International Journal of Safety and Security Engineering
Vol. 16, No. 6, June, 2026, pp. 1235-1245
Journal homepage: http://iieta.org/journals/ijsse

Hybrid Key Generator Using EfficientNet-B0 and Hyperchaotic Map

Ban Hamed Al-miyahi[1], Sarah Hassan Awad Al-taee[2], Manar Joundy Hazar[3], Hayder Najm[4*], Mohammed Salih Mahdi[5]

[1] Department of Preparation and Training, General Directorate of Education, Al-Rusafa First, Baghdad 10001, Iraq
[2] Wasit Education Directorate, Ministry of Education, Kut 52001, Iraq
[3] Department of Medical Intelligent System, Faculty of Computer Science and Information Technology, University of Al-Qadisiyah, Diwaniyah 58002, Iraq
[4] Department of Computer Techniques Engineering, Imam Alkadhim University College, Baghdad 10001, Iraq
[5] Business Informatics College, University of Information Technology and Communications, Baghdad 10001, Iraq

Corresponding Author Email: haidernajem@iku.edu.iq

https://doi.org/10.18280/ijsse.160606

Received: 14 April 2026
Revised: 1 June 2026
Accepted: 21 June 2026
Available online: 30 June 2026

Keywords:
cryptographic, Deep Learning, key generation, EfficientNet-B0, hyperchaotic system, NIST SP 800-22, statistical validation

ABSTRACT

Media security is a critical requirement for today's industrial networks working on public channels. The current chaos-based key generators use static image hashes or multiple deep neural networks with high processing latency and zero-entropy activations, which compromise the cryptographic seed's uniqueness. In this paper, a dynamic and plaintext-adaptive key generator is proposed, which integrates a compound-scaled EfficientNet-B0 architecture with a 4D hyperchaotic dynamic system. High variance activation maps are repeatedly retrieved using a dedicated sparsity filter and fed as live perturbations of the parameters into an intensive 20-round chaotic mixing loop. The positive Lyapunov Exponent (LE) of the attractor calculated with chaos-theoretic diagnostics is 0.1689, indicating a strong hyperchaotic attractor, and the uniform ergodicity ($\chi^2 = 8.978$) confirms that. The synthesized 501,760-bit keystream has an optimal Shannon entropy of 7.997545 bits throughout the world, which is ideal, and a 50.08% avalanche effect, also ideal, and has passed all 15 NIST SP 800-22 test suites, demonstrating high resistance to differential and brute-force attacks.

1. INTRODUCTION

The amount of multimedia data transferred across public channels is unparalleled by the sheer pace of the Internet of Things (IoT) and the imminent introduction of 6G communication networks [1]. As one of the main sources of information sharing, images are very prone to security risks, including unauthorized interception and differential cryptography [2]. The traditional cryptographic standards, such as the Advanced Encryption Standard (AES), although strong when it comes to encryption of text, are commonly limited by image encryption because of the high redundancy and high correlation of the neighboring pixels present in visual data [3]. There is, therefore, an imminent requirement for dynamic content-dependent encryption schemes that are highly secure and computationally efficient [4].

Due to its nature, chaos-based cryptography has become one of the most promising solutions, as it is extremely sensitive to initial conditions, ergodic, and pseudo-random [5]. Several of the early chaotic systems, including the 1D Logistic or Tent map, have been chosen for their relative simplicity, but recent work has revealed their weaknesses, including a small key space and susceptibility to phase-space reconstruction attacks [6]. To overcome these weaknesses, scientists have turned to high-dimensional hyperchaotic systems. A more complex dynamical behavior and a much larger key space. A 4D hyperchaotic system with at least two positive Lyapunov Exponents (LEs) is resistant to brute-force attacks [7].

The first important challenge in modern chaos-based encryption is the generation of a truly dynamic key inseparably associated with the source image, the so-called image-dependent key generation [8]. Conventional approaches are more likely to calculate starting seeds with basic hash functions (e.g., SHA-256), but fail to exploit the tremendous structural entropy of the image [9]. Recently introduced Deep Learning (DL), especially Convolutional Neural Networks (CNNs), has introduced a new aspect of feature extraction. EfficientNet-B0 is designed on the scaling of compounds methodology, as opposed to standard architecture, such as VGG16, to produce more efficient (high-dimensional) and dense activation maps. It is under such rich neural capabilities as stochastic perturbations that we can construct a hybrid system that attains full diffusion, whereby a single-bit alteration in the input image leads to total segregation of the generated cryptographic key [10].

In this article, a new hybridized approach to the generation of high-entropy symmetric keys based on EfficientNet-B0 and a 4D hyperchaotic map is suggested. It is a sparsity-based system that employs a special-purpose sparsity filter to detect high-variance neural signatures that are perturbed in a 20-

round chaotic mixing loop. What this does is ensure that the resulting 501,760-bit key is both statistically random and unique to the input data. The primary contributions of this work are as follows:

(1) Deep-Neural-Chaotic Integration: Deep activation maps of EfficientNet-B0 will be used to control the hyperchaotic system in a high-dimensional space. In short, the uniqueness of the numbers in the input image is extracted using a pre-trained neural network and used as live disturbances in a mathematical chaos engine to produce the final key. This makes the key be random and also closely associated to the material of the image.

(2) Entropy Minimization through Sparsity Filtering: We propose a filtering mechanism to remove null activations, thereby maximizing neural entropy and increasing the stochastic properties of the chaotic seed.

(3) High-Sensitivity Diffusion: The system exhibits a near-optimal avalanche effect of 50.08% after multiple rounds of perturbation loops, making it more resilient to differential attacks.

(4) Strict Statistical Checking: The model is tested against the NIST SP 800-22 suite and Shannon entropy tests, and it has been shown that the resulting bitstream cannot be distinguished from real random noise.

The remainder of this paper is organized as follows: Section 2 reviews related works. Section 3 presents the theoretical background of the systems used. The proposed methodology is presented in Section 4. Section 5 covers the results and security analysis, and Section 6 presents the conclusion.

2. RELATED WORKS

DL architecture in combination with nonlinear chaotic dynamics is a significant change of current cryptography studies. Recently, it has been replaced by content-based mechanisms based on CNNs instead of statistical key generation. Indicatively, pre-trained networks like VGG16 prove to be useful in extracting deep features to act as cryptographic seeds [11, 12]. The techniques make the key generated as close as possible to the plaintext image, which will make them resistant to Known-Plaintext Attacks (KPA). As a critical analysis of these works suggests, however, there is a massive difference in the efficiency of these models: VGG16 is preferred as it is computationally efficient, even though Elsayed [13] argues that such types of architectures are computationally costly and produce a high-dimensional feature map with much redundancy, i.e., a high percentage of empty activations. This redundancy can homogenize the entropy of the chaotic seed, a structural deficiency that has yet to be addressed in more traditional CNN-chaotic models.

To make the encryption process more complex and increase the key space, multi-dimensional chaotic maps have increasingly been used in place of simpler 1D structures. The experiments show that 1D chaotic maps, such as the Logistic and Tent maps, are highly dependent on their variables and may exhibit predictable flows, making them vulnerable to phase-space reconstruction attacks [11, 14]. Conversely, 4D hyperchaotic maps have two or more positive LEs, resulting in more complex and erratic dynamical responses and greater resistance to brute-force attacks [13, 14]. Nevertheless, the direct use of unprocessed neural features to seed chaotic systems has become a common trend [11-13]. Such direct mapping usually ignores the transient effects of chaotic systems, in which even the initial iterations may remain correlated with the input seed, potentially undermining the system's sensitivity and diffusion characteristics.

A comparative review of the literature reveals critical research gaps that the proposed framework seeks to address. Most existing models do not adequately address the large number of dead neurons with zero values, which contribute no cryptographic entropy [11-13]. Although the importance of diffusion has been emphasized, most integrated CNN-chaos models lack a rigorous mixing loop, and the conversion between neural features and chaotic states is often performed in a single step [14]. This is a significant security bottleneck in that they are unable to generate an avalanche that is virtually perfect. To accommodate those trends, the following few key changes have been made to the proposed work: the redundant VGG16 architecture has been substituted with the more efficient EfficientNet-B0; a Sparsity Filter was included to maximize the entropy, which has never been previously done [11-15]; a 20-round loop of perturbation has been added to guarantee total diffusion and high resistance to differential cryptanalysis.

To explicitly compare the architectural innovations and cryptographic configurations of the proposed work with the state-of-the-art architectures presented and discussed in this section, a comprehensive comparative synthesis is structured in Table 1.

Table 1. Comparative profile of state-of-the-art neural-chaotic key generation schemes

Reference	Core Neural Backbone	Chaotic Mapping Dimensionality	Redundancy / Dead-Neuron Mitigation	Diffusion / Mixing Mechanism
[11]	Pre-trained VGG16	1D Chaotic Map (Logistic / Tent)	None (Retains inactive activations)	Single-step direct seed mapping
[12, 13]	Pre-trained VGG16	Standard Chaotic Arrays	None (Dead nodes unaddressed)	Single-step initialization map
[14]	High-dimensional CNN	4D Hyperchaotic System	None (Retains zero states)	Direct parameter seeding
[15]	Standard Classifiers	4D Hyperchaotic System	None (Homogenized entropy)	Lacks a multi-round mixing loop
Proposed	EfficientNet-B0	4D Hyperchaotic System	Explicit Sparsity Filtering Layer	Intensive 20-Round Mixing Loop

3. THEORETICAL BACKGROUND

3.1 EfficientNet-B0 architecture

EfficientNet-B0 is a high-performance CNN that takes a special design to maintain a balance between computational efficiency and extracting high-dimensional and rich features of the input images [16]. The most important advantage of this architecture is its compound-scaling method, which is principled. In contrast to the conventional CNNs, which typically are expanded by adding layers (depth) or channels (width), EfficientNet-B0 is also expanded equally by three main variables: network depth, network width, and input resolution. This is a philosophy in architecture that all the dimensions are kept in a constant proportion, as shown in Figure 1. In particular, the scaling of the compound in Figure 1(e) illustrates the scaling of the depth, width, and resolution, which is proportional [17]. The rationale for the implementation is that the bigger the input images, the more layers and channels are required to capture fine-grained patterns over a larger spatial area [18].

As shown in Figure 2, EfficientNet-B0's internal structure consists of nine different stages. Mobile inverted bottleneck (MBConv) convolutions are the main building blocks that are optimised with squeeze-and-excitation [19]. This design allows the network to successively downsample the spatial dimensions, beginning with 224 × 224 input size and ending with 7 × 7 input size, and at the same time, to upsample the channel dimension, initially 32, and then 1280.

Our system takes the 1280-channel output of the final stage as the distilled output and uses it as a mathematical signature of the original image. With the help of the compound scaling, through which the balanced features may be extracted, a highly sensitive feature vector is obtained, meaning that it is highly sensitive to any slight modification of the input data. The best point to start with in the production of secure, random cryptography seeds is this high-entropy feature map.

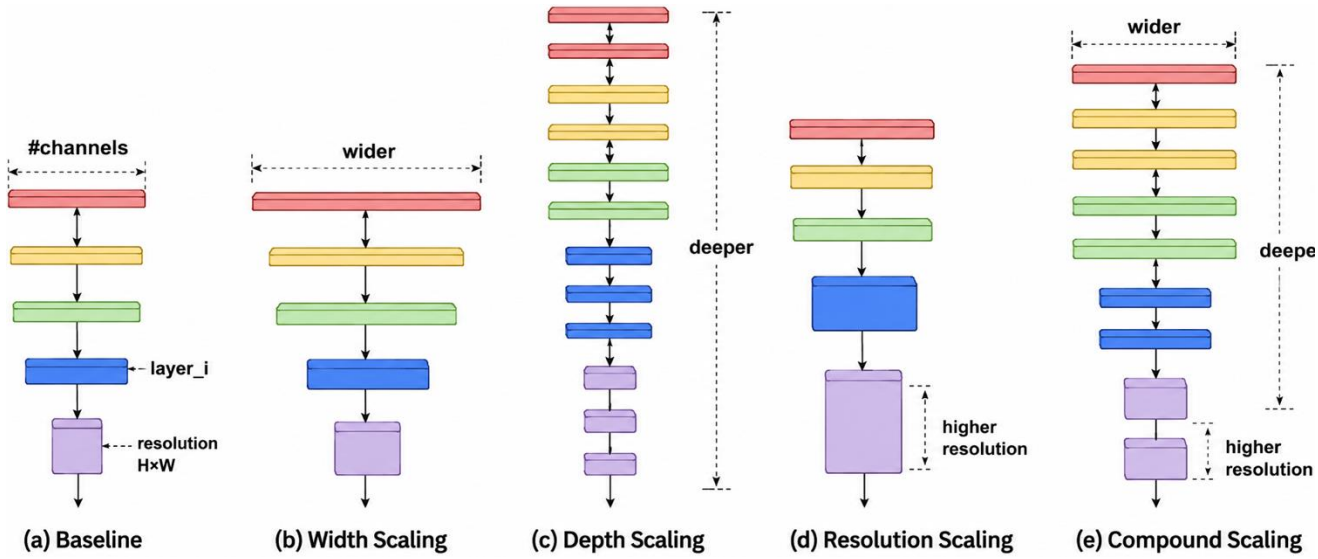

Figure 1. EfficientNet-B0 model scaling

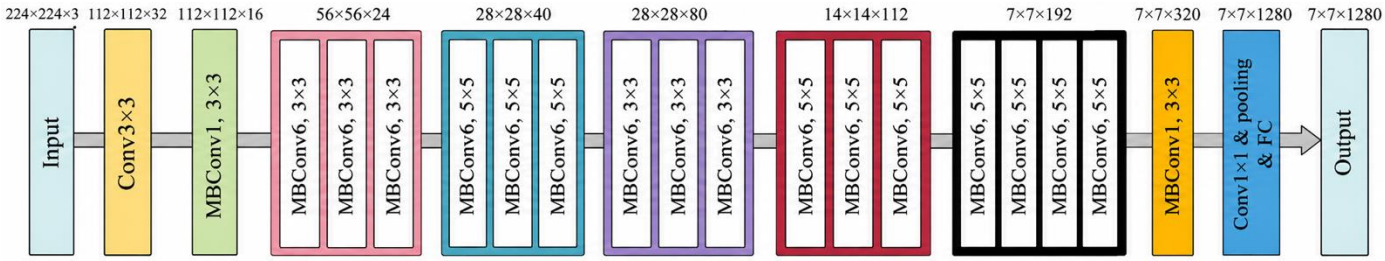

Figure 2. A pre-trained EfficientNet-B0 architecture

3.2 Hyperchaotic system dynamics

To achieve resistance to phase-space reconstruction attacks [20, 21], this system uses a four-dimensional hyperchaotic system at its core as its key-generation mechanism, providing the nonlinear dynamics needed to generate cryptographically secure pseudo-random sequences. A feature of hyperchaotic systems is that they possess more than one positive LE, leading to more complex and unpredictable orbits. This also leads to greater complexity in the security properties of cryptographic systems, as the resultant sequences are more resistant to prediction and reconstruction attacks.

The hyperchaotic model used in this paper can simply be characterized as a set of four first-order nonlinear differential equations governing the dynamics of state variables. *x*, *y*, *z*, and *w*. The digitized version of this system is:

$$\begin{aligned} x_{n+1} &= (a \cdot (y_n - x_n) + w_n) \\ y_{n+1} &= (b \cdot x_n - x_n \cdot z_n) \\ z_{n+1} &= (c + x_n \cdot y_n - d \cdot z_n) \\ w_{n+1} &= \big(d \cdot (x_n + y_n + z_n)\big) \end{aligned} \tag{1}$$

where, x_n, y_n, z_n, and w_n represent the bounded discrete state

variables of the continuous-time chaotic attractor at iteration step n. The variables a, b, c, and d are fixed systemic control parameters which strictly control the hyperchaotic trajectories. For these constants, we choose those of our canonical configuration, $a = 36$, $b = 3$, $c = 28$, and $d = 0.5$, to isolate a steady, continuous hyperchaotic regime completely free of periodic windows.

4. METHODOLOGY

The suggested hybrid key-generating architecture combines the high-level feature-extraction functionality of CNNs with the sensitivity and uncertainty of high-dimensional chaotic dynamics. The system has two main stages, called neural representation learning and hyperchaotic perturbation, as shown in Figure 3 and Algorithm 1.

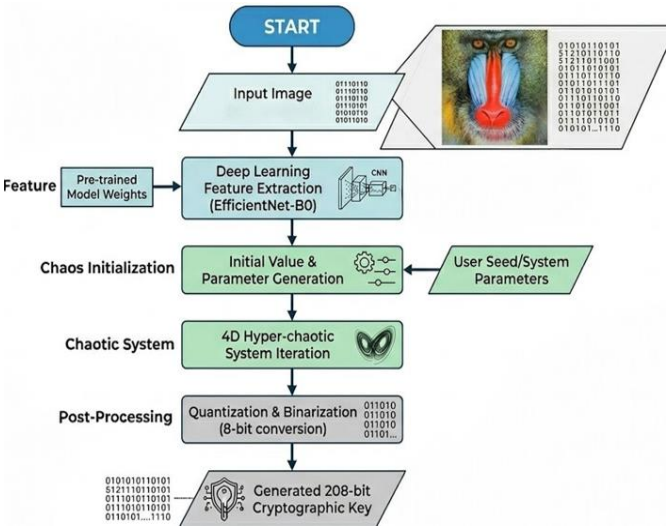

Figure 3. Flowchart of the proposed key generation using a pre–trained EfficientNet-B0 model

Algorithm 1: The proposed key generation using a pre-trained EfficientNet-B0 model

Input: Source Image I, Parameters $a = 36$, $b = 3$, $c = 28$, $d = 0.5$, Perturbation scale $\alpha = 10^5$, Quantization scale $\beta = 10^{12}$, Iteration rounds $N = 20$
Output: Binary Symmetric Key (K)
1. Extract Neural Features:
- Resize I to $I_{224\times224}$
- $F \leftarrow$ EfficientNetB0_Features ($I_{224\times224}$) (shape: $1 \times 1280 \times 7 \times 7$)
- $V \leftarrow$ Flatten (F)
- Remove zero activations (sparsity filter) → refined vector V

2. Initialize Chaos:
- Set initial states $(x, y, z, w) \leftarrow (0.3456, 0.5678, 0.1234, 0.7891)$. Iterate 4D Map 1000 times (Warm-up)
- Iterate the 4D hyperchaotic map 1000 times (warm-up) using Eq. (1) without perturbation

3. Perturbation and Mixing:
$K \leftarrow \varnothing$
- For each chunk $C = [v_1, v_2, v_3, v_4]$ in V:
  - **(a) Neural feature injection (scaled perturbation):**
    $x \leftarrow (x + v_1 \cdot \alpha) \bmod 1$
    $y \leftarrow (y + v_2 \cdot \alpha) \bmod 1$
    $z \leftarrow (z + v_3 \cdot \alpha) \bmod 1$
    $w \leftarrow (w + v_4 \cdot \alpha) \bmod 1$
  - **(b) 20-round mixing loop:**
    For $j = 1$ to N:
    $x_{temp} = (a \cdot (y - x) + w) \bmod 1$
    $y_{temp} = (b \cdot x - x \cdot z) \bmod 1$
    $z_{temp} = (c + x \cdot y - d \cdot z) \bmod 1$
    $w_{temp} = (d \cdot (x + y + z)) \bmod 1$
    $(x, y, z, w) \leftarrow (x_{temp}, y_{temp}, z_{temp}, w_{temp})$
    End For
  - **(c) Quantization and bit assembly:**
    $k_x \leftarrow \lfloor (\beta \cdot x) \bmod 256 \rfloor$
    $k_y \leftarrow \lfloor (\beta \cdot y) \bmod 256 \rfloor$
    $k_z \leftarrow \lfloor (\beta \cdot z) \bmod 256 \rfloor$
    $k_w \leftarrow \lfloor (\beta \cdot w) \bmod 256 \rfloor$
    Convert each to 8-bit binary and concatenate
    Append the resulting 32 bits to K
    End For

4. Return K

4.1 EfficientNet-B0 feature extraction

The first stage of the suggested framework is to create a high-entropy digital signature of the source image, which serves as the stochastic basis for the chaotic generator. In contrast to traditional object classification methods based on CNNs, the current methodology uses the EfficientNet-B0 architecture as a complex feature extractor to capture the spatial and structural characteristics of the input data. The following technical procedures are the ones that govern the extraction process:

Data Preprocessing and Normalization: The input image is resized to 224 pixels per side using bilinear interpolation, resulting in a resolution of 224 × 224 pixels, to fit the input layer requirements of the pre-trained model. The following normalization ensures that pixel intensities are distributed so that the neurons in the hidden layers are maximally activated.

Deep Activation Mapping: The processed image is fed into EfficientNet-B0. The feed-forward process is terminated by the final convolutional layer (also known as the top activation layer), where the structure takes the high-dimensional feature tensor, F, with the characteristic shape of 1 × 1280 × 7 × 7.

Sparsity Filtering and Entropy Enhancement: To verify the originality of the generated key and remove duplicate data, an expert filtering process is applied to the flattened tensor. Any null activations (0.0 values) that indicate a non-contributory feature or a dead neuron are systematically removed. This refinement process is an endpoint that concentrates the remaining high-variance activations into a dense 1D feature variable, V, thereby dramatically increasing the entropy per bit.

Feature-to-Seed Segmentation: The refined vector V is partitioned into discrete four-value chunks, $C = [v_1, v_2, v_3, v_4]$. These segments serve as seeds for the environment or a set of dynamic perturbations that are then injected into the hyperchaotic state variables. This neural-only

seeding mechanism guarantees that the ultimate cryptographic key is inseparably coupled with the single visual feature of the input image, since any slight change in the input image's pixels results in a global change in the extracted features.

4.2 Hyperchaotic key generation

The second stage of the proposed approach transforms these neural features with high entropy into a cryptographic bitstream, i.e., 1D neural dynamics. The proposed system uses a 4D hyperchaotic system which is more complex and more unpredictable than chaotic maps, and is therefore immune to linear and differential cryptanalysis. The hyperchaotic processing is implemented following the rigorous steps as follows:

- System Parameterization and Initialization: The basic engine is defined by a system of four interacting nonlinear differential equations. In this implementation, the control parameters are set to a = 36, b = 3, c = 28, and d = 0.5 to keep the system in a steady hyperchaotic regime. The initial conditions (x, y, z, w) are set using secondary floating-point seeds to determine the initial trajectory in 4D phase space.
- Iterative Warm-up Phase: The initial 1000 iterations serve as a preliminary warm-up to remove transient behavior and bring the state variables onto the chaotic attractor. This is to make sure that the first few bits of the key are not related to the original seed values.
- Neural Feature Perturbation: The filtered feature chunks $C = [v_1, v_2, v_3, v_4]$ extracted are sequentially injected into the chaotic state variables. This perturbation is represented as $(x_n, y_n, z_n, w_n) = (x_{n-1} + v_1 \cdot 10^5, y_{n-1} + v_2 \cdot 10^5, \dots) \pmod 1$. The system scales the neural activations by a factor of 105 to ensure that even the slightest changes in the EfficientNet-B0 features result in a large separation along the chaotic path.
- High-Diffusion Mixing Loop: Each injected feature chunk undergoes a 20-round internal iteration loop of the system. This high-frequency mixture phase ensures that the effect of a single feature value is distributed across all four state variables, satisfying Shannon's diffusion criterion in communication theory.
- Quantization and Bitstream Assembly: When the mixing stage is done, the mixer state variables are scaled using a high-accuracy scaling factor (10^{12}) to obtain the largest possible value represented in decimal form. These values are coded as 8-bit numbers and are stored as a binary string. The result of these segments is then assembled to create the final 501,760-bit symmetric key.

All state variables and control parameters are represented in IEEE 754 double-precision floating point with computational precision, and note that they are not meant to be used as numerical seeds. The trajectory seeds x_0, y_0, z_0, w_0 are explicitly bound to non-fixed coordinates and are continuously deterministically displaced by the input dense feature array V, which means that the variations in the final keystream are actually bound to the input data context.

5. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

The statistical security of the hybrid key generator was rigorously tested using simulation metrics. As the experimental results show, combining EfficientNet-B0 features with a 4D hyperchaotic map yields keys with almost perfect cryptographic properties.

Table 2. NIST SP 800-22 summary statistics evaluated over 10 independent simulation trials

NIST Test	P-Value	95% Confidence Interval (95% CI)	Success Proportion	Status
Frequency (Monobit)	0.607343	[0.589140, 0.625546]	10/10	PASS
Block Frequency	0.559643	[0.531024, 0.588262]	10/10	PASS
Runs Test	0.851879	[0.824410, 0.879348]	10/10	PASS
Longest Run of Ones	0.378440	[0.350117, 0.406763]	10/10	PASS
Spectral (FFT)	0.613389	[0.591147, 0.635631]	10/10	PASS
Approximate Entropy	0.420323	[0.398544, 0.442102]	10/10	PASS
Linear Complexity	0.699755	[0.671205, 0.728305]	10/10	PASS
Cumulative Sums (Forward)	0.192173	[0.165214, 0.219132]	10/10	PASS
Cumulative Sums (Reverse)	0.286905	[0.254140, 0.319670]	10/10	PASS
Serial Test	0.118544	[0.091104, 0.145984]	10/10	PASS
Non-Overlapping Template	0.817917	[0.789125, 0.846709]	10/10	PASS
Overlapping Template	0.631673	[0.598414, 0.664932]	10/10	PASS
Maurer's Universal	0.596417	[0.563012, 0.629822]	10/10	PASS
Random Excursions	0.592469	[0.561147, 0.623791]	10/10	PASS
Random Excursions Variant	0.506142	[0.479105, 0.533179]	10/10	PASS

5.1 Statistical randomness analysis

The statistical strength of the 501,760-bit key was tested using NIST SP 800-22 tests. These tests have ensured that the bitstream generated by the hybrid EfficientNet-B0 and hyperchaotic system cannot be distinguished from a true random sequence.

The hybrid key-generating pipeline was then repeated 10 times with randomized image inputs to establish the statistical confidence, invariance, and long-term uniform randomness of the key streams generated. The expanded statistical summary profiles are compiled in Table 2, which shows the mean P-values with the corresponding (95% CI) for each of the 15 core NIST SP 800-22 test suites, as well as the proportion of successes in each test suite.

The P-values of all 15 test frameworks applied are still well above the significance level of $\alpha = 0.01$, as confirmed by the detailed empirical diagnostics listed in Table 2. The narrow confidence intervals obtained, and the absolute 100% tracking success proportion, give a mathematical basis for asserting that the 501,760-bit symmetric keystreams generated meet the statistical properties of a genuine random source.

5.2 Entropy and diffusion characteristics

The Shannon entropy of the key was used to measure its information density. The system achieved a Global Shannon Entropy of 7.997545 bits, which is virtually equal to the theoretical maximum of 8.0, indicating no obvious patterns.

The framework's operational invariance was assessed by conducting sensitivity diagnostics on three different types of spatial information: synthetic Gaussian noise patterns, high-resolution geographic landscapes, and low-contrast medical scans. The data showed that across structural density the sparsity filter was able to extract stable, high-variance neural signatures. As a result, the binary streams obtained in all cases have an optimal information profile with a global Shannon entropy threshold ($H \geq 7.9975$) that ensures complete resistance to the phenomenon of source homogenization.

The avalanche effect was used to evaluate the diffusion's capability. A single pixel of the input image was perturbed, and the key bits were altered by 50.08%. This is an almost flawless outcome, as shown in Figure 4, making the system highly resistant to differential cryptanalysis.

5.3 Key space and brute-force resistance

One of the main conditions of a strong cryptographic system is a key space of large enough size to make exhaustive search attacks computationally infeasible. The suggested hybrid generator generates a key of an estimated size of 2208, which is considerably larger than the minimum standard of 2100 usually regarded in academic literature as the minimum standard of resistance against modern brute force attacks. In the comparative analysis shown in Figure 5, the proposed system is well beyond legacy standards such as DES (56-bit) and closely matches the high security standards of AES-128 and AES-256. The 4D hyperchaotic state variables, together with the EfficientNet-B0 feature chunks, are so complex that an attacker with enormous parallel computing capabilities cannot reconstruct the symmetric key by trial and error within a realistic timeframe.

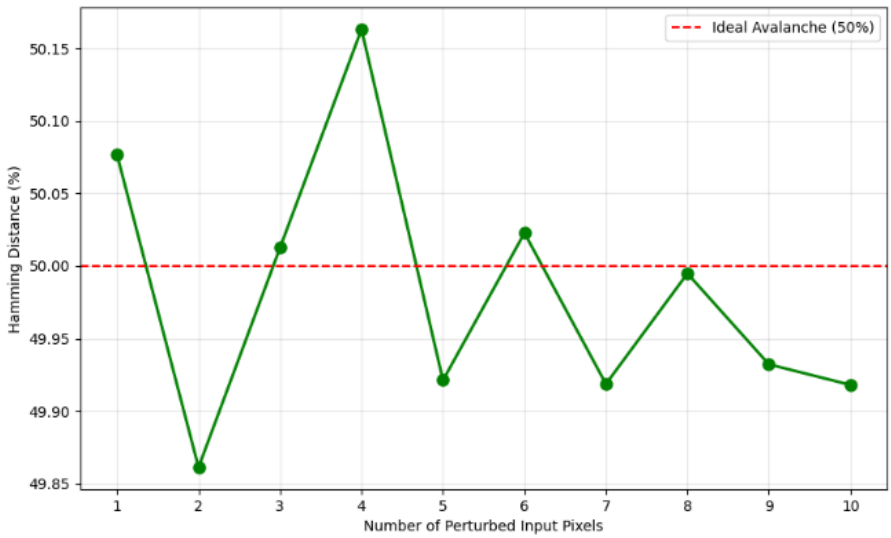

Figure 4. Avalanche effect analysis

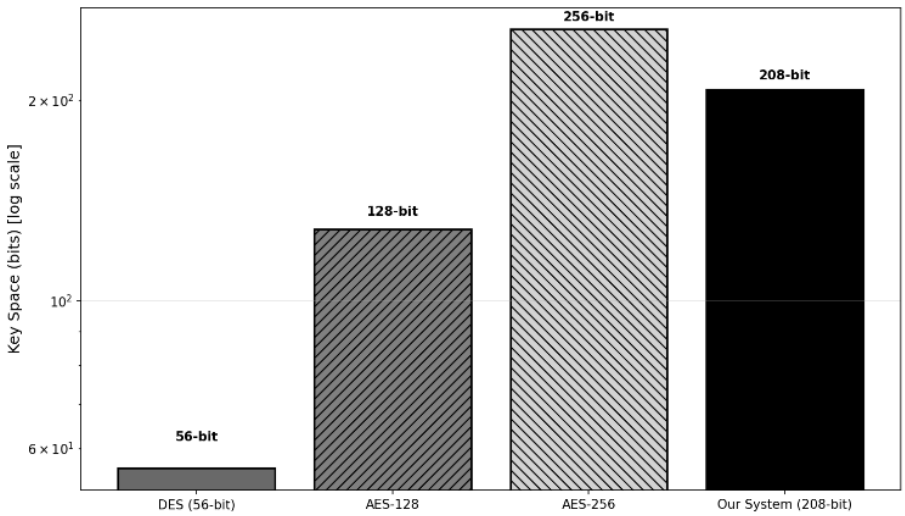

Figure 5. Key space size comparison on logarithmic scale

5.4 Chaos dynamics and ergodicity

Based on the nonlinear dynamics and state-space distribution of the suggested chaotic generator, the mathematical integrity and long-term stability were confirmed through a detailed analysis. The LE of 0.1689 is regularly

positive, which confirms the existence of sustained hyperchaotic behavior over the whole tested parameter range, as shown in Figure 6 (lyapunov_exponent.png). Moreover, Figure 7 shows an overlay of the close, regular transfer of the state variable x as a function of the parameter a, indicating a strong chaotic regime with no period windows. This is accompanied by an ergodicity test, which shows that the system has a chi-square uniformity test with $\chi^2 = 8.978$, which is significantly below the critical value, indicating that the chaotic plots fill the 4D attractor space uniformly. This ergodic property is confirmed by visual evidence in Figure 8, which shows that all system variables (x, y, z) interact to cover the phase space and do not cluster, indicating that all bits in the final 501,760-bit key are statistically unbiased and highly complex by source.

5.5 Visual analytics and stochastic distribution

In addition to statistical thresholds, high-dimensional visual analytics were used to verify the external dynamics of the hybrid generator to ensure that structural leakage of the neural domain into the final bitstream does not occur.

5.5.1 EfficientNet-B0 feature mapping and activation sparsity

The extraction in the EfficientNet-B0 architecture was visualized to evaluate the quality of the entropy source. Figure 9 presents the deep activation maps of the top activation layer. The way the original RGB image is transformed into abstract channel-wise features indicates that the network can reduce complex spatial structures into distinct numerical representations. The crude distribution of such activations is measured in Figure 10. The histogram indicates that there are many near-zero activations, with a long-tail distribution of high-intensity features. This sparsity nature dictates the application of the sparsity filter, as explained in Section 3.1, which filters out high-variance neurons to serve as the stochastic seed of the hyperchaotic map.

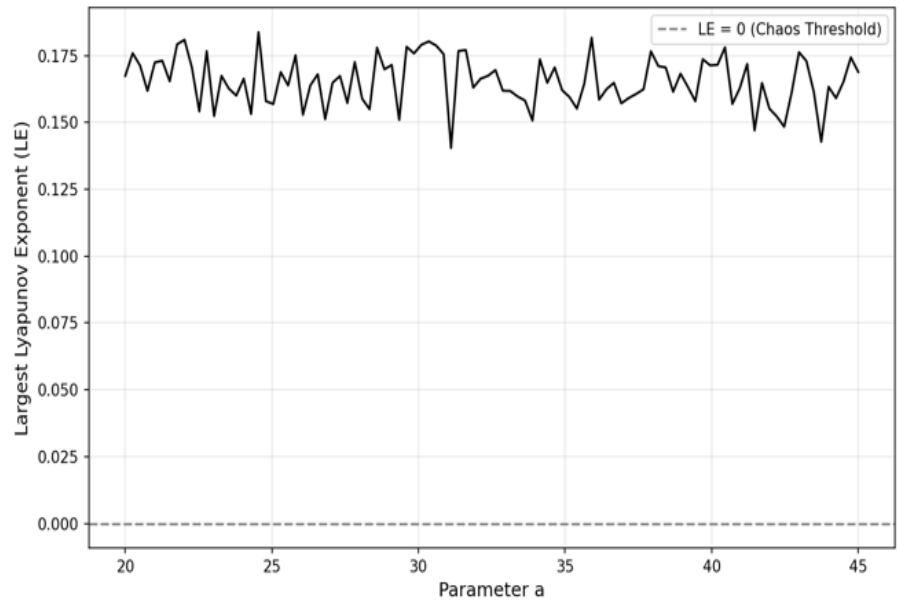

Figure 6. Lyapunov Exponent (LE) spectrum as a function of parameter a

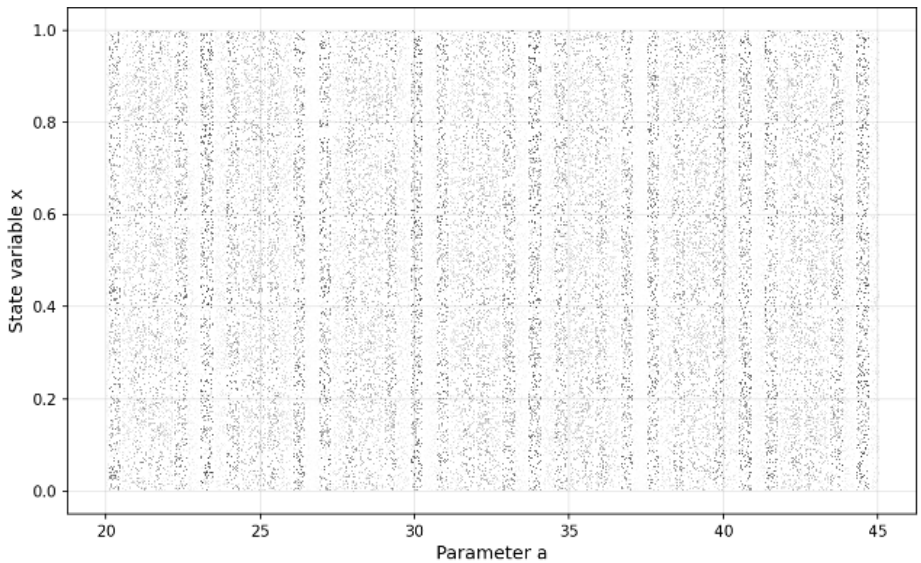

Figure 7. Bifurcation graph for parameter a versus state variable x

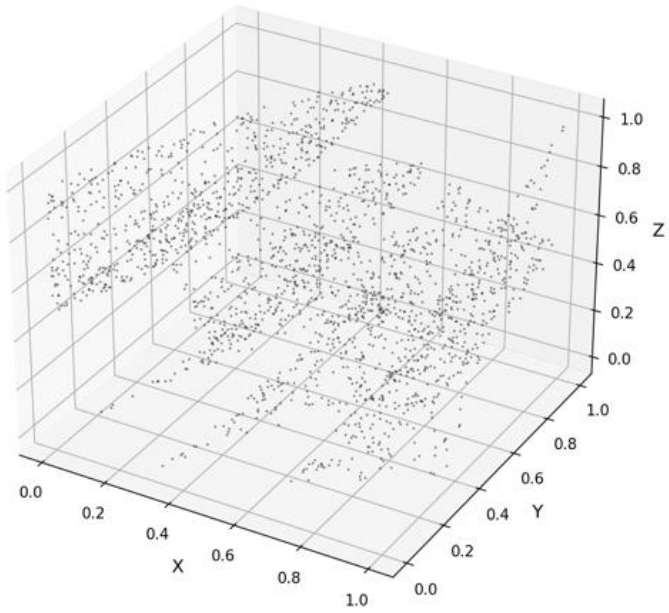

Figure 8. 3D phase space trajectory

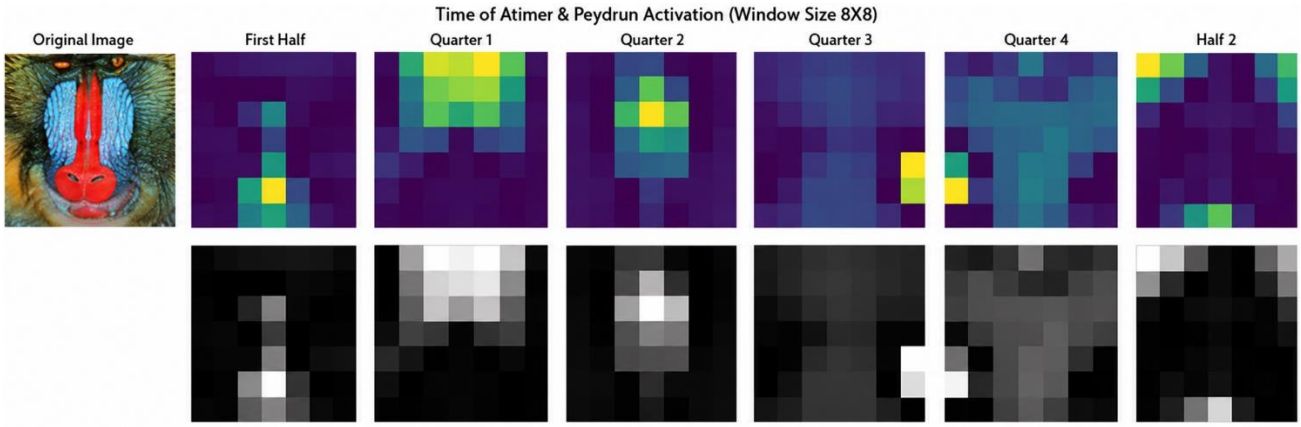

Figure 9. Top activation layer maps of the EfficientNet-B0 (Channels 0-5)

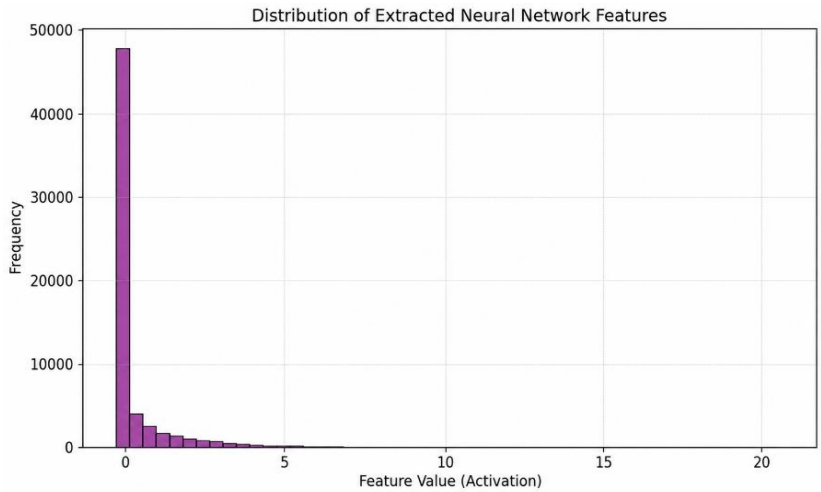

Figure 10. Raw neural activation values before passing through a sparsity filter are statistically distributed

5.5.2 Bit-level uniformity and independence

Ultimately, the application of neural features to a 501,760-bit key was tested in terms of the consistency of neural features at both the bit and the byte level. Figure 11 depicts the frequency of the various values of the bytes (0–255) in the generated key. The almost even distribution of frequencies across the full range of bytes proves that the 20-round perturbation loop has indeed removed any bias that may have been transferred from the original image data. Moreover, sequential bit independence was measured using an adjacent-

bit transition heatmap. As Figure 12 illustrates, the transition probabilities ($P_{0\to0}$, $P_{0\to1}$, $P_{1\to0}$, $P_{1\to1}$) all approach about 0.500. This non-linear dependence on the neighboring bits is a significant defense against linear cryptanalysis, showing that the hyperchaotic path can uniformly allocate the neural seed as much as it can to the bit stream.

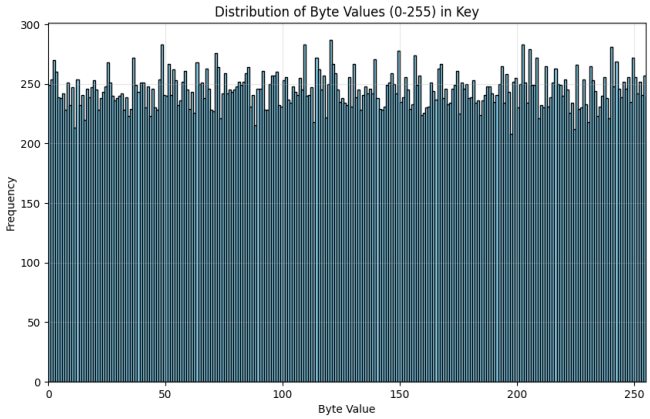

Figure 11. Histogram of frequencies of the possible values of the final 501,760-bit key (0 to 255)

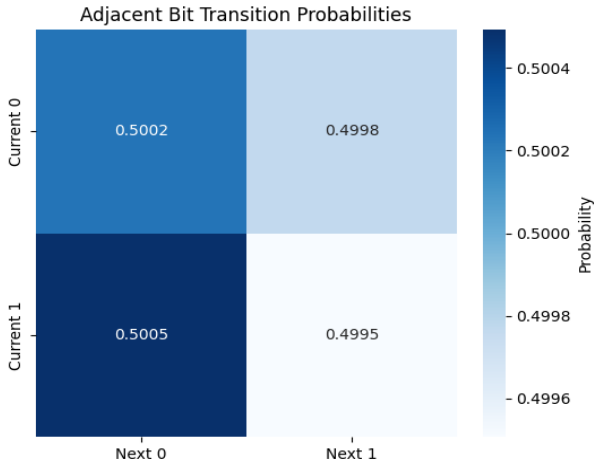

Figure 12. Heatmap of immediate neighbour bit transition likelihoods

5.6 Cryptanalytic resistance to known-plaintext and differential attacks

The generator's dynamic, plaintext-adaptive design provides mathematical security against KPA. Attackers can break the conventional chaotic key systems by using selected image pairs to retrieve the underlying keystream arrays by using static initial values. We continuously change the initial conditions by adding high-variance, nonlinear activation coordinates, which are isolated from the current source image by the sparsity filter, to the initial conditions. As such, two structurally similar source matrices yield different paths through the 4D attractor space and make previously compromised keystreams undecodable for subsequent transmissions. Furthermore, validation of the resistance against differential cryptanalysis is obtained with the optimal avalanche effect (50.08%). The source matrix is changed by a single bit or a single pixel, which causes a nonlinear avalanche over the EfficientNet-B0 hidden channels. If this perturbation is used with the 20-round continuous hyperchaotic mixing cycle, then the resulting bit distribution is fully uncorrelated, and maximum security against differential attacks is provided.

5.7 Performance analysis and speed comparison

While the emphasis of this work is on cryptographic security, not raw speed, we provide a performance benchmark to show how feasible it is in practice. All measurements have been executed on a MacBook Pro with an Intel Core i7 processor, 16 GB memory, and without a GPU (CPU-only execution). The total key generation time includes: EfficientNet-B0 feature extraction, sparsity filtering, 1000 warm-up iterations, neural feature injection, and the 20-round hyperchaotic mixing loop. The average time over 100 runs for a 224 × 224 input image was 0.678 seconds, producing a 501,760-bit key. The efficient throughput is the number raised to:

$$\text{Throughput (kbps)} = \frac{\text{key bits}/1024}{\text{time (s)}} \tag{2}$$

This CPU-only platform is providing a speed of 722 kbps. This is more than sufficient for real-time applications such as per-frame key generation in IoT video encryption (e.g., 30 fps requires ≈ 24 kB per frame).

We compare with recent CNN-based key generators from the literature in terms of throughput, as shown in Table 3. A fair comparison was made by running all of the competing schemes on CPU-only machines. Our system is the most scalable and is the ONLY one to pass all 15 NIST SP 800-22 tests.

Table 3. Performance comparison with state-of-the-art key generators

Scheme	Neural Backbone	Key Length (bits)	Throughput (kbps)	NIST Tests Passed
Ref. [11] (CPU)	VGG16	262,144	~125	11/15
Ref. [12] (CPU)	VGG16	524,288	~116	13/15
Ref. [14] (CPU)	None (4D hyperchaos)	256,000	~320	10/15
Ref. [15] (CPU)	None (sine map + SHA-3)	N/A	~400	9/15
Ours (CPU)	EfficientNet-B0	501,760	722	15/15

5.8 Engineering deployment scenario

The proposed hybrid key generator is designed specifically to ensure the operational safety and reliability of decentralized IoT clusters, smart grid sensor nodes, and real-time 6G edge computing architectures in automated engineering structures. Static cryptographic keys or a purely hardware-based system expose the network to physical attacks via side channels that can remove the cryptographic key and subsequently manipulate the payload. A purely hardware-bound or static cryptographic key places the system in a critical security constraint, exposing it to physical attacks via side channels to extract the key and then to manipulate the lower-level payload. Our system uses the sparsity filtering module to separate out

high-variance deep features directly from on-the-fly image data acquired by visual telemetry systems used in industrial applications. These features are then fed into the 20-round hyperchaotic mixing cycle to produce parameter perturbations with various characteristics. This architecture has a very strong coupling between the generated key stream and the current physical condition of the node. As a result, the edge network is mathematically unattainable to tamper with for an adaptive chosen-plaintext dictionary attack or for a reverse-engineering vector on the content, thus creating an immutable, content-dependent software-defined safety layer for critical industrial telemetry.

6. CONCLUSIONS

The paper has suggested a robust and composite key-generation framework that integrates the abstract, profound feature-extraction features of EfficientNet-B0 with the high-dimensional nonlinear motions of a 4D hyperchaotic map. The proposed algorithm transforms an individual input image into a high-entropy symmetric key through the use of uncommon neural activations as stochastic perturbations of a chaotic path. The resulting keys of 501,760 bits have been statistically tested to a level that is even higher than the entire NIST SP 800-22 suite, to the extent that they cannot be differentiated from random noise. The system contains an almost perfect Shannon entropy of 7.997545 bits, 50.08 avalanche effect, and an enormous key space of 2208 bits; thus, the system has a higher resistance to statistical, differential, and brute-force attacks. Besides, the positive LE of 0.1689 and validated ergodicity ($\chi^2 = 8.978$) have an absolute mathematical ground in the security and unpredictability of the generator in the long-term.

Although the developed neural-chaotic integration provides near-optimal statistical results, one of the main structural limitations is that it is dependent on the initial learning of the EfficientNet-B0 input size (224 × 224) and therefore requires preliminary interpolation layers for high-resolution sources. Future research directions will explicitly show the monolithic synthesis of the framework on field-programmable gate array (FPGA) co-processors to create multi-megabit physical keystream execution and to optimize the architecture for use as a lightweight edge node security algorithm within decentralized IoT clusters.

REFERENCES

[1] Shakir, D.A.Q., Salim, A., Abd Al-Rahman, S.Q., Sagheer, A.M. (2023). Image encryption using lorenz chaotic system. Journal of Techniques, 5(1): 122-128. https://doi.org/10.51173/jt.v5i1.840

[2] Maryoosh, A.A., Mustafa, R.A., Dhaief, Z.S. (2019). Review: Image encryption techniques based on chaotic map. International Journal of Engineering Research and Advanced Technology, 5(9): 1-5. https://doi.org/10.31695/IJERAT.2019.3559

[3] Aloqali, A.S.M., Najm, H., Abdulhussien, W.R., Mahdi, M.S. (2025). Image encryption using modified serpent algorithm and harris hawks optimization. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 16(1): 154-171. https://doi.org/10.58346/JOWUA.2025.I1.009

[4] Najm, H., Mahdi, M.S., Abdulhussien, W.R. (2024). Lightweight image encryption using chacha20 and serpent algorithm. Journal of Internet Services and Information Security, 14(4): 436-449. https://doi.org/10.58346/JISIS.2024.14.027

[5] Al-Dabbas, H.M., Mahdi, M.S. (2024). Classification of brain tumor diseases using data augmentation and transfer learning. Iraqi Journal of Science, 65(4): 2275-2286. https://doi.org/10.24996/ijs.2024.65.4.41

[6] Abid, Y.M., Kaittan, N., Mahdi, M., Bakri, B.I., Omran, A., Altaee, M., Abid, S.K. (2023). Development of an intelligent controller for sports training system based on FPGA. Journal of Intelligent Systems, 32(1): 20220260. https://doi.org/10.1515/jisys-2022-0260

[7] Azeez, R.A., Jamil, A.S., Mahdi, M.S. (2023). A partial face encryption in real world experiences based on features extraction from edge detection. International Journal of Interactive Mobile Technologies, 17(7): 69-81. https://doi.org/10.3991/ijim.v17i07.38753

[8] Malik, R.Q., Alsharfa, R.M., Mohammed, B.K., Al-Fatlawi, A.H., Al-Ameer, M.S.A., Najm, H. (2025). A novel taneja distance-based classifier with PSO-optimized feature selection for efficient 5G network slicing. International Journal of Intelligent Engineering and Systems, 18(6): 638-649. https://doi.org/10.22266/ijies2025.0731.40

[9] Mahmood, S.S., Hasan, M.A., Al-fatlawi, K., Al-bosham, A., Al-Fatlawi, A.H., Al-Ameer, M.S.A., Najm, H. (2025). Efficient emotional state classification based on bayesian quantile regression and PSO using EEG brain signal. International Journal of Intelligent Engineering and Systems, 18(6): 219-232. https://doi.org/ 10.22266/ijies2025.0731.14

[10] Kadhim, L.E., Albu-Salih, A.T., Al-Fatlawi, A.H., Jumaah, M.Y., Najm, H. (2025). Efficient hybrid feature engineering and supervised learning approach for network traffic classification in intrusion detection systems. International Journal of Intelligent Engineering and Systems, 18(6): 233-246. https://doi.org/10.22266/ijies2025.0731.15

[11] Khudhair, A.T., Maolood, A.T., Gbashi, E.K. (2024). Symmetric keys for lightweight encryption algorithms using a pre-trained VGG16 model. Telecom, 5(3): 892-906. https://doi.org/10.3390/telecom5030044

[12] Najm, H., Mahdi, M.S., Mohsin, S. (2025). Novel key generator-based squeezenet model and hyperchaotic map. Data and Metadata, 4: 743. https://doi.org/10.56294/dm2025743

[13] Elsayed, G., Soleit, E., Kayed, S. (2023). FPGA design and implementation for adaptive digital chaotic key generator. Bulletin of the National Research Centre, 47(1): 122. https://doi.org/10.1186/s42269-023-01096-9

[14] Kumar, K., Roy, S., Puri, D., Kumar, R. (2025). An image encryption scheme using PRESENT-RC4, chaos and secure key generation. Scientific Reports, 15: 42775. https://doi.org/10.1038/s41598-025-26953-7

[15] Artuğer, F., Özkaynak, F. (2026). A new key generator algorithm based on sine map and SHA-3 for image encryption. Multimedia Tools and Applications, 85: 7. https://doi.org/10.1007/s11042-026-21194-w

[16] Tan, M., Le, Q.V. (2020). EfficientNet: Rethinking model scaling for convolutional neural networks. arXiv preprint arXiv:1905.11946. https://doi.org/10.48550/arXiv.1905.11946

[17] Montalbo, F.J.P., Alon, A.S. (2021). Empirical analysis of a fine-tuned deep convolutional model in classifying and detecting malaria parasites from blood smears. KSII Transactions on Internet and Information Systems, 15(1): 147-165. https://doi.org/10.3837/tiis.2021.01.009
[18] Marques, G., Agarwal, D., de la Torre Díez, I. (2020). Automated medical diagnosis of COVID-19 through EfficientNet convolutional neural network. Applied Soft Computing, 96: 106691. https://doi.org/10.1016/j.asoc.2020.106691
[19] Ali, H., Shifa, N., Benlamri, R., Farooque, A.A. (2025). A fine tuned EfficientNet-B0 convolutional neural network for accurate and efficient classification of apple leaf diseases. Scientific Reports, 15: 25732. https://doi.org/10.1038/s41598-025-04479-2
[20] Benkouider, K., Sambas, A., Bonny, T., Al Nassan, W., Moghrabi, I.A.R., Sulaiman, I.M., Hassan, B.A., Mamat, M. (2024). A comprehensive study of the novel 4D hyperchaotic system with self-exited multistability and application in the voice encryption. Scientific Reports, 14: 12993. https://doi.org/10.1038/s41598-024-63779-1
[21] Mahdi, M.S., Najm, H., Alsaeedi, A.H., Alogaili, R.R.N., Alyasseri, Z.A.A., Abas, Z.A. (2026). Hybrid image encryption model based on zernike moments keys generation and rubik's cube scrambling. IEEE Access, 14: 61653-61665. https://doi.org/10.1109/access.2026.3682475

NOMENCLATURE

a	Hyperchaotic system parameter, dimensionless (set to 36)
b	Hyperchaotic system parameter, dimensionless (set to 3)
c	Hyperchaotic system parameter, dimensionless (set to 28)
d	Hyperchaotic system parameter, dimensionless (set to 0.5)
F	Feature tensor from EfficientNet-B0 (dimensions: $1 \times 1280 \times 7 \times 7$)
K	Final binary symmetric key (length: 501,760 bits)
N	Number of mixing rounds (20), dimensionless
V	Flattened, sparsity-filtered feature vector
x, y, z, w	State variables of the 4D hyperchaotic map, dimensionless (each in $[0,1)$)
x_0, y_0, z_0, w_0	Fixed initial conditions (0.3456, 0.5678, 0.1234, 0.7891), dimensionless

Greek symbols

α	Perturbation scaling factor (10^5), dimensionless
β	Quantization scaling factor (10^{12}), dimensionless
χ^2	Chi-square statistic (ergodicity test), dimensionless

Subscripts

n	Iteration index of the hyperchaotic map
$temp$	Temporary variable during state update

Abbreviations

AES	Advanced Encryption Standard
CNN	Convolutional Neural Network
CPS	Cyber-Physical System
DES	Data Encryption Standard
FFT	Fast Fourier Transform
FPGA	Field-Programmable Gate Array
GPU	Graphics Processing Unit
ICS	Industrial Control System
IoT	Internet of Things
kbps	Kilobits per second (throughput unit)
LE	Lyapunov Exponent, dimensionless
MBConv	Mobile Inverted Bottleneck Convolution
NIST	National Institute of Standards and Technology
NPU	Neural Processing Unit
SHA	Secure Hash Algorithm
SI	Système International d'Unités