographic properties*, Algorithms 16(3), 157, (2023).
5. Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., & Kaçar, S., *A novel approach for strong S-box generation based on chaotic systems*, Nonlinear Dynamics 87(2), 1081–1094, (2017).
6. Solak, E., *Differential uniformity of vectorial Boolean functions: Recent trends and applications to S-box design*, Designs Codes Cryptography 92(4), 885–902, (2024).
7. Wang, L., & Liu, J., *Linear approximation properties of algebraic and chaotic S-boxes for block cipher applications*, J. Inf. Security Appl. 75, 103250, (2023).
8. Zhao, H., & Wang, R., *Fixed points and cycle structure analysis of cryptographic S-boxes*, IEEE Trans. Computers 72(4), 931–943, (2023).
9. Carlet, C., *Vectorial Boolean functions for cryptography*, in *Boolean Functions for Cryptography and Coding Theory*, Cambridge Univ. Press, 398–469, (2021).
10. Cintas Canto, A., Kaur, J., Mozaffari Kermani, M., & Azarderakhsh, R., *Algorithmic security is insufficient: A comprehensive survey on implementation attacks haunting post-quantum security*, ACM Comput. Surveys 56(1), Art. 14, (2023).
11. Alkhzaimi, H. A., Lauridsen, M. M., & Rijmen, V., *Benchmarking lightweight block ciphers on constrained platforms*, IEEE Trans. Computers 72(9), 2591–2604, (2023).
12. Shannon, C. E., *Communication theory of secrecy systems*, Bell Syst. Tech. J. 28(4), 656–715, (1949).
13. Daemen, J., & Rijmen, V., *The design of Rijndael: AES — The advanced encryption standard*, Springer, (2002).
14. Carlet, C., & Ding, C., *Highly nonlinear mappings and their applications in cryptography*, IEEE Trans. Inf. Theory 65(3), 1937–1952, (2019).
15. Alexan, W., Faragallah, O. S., El-Sayed, H. S., & Shaheen, S. I., *Design and analysis of a secure image encryption algorithm using a nonlinear chaotic system and elliptic-curve-based key derivation*, Sci. Reports 15, 14050, (2025).
16. El Gaabouri, I., Senhadji, M., Belkasmi, M., & Zenkouar, K., *A new S-box pattern generation based on chaotic enhanced logistic map: Case of 5-bit S-box*, Cybersecurity 7, 59, (2024).
17. Özpolat, E., *Hyperchaotic system-based PRNG and S-box design for a secure image encryption algorithm*, Entropy 27(3), 299, (2025).
18. Dutra e Silva Junior, É. C., Cruz, C. A. d. M., Saraiva, I. A. L., & Rocha, A., *Chaos-based S-boxes as a source of confusion in cryptographic primitives*, Electronics 13(21), 4325, (2024).
19. Jamal, S. S., Farwa, S., & Shah, T., *Secure S-box construction with one-dimensional chaotic maps and finite fields*, J. Cryptographic Engineering 14(3), 301–317, (2024).
20. Fadhil, A. F., Alhusseini, M. M., & Feizi-Derakhshi, M.-R., *Enhanced CAST-128 with adaptive S-box optimization for image protection*, arXiv, (2025).

21. Bayesh, M. R., Das, D., & Ahadullah, M., *A dual-layer image encryption framework using chaotic AES with dynamic S-boxes and steganographic QR codes*, arXiv, (2025).

22. Zia, U., *Survey on image encryption techniques using chaotic maps in spatial, transform, and spatiotemporal domains*, Int. J. Inf. Security 21(6), 1149–1173, (2022).

23. Alotaibi, F., & Abutaleb, A., *Cryptanalysis of image confidentiality schemes based on hybrid chaotic maps*, J. King Saud Univ. Comput. Inf. Sci. 37, 130, (2025).

24. Özpolat, E., *Hyperchaotic system-based PRNG and S-box design for secure image encryption*, Entropy 27(3), 299, (2025).

25. El Gaabouri, I., Senhadji, M., Belkasmi, M., & Zenkouar, K., *A new S-box pattern generation based on chaotic enhanced logistic map*, Cybersecurity 7, 59, (2024).

26. Zia, U., *Survey on image encryption techniques using chaotic maps in spatial and transform domains*, Int. J. Inf. Security 21(6), 1149–1173, (2022).

27. Jamali, S. S., Shah, T., & Hussain, I., *Secure S-box construction using chaotic maps and finite fields*, J. Cryptographic Engineering 14(1), 45–60, (2024).

28. Álvarez, G., & Li, S., *Some basic cryptographic requirements for chaos-based cryptosystems*, Theor. Comput. Sci. 354(1), 1–14, (2006).

29. Li, C., Lin, D., & Lü, J., *Cryptanalysis of permutation–diffusion based image ciphers*, Multimedia Tools Appl. 82, 10943–10969, (2023).

30. Shannon, C. E., *Communication theory of secrecy systems*, Bell Syst. Tech. J. 28(4), 656–715, (1949).

31. Daemen, J., & Rijmen, V., *The design of Rijndael: AES — The advanced encryption standard*, Springer, (2002).

32. Carlet, C., *Boolean functions for cryptography and error correcting codes*, Cambridge Univ. Press, (2010).

33. Nyberg, K., *Differentially uniform mappings for cryptography*, in *Advances in Cryptology — EUROCRYPT 1993*, Lecture Notes Comput. Sci. 765, 55–64, (1994).

34. Webster, A. F., & Tavares, S. E., *On the design of S-boxes*, in *Advances in Cryptology — CRYPTO 1985*, Lecture Notes Comput. Sci. 218, 523–534, (1986).

35. Courtois, N. T., & Pieprzyk, J., *Cryptanalysis of block ciphers with overdefined systems of equations*, in *Advances in Cryptology — ASIACRYPT 2002*, Lecture Notes Comput. Sci. 2501, 267–287, (2002).

36. Carlet, C., *Boolean functions for cryptography and coding theory*, Cambridge Univ. Press, (2021).

37. Silva Junior, E. C., Cruz, C. A. M., Saraiva, I. A. L., & Rocha, A., *Chaos-based S-boxes as a source of confusion in cryptographic primitives*, Electronics 14(11), 2198, (2025).

38. Zhang, B., & Liu, L., *Chaos-based image encryption: Review, applications, and challenges*, Mathematics 11(11), 2585, (2023).

39. Li, C., & Zhang, Y., *On the misuse of statistical tests in image encryption*, Multimedia Tools Appl. 83, 28791–28812, (2024).

40. Hamadi, S. J., & Mohammed, E. A., *Chaotic systems in cryptography: An overview of feature-based methods*, Al-Salam J. Eng. Technol. 4(1), 164–172, (2024).

41. Baptista, M. S., Kurths, J., & Grebogi, C., *On the use of dynamical systems in cryptography*, Chaos Solitons Fractals 183, 114952, (2024).

42. Zhou, Y., Hua, Z., & Pun, C. M., *Image encryption using chaotic maps: Development, application, and analysis*, Mathematics 13(16), 2588, (2025).

43. Al-Dayel, I., Nadeem, M. F., Khan, M. A., & Khan, S., *An image encryption scheme using a four-dimensional chaotic system and cellular automaton*, Sci. Reports 15, 19499, (2025).

44. Zhou, Y., Hua, Z., Pun, C. M., & Chen, C. L. P., *Image encryption using chaos and deep learning: A survey*, Information Sciences 625, 784–815, (2023).

45. Shannon, C. E., *Communication theory of secrecy systems*, Bell Syst. Tech. J. 28(4), 656–715, (1949).

46. Li, C., Lin, D., Lü, J., & Hao, F., *Cryptanalysis and improvement of chaos-based image encryption schemes*, IEEE Trans. Circuits Syst. Video Technol. 34(2), 1281–1295, (2024).

47. Rhouma, R., Solak, E., & Belghith, S., *Cryptanalysis of permutation-only image encryption algorithms*, Signal Process.: Image Commun. 26(4–5), 241–250, (2011).

48. Wang, X., Gao, S., & Zhang, Y., *A novel chaotic image encryption algorithm based on pixel diffusion*, J. Inf. Security Appl. 72, 103418, (2023).

49. Álvarez, G., & Li, S., *Some basic cryptographic requirements for chaos-based cryptosystems*, Theor. Comput. Sci. 354(1), 1–14, (2006).

50. Banerjee, S., & Sarkar, P., *Finite precision effects in digital chaotic cryptosystems*, Nonlinear Dynamics 117, 3251–3270, (2024).

51. Khan, M. A., Ahmed, F., & Batool, S. I., *Chaos-based dynamic S-box design for secure image encryption*, IEEE Access 12, 22431–22446, (2024).

52. Hua, Z., Jin, F., Xu, B., & Huang, H., *Two-dimensional logistic–sine-coupling map for image encryption*, Signal Processing 204, 108816, (2023).

53. Chen, G., Mao, Y., & Chui, C. K., *A symmetric image encryption scheme based on 3D chaotic cat maps*, Chaos Solitons Fractals 21(3), 749–761, (2004).

54. Li, C., Zhang, Y., & Xie, E. Y., *Breaking permutation–diffusion based image encryption schemes*, IEEE Trans. Multimedia 26, 512–525, (2024).

55. Wang, X., & Liu, C., *On the insecurity of permutation-only image encryption algorithms*, J. Inf. Security Appl. 70, 103041, (2023).

56. Li, C., Zhang, Y., & Xie, E. Y., *Cryptanalysis of a chaotic image encryption algorithm based solely on permutation*, IEEE Access 12, 15234–15245, (2024).

57. Zhou, Y., & Zhang, T., *Security analysis of permutation-only image encryption*, Multimedia Tools Appl. 81, 18797–18817, (2022).

58. Chen, G., Wang, X., & Li, C., *Chosen-plaintext attacks on permutation-based image ciphers*, IEEE Trans. Circuits Syst. Video Technol. 34(5), 2156–2165, (2024).

59. Sun, B., Liu, J., & Wang, L., *Key space and complexity evaluation of permutation-based image encryption*, Entropy 25(8), 1209, (2023).

60. Liu, J., & Wang, L., *On the redundancy of repeated permutations in image encryption*, J. Vis. Commun. Image Represent. 94, 103247, (2023).

61. Gupta, R., & Singh, M., *Correlation analysis of permutation-only image encryption schemes*, Signal Processing 197, 109648, (2024).

62. Huang, F., & Lin, J., *Statistical vulnerabilities in permutation-only encryption under homogeneous images*, Digital Signal Processing 129, 103735, (2023).

63. Zhang, B., & Liu, L., *Breaking a pixel permutation image cipher using plaintext attacks*, Mathematics 12(4), 578, (2024).

64. Zhou, Y., Pun, C. M., & Chen, C. L. P., *A comprehensive survey on image encryption techniques*, Information Sciences 620, 480–510, (2023).

65. Wang, X., Zhang, Y., & Bao, C., *Permutation–diffusion architecture for chaos-based image encryption*, Multimedia Tools Appl. 80(4), 5883–5908, (2021).

66. Patidar, V., Pareek, N. K., & Sud, K. K., *A robust image encryption scheme based on permutation–diffusion architecture*, Procedia Comput. Sci. 171, 24–33, (2020).

67. Belazi, A., El-Latif, A. A. A., & Belghith, S., *A novel image encryption scheme based on substitution–permutation network and chaotic S-box*, IEEE Access 7, 103071–103086, (2019).

68. Hua, Z., & Zhou, Y., *Dynamic S-box construction based on chaotic systems for image encryption*, Sensors 22(4), 1322, (2022).

69. Li, C., Lin, D., & Lü, J., *Cryptanalysis of chaos-based cryptosystems under finite precision*, Information Sciences 622, 598–615, (2023).

70. Zhang, Y., Li, C., & Wang, S., *A survey on DNA computing-based image encryption*, Information Sciences 547, 191–215, (2021).

71. Liu, H., & Wang, X., *Color image encryption based on DNA computing and chaotic systems*, Signal Processing 173, 107578, (2020).

72. Hua, Z., & Zhou, Y., *Bit-plane DNA image encryption using chaotic systems*, Sensors 22(7), 2714, (2022).

73. Chen, J., Zhang, L., & Li, C., *Hyperchaotic DNA-based image encryption algorithm*, Chaos Solitons Fractals 142, 110504, (2021).

74. Wang, X., & Zhao, Y., *Image encryption using DNA encoding and chaotic permutation*, Multimedia Tools Appl. 79, 20015–20034, (2020).

75. Zhou, Y., Hua, Z., & Huang, H., *Dynamic DNA coding based image encryption scheme*, IEEE Access 10, 42112–42125, (2022).

76. Zhang, L., & Li, C., *Entropy analysis of DNA-chaos image encryption*, Information Sciences 563, 27–45, (2021).

77. Liu, H., Wang, X., & Kadir, A., *Key-sensitive DNA-chaos image encryption*, Signal Process.: Image Commun. 82, 115770, (2020).

78. Hua, Z., & Zhou, Y., *Large key space image encryption using DNA computing and chaos*, Sensors 22(11), 4123, (2022).

79. Wang, X., & Liu, C., *Parallel DNA image encryption based on chaotic systems*, IEEE Access 9, 87455–87468, (2021).

80. Ahmad, M., Doja, M. N., & Beg, S., *Lightweight DNA-chaos image encryption for IoT*, Future Gener. Comput. Syst. 128, 194–207, (2022).

81. Li, Y., & Wang, X., *Image encryption using Hamiltonian chaos and DNA encoding*, Chaos Solitons Fractals 150, 111078, (2021).

82. Kumar, S., & Mishra, R., *Hash-driven dynamic DNA-chaos image encryption*, J. Inf. Security Appl. 72, 103392, (2023).

83. Li, C., Lin, D., & Lü, J., *Cryptanalysis of DNA-based chaotic image encryption*, IEEE Trans. Inf. Forensics Security 14(9), 2262–2275, (2019).

84. Li, C., & Lü, J., *Finite precision degradation of chaotic cryptosystems*, Information Sciences 622, 598–615, (2023).

85. Belazi, A., & Abd El-Latif, A. A., *Efficiency evaluation of DNA-chaos image encryption*, Multimedia Tools Appl. 80, 21357–21378, (2021).

86. Zhou, Y., & Hua, Z., *Future directions of DNA-based image encryption*, Information Fusion 92, 68–86, (2023).

87. Zhang, Y., Wang, X., & Liu, J., *A lightweight chaotic image encryption scheme for real-time applications*, Signal Process.: Image Commun. 110, 116872, (2023).

88. Li, S., Chen, H., & Hua, Z., *Lightweight chaos-based image encryption for IoT devices*, IEEE Internet Things J. 9(14), 12045–12057, (2022).

89. Singh, P., & Singh, R. K., *A comprehensive survey on lightweight image encryption techniques*, ACM Comput. Surveys 56(2), Art. 35, (2024).

90. Abdullah, A., Jamil, N., & Zaba, M. R., *FPGA-based real-time chaotic image encryption system*, Microprocessors Microsystems 83, 104014, (2021).

91. Zhou, Y., Pun, C. M., & Chen, C. L. P., *Chaos-based image encryption: A comprehensive survey*, Information Sciences 620, 480–510, (2023).

92. Liu, H., & Wang, X., *Evaluating confusion–diffusion balance in chaos-based image ciphers*, J. Vis. Commun. Image Represent. 89, 103554, (2023).

93. Li, S., Chen, Z., & Hua, Z., *Nonlinearity and differential uniformity in chaos-derived S-boxes*, Multimedia Tools Appl. 81, 20001–20022, (2022).

94. Zhang, T., Wang, L., & Liu, J., *Key space analysis of chaos-based multimedia encryption*, Entropy 24(5), 722, (2022).

95. Alawida, M., Samsudin, A., & Teh, J. S., *Lightweight chaotic image encryption and hardware implementation*, J. Real-Time Image Process. 19, 899–914, (2022).

96. Wang, S., & Liu, Y., *Hardware acceleration of chaos-based ciphers for real-time imaging*, ACM J. Emerg. Technol. Comput. Syst. 19(3), Art. 45, (2023).

97. Xu, B., Huang, H., & Zhao, F., *Empirical evaluation of chaos-based encryption performance metrics*, IEEE Trans. Multimedia 25, 964–978, (2023).

98. Zhou, Y., & Huang, H., *Comparative analysis of permutation and permutation–diffusion image ciphers*, Signal Process.: Image Commun. 99, 116470, (2021).

99. Belazi, A., El-Latif, A. A., & Belghith, S., *Chaotic S-box design for secure image encryption*, IEEE Access 7, 103071–103086, (2019).

100. Zhou, Y., & Hua, Z., *DNA-chaos hybrid schemes for image encryption: Trends and challenges*, Chaos Solitons Fractals 148, 110961, (2021).

101. Li, C., Lin, D., & Lü, J., *A review on the security of chaos-based image encryption*, J. Inf. Security Appl. 78, 103467, (2024).

102. Xu, B., Huang, H., & Zhao, F., *Attack models and security analysis in image encryption*, IEEE Trans. Inf. Forensics Security 18, 2157–2173, (2023).

103. Wang, X., & Liu, C., *On the insecurity of permutation-only image encryption algorithms*, J. Inf. Security Appl. 70, 103041, (2023).

104. Zhou, Y., Pun, C. M., & Chen, C. L. P., *Diffusion enhancement in chaos-based image encryption*, Signal Process.: Image Commun. 106, 116569, (2022).

105. Zhu, Y., Wei, Z., & Liu, X., *Histogram and pixel correlation analysis for evaluating encryption systems*, J. Inf. Security Appl. 47, 241–250, (2019).

106. Chen, G., Li, H., & Shen, Z., *Known-plaintext attacks on chaotic image encryption systems*, IEEE Trans. Circuits Syst. Video Technol. 34(8), 2423–2436, (2024).

107. Zhou, Y., & Huang, H., *Permutation leakages under known-plaintext attack*, J. Vis. Commun. Image Represent. 75, 102976, (2021).

108. Liu, J., & Wang, L., *Impact of weak substitution on differential analysis*, Entropy 24(12), 1845, (2022).

109. Singh, P., & Kaur, R., *Static S-box reuse vulnerabilities in image encryption*, Cryptography 7(2), 52, (2023).

110. Rai, S., & Singh, R., *Chosen-plaintext attacks against image encryption algorithms*, J. Cryptographic Engineering 13, 311–329, (2023).

111. Gupta, R., & Verma, D., *Differential analysis of chaos-based image ciphers*, Multimedia Tools Appl. 82, 4567–4590, (2023).

112. Zhang, L., & Li, Y., *Dynamic S-box generation with hash chaining*, J. Systems Architecture 129, 102272, (2022).

113. Khan, M. A., & Ahmad, F., *Cryptanalytic key recovery strategies under chosen-plaintext attacks*, IEEE Access 12, 90567–90582, (2024).

114. Zhu, Y., Wei, Z., & Liu, X., *Histogram and pixel correlation analysis for evaluating encryption systems*, J. Inf. Security Appl. 47, 241–250, (2019).

115. Wang, S., & Liu, Y., *Analysis of chaos-based permutation–diffusion image ciphers: Statistical measures and security*, Signal Process.: Image Commun. 89, 115932, (2020).

116. Zhang, T., & Sun, G., *Statistical evaluation and security of hybrid chaos image encryption schemes*, Sensors 23(4), 1322, (2023).

117. Zhao, F., Zhou, Y., & Huang, H., *On the effectiveness of chaotic S-boxes in image encryption*, IEEE Access 9, 14258–14271, (2021).

118. Zhu, Y., & Wei, Z., *Correlation analysis of encrypted images using chaos-based methods*, IEEE Access 7, 172589–172601, (2019).

119. Xu, B., Huang, H., & Zhao, F., *Finite precision effects in chaotic cryptosystems*, IEEE Trans. Circuits Syst. Video Technol. 33(10), 5502–5514, (2023).

120. Li, S., & Lü, J., *Digital chaos behavior and its impact on image encryption*, Int. J. Bifurcation Chaos 32(12), 2250203, (2022).

121. Zhang, X., & Huang, F., *Breaking image encryption schemes based on chaos due to finite precision*, J. Vis. Commun. Image Represent. 70, 102725, (2020).

122. Zhou, Y., & Wei, J., *State space collapse in digital chaos systems and cryptanalysis implications*, Chaos Solitons Fractals 145, 110824, (2021).

123. Chen, Q., & Li, C., *Cryptanalysis of finite-precision chaos-based ciphers exploiting cycle structures*, IEEE Access 11, 38971–38984, (2023).

124. Alotaibi, F., & Abutaleb, A., *Cryptanalysis of digital chaotic S-box schemes under finite precision*, J. King Saud Univ. Comput. Inf. Sci. 37(2), 245–258, (2025).

125. Jun, T., & Li, Y., *Perturbed chaotic maps for improved sequence diversity in cryptography*, Entropy 21(7), 689, (2019).

126. Yamamoto, H., & Sato, M., *Hyperchaotic behavior in finite-precision digital implementations*, Nonlinear Dynamics 109, 1539–1552, (2022).

127. Rahman, A., & Hasan, M., *Quantization-aware chaotic sequence generation for secure image encryption*, Signal Process.: Image Commun. 93, 116132, (2021).

128. Hu, L., & Gao, S., *Neural network augmented chaotic sequences for robust encryption*, Neural Comput. Appl. 34, 17459–17475, (2022).

129. Wang, Z., & Zhou, X., *Key space and chaotic parameter analysis in digital chaos-based cryptography*, Signal Process.: Image Commun. 96, 116241, (2021).

130. Deng, R., Fang, J., & Li, C., *Enhancing key space using hybrid key derivation for chaos-based ciphers*, IEEE Trans. Inf. Forensics Security 18, 3130–3142, (2023).

131. Ahsan, M., & Alghathbar, K., *Effective key space estimation for chaos-based encryption schemes*, J. Cryptographic Engineering 13(3), 451–466, (2023).

132. Zhou, Y., Huang, H., & Xu, B., *Key sensitivity analysis in chaotic image encryption*, IEEE Access 9, 86043–86058, (2021).

133. Li, S., Lin, D., & Lü, J., *Chaos cryptography key equivalence and weak key classes*, IEEE Trans. Circuits Syst. II: Express Briefs 69(9), 3797–3801, (2022).

134. Alotaibi, F., Abutaleb, A., & El-Gamal, M., *Cryptanalysis of chaos-based S-box and key space vulnerabilities*, J. King Saud Univ. Comput. Inf. Sci. 37(4), 301–316, (2025).

135. Liu, H., & Wang, X., *Security evaluation of chaos-based image encryption: Limitations of statistical testing*, Multimedia Tools Appl. 82(15), 24311–24335, (2023).

136. Wang, S., & Liu, Y., *Analysis of chaos-based permutation–diffusion image ciphers: Statistical measures and security*, Signal Process.: Image Commun. 89, 115932, (2020).

137. Gupta, R., & Kumar, A., *Limitations of statistical metrics in assessing image encryption security*, IEEE Access 11, 45612–45626, (2023).

138. Xu, B., Huang, H., & Zhao, F., *Attack models and security analysis in image encryption*, IEEE Trans. Inf. Forensics Security 18, 2157–2173, (2023).

139. Alotaibi, F., Abutaleb, A., & El-Gamal, M., *Cryptanalysis of chaos-based image ciphers with high NPCR and UACI*, J. King Saud Univ. Comput. Inf. Sci. 37(4), 301–316, (2025).

140. Wang, Z., & Chen, Y., *Finite precision effects in chaos-based encryption: Impact on statistical profiles*, IEEE Trans. Circuits Syst. Video Technol. 31(9), 3281–3292, (2021).

141. Zhao, F., Zhou, Y., & Huang, H., *Cryptanalysis of an image encryption algorithm based on a two-dimensional hyperchaotic map*, Entropy 26(11), 951, (2024).

142. Li, C., Lin, D., & Lü, J., *A review on the security of chaos-based image encryption*, J. Inf. Security Appl. 78, 103467, (2024).

143. Zhang, T., Sun, G., & Wang, L., *Hybrid S-box constructions combining chaotic and algebraic models for enhanced cryptographic metrics*, AIMS Mathematics 10(3), 5671–5695, (2025).

144. Rai, S., & Singh, R., *Implementation vulnerabilities and risk assessment in cryptographic systems*, J. Cryptographic Engineering 14(2), 155–172, (2024).

145. Khan, M. A., Ahmed, F., & Batool, S. I., *Security and compliance considerations for cryptographic algorithms in IoT environments*, Int. J. Sci. Technol. 16(3), 221–235, (2025).

146. Zhou, Y., Hua, Z., & Pun, C. M., *A comprehensive survey on image encryption: Taxonomy, challenges, and future directions*, Chaos Solitons Fractals 178, 114361, (2024).

147. Hanif, F., Raza, A., & Shajib, M. D., *Investigating signless Laplacian spectra and network topology in helical phenylene quadrilateral structures*, J. Math., (2025).

148. Singh, P., & Singh, R. K., *Image encryption algorithms: Design principles and evaluation metrics*, ACM Comput. Surveys 57(1), Art. 12, (2025).

149. Hua, Z., Zhou, Y., & Huang, H., *A chaotic-based image encryption scheme using elliptic curve cryptography and genetic algorithm*, Artif. Intell. Rev. 57, 102, (2024).

150. Khan, M. A., Nadeem, M. F., & Al-Dayel, I., *An image encryption scheme using PRESENT–RC4, chaos, and secure key generation*, Sci. Reports 15, 19412, (2025).

151. Rasheed, A. M., & Kumar, R. M. S., *Improved lightweight image encryption for medical IoT devices using six-dimensional chaotic maps with XOR diffusion, permutation, and substitution*, J. Electrical Systems 20(11), 345–362, (2024).

152. Raza, A., Hanif, F., & Mohammed, H. A., *Efficient crack and surface-type recognition via CNN-block development mechanism and edge profiling*, Sci. Reports 15, 40073, (2025).

153. Zhou, Y., Huang, H., & Liu, J., *LCA-SM-IoT: Lightweight image encryption based on Rule 60 cellular automata and sine map for IoT devices*, Discover Appl. Sci. 7, 118, (2025).

154. Kumar, R., & Singh, P., *Post-quantum threats and cryptographic readiness: Implications for secure communications*, IEEE Security & Privacy 23(2), 12–19, (2025).

155. Song, K., Zhang, Y., & Liu, H., *A hybrid chaos-based cryptographic framework for post-quantum secure communications*, IEEE Trans. Inf. Forensics Security 20, 1543–1557, (2025).

156. Raza, A., Hanif, F., & Mohammed, H. A., *Analyzing the enhancement of CNN-YOLO and transformer based architectures for real-time animal detection in complex ecological environments*, Sci. Reports 15, 39142, (2025).

157. Zhou, Y., Bao, L., & Chen, C. L. P., *Image encryption using deep learning and chaotic systems*, IEEE Trans. Neural Netw. Learn. Syst. 33(12), 7121–7135, (2022).

158. Farash, M. S., & Yaghoobi, M. E., *Adaptive cryptographic systems driven by artificial intelligence*, IEEE Access 11, 84521–84538, (2023).

159. Liu, H., & Hua, Z., *Neural-network-based adaptive S-box construction for secure image encryption*, Signal Processing 205, 108856, (2023).

160. Hanif, F., & Raza, A., *Effects of duplication operations on signless Laplacian spectrum and network measures*, Bol. Soc. Parana. Mat. 43, (2025).

161. Zahra, R., & Ali, A., *Adaptive neural S-box design for CAST-128 based image encryption*, Multimedia Tools Appl. 82, 35641–35663, (2023).

162. Wang, X., & Zhang, Y., *CNN-assisted chaotic key generation for secure image encryption*, Expert Syst. Appl. 197, 116707, (2022).

163. Chen, J., Xiao, D., & Liao, X., *Hyperchaotic image encryption driven by deep convolutional neural networks*, Nonlinear Dynamics 112, 987–1006, (2023).

164. Raza, A., & Munir, M. M., *Laplacian spectra and structural insights: applications in chemistry and network science*, Front. Appl. Math. Stat. 11, 1519577, (2025).

165. Gupta, K., & Singh, P., *Feedback-driven adaptive chaotic encryption using machine learning*, Future Gener. Comput. Syst. 145, 236–248, (2023).

166. Belazi, A., Abd El-Latif, A. A., Belghith, S., & Taha, M., *Block-wise adaptive image encryption using machine learning and chaos*, J. Inf. Security Appl. 65, 103115, (2022).

167. Alani, N., & Khan, M. A., *Machine learning for cryptanalysis: Advances and challenges*, ACM Comput. Surveys 55(8), Art. 170, (2023).

168. Ben-Sasson, E., Cohen, A., & Shamir, A., *Deep learning based distinguishers for image ciphers*, IEEE Trans. Inf. Forensics Security 17, 2845–2858, (2022).

169. Ravi, S., & Joye, M., *Adversarially aware adaptive cryptographic systems*, Cryptography and Communications 15, 789–812, (2023).

170. Zhang, L., & Liu, Y., *Reinforcement learning based adaptive encryption strategies*, IEEE Access 11, 102331–102345, (2023).

171. Kaur, M., & Kumar, R., *Adaptive cipher optimisation using reinforcement learning*, Appl. Soft Comput. 118, 108485, (2022).

172. Papernot, N., *Challenges of machine learning in cryptographic systems*, IEEE Security & Privacy 21(3), 72–79, (2023).

173. Hua, Z., & Chen, C., *Future directions in machine-learning-assisted cryptography*, Information Fusion 95, 102729, (2024).

174. Jolfaei, A., & Li, F., *Machine learning empowered chaos-based cryptography: Trends and prospects*, Chaos Solitons Fractals 178, 114322, (2024).

175. Singh, P., & Singh, R. K., *Image encryption algorithms: Design principles and evaluation metrics*, ACM Comput. Surveys 57(1), Art. 12, (2025).

176. Hua, Z., Zhou, Y., & Pun, C. M., *Lightweight chaos-based S-box construction for secure image encryption*, IEEE Access 13, 45871–45886, (2025).

Saba Fatima,
Department of Mathematics,
University of Education, Vehari Campus, Pakistan.
E-mail address: sabasyeda546@gmail.com

and

Abid Mahboob,
Department of Mathematics,
University of Education, Vehari Campus, Pakistan.
E-mail address: abid.mahboob@ue.edu.pk

and

Ali Raza,
Department of Mathematics,
University of the Punjab, Lahore, Pakistan.
E-mail address: alleerazza786@gmail.com