Research Article

Lal Said, Majid Khan* and Muhammad Amin

An efficient recurrent neural network based confusion component construction and its application in protection of saliency in digital information

https://doi.org/10.1515/nleng-2025-0188
Received December 31, 2024; accepted November 21, 2025;
published online January 15, 2026

Abstract: The explosive growth of Internet of Things (IoT)-driven imaging in medicine, city surveillance, and intelligent infrastructure requires secure, timely transportation of delicate visual information with salient information, like faces and diagnostically important medical areas. Standard block ciphers, including AES, are unable to consistently retain these attributes under burst errors, partial data corruption, or focused cropping. In this paper, we introduce a lightweight substitution–permutation network (SPN) oriented encryption paradigm purpose-built for salient information secrecy in resource-limited IoT applications. We integrate permutation-driven block shuffle by chaos, recurrent neural network (RNN)-guided nonlinear static S-box generation, and bit-parity scrambling at the bit level to improve confusion–diffusion properties. We demonstrate experimental results of NPCR $> 99.60\,\%$, UACI $> 33.40\,\%$, near-zero correlation, and satisfactory key sensitivity. The technique maintains integrity of the salient region even with 50 % pixel loss, with throughput acceptable for real-time applications. Compared with previous work on lightweight approaches, we provide improved salient feature retention and lower computational complexity, and thus an ideal solution to security-critical applications of IoT-driven imaging.

***Corresponding author: Majid Khan**, Department of Mathematics, College of Science and Humanities in Alkharj, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia, E-mail: mk.cfd1@gmail.com
Lal Said, Department of Electrical Engineering, Institute of Space Technology, Islamabad, Pakistan; and Department of Avionics Engineering, Institute of Space Technology, Islamabad, Pakistan
Muhammad Amin, Department of Avionics Engineering, Institute of Space Technology, Islamabad, Pakistan

Keywords: lightweight image encryption; recurrent neural networks based S-boxes; saliency protection; security analysis

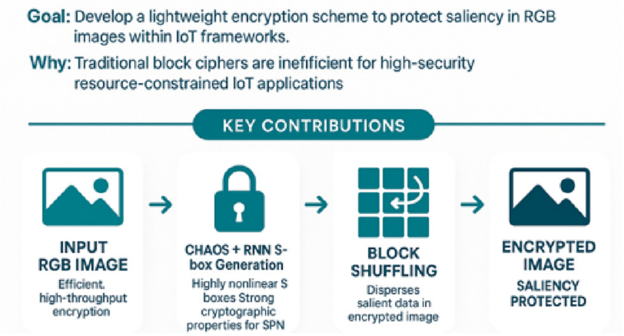
1 Introduction

Recent computing technological advancements have transformed the generation, processing, and transmission of information, reforming the very essence of our connected globe. The spread of the Internet of Things (IoTs) and massive IoT systems has brought into being huge networks of billions of devices, interchanging voluminous data in real-time to drive automation, industrial intelligence, and smart infrastructures. Blockchain technology has brought into being decentralized, tamper-proof ledgers, permitting secure and transparent digital transactions. Quantum computing approaches a tipping point where problems are solved by quantum computers but are unsolvable by classical devices, but such power itself holds a huge threat to conventional cryptographic mechanisms. Artificial intelligence (AI)-powered intelligent computing, with deep learning and neural networks, optimizes at hitherto unimaginable scales the decision-making and predictive analytics. In the age of global village of internet linking at ultra-high data rates, data flows unimpeded across borders, promoting worldwide collaboration and innovation. But such hyperconnectivity exacerbates exposure to data breaches, privacy intrusion, and cyberattacks. Cryptography does not appear as an optional solution but as the foundation of digital trust mathematical armor preserving confidentiality, integrity, and authentication of the source of every transmitted bit. Cryptography absence renders immutability useless in blockchain, IoTs become exploitable surveillance tools, AI models can be poisoned, and quantum breakthroughs could unravel the very ciphers protecting our most sensitive data. In this period, information security is at data gathering, transmission, storage, and even during handling transcends as more than a technical necessity but as the cornerstone of future safe, resilient, and trustworthy digital system bases. In the last few years, number of lightweight encryption schemes has been developed by researchers in the field of cryptography [1]. The motivation of all researchers is to design between low latency, high throughput and reduced computation [2]. In most cases security is compromised at the cost of lightweight. The work presented in ref. [3] proposes a privacy-preserving learning mechanism (PPLM) coupled with an industrial IoT system for the detection of bearing failures using lightweight edge-based model aggregation and a 2 dimensional Convolutional Neural Network. The scheme ensures privacy but the use of Cryptonet, introduces processing delays when implemented real-time and the scheme does not discuss saliency protection. The work presented in ref. [4] presents a lightweight encryption scheme for IoT devices that utilize quantum encryption; chaotic maps, confusion-diffusion operations, and discrete wavelet transform (DWT). The scheme possesses resistance against statistical differential attacks and brute force attacks. However, converting between quantum and classical domains introduce computational overhead, lack of saliency protection and real-world deployment on constrained IoT hardware remains invalidated. The work presented in ref. [5], evaluates the S-boxes before implementing in the lightweight encryption scheme, using a machine learning-based model. The machine learning model utilizes the key cryptographic properties and selects best S-boxes from a pool of generated S-boxes to be utilized in the encryption scheme. This approach enhances security at the cost of computational overhead and latency. To secure IoT communications, the work presented in ref. [6] introduces a lightweight encryption scheme. The scheme utilizes DNA sequences to generate keys and ECC to form a private key for encryption and decryption. The encryption scheme possesses strong immunity to differential, statistical and brute force attacks. The work lacks discussion on the scalability and saliency protection in real world images. To balance the processing efficiency and security in a constraint environment, a lightweight encryption scheme is proposed in ref. [7]. The scheme follows SPN architecture, and it is evaluated across various metrics and shows improvements in both encryption speed and security performance. However, the paper lacks technical specifics about the cryptographic primitives used, and potential limitations under adversarial conditions, lack of saliency protection or large-scale deployment are not explored. A lightweight image encryption scheme that is designed for IoT based environment is presented in ref. [8]. The encryption scheme utilizes chaotic mapping, password-based fuzzy shifts, and logical XOR with shift registers to enhance key complexity. The scheme is implemented on MATLAB and AVR microcontroller. The scheme shows strong immunity to various cryptographic attacks. However, its reliance on fuzzy logic and specific hardware modeling limit generalizability and real-time adaptability across diverse IoT platforms. The work presented in ref. [9] a multiple-image encryption scheme utilizing spatial multiplexing, encryption is achieved via Fresnel diffraction and Fibonacci Lucas transform, creating a rich key space for improved security. While offering strong theoretical and experimental validation, the system's optical complexity and hardware dependency may limit scalability and integration into typical IoT or low-resource environments. The work presented in ref. [10] proposes a new image encryption scheme based on a one-dimensional piece-wise quadratic polynomial chaotic map (PWQPCM), offering enhanced chaotic behavior. It utilizes pixel segmentation, substitution, and diffusion for secure encryption with low time cost. While the scheme shows promising results in simulations, its performance under hardware constraints and resistance to advanced crypt-analysis require further exploration for practical deployment. The use of deep learning algorithms has also gained significant attention from the researchers in the field of cryptography. Due to the ability to learn complex patterns and optimized performance of neural networks, are being widely utilized in the generation of nonlinear mapping S-boxes and random sequences for cryptography. By adjusting the parameters in training, deep learning frameworks have been utilized to increase the nonlinearity and avalanche effects of S-boxes. The work presented in ref. [11], has presented a novel algorithm that utilizes a Generative Adversarial Network (GAN) to create cryptographic keys with high entropy, enhancing resistance to brute force attacks. To secure wireless sensor networks (WSN) in vehicular networks, the work presented [12], introduces a deep learning-based intrusion detection and prevention system. In this mechanism, to analyze the data from the WSN-DS dataset, CNN is utilized. The proposed approach addresses security challenges in WSNs and demonstrates significant improvements over existing methods. The study presented in ref. [13] introduces a deep-learning-based framework, DeepEDN that can be utilized for secure medical image encryption. Using a Cycle-GAN network, medical images are transformed between original and encryption and restored via a reconstruction network for decryption. The schemes discussed in this section do not protect salient information under data loss or cropping attack. This study fills the research gap by introducing lightweight encryption scheme that safeguards image saliency within an SPN structure, balancing security with high throughput. In this SPN architecture, the substitution is done through pre-computed S-boxes that are generated by utilizing chaotic maps and RNNs. The S-box generation approach employs the Logistic Chaotic Map to generate a sequence that serves as input to an RNN, which undergoes iterative training to t optimized S-box values. These values are designed to meet critical cryptographic criteria, including Nonlinearity (NL), Strict Avalanche Criterion (SAC), Bit Independence Criterion (BIC), and Linear Approximation Probability (LAP), ensuring robust security properties. The encryption framework incorporates block and bit-level permutations to effectively distribute salient image features, while multiple rounds of S-box substitutions ensure confusion. This layered approach significantly amplifies protection for critical information while maintaining a lightweight architecture, Important for resource-constrained IoT devices.

1.1 Research objective

This research addresses the protection of saliency in images within an IoT framework. By developing an advanced, lightweight encryption scheme, we aim to overcome the limitations of traditional block ciphers in high-security IoT applications [14–40]. The primary contributions of this work are as follows (see Figure 1):

1. To protect saliency in RGB images, we introduce a lightweight encryption scheme that safeguards image saliency within an SPN structure, balancing security and computational complexity with high throughput.
2. For the SPN encryption scheme we proposed chaos and RNN based highly nonlinear S-box generation method achieving robust cryptographic properties.
3. To disperse the salient information in the encrypted image a block shuffling algorithm is implemented.



Goal: Develop a lightweight encryption scheme to protect saliency in RGB images within IoT frameworks.

Why: Traditional block ciphers are inefificient for high-security resource-constrained IoT applications

KEY CONTRIBUTIONS
INPUT RGB IMAGE
Efficient. high-throughput encryption
CHAOS + RNN S-box Generation
Highly nonlinear S boxes Strong cryptographic properties for SPN
BLOCK SHUFFLING
Disperses salient data in encrypted image
ENCRYPTED IMAGE
SALIENCY PROTECTED

Figure 1: Research objectives of proposed study.

1.2 Organization of the paper

The paper is organized as follows: Section 2 added the problem formulation by highlighting the strengths and gap analysis for the proposed investigation. Section 3 provides a detailed setup of the experimental environment and the specifications of the dataset utilized in the security analysis of the proposed saliency-preserving lightweight encryption scheme. The proposed encryption scheme follows SPN architecture; for the Substitution, S-boxes are pre-generated using RNN. Section 4 is devoted to the discussion on the generation of these S-boxes. To check the cryptographic strength and feasibility of the generated S-boxes in the proposed scheme, the analysis of the proposed S-boxes is carried out and listed in Section 5 of the paper. Section 6 is devoted to the discussion on the proposed encryption scheme, and Section 7 carries out the analysis of the proposed encryption scheme. Finally, the conclusion is drawn in Section 8 of the article.

2 Problem formulation

The rapid advancement of Internet of Things (IoT) technologies has transformed the acquisition, processing, and exploitation of real-time imaging data in applications such as smart infrastructure and public safety, surveillance, intrusion detection, driverless vehicles, medicine diagnostics, and robots. In these applications, the imagery acquired has salient components faces, license plates, signs of disease, or other objects of significance in assisting humans and computer vision systems to make decisions. These salient components must be preserved because of corruption or loss of them during transmission and decryption might render the data useless for operations purposes. Traditional block ciphers, like advanced encryption standard (AES) is applied to fixed-size data blocks of substitution–permutation rounds tailored for generic secrecy with no built-in capability to privilege or protect prominent visual information. As such, in practical transmission applications with burst errors, partial data corruption, or deliberate cropping, traditional cryptographic methods tend to lead to permanent distortion of important areas (see Figure 2). This deficiency undermines the integrity and usability of security sensitive and mission-critical IoT-enabled imaging applications.

The importance of the problem inability of traditional encryption mechanisms to preserve salient regions offers a direct threat to operational decision-making under high-stakes scenarios such as identifying suspects in video surveillance, identifying abnormalities in radiological

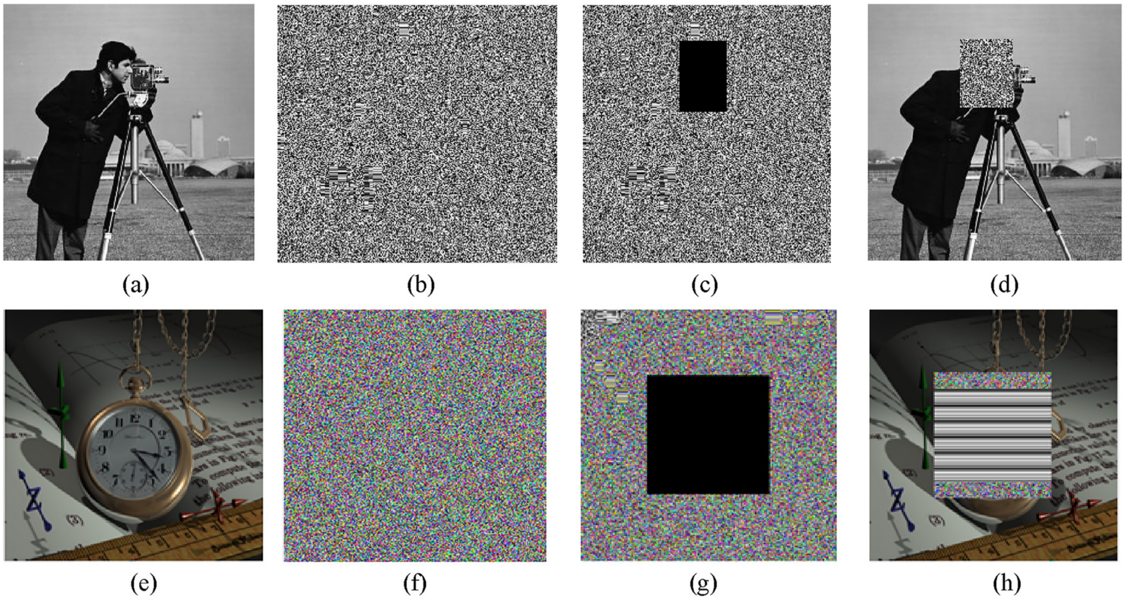


Figure 2: Cropped AES-encrypted images from the center region and their corresponding decrypted cat images for different crop sizes: (a) original image, (b) AES encrypted image, (c) cropped image, (d) recovered image, (e) original image, (f) AES encrypted image, (g) cropped image, (h) recovered image.

images, or detecting perils in driverless navigation. Under scenarios where each pixel of critical information has the potential to make or break safety, security, or life-saving responses, loss of these features undermines the very purpose of the imaging system itself. Bridging this gap requires creating a fast, salient-information-preservation-oriented encryption scheme where secure confidentiality is ensured and, simultaneously, ensures these decision-critical regions are saved and readable even under uncooperative transmission scenarios.

3 Experimental setup

The image encryption scheme was implemented using MATLAB 2017b on a personal computer featuring an Intel(R) Core(TM) i7-7700 CPU, operating at 3.60 GHz, with 8GB of RAM and running on the Windows 10 platform. The effectiveness of the scheme was assessed using a dataset comprising ten RGB images as shown in Figure 3. The dataset comprises a diverse collection of images varying in content, resolution, and file size, making it well-suited for evaluating image encryption schemes. It includes standard benchmark images like Barbara, Peppers, and Baboon, as well as high-resolution real-world scenes such as Riverfront Walkway and Outdoor Gathering. Resolutions range from 512 × 512 to 1,916 × 1,078, and file sizes vary from approximately 110–800 KB, as shown in Table 1. This mix of synthetic and natural images, with varying textures and complexities, ensures a comprehensive assessment of the encryption algorithm's performance across different visual scenarios. We have used standard test images data set [14] and VisDrone2019-DET datasets [15] and are commonly utilized in image processing literature, making comparisons possible with another research.

4 S-box generation methodology

The encryption scheme immunity to differential and linear cryptanalysis depends heavily on the S-boxes. In this section, we present a novel S-box generation technique using RNNs and chaotic maps. The proposed method utilizes RNN architecture with a Long Short-Term Memory (LSTM) layer. The LSTM layer contains 100 hidden units. This is followed by a fully connected layer of size 256 (matching the number of 8-bit S-box values), a softmax layer for class probability distribution, and a classification layer. The technique relies on a formal mathematical framework using matrix algebra and modular arithmetic. The sequence of steps involved in this algorithm is given as follows (see Figure 4):

Step 1: Initialization of Parameters

The initialization of parameters is a critical step to ensure the stability and performance of the chaotic sequence and neural network-based S-box generation process. The chaotic sequence is initialized using the Logistic Map with a control parameter $r = 3.99$ and an initial value

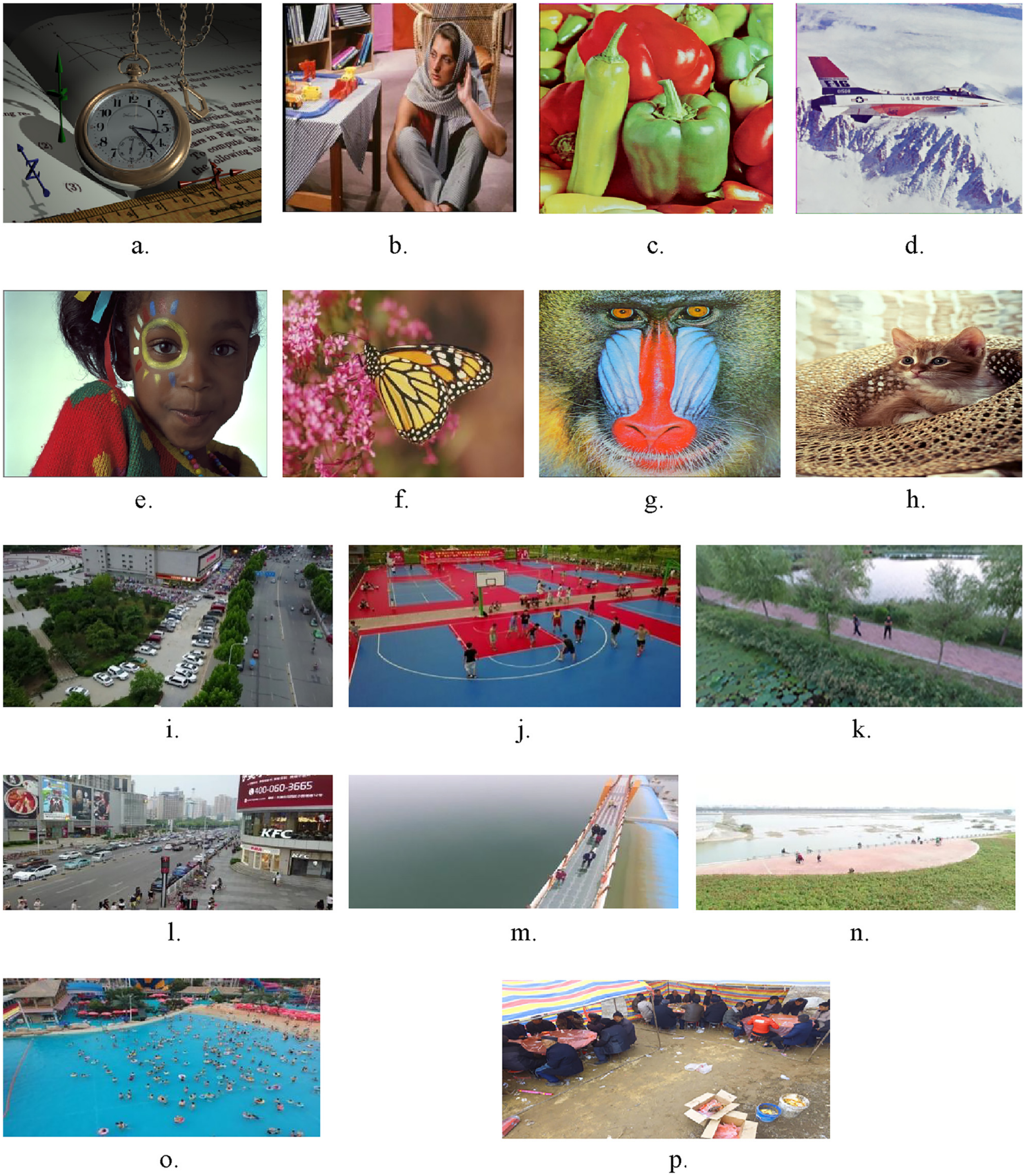


Figure 3: Image dataset used for performance evaluation. The dataset includes twelve color images of varying resolutions and sizes, representing both natural and synthetic scenes. (a) Watch, (b) Barbara, (c) Peppers, (d) airplane, (e) girl, (f) monarch, (g) Baboon, (h) cat, (i) aerial parking view, (j) outdoor sports court, (k) lakeside pathway, (l) urban street view, (m) glass bridge walkway, (n) riverfront walkway, (o) waterpark crowd, (p) outdoor gathering.

Table 1: Specifications of images used for the evaluation of proposed encryption scheme.

Image	Dimension	Size	Bit depth
Watch	1,024 × 768	700	24
Barbara	787 × 576	650	24
Peppers	512 × 512	550	24
Airplane	512 × 512	450	24
Girl	768 × 512	610	24
Monarch	768 × 512	600	24
Baboon	512 × 512	620	24
Cat	490 × 733	650	24
Aerial parking view	960 × 540	110	24
Riverfront walkway	1,916 × 1,078	380	24
Waterpark crowd	1,389 × 1,042	234	24
Outdoor gathering	1,400 × 1,050	225	24

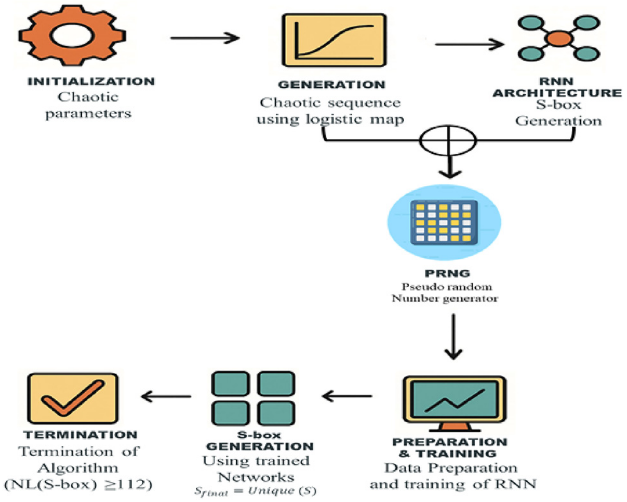


Figure 4: Flowchart of the proposed chaotic RNN-based S-box generation. The process starts with initialization of control parameter $r = 3.99$ and an initial value $x_0 = 0.5$, followed by generation of chaotic sequences using a logistic map. These sequences are used in the RNN architecture for S-box generation.

$x_0 = 0.5$, both chosen to ensure high sensitivity and chaotic behavior. For the RNN, the number of hidden units is set to 100 to balance model complexity and training efficiency. The network is trained using the Stochastic Gradient Descent with Momentum (SGDM) optimizer, with a learning rate of 0.01 and a total of 100 epochs. The parameters for chaotic map and S-box generation using RNN are initialized.

Step 2: Generation of Chaotic Sequence Using Logistic Map

The parameter space as a transformation on a metric space $\mathbb{R}^n$, extended to matrix space $M_{m\times n}(\mathbb{Z}_n)$. Define the chaotic mapping $\mathcal{F}: M_{m\times n}(\mathbb{Z}_n) \to M_{m\times n}(\mathbb{Z}_n)$ as:

$$X_{t+1} = \lambda X_t (I - X_t) \bmod n, \quad X_0 \in M_{m\times n}(\mathbb{Z}_n) \tag{1}$$

The normalization mapping $\mathcal{N}: M_{m\times n}(\mathbb{Z}_n) \to [0,1]^{m\times n}$ is given by:

$$X_t^{(\text{norm})} = \frac{X_t - \min(X)}{\max(X) - \min(X)} \tag{2}$$

Step 3: RNN Architecture for S-box Generation

The transformation from input X_t output Y_t modeled as:

- Hidden state update (Recursive transformation in modular Hilbert space $\mathcal{H}_n$)

$$H_t = f(W_h H_{t-1} + U_h X_t + b_h) \bmod n. \tag{3}$$

- Activation function as a nonlinear mapping in modular space

$$f(Z) = \tanh(Z) \bmod n. \tag{4}$$

- Output computation with softmax projection in modular space

$$Y_t = \sigma(W_y H_t + b_y) \bmod n, \tag{5}$$

where W_h, U_h, b_h, W_y, b_y are trainable weight matrices over $M_{m\times n}(\mathbb{Z}_n)$).

Step 4: Data Preparation and Training of RNN

Define the categorical target modular vector space $Y_n = \{0, 1, \ldots, 255\} \bmod n$. The RNN is trained by minimizing the cross-entropy loss function:

$$L = -\sum_{i=1}^{n} Y_i \log(\hat{Y}_i) \bmod n. \tag{6}$$

The parameter updates using modular gradient descent on the loss manifold are given by:

$$\begin{cases} \Delta W_h = -\eta \nabla_{W_h} L \bmod n, \\ \Delta U_h = -\eta \nabla_{U_h} L \bmod n, \\ \Delta b_h = -\eta \nabla_{b_h} L \bmod n, \\ \Delta W_y = -\eta \nabla_{W_y} L \bmod n, \\ \Delta b_y = -\eta \nabla_{b_y} L \bmod n, \end{cases} \tag{7}$$

where η is the learning rate controlling convergence over $M_{m\times n}(\mathbb{Z}_n)$.

Step 5: S-box Generation using Trained Network

The trained network generates Y_t iteratively, and the S-box values S are extracted as:

$$S[i] = \arg\max Y_t \bmod n. \tag{8}$$

Ensuring uniqueness via an injective mapping:

$$S_{\text{final}} = \text{Unique}(S) \mod n. \tag{9}$$

where duplicate values are replaced iteratively to maintain bijection over $M_{m \times n}(\mathbb{Z}_n)$.

Step 6: Termination of Algorithm

The S-box nonlinearity NL(S) is computed as a measure of security strength with the condition:

$$\text{NL}(S) \geq 112 \mod n, \tag{10}$$

then the algorithm terminates. Otherwise, the initial chaotic parameter is perturbed infinitesimally:

$$X_0 \leftarrow X_0 + \delta \mod n, \quad \delta \ll 1, \tag{11}$$

Leading to a new transformation $\mathcal{F}$, followed by retraining the RNN and regenerating NL($\boldsymbol{S}$) meets the required cryptographic threshold. The generated S-boxes are shown in Tables 2–4.

5 Evaluation of S-boxes

Substitution boxes are assessed based on a range of criteria that determine their effectiveness. Key attributes considered in this evaluation are Nonlinearity (NL), Bit Independence Criteria (BIC), Strict Avalanche Criteria (SAC), Linear Approximation Probability (LAP), and Differential Approximation Probability (DP).

5.1 Nonlinearity (NL)

S-box is designed to mask the relationship between the encryption key and the resulting cipher text, enhancing the security of the encryption process. One way to measure the effectiveness of an S-box in achieving this goal is through its nonlinearity. Nonlinearity quantifies how well the S-box resists linear approximations. This measure of nonlinearity for an S-box can be determined by using the mathematical formula in Eq. (12):

$$\text{NL} = 2^{n-1} - \frac{1}{2}\max\left(\left|W_f(a)\right|\right). \tag{12}$$

The nonlinearity of the projected S-boxes is computed and tabulated in Table 5. Table 6 shows the comparison of the nonlinearities of the projected S-boxes and state of the art S-boxes.

Figure 5 shows the nonlinearity values of all eight Boolean functions of each of the proposed S-boxes, with each of them attaining the best score of 112. The nonlinearity measures the minimum Hamming distance of a Boolean function from the set of affine functions, and larger values reflect greater resilience against linear cryptanalysis. The uniform attainment of the highest possible magnitude among all Boolean components across the substitution level ensures no output bit has lower security, eliminating potential weaknesses exploitable by linear approximations of outputs. In addition, the consistent outcomes among the three proposed S-boxes demonstrate the strength and reproducibility of the utilized RNN-aided nonlinear S-box

Table 2: RNN based nonlinear S-box 1.

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

Table 3: RNN based nonlinear S-box 2.

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

Table 4: RNN based nonlinear S-box 3.

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

Table 5: Nonlinearity of proposed S-boxes.

	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	**Average**
Proposed S-box 1	112	112	112	112	112	112	112	112	112
Proposed S-box 2	112	112	112	112	112	112	112	112	112
Proposed S-box 3	112	112	112	112	112	112	112	112	112

generation technique. The uniform attainment ensures even confusion properties across the substitution layer, essentially improving the whole cipher's resistance to analytical attack in both lightweight and cryptographic applications of high security.

5.2 Bit Independence Criteria (BIC)

A vector Boolean function $f\colon \{0,1\}^n \rightarrow \{0,1\}^n$ meets the Bit Independence Criteria (BIC) if a single bit change in the input causes a change in the output. This means that

Table 6: Comparison of cryptographic characteristics of proposed S-boxes with existing nonlinear confusion components of modern block ciphers.

	Nonlinearity	SAC	BIC-NL	BIC-SAC	LAP	DAP
Proposed S-box 1	112	0.5022	112	0.500	0.0620	0.0156
Proposed S-box 2	112	0.5002	112	0.505	0.0620	0.0156
Proposed S-box 3	112	0.4899	112	0.5046	0.0620	0.0156
Ref. [16]	114	0.4975	112	0.508	0.1360	0.1000
Ref. [17]	112	0.5063	104.3	0.5083	0.1250	0.0468
Ref. [18]	106.75	0.5020	103.6	0.5023	0.1328	0.0391
Ref. [19]	108	0.4941	108	0.5141	0.0781	0.0156
Ref. [20]	110	0.500732	108	0.5036	0.0781	0.0156
Ref. [21]	110	0.500732	108	0.5036	0.0781	0.0156
Ref. [22]	110.25	0.4951	103.36	0.4951	0.0625	0.0156
Ref. [23]	112	0.5031	112	0.5112	0.0926	0.0291
Ref. [24]	110	0.5005	102.78	0.5001	0.1328	0.0390

each bit in the output is independently influenced by any bit change in the input, helping ensure that minor changes in the input data lead to unpredictable, widespread changes in the output. The Bit Independence Criteria (BIC) value ranges from 0 to 1, with a value near 0.5 indicating optimal performance for a cryptographic S-box. Table 6 presents the BIC measurements for each of the proposed S-boxes.

5.3 Strict Avalanche Criteria (SAC)

The Strict Avalanche Criterion (SAC) for an S-box $S\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ states that for any input $x \in x \in \mathbb{F}_2^n$ and any bit i of x, flipping x_i should change each output bit $S_j(x)$ with probability 0.5. Mathematically, SAC is defined as:

$$\Pr\big(S_j(x) \neq S_j\big(x \oplus e_i\big)\big) = 0.5, \quad \forall x \in \mathbb{F}_2^n, \quad \forall i \in \{1, \ldots, n\}, \quad \forall j \in \{1, \ldots, m\}, \tag{13}$$

where e_i is the unit vector with a 1 in the i-th position. For a cryptographic S-box to meet this criterion, it must achieve a SAC value of 0.5, reflecting its ability to disrupt predictable patterns in the output and enhance overall security.

5.4 Differential Approximation Probability (DAP)

Let $S\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be an S-box. The Differential Approximation Probability (DAP) is given by [29]:

$$\mathrm{DAP}(S) = \max_{\Delta x \in \mathbb{F}_2^n \setminus \{0\}, \Delta y \in \mathbb{F}_2^m} \frac{D_S\big(\Delta x, \Delta y\big)}{2^n}, \tag{14}$$

where the differential distribution table (DDT) entry is defined as:

$$\mathrm{DS}\big(\Delta x, \Delta y\big) = \#\big\{x \in \mathbb{F}_2^n \big| S(x) \oplus S(x \oplus \Delta x) = \Delta y\big\}, \tag{15}$$

Thus, DAP(S) quantifies the maximum probability over all nonzero input differences Δx and output differences Δy, satisfying:

$$\frac{1}{2^m} \leq \mathrm{DAP}(S) \leq \frac{\delta(S)}{2}, \tag{16}$$

where the differential uniformity is:

$$\delta(S) = \max_{\Delta x \neq 0} \max_{\Delta y} D_S\big(\Delta x, \Delta y\big). \tag{17}$$

A lower DAP(S) value corresponds to higher resistance against differential cryptanalysis. The ideal DAP is close to zero, while the theoretical maximum is 1. Evaluating DAP is important for assessing the S-box's resilience against differential analysis, with results for both the proposed and literature-based S-boxes shown in Table 7.

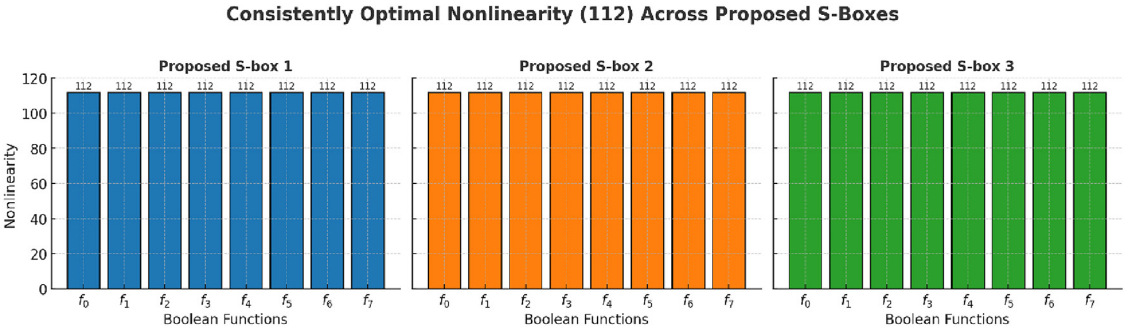


Figure 5: Comparison of nonlinearity values for Boolean functions $f_0 - f_7$ across three proposed S-boxes. Each proposed S-box achieves consistently optimal nonlinearity of **112**, demonstrating strong resistance to linear cryptanalysis and uniform performance across all Boolean components.

Table 7: Fixed point analysis of proposed mechanism.

S-box	Fixed point	Repulsive fixed points
Ref. [16]	0	0
Ref. [17]	3	1
Proposed S-box 1	0	0
Proposed S-box 2	0	0
Proposed S-box 3	0	0

5.5 Linear Approximation Probability (LAP)

For an S-box $S\colon \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, the Linear Approximation Probability (LAP) quantifies the maximum bias of any linear approximation between input and output bits. It is defined as:

$$\mathrm{LAP}(S) = \max_{\alpha \in \mathbb{F}_2^n \setminus \{0\}, \beta \in \mathbb{F}_2^m} \left| \frac{2W_S(\alpha, \beta)}{2^n} - 1 \right|, \tag{18}$$

where the Walsh-Hadamard correlation is given by:

$$W_S(\alpha, \beta) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha \cdot x} \oplus \beta \cdot S(x) \tag{19}$$

LAP values for the proposed and literature-based S-boxes are presented in Table 6 to show their resistance to linear cryptanalysis.

Figure 6 show a side-to-side comparison of the given S-boxes (S-box 1, S-box 2, and S-box 3) with the existing nonlinear confusion components of contemporary block ciphers, evaluated across six basic cryptographic strength indicators having a direct impact on cryptanalytic attack resistance.

In nonlinearity metric, all the proposed S-boxes achieve an ideal uniform level of 112, which approaches the upper theoretical limit of 8-bit balanced S-boxes and offers fair resistivity against linear cryptanalysis by minimizing the correlation of the linear approximations and true input–output mapping to a minimum degree. The output of the Strict Avalanche Criterion (SAC) is kept decisively around the ideal 0.5 boundary level, such that single-bit input variation induces an even and extensive output variation and boosts unpredictability and slows down differential and statistical attack analyses. In the case of BIC with reference to BIC-NL, the designs put forward again achieve the ideal 112, with no exploitable linear relationships of output bits among them which is a property useful in defying correlation attack types. The BIC-SAC scores, again close to ideal 0.5, confirm this independence of avalanche spread, defying once more any statistical guess an attacker might make.

The proposed S-boxes have the LAP among the lowest seen (0.0620), thereby directly improving immunity to Matsui's linear cryptanalysis by minimizing the highest success probability of linear approximations. Finally, the DAP results (0.0156) are tied to the minimum achievable limit for 8-bit S-boxes, thereby drastically restricting the practicability of Biham–Shamir differential cryptanalysis by minimizing the highest differential propagation probability. Figure 6 and Table 6, clearly reveal the fact that the proposed S-boxes are not only comparable but, in some cases, superior to existing confusion elements in cryptographic power, and they possess better resistivity to a vast spectrum of classical and modern block cipher assaults.

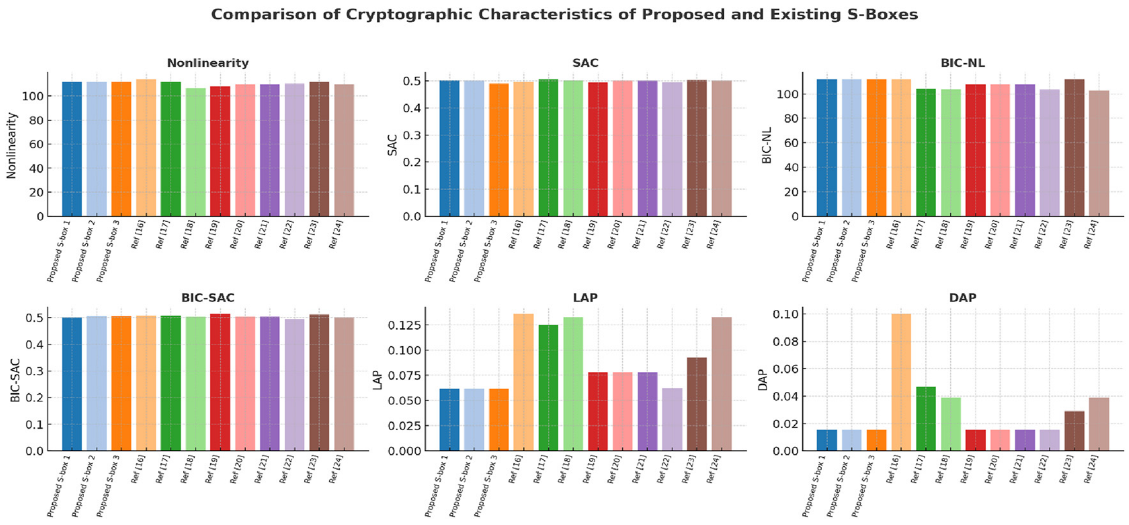


Figure 6: Visual comparison of cryptographic characteristics for the proposed S-boxes and existing nonlinear confusion components from modern block ciphers.

5.6 Bijectivity

Bijectivity is an important property of S-boxes in cryptography, ensuring each input maps to a unique output and every output have a distinct input. This one-to-one mapping prevents attackers from inferring input values from outputs and adds critical confusion and diffusion to the cryptographic process. In our case, the S-boxes meet the bijectivity criterion by containing unique values from 0 to 255.

5.7 Fixed point analysis

A strong fixed point satisfies:

$$S^{-1}(x) = x \text{ and } S(x) = x. \tag{20}$$

The number of strong fixed points is:

$$\mathrm{SF}(S) = \left\{x \in \mathbb{F}_2^n \middle| S(x) = x \text{ and } S^{-1}(x) = x\right\}. \tag{21}$$

A cryptographically strong S-box should minimize $|\mathcal{F}(S)|$ to resist fixed-point attacks. Ideally, a secure S-box has no fixed points (i.e., $|F(S)| = 0$). If FPR(S) deviates significantly from $\frac{1}{2^n}$, it may indicate structural weaknesses exploitable in certain cryptographic attacks. The proposed S-boxes (1, 2, and 3) contain no fixed points and no repulsive fixed points, which mean good resistance to fixed-point attacks as shown in Table 8. Compared with [16, 17], the proposed S-boxes are superior, particularly to the potential cryptanalytic weaknesses concerning fixed points. The absence of fixed points ensures that no input remains invariant under substitution, which enhances nonlinearity and differential properties necessary for cryptographic strength.

Table 7 outlines the fixed point analysis of the provided S-boxes against prevalent nonlinear confusion elements. In cryptography design, a fixed point, where $S(x) = x$, or a repulsive fixed point, where inputs map close to themselves under repeated application, introduces structural vulnerabilities exploitable in chosen-plaintext and algebraic attacks. The proposed S-box 1, S-box 2, and S-box 3 exhibit zero fixed points and zero repulsive fixed points, ensuring the absence of identity mappings or short cycles that could weaken cipher strength. This structural robustness, combined with the high nonlinearity, optimal SAC, and low LAP/DAP values demonstrated in Table 7, confirms the proposed mechanism's enhanced resistance to linear, differential, and structural cryptanalysis, making it a highly effective and secure choice for modern block cipher architectures.

Table 8: Number of rows and columns to be added after zero padding.

Image	Dimension	Number of rows to be added	Number of columns to be added	Size after zero padding
Watch	1,024 × 768	0	0	1,024 × 768
Barbara	787 × 576	1	0	788 × 576
Peppers	512 × 512	0	0	512 × 512
Airplane	512 × 512	0	0	512 × 512
Girl	768 × 512	0	0	768 × 512
Monarch	768 × 512	0	0	768 × 512
Baboon	512 × 512	0	0	512 × 512
Cat	490 × 733	2	3	490 × 736
Aerial parking view	960 × 540	0	0	960 × 540
Riverfront walkway	1,916 × 1,078	0	2	1,916 × 1,080
Waterpark crowd	1,389 × 1,042	3	2	1,389 × 1,044
Outdoor gathering	1,400 × 1,050	0	2	1,400 × 1,052

6 Proposed encryption scheme

The proposed encryption scheme follows SPN architecture, leveraging structured linear transformations, algebraic mappings, and modular arithmetic in $M_{m\times n}(\mathbb{Z}_n)$ to ensure high security via diffusion and confusion mechanisms. The steps are given as follows:

Step 1: Preprocessing and Image Partitioning

The image is partitioned into $b \times b$ blocks. If the image is not multiple of $b \times b$, zero padding is done. To make the image divisible by block size 4 × 4, Table 8 lists the number of rows and zeros to be added. By doing this the image gets divisible by block size and can be portioned into blocks for further process. Define the image as a matrix $I \in M_{m\times n}(\mathbb{Z}_n)$ within the modular vector space. A projection mapping is applied:

$$I' = P(I), \quad P\colon M_{m\times n}(\mathbb{Z}_n) \to M_{m'\times n'}(\mathbb{Z}_n), \tag{22}$$

where m', n' are the nearest multiples of block size b, ensuring uniform partitioning into $b \times b$ subspaces for encryption operations.

Step 2: Permutation Transformation

To disperse the salient information in the image, the blocks of images are permuted using a permutation transformation. Using a logistic chaotic map, construct a permutation matrix $P_M \in M_{b\times b}(\mathbb{Z}_n)$ as an algebraic transformation:

$$\text{Row } P_M = \text{sort}\left(\lambda x_t\left(1 - x_t\right) \bmod n\right), \tag{23}$$

where x_t follows a chaotic sequence. The number of rows and blocks are checked in the image and based on that the first row or column of the permutation matrix is generated using Eq. (23), the remaining rows/columns are the shifted version of first row/column. The dimensions of the permutation matrix depend on the dimensions of blocks. Apply a block-wise transformation via conjugation:

$$I'' = P_M I' P_M^T, \tag{24}$$

The scrambling and information spreading in the modular space are ensured. The mapping matrix should be such that the first row should contain unique numbers randomly from 1 to G and the remaining rows will consist of numbers that are shifted version of row 1 and it is also essential that the columns must also contain unique values.

Step 3: Bit-Level Parity Mapping

The parity based mapping is data-dependent and provides immunity against the chosen plaintext. For this, define a parity mapping operator $\mathcal{P}$ as an injective function action on $M_{b\times b}(\mathbb{Z}_n)$:

$$\mathcal{P}: \{0,1\}^8 \rightarrow \{0,1\}^8 \tag{25}$$

where the bijective reordering function is defined as in Eq. (26) ensuring permutation within each block by altering the even and odd bit distributions.

$$P(b_i) = b_{\pi(i)}, \quad \pi: \text{even}(b) \mapsto \text{odd}(b) \tag{26}$$

Step 4: Nonlinear Algebraic Substitution

Substitution replaces pixel values or bits using nonlinear mappings, which breaks direct statistical relationships between the original image and encrypted image, making cryptanalysis much harder. Substitution is performed using structured S-box transformations in the modular space:

$$S(I'') = S_{8\times 8}(I'') \bmod n, \tag{27}$$

for an 8-bit substitution:

$$S(I'') = S_{4\times 4}(I'') \bmod n, \tag{28}$$

for a **4**-bit transformation, ensuring cryptographic nonlinearity via structured algebraic mappings as shown in Figure 7.

Step 5: Affine Key Mixing via XOR

Introduce a 128-bit encryption key K and apply an affine transformation via modular XOR:

$$I''' = I'' \oplus K \bmod n, \tag{29}$$

where $\oplus$ denotes the affine transformation under modular addition in $M_{m\times n}(\mathbb{Z}_n)$.

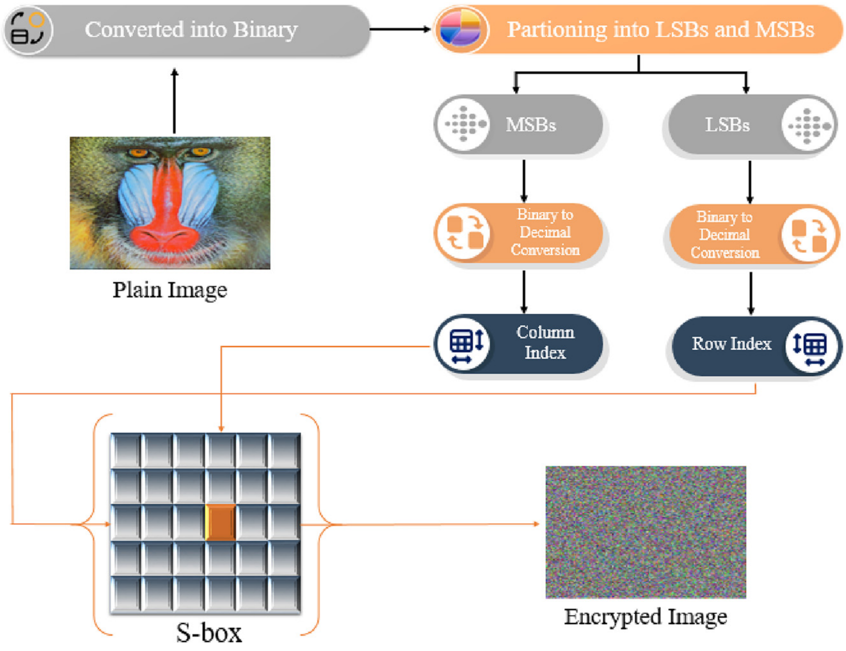

Converted into Binary
Partioning into LSBs and MSBs
MSBs
LSBs
Binary to Decimal Conversion
Binary to Decimal Conversion
Column Index
Row Index
Plain Image
S-box
Encrypted Image

Figure 7: Illustration of the image encryption process using the proposed S-box. The plain image is first converted into binary form, and then partitioned into least significant bits (LSBs) and most significant bits (MSBs). After binary-to-decimal conversion, the resulting values determine the row and column indices used for S-box substitution. This mapping produces the encrypted image, ensuring strong pixel confusion and enhanced security.

Step 6: Circular Shift Transformation

Apply a cyclic shift operator CSCS over the modular space:

$$I'''' = \mathrm{CS}(I'''), \tag{30}$$

where

$$\mathrm{CS}(I)_{i,j} = I_{(i+k) \bmod m, (j+k) \bmod n}, \tag{31}$$

ensuring uniform spreading via structured matrix shifts in $M_{m\times n}(\mathbb{Z}_n)$.

Step 7: Final Nonlinear Substitution and Key Mixing

A final round of S-box substitution is performed, followed by key mixing:

$$I_{\mathrm{enc}} = S(I'''') \oplus K \mod n, \tag{32}$$

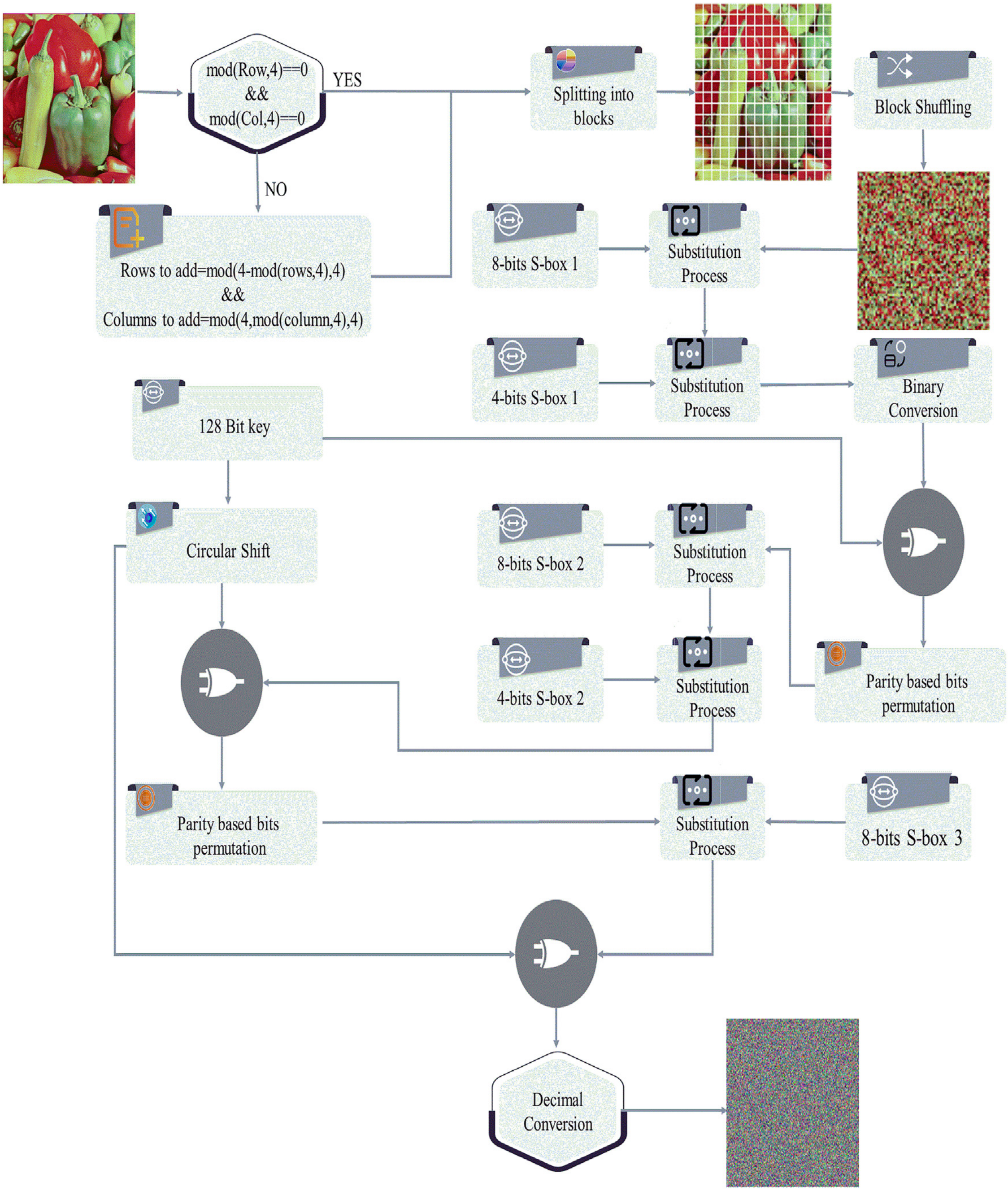


Figure 8: Flowchart of the proposed hybrid image encryption scheme. The plain image is divided into blocks and processed through multiple S-box substitution stages (4-bit and 8-bit), guided by modular conditions and a 128-bit key. Circular shift and parity-based bit permutation operations enhance diffusion and confusion.

ensuring maximal nonlinearity and resistance against cryptanalytic attacks.

Decryption via Inverse Transformations

Decryption follows a structured sequence of inverse transformations, restoring the original image:

$$I = S^{-1}\left(\mathrm{CS}^{-1}\left(I_{\mathrm{enc}} \oplus K\right)\right)P_M^{-1}, \tag{33}$$

where each inverse function is systematically applied in $M_{m\times n}\left(\mathbb{Z}_n\right)$ to ensure accurate recovery. This encryption framework provides robust diffusion, confusion, and algebraic security, making it highly resilient to differential and statistical attacks while ensuring computational efficiency in modular arithmetic spaces. The encryption scheme is shown in Figure 8.

7 Security analysis

To check the immunity of the proposed scheme against various cryptographic threads, the security analysis is of vital importance. The security analysis includes key analysis, histogram, differential, correlation and entropy analysis. To check the protection of salient information we utilize cropping analysis. For the speed of the encryption, throughput analysis is carried out.

7.1 Encryption key analysis

In this examination, two critical analyses, Key Space analysis and key sensitivity analysis, are employed and presented accordingly.

7.1.1 Brute force analysis

A brute-force attack tries each possible encryption key in a systematic way until the proper one is located. With the scheme envisioned here, the implementation of a 128-bit encryption key implies a key space of 2^{128} possible combinations, which significantly exceeds the commonly recommended cryptographic security threshold of 2^{100} [26]. Such a large key space makes comprehensive key searches computationally infeasible for any practical adversary, even one with powerful computing capabilities. Table 9 provides a comparative evaluation of the new scheme's key space with recently established algorithms, showing large variability across schemes. The AES standard, for example, also uses 128-bit key space (2^{128}), with strong and highly reputable security. While widening the key space particular beyond 2^{512} practical for brute-force resistance and future-proof security for the advent of new threats like quantum computing but also provides trade-offs. Relatively large key sizes require larger memory and increased processor power for encryption and decryption and can have effects in real-time or processor-starving environments, like IoT devices [27]. Our proposed scheme puts such consideration in a balanced state with secure yet computationally feasible design.

Table 9: Comparison of key space analysis of recently projected encryption scheme.

Algorithm	Key space length	Comparison with 2^{100}
Ref. [21]	2^{1754}	Exceeds threshold significantly
Ref. [28]	2^{212}	Exceeds threshold
Ref. [29]	2^{4624}	Exceeds threshold significantly
Ref. [30]	2^{512}	Exceeds threshold significantly
Ref. [31]	2^{100}	Matches threshold
Ref. [32]	2^{200}	Exceeds threshold
Ref. [33]	2^{279}	Exceeds threshold
Proposed	2^{128}	Exceeds threshold

7.1.2 Key sensitivity analysis

We carried out an exhaustive key sensitivity analysis to test the strength of our encryption system. In experiment 1, the encryption and decryption operation with Key 1 effectively recovered the original image, validating the accuracy of the decryption process. In Experiment 2, the original image was encrypted using Key 1 but decrypted with Key 2, which had only a single-bit change from Key 1. The output was a totally distorted and unrecognizable image, as can be seen from Figure 9. The radical change indicates the high key sensitivity of our scheme, withstanding unauthorized decryption and strengthening the system's capability in protecting sensitive information.

7.2 Histogram analysis

The three dimensional (3D) histogram is the graphical representation of the frequency distribution of the pixel intensities within an image, plotting the range of color combinations within the RGB color space. For a flat image, natural patterns and structures cause noticeable differences in the histogram representation. This can be seen in Figure 10, whereas some of the spheres in the 3D space are clearly larger, and others are smaller. The varying sizes of the spheres indicate that certain color combinations occur more frequently than others. The random placement of spheres at different positions in the 3D cube signifies the presence of different distributions of colors in the original image.

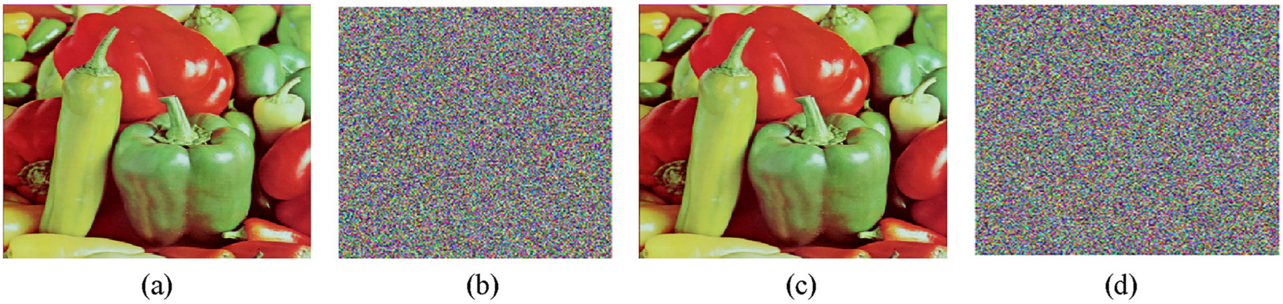


Figure 9: Key sensitivity analysis of suggested encryption algorithm. The image decrypted with one bit changed key does not convey any useful information. (a) Plain image, (b) enciphered image, (c) correctly decrypted image, (d) decrypted image with changed key.

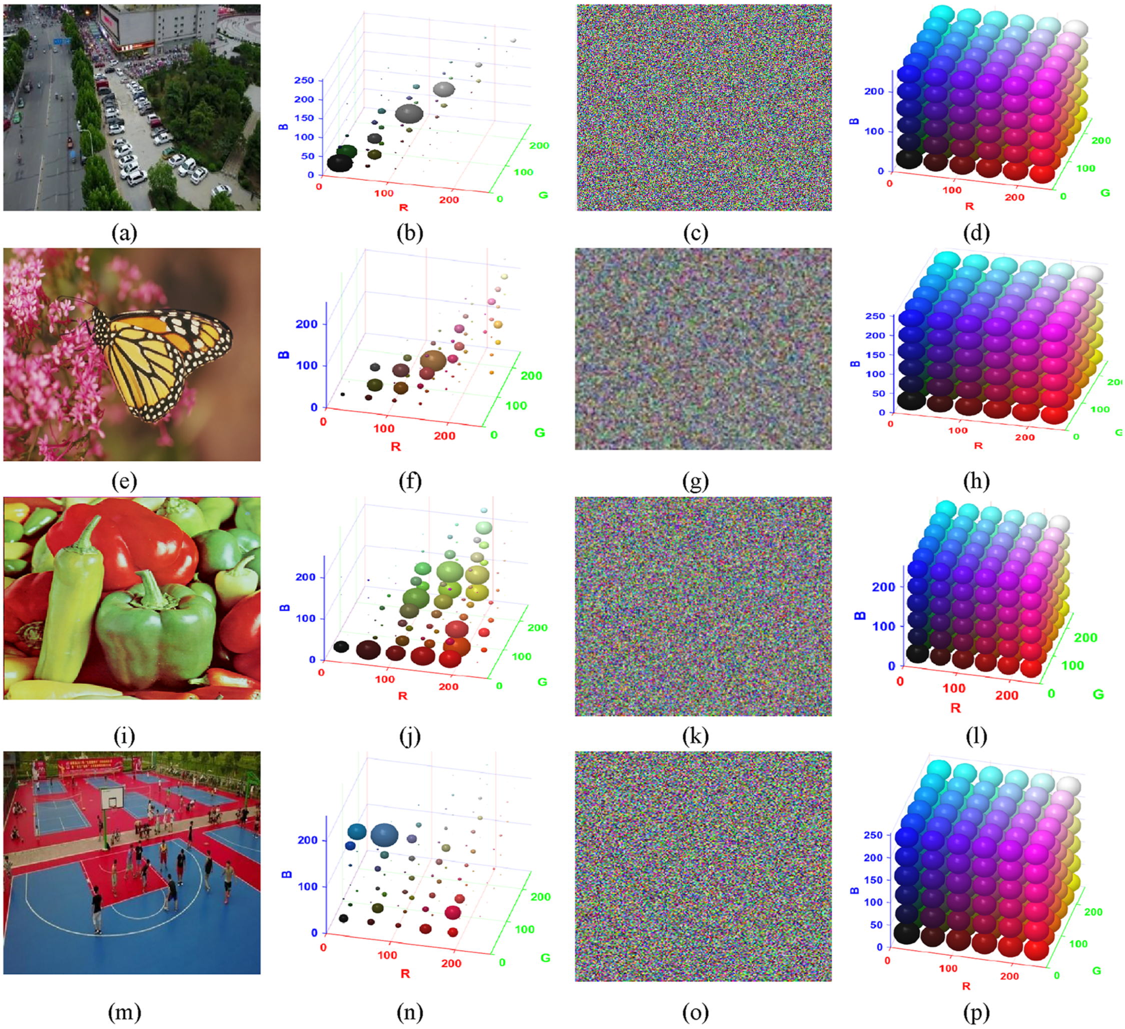


Figure 10: Histogram analysis of the encrypted image. The pixel intensity distribution appears nearly uniform, indicating that encryption effectively conceals statistical features of the original image. This uniformity demonstrates strong resistance against histogram-based and statistical attacks.

When the image is encrypted using the proposed scheme, the cryptographic operation destabilizes the inherent patterns, achieving a high level of diffusion and confusion. The 3D histogram is now evenly distributed, tiling the cube with spheres of equal area. This homogeneity suggests that all color combinations are equally probable, eliminating any prevailing colors or structural dependencies. The absence of variation among the sizes of spheres shows that the distribution of pixel intensity is ideally balanced, in favor of the strength of the encryption mechanism. The transformation of the histogram from non-uniform to a uniform distribution confirms the success of the proposed encryption technique. A uniformly distributed 3D histogram is one of the main signs of high entropy, reducing statistical leakages that might be used in cryptanalysis. The elimination of structured patterns in the encrypted image demonstrates better resistance to statistical and color-based differential attacks. Effectively, the uniformity illustrated in Figure 10 that verifies the proposed scheme achieves a good security level by keeping an equal distribution of colors across the RGB space, making it highly resistant to cryptographic attacks. The detail of three dimensional histograms was introduced.

Figure 11 presents the histogram analysis of the proposed encryption scheme for two test images. The subfigures (a–d) and (i–l) show the original images with their respective red, green, and blue channel histograms, where distinct peaks reflect the uneven distribution of pixel

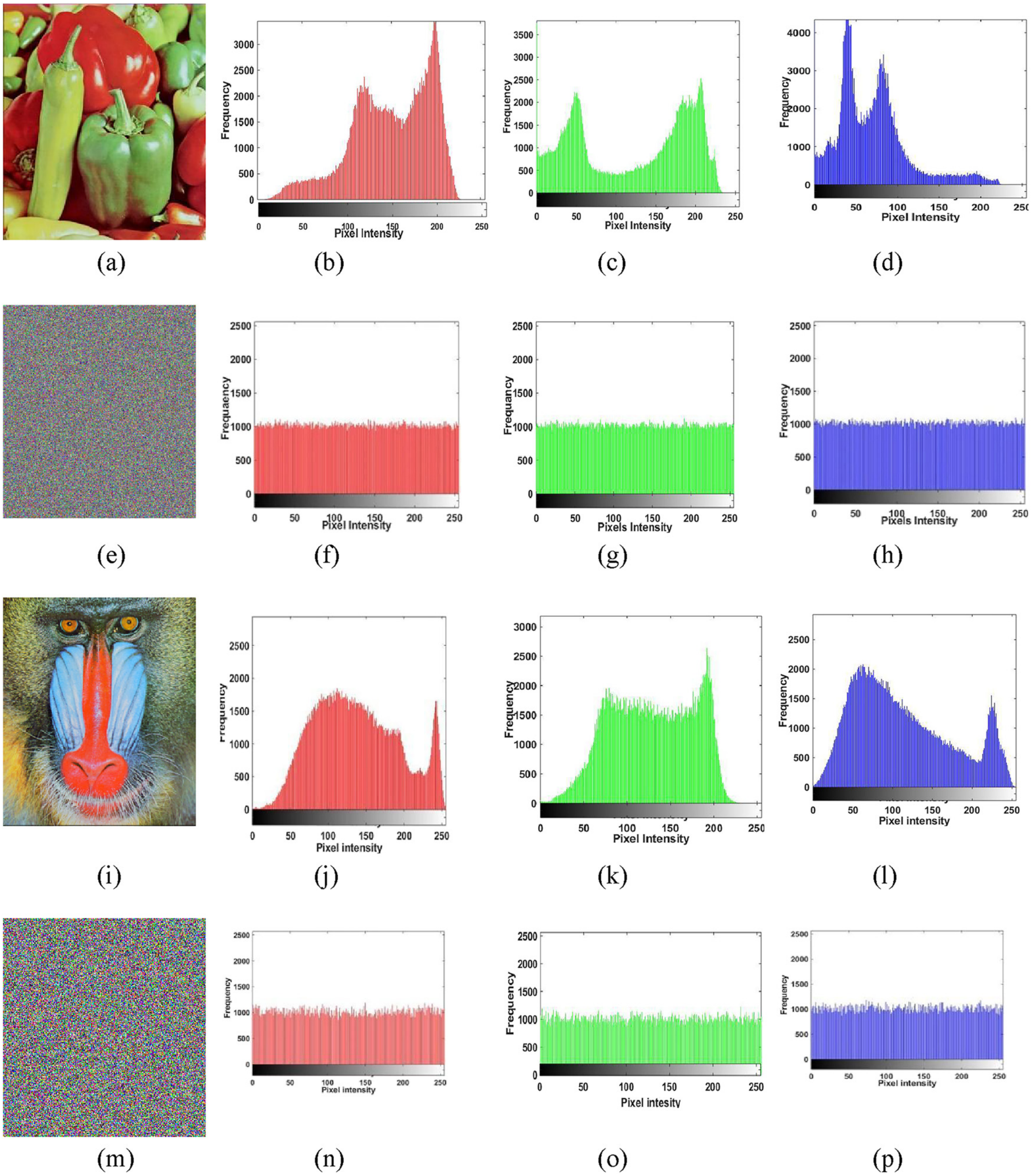


Figure 11: Histogram analysis of the encrypted image. The pixel intensity distribution appears nearly uniform, indicating that encryption effectively conceals statistical features of the original image. This uniformity demonstrates strong resistance against histogram-based and statistical attacks.

intensities typical of natural images. After encryption, shown in (e–h) and (m–p), the histograms for all three color channels become uniformly distributed, indicating that the encrypted images have no visible statistical patterns from the originals. This uniformity demonstrates the scheme's effectiveness in concealing image characteristics, thereby enhancing resistance against statistical attacks.

Figure 12 shows the three-dimensional histograms of the plain and encrypted images for two test cases. In the original images (a–d, i–l), the histograms exhibit sharp peaks and concentrated clusters, indicating strong correlations between neighboring pixel intensities, which is a common trait in natural images. After encryption (e–h, m–p), the histograms become uniformly dispersed across all intensity bins, with no visible peaks or patterns. This transformation confirms that the proposed encryption scheme effectively removes inherent pixel correlations, making the encrypted images statistically indistinguishable and more secure against histogram-based cryptanalysis.

7.3 Differential analysis

Exploiting the encryption algorithm's sensitivity to small changes in the original image, attackers conduct differential attacks. By making minute alterations to the original image, they encrypt both versions using the same secret key, aiming

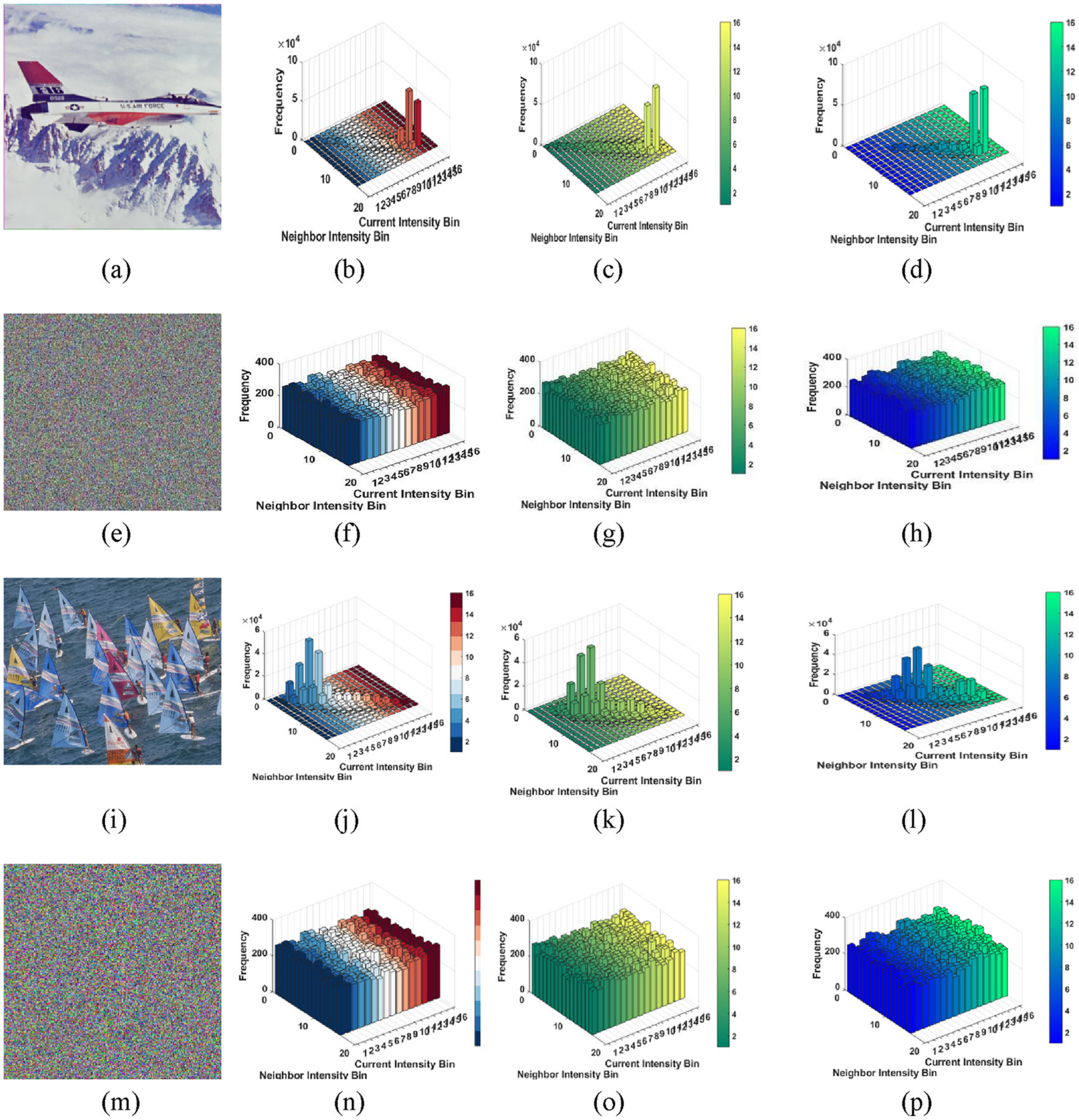


Figure 12: Three dimensional histograms analysis of the encrypted image. The pixel intensity distribution appears nearly uniform, indicating that encryption effectively conceals statistical features of the original image. This uniformity demonstrates strong resistance against histogram-based and statistical attacks.

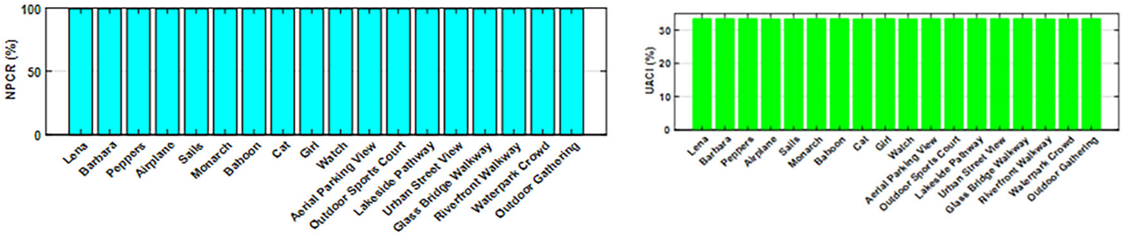


Figure 13: Differential analysis of the proposed encryption scheme. The metrics NPCR and UACI show high values, indicating that small changes in the plain image produce significant differences in the encrypted image. This confirms strong resistance against differential attacks.

to discern the relationship between the resulting cipher texts. To thwart such attacks, the encryption system should produce vastly different cipher texts even with slight modifications to the original image, indicating strong sensitivity. Two analyses are employed to assess the system's resilience against such attacks one is the universal average change intensity (UACI) and the other is the number of pixels change rate (NPCR). UACI measures the disparity in average intensity between two encrypted images derived from an original and a slightly altered single-pixel version. The mathematical expression for NPCR is given as Eq. (34):

$$\text{UACI} = \sum_{a,b} \frac{E(a,b) - E''(a,b)}{255 \times N \times M}, \tag{34}$$

where $N \times M$ represents image dimensions, $E(a,\ b)$ denotes the encrypted plain image, and $E''(a,b)$ signifies the encrypted modified image. UACI values are displayed in Figure 13, compared with a recently developed cryptosystem in Table 10. NPCR, calculated between encrypted images derived from the original and a single pixel modified version, quantifies the percentage change in pixels. A high NPCR value indicates robust immunity to differential attacks in a cryptosystem. Equations (35) and (36), outlines its computation:

$$\text{NPCR} = \frac{\sum_{a,b} D(a,b)}{M \times N} \times 100\ \%, \tag{35}$$

Table 10: Comparison of NPCR and UACI of recently encryption scheme for 512 × 512 images of Lena.

Algorithm	NPCR	UACI
Ref. [34]	99.61	33.46
Ref. [35]	99.63	–
Ref. [29]	99.61	32.50
Ref. [36]	99.60	32.18
Proposed	99.60	33.50

$$D(a,b) = \begin{cases} 0 & \text{if } E(a,b) = E'(a,b) \\ 1 & \text{if } E(a,b) \neq E''(a,b) \end{cases} \tag{36}$$

where $N \times M$ represents image dimensions, $E(a,\ b)$ stands for the encrypted plain image, and $E''(a,b)$ denotes the encrypted modified image are shown in Figure 13, NPCR values are compared with a recently developed cryptosystem in Table 11.

7.4 Correlation analysis

The correlation coefficient (CC) is a key statistical measure for dependency of the neighboring pixels and offers a direct estimate of the encryption efficiency in disturbing the spatial redundancies. In the case of any image, the values of the CC are calculated in the horizontal direction (HC), vertical direction (VC), and diagonal direction (DC) and are bounded in the range [−1, 1]. A CC of 1 reflects perfect linear dependency, a CC of 0 indicates no correlation, and a CC of −1 denotes complete negative correlation. In the flat image, Table 11 depicts CC values near unity (≈0.98) in all orientations for the Lena benchmark, highlighting its inherent vulnerability due to strong pixel associations. In contrast, our proposed RNN–chaos-based S-box encryption mechanism drastically suppresses these correlations, yielding CC values near zero across all directions, thereby eliminating exploitable patterns. This substantial decorrelation serves as a formidable defense against statistical and differential cryptanalysis, ensuring that the cipher image exhibits near-random structural properties. The visual evidence in Figure 14 further corroborates the numerical results. In the plain image correlation plots (Figure 14a, c, and e), pixel clusters are tightly concentrated along the principal diagonal, indicative of strong linear associations. Post-encryption (Figure 14b, d, and f), the pixel distributions become uniformly scattered, illustrating the algorithm's capacity to dismantle deterministic dependencies. This decorrelation, driven by the synergy of chaotic sequence-driven pseudo-random number

Table 11: Correlation analysis of the proposed encryption scheme.

Image		Original	Encrypted	Image		Original	Encrypted
Lena	Vertical	0.97266	0.00231	Monarch	Vertical	0.8953	0.0154
	Horizontal	0.94555	0.0032		Horizontal	0.8433	0.0542
	Diagonal	0.921301	0.0008		Diagonal	0.8129	0.0046
Barbara	Vertical	0.949987	−0.0051	Baboon	Vertical	0.8261	0.0047
	Horizontal	0.91338	−0.0034		Horizontal	0.8737	0.0060
	Diagonal	0.8707	−0.00233		Diagonal	0.7843	0.0020
Peppers	Vertical	0.97051	−0.0015	Cat	Vertical	0.9091	−0.0034
	Horizontal	0.96347	0.0018		Horizontal	0.9623	−0.0019
	Diagonal	0.93652	0.0035		Diagonal	0.8798	−0.0034
Airplane	Vertical	0.930144	−0.0034	Girl	Vertical	0.9921	0.0049
	Horizontal	0.93640	0.0031		Horizontal	0.9755	0.0034
	Diagonal	0.88191	0.0073		Diagonal	0.9705	−0.0023
Sails	Vertical	0.884244	0.0010	Watch	Vertical	0.9206	−0.0037
	Horizontal	0.8389	−0.0198		Horizontal	0.9208	−0.0052
	Diagonal	0.7817	−0.01251		Diagonal	0.8988	−0.0069
Aerial parking view	Vertical	0.989939	0.000928	Glass bridge walkway	Vertical	0.941963	0.001202
	Horizontal	0.918405	0.006507		Horizontal	0.972396	0.000852
	Diagonal	0.964264	0.003373		Diagonal	0.996383	0.006049
Outdoor sports court	Vertical	0.948632	0.002375	Riverfront walkway	Vertical	0.924528	0.000552
	Horizontal	0.961195	0.002576		Horizontal	0.972169	0.003173
	Diagonal	0.999272	0.004021		Diagonal	0.993953	0.005287
Lakeside pathway	Vertical	0.898726	0.006727	Waterpark crowd	Vertical	0.941963	0.0068
	Horizontal	0.978619	0.007899		Horizontal	0.972396	0.002985
	Diagonal	0.900481	0.006322		Diagonal	0.996383	0.004454
Urban street view	Vertical	0.911549	0.002805	Outdoor gathering	Horizontal	0.967445	0.005177
	Horizontal	0.897174	0.004935		Diagonal	0.980877	0.00321
	Diagonal	0.968902	0.005121		Vertical	0.96752	0.008616

generation and RNN-optimized S-box transformations, exemplifies the strength of the proposed scheme in concealing salient visual structures and preserving confidentiality under high-stakes imaging scenarios.

7.5 Cropping analysis

As discussed in the earlier sections of this write up that the available lightweight encryption schemes are subjected to cropping and noise attack. In this section of the article, we have to check the immunity of the encryption scheme against cropping and noise attacks. The noise and cropping alter pixels values; therefore, separate analysis is not necessary. Figure 15 shows the Impact of increasing pixel loss on the decryption quality of an encrypted cameraman image using the proposed scheme. Figure 15(a) shows the encrypted image and Figure 15(b) shows the decrypted cameraman. In (c, e, g, i, k), progressive pixel loss is introduced in the top-left region of the encrypted image 12.5 %, 16.7 %, 25 %, 33.3 %, and 50 %, respectively. The corresponding decrypted results in (d, f, h, j, l) show preserved structural and salient features, such as face details, despite significant data loss. This demonstrates the scheme of strong resistance to cropping attacks and its ability to retain critical visual information under pixel loss conditions. To quantitatively assess the encryption scheme's ability to preserve structural integrity under conditions such as burst errors, cropping, or data loss, the Structural Similarity Index (SSIM) is employed. SSIM evaluates the perceived quality and structural similarity between two images, with values ranging from 0 to 1. A score near 1 indicates strong structural resemblance, while a score near 0 reflects significant differences. Given an original image I_{orig} and an encrypted image I_{enc}, SSIM is computed as:

$$\text{SSIM}\left(I_{\text{orig}}, I_{\text{enc}}\right) = \frac{\left(2\mu_{\text{orig}}\mu_{\text{enc}} + C_1\right)\left(2\sigma_{\text{orig,enc}} + C_2\right)}{\left(\mu_{\text{orig}}^2 + \mu_{\text{enc}}^2 + C_1\right)\left(\sigma_{\text{orig}}^2 + \sigma_{\text{enc}}^2 + C_2\right)}, \tag{37}$$

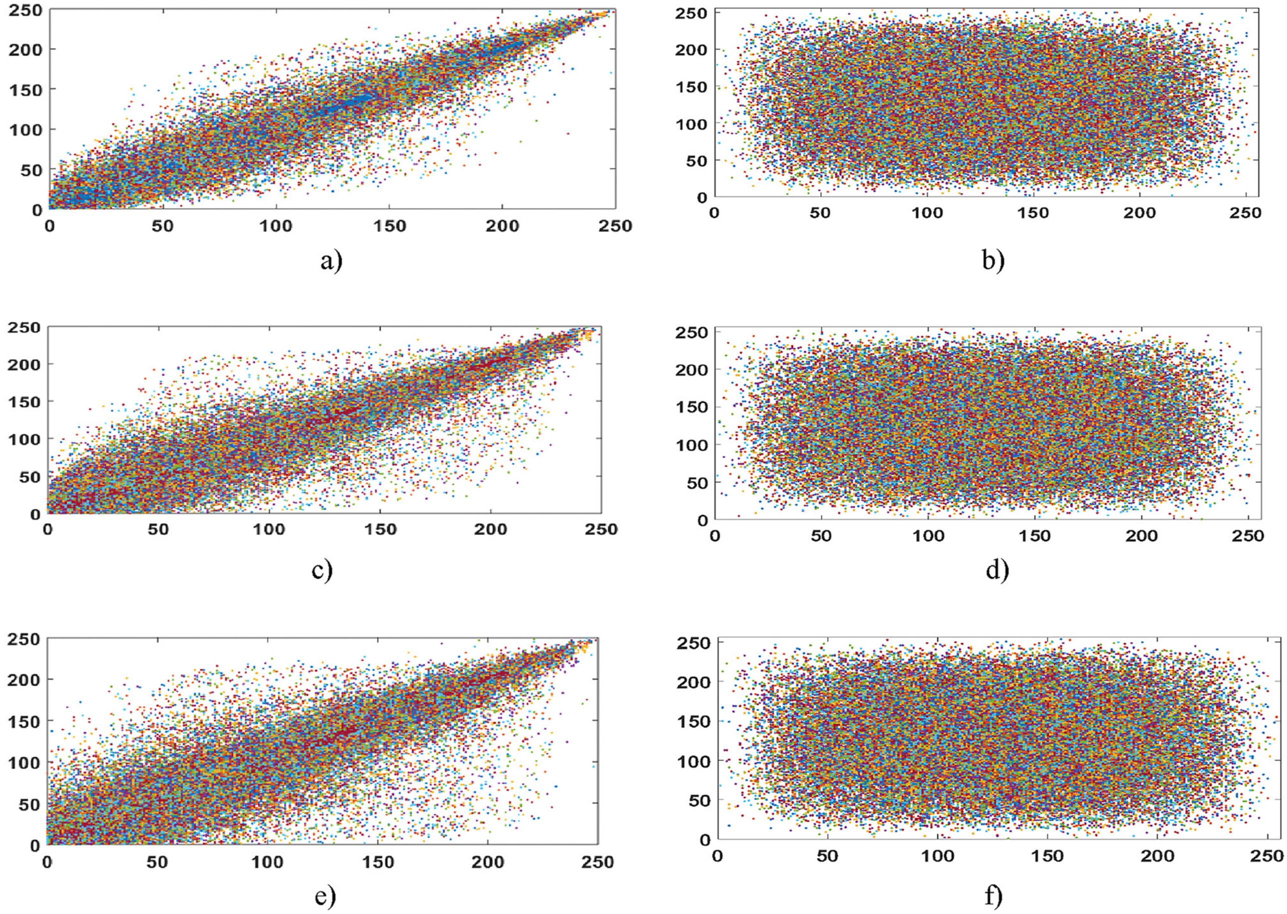


Figure 14: Visualization of horizontal (HC), vertical (VC), and diagonal (DC) pixel correlations for the original and encrypted Baboon images. The original image shows strong pixel correlations, while the encrypted image exhibits a random scatter distribution, confirming effective decorrelation and high security against statistical attacks. (a) Vertical CC analysis of Baboon, (b) vertical CC analysis of encrypted Baboon, (c) horizontal CC analysis of original Baboon, (d) horizontal CC analysis of encrypted Baboon, (e) diagonal CC analysis of original Baboon, (f) diagonal CC analysis of encrypted Baboon.

where μ_{orig} and μ_{enc} are the mean luminance values of the original and encrypted images, σ^2_{orig} and σ^2_{enc} are their variances, $\sigma_{\text{orig,enc}}$ is the covariance between them, C_1 and C_2 are small positive constants that stabilize the computation when the denominators are near zero. In cryptographic image evaluation, a low SSIM value between I_{orig} and I_{enc} indicates strong encryption, as it implies minimal structural similarity and hence negligible leakage of visual information. Conversely, in salient-information-preserving encryption schemes, SSIM may be deliberately higher within predefined Regions of Interest (ROIs) to maintain decision-critical details while remaining low in non-salient regions to ensure confidentiality. SSIM is calculated between the original images and the decrypted images affected by cropping. The SSIM results for various cropping ratios are presented in Table 12. SSIM values approaching 1 indicate that the structural content of the original image is well preserved, even after significant pixel loss. This confirms the encryption scheme's robustness, as it prevents unauthorized extraction of meaningful visual information while maintaining high structural fidelity.

Table 12 listed SSIM values for the image subjected to varying levels of cropping. Higher SSIM values indicate stronger structural resemblance between the cropped decrypted images and the originals. The results demonstrate the proposed encryption scheme's robustness against cropping and burst errors, effectively preserving structural integrity even under substantial pixel loss.

7.6 Man-in-the-Middle (MITM) attack

Man-in-the-Middle (MITM) attack is a severe threat where data is intercepted, modified, or injected in between communicating parties. In encrypted image transmission,

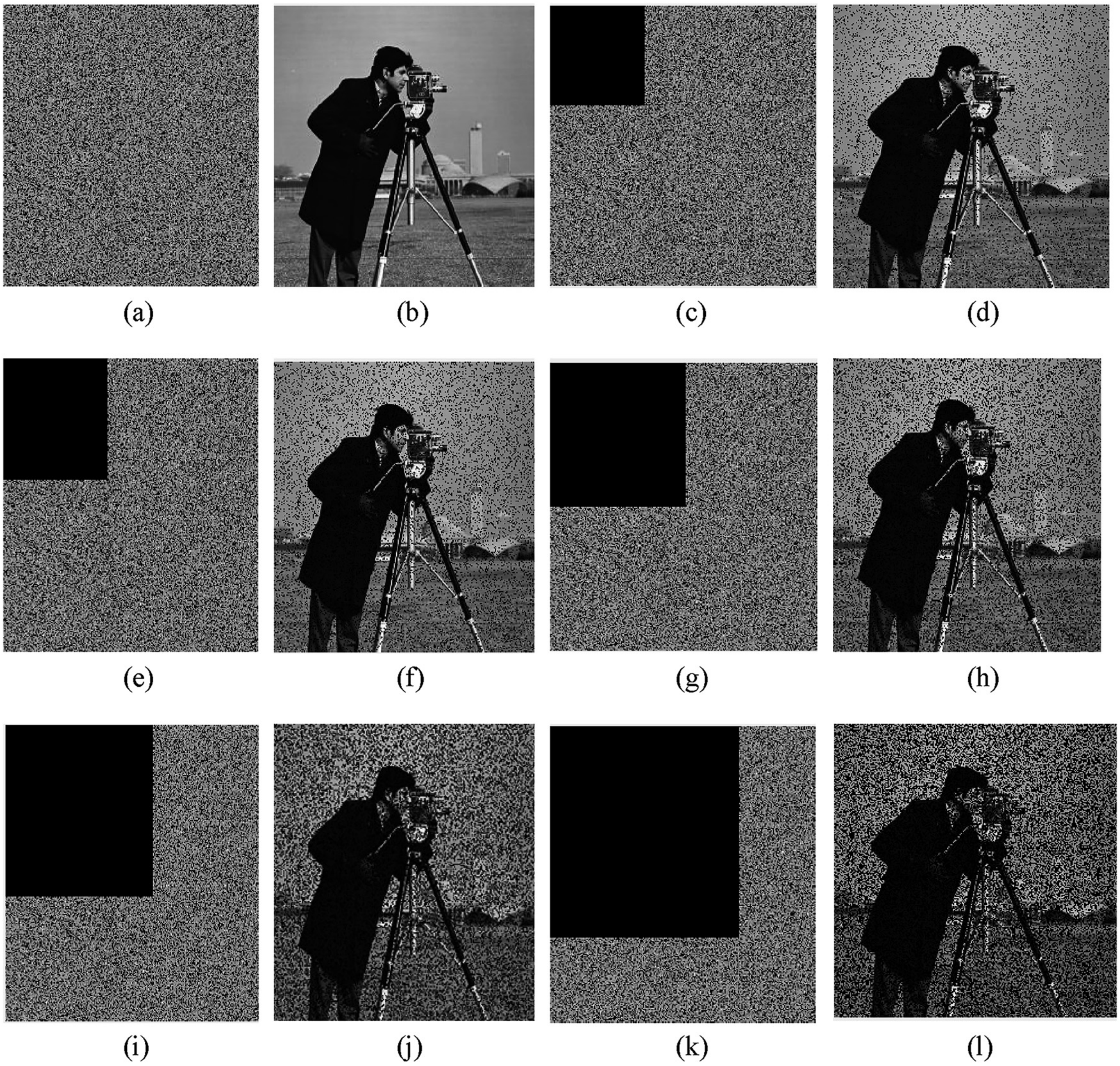


Figure 15: Decryption results under pixel loss conditions. The proposed encryption scheme demonstrates strong robustness against cropping and data loss, successfully recovering the main visual content and preserving salient image features despite missing pixel regions.

attackers may attempt chosen-ciphertext attacks to modify ciphertext and monitor system behavior when decrypting. The proposed chaos and RNN-based encryption algorithm offer strong resistance to MITM attacks through multiple security layers. In the first place, it employs a 128-bit secret key, offering 2^{128} combinations, making brute-force attacks infeasible. Even a single change in the key produces a totally different ciphertext, as can be seen from Figure 11, foiling the attempts of attackers to predict or manipulate encrypted data. Second, disorderly block shuffling confuses image blocks with a logistic chaotic map so that attackers cannot restore the original image without accurate information about block locations. Third, a nonlinear S-box generated using RNN improves confusion, satisfying the Strict Avalanche Criterion (SAC) that even slight changes in ciphertext produce extremely different decrypted results, disabling any effort to inject or alter data. These collective mechanisms make MITM interception ineffective, providing unbroken security for IoT-based image encryption.

Table 12: SSIM measurements of cropped images with original image.

Cropping ratio	SSIM
No cropping	1.0000
1/8 cropping	0.9986
1/6 cropping	0.9987
1/4 cropping	0.9824
1/3 cropping	0.8781
1/2 cropping	0.7598

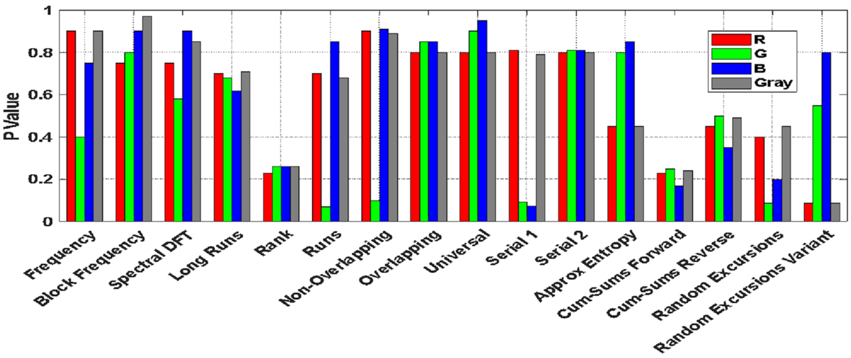


Figure 16: Test findings of the proposed cryptosystem based on NIST SP 800-22 statistical experiments. The results show that all tested sequences pass the randomness criteria, confirming the proposed system's strong statistical performance and suitability for secure cryptographic applications.

7.7 Data injection attack

The proposed encryption technique enhances image security against data injection attacks by causing even cropped or manipulated encrypted images to retain essential visual information upon decryption though with degradation, as shown in Figure 16. The application of chaotic block shuffling disrupts the location of injected or manipulated data, rendering unauthorized alteration meaningless. The RNN-based nonlinear S-box transformation also increases confusion so that even a slight alteration in encrypted data causes drastically different decrypted output, thereby effectively thwarting pattern injections and desired changes. By combining multi-round XOR operations, bit permutations, and S-box substitutions, the scheme diffuses information in a chaotic way, destroying any tampering attempt. Despite cropping attacks or burst errors, the encryption scheme preserves the integrity of key visual content such as facial contours in surveillance videos ensuring aggressive protection in IoT applications. Data injection attempts ultimately collapse, being unable to manipulate meaningful content, embedding uncompromising security and tenacity in real-world applications.

7.8 NIST analysis

To validate the randomness in the encrypted image, encrypted through the proposed lightweight encryption scheme is tested utilizing the NIST 800-22 test suite. For successful passage of each test in the suit a *p* value exceeding 0.01 is required. The outcomes are presented in Figure 16, and it is affirmed from this investigation that the encrypted image complies with all the tests listed in NIST 800-22.

7.9 Chosen plaintext attack

The 128-bits key and its circular shifted version XORed with each block and the blocks are permuted using chaotic generated permutation matrix. The resulting image is heavily dependent on key and permutation matrix. Hence it is not possible for the attacker to predict the output, even by choosing the plaintext. Moreover, the bit level parity making further harder the success of chosen plaintext attacks. This combination of block permutations, key XORing and bit level parity mapping hides the relation between the chosen plain image and its cipher image.

7.10 Chosen cipher text attack

The same complex process is used in the decryption phase. The proposed encryption scheme applies nonlinear substitution at two distinct stages (Steps 4 and 7). These layers introduce high confusion and nonlinearity, making differential patterns difficult to trace in chosen cipher text attack. Secondly the encryption scheme utilizes a chaotic permutation matrix derived from a logistic map to disrupt the spatial locality of image pixels. Even minor changes in cipher text blocks result in unpredictable shifts, making it infeasible for the attacker to isolate meaningful patterns.

7.11 Throughput analysis

Encryption speed analysis measures the time an algorithm takes to process data, expressed as throughput. High throughput is crucial for performance, especially in data communication and IoT applications. The proposed encryption scheme's throughput was assessed on a personal

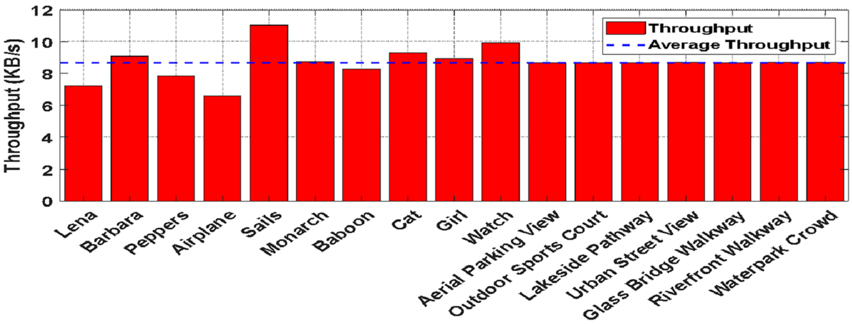


Figure 17: Throughput analysis of the proposed encryption scheme. The results indicate a high throughput, demonstrating the scheme's computational efficiency and suitability for real-time or large-scale image security applications.

Table 13: Throughput analysis of the proposed LWE and comparison with state of the art LWEs.

Encryption scheme	Time in seconds	Size of data (bytes)	Throughput in KB/s
AES [37]	64	513,024	7.828125
HIGHT [38]	159	513,024	3.1509433962
ITUBee [39]	0.0842	40	0.463925178
Lilliput [40]	0.1218	32	0.2565681
PRESENT	0.1488	128	0.840053
Proposed	59	513,024	8.695322

Table 14: Comparison of algorithm size with state of the art lightweight encryption techniques.

Encryption scheme	Size in bytes
AES [37]	43,119
PRESENT	3,430
ITUBee [39]	6,207
Lilliput [40]	4,394
HIGHT [38]	12,744
Proposed	40,812

computer featuring an Intel(R) Core(TM) i7-7700 CPU, operating at 3.60 GHz, with 8GB of RAM and running on the Windows 10 platform. The results, shown in Figure 17, and Table 14, show that the proposed scheme outperforms recent LWE schemes in throughput.

Figure 17 presents a bar chart illustrating the throughput analysis of the proposed encryption scheme across various images. The average throughput benchmark (8.675 kB/s) serves as a reference point for evaluating performance consistency. Higher throughput values indicate faster encryption processing, making the proposed scheme suitable for high-speed encryption applications in real-world scenarios (see Table 13).

7.12 RAM storage and suitability for IoT deployment

The RAM footprint of an encryption algorithm is a decisive factor in determining its suitability for resource-constrained environments such as IoT and embedded systems. As shown in Table 14, the proposed chaos–RNN-based scheme requires 40,812 bytes of RAM, which is slightly lower than AES (43,119 bytes) yet higher than ultra-lightweight algorithms such as PRESENT (3,430 bytes), Lilliput (4,394 bytes), and ITUBee (6,207 bytes). While these smaller ciphers offer superior memory efficiency, they do so at the expense of reduced cryptographic strength and limited resistance to advanced attacks. In contrast, the proposed scheme strikes a deliberate balance between security and efficiency, integrating high-strength cryptographic features, such as an S-box nonlinearity of 112, effective linear and differential attack resistance, and information-preserving functions for key information, in a memory size variable for implementation in mid-level edge computing and IoT devices. Minimizing S-box storage, RNN calculations, and buffer space will form the future research agenda for ultra-constrained IoT nodes with small memory of a few kilobytes for decreasing the memory required without losing the efficacy of the encryption.

7.13 Discussion on lightweight encryption

Due to the low computational complexity, efficient memory usage, and high throughput, the proposed encryption scheme qualifies for lightweight cryptographic solutions for the IoT devices. The proposed encryption scheme utilizes a block-based design, dividing the image into 4 × 4 blocks, which allows for localized and parallelizable operations, minimizing both processing time and memory overhead. The use of a simple one-dimensional logistic map for permutation ensures efficient key-dependent scrambling with minimal arithmetic operations. Additionally, the bit-level parity mapping is implemented using lightweight logic operations that do not introduce any significant computational burden. Substitution is achieved using pre-generated S-boxes obtained from RNN models, which are stored as lookup tables to avoid runtime neural computations, thereby reducing complexity and memory access latency. The affine key mixing is performed via XOR operations, which are natively supported by hardware and the operation is computationally inexpensive. The use of modular arithmetic, simple logic, and avoidance of heavy mathematical primitives like matrix inversion or elliptic curve operations further reinforce its lightweight nature. Based on the throughput and RAM analysis provided in Table 14, the proposed encryption scheme demonstrates favorable lightweight characteristics when compared with state-of-the-art lightweight encryption (LWE) algorithms. Although the RAM usage of the proposed scheme is 40,812 bytes, which is higher than most lightweight schemes like PRESENT (3,430 bytes), Lilliput (4,394 bytes), and ITUBee (6,207 bytes), it remains lower than AES (43,119 bytes). Given that all schemes were implemented and tested under the same MATLAB 2017b environment on the same hardware, the trade-off between higher speed and moderate RAM usage is acceptable, especially for image-based applications where performance is critical. Therefore, the proposed scheme can still be classified as lightweight, offering a balance between computational efficiency and memory requirements.

8 Conclusion with future recommendations

This paper puts forward a chaos–RNN-based lightweight encryption system for the encryption of the most prominent image regions in IoT applications. The new design sustains an average S-box nonlinearity of 112, near the theoretical optimal and directly supporting resistance to linear attack by decreasing linear correlations, improves the Strict Avalanche Criterion (SAC) and Bit Independence Criterion (BIC) for improved diffusion, reduces Linear Approximation Probability (LAP), and indirectly the Differential Approximation Probability (DAP), supporting resistance to linear and differential attack respectively. These cryptographic strengths are tempered by a UACI of 33.50 % and NPCR of 99.60 %, ensuring high sensitivity to plaintext changes. The scheme provides a throughput of 8.695 KB/s, outperforming AES and other lightweight cryptosystems, and demonstrates robustness against cropping and burst errors, enabling accurate reconstruction even after 30 % data loss. NIST SP 800-22 tests validate utmost statistical randomness. Though RNN training and S-box generation add computational overhead for highly resource-constrained IoT devices, future research will address optimizing computational efficiency, minimizing the memory footprint, applying the approach to multimedia formats, and adding post-quantum resilience. These results represent a critical step toward AI-driven, cryptographically secure, and lightweight encryption optimally tailored for next-generation IoT environments.

Funding information: This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2025/R/1447).

Author contributions: All authors have accepted responsibility for the entire content of this manuscript and approved its submission.

Conflict of interest: Authors state no conflict of interest.

Data availability statement: All data generated or analysed during this study are included in this published article.

References

1. Wenhua Z, Hasan MK, Jailani NB, Islam S, Safie N, Albarakati HM, et al. A lightweight security model for ensuring patient privacy and confidentiality in telehealth applications. Comput Hum Behav 2024;153:108134.
2. Islam MOU, Parah SA. Fast and lightweight image cryptosystem for IoMT applications. Internet Things 2024;25:101083.
3. Deebak BD, Hwang SO. Privacy-preserving learning model using lightweight encryption for visual sensing industrial IoT devices. IEEE Trans Emerg Top Comput Intell 2025; 9:3039—56.
4. Aljaedi A, Alharbi AR, Aljuhni A, Alghuson MK, Alassmi S, Shafique A. A lightweight encryption algorithm for resource-constrained IoT devices using quantum and chaotic techniques with metaheuristic optimization. Sci Rep 2025;15:14050.
5. Shafique A, Mehmood A, Alawida M, Khan AN, Shuja J. Lightweight image encryption scheme for IoT environment and machine learning-driven robust S-box selection. Telecommun Syst 2025;88:17.
6. Aqeel S, Khan AS, Abbasi IA, Algarni F, Grzonka D. Enhancing IoT security with a DNA-based lightweight cryptography system. Sci Rep 2025;15:13367.
7. Mehmood A, Khan AN, Natgunanathan I, Shafique A, Khan IA, Khan AUR. Enhanced lightweight and compromised-resilient image encryption for resource constrained environments. PLoS One 2025;20:e0320046.
8. Gilmolk AMN, Aref MR. Lightweight image encryption using a novel chaotic technique for the safe internet of things. Int J Comput Intell Syst 2024;17:146.
9. Tian H, Zhuang X, Yan A, Zhang H. A novel multiple-image encryption with multi-petals structured light. Sci Rep 2024;14:19559.

10. Zhu S, Deng X, Zhang W, Zhu C. Secure image encryption scheme based on a new robust chaotic map and strong S-box. Math Comput Simulat 2023;207:322–46.
11. Kumar M, Chivukula AS, Barua G. Deep learning-based encryption scheme for medical images using DCGAN and virtual planet domain. Sci Rep 2025;15:1211.
12. Choudhary D, Pahuja R. Deep learning approach for encryption techniques in vehicular networks. Wirel Pers Commun 2022;125:1–27.
13. Ding Y, Wu G, Chen D, Zhang N, Gong L, Cao M, et al. DeepEDN: a deep-learning-based image encryption and decryption network for internet of medical things. IEEE Internet Things J 2020;8:1504–18.
14. University of Southern California. Signal and image processing institute. Image databases; 1997. Available from: http://www.imageprocessingplace.com/root_files_V3/image_databases.htm.
15. Zhu P, Wen L, Du D, Bian X, Fan H, Hu Q, et al. VisDrone dataset [Dataset]. GitHub; 2021. Available from: https://github.com/VisDrone/VisDrone-Dataset.
16. Waheed A, Subhan F, Su'ud MM, Alam MM. Molding robust S-box design based on linear fractional transformation and multilayer perceptron: applications to multimedia security. Egypt Inform J 2024;26:100480.
17. Waheed A, Subhan F, Suud MM, Malik MYH, Mirza A, Afzal F. Construction of nonlinear component of block cipher using coset graph. AIMS Math 2023;8:21644–67.
18. Malik AW, Zahid AH, Bhatti DS, Kim HJ, Kim KI. Designing S-box using tent-sine chaotic system while combining the traits of tent and sine map. IEEE Access 2023;11:79265–74.
19. Alexan W, Korayem Y, Gabr M, El-Aasser M, Maher EA, El-Damak D, et al. Anteater: when Arnold's cat meets Langton's ant to encrypt images. IEEE Access 2023;11:106249–76.
20. Alexan W, El-Damak D, Gabr M. Image encryption based on Fourier-DNA coding for hyperchaotic Chen system, Chen-based binary quantization S-box, and variable-base modulo operation. IEEE Access 2024;12:21092–113.
21. Artuğer F. A novel algorithm based on DNA coding for substitution box generation problem. Neural Comput Appl 2024;36:1283–94.
22. Abughazalah N, Said L, Khan M. Construction of optimum multivalued cryptographic Boolean function using artificial bee colony optimization and multi-criterion decision-making. Soft Comput 2024;28:5213–23.
23. Qazi AS, Zahid AH, Baz A, Arslan F, Ali M, Ali J. Innovative transformation of S-box through chaotic map using a pragmatic approach. IEEE Access 2024;12:42725–36.
24. Khan M, Alanazi AS, Khan LS, Hussain I. An efficient image encryption scheme based on fractal Tromino and Chebyshev polynomial. Complex Intell Syst 2021;7:2751–64.
25. Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurc Chaos 2006;16:2129–51.
26. Rana M, Mamun Q, Islam R. Enhancing IoT security: an innovative key management system for lightweight block ciphers. Sensors 2023;23:7678.
27. Alexan W, Aly L, Korayem Y, Gabr M, El-Damak D, Fathy A, et al. Secure communication of military reconnaissance images over UAV-assisted relay networks. IEEE Access 2024;12:78589–610.
28. Alexan W, Elabyad N, Khaled M, Osama R, El-Damak D, Abd El Ghany MA, et al. Triple layer RGB image encryption algorithm utilizing three hyperchaotic systems and its FPGA implementation. IEEE Access 2024;12:118339–61.
29. Xu C, Shang Y, Yang Y, Zou C. An encryption algorithm for multiple medical images based on a novel chaotic system and an odd-even separation strategy. Sci Rep 2025;15:2863.
30. Hosny KM, Elnabawy YM, Salama RA, Elshewey AM. Multiple image encryption algorithm using channel randomization and multiple chaotic maps. Sci Rep 2024;14:30597.
31. Niu Y, Zhou H, Zhang X. Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators. Sci Rep 2024;14:7033.
32. Zhu S, Zhu C. A visual security multi-key selection image encryption algorithm based on a new four-dimensional chaos and compressed sensing. Sci Rep 2024;14:15496.
33. Zhu S, Deng X, Zhang W, Zhu C. Image encryption scheme based on newly designed chaotic map and parallel DNA coding. Mathematics 2023;11:231.
34. Alexan W, Elkandoz M, Mashaly M, Azab E, Aboshousha A. Color image encryption through chaos and KAA map. IEEE Access 2023;11:11541–54.
35. El-Damak D, Alexan W, Mamdouh E, El-Aasser M, Fathy A, Gabr M. Fibonacci q-matrix, hyperchaos, and Galois field (28) for augmented medical image encryption. IEEE Access 2024;12:102718–44.
36. Daemen J, Rijmen V. The design of Rijndael. New York: Springer-Verlag; 2002, vol 2.
37. Hong D, Sung J, Hong S, Lim J, Lee S, Koo BS, et al. HIGHT: a new block cipher suitable for low-resource device. In: International workshop on cryptographic hardware and embedded systems. Berlin: Springer; 2006:46–59 pp.
38. Karakoç F, Demirci H, Harmancı AE. ITUbee: a software oriented lightweight block cipher. In: International workshop on lightweight cryptography for security and privacy. Berlin: Springer; 2013:16–27 pp.
39. Berger TP, Francq J, Minier M, Thomas G. Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. IEEE Trans Comput 2015;65:2074–89.
40. Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJ, et al. PRESENT: an ultra-lightweight block cipher. In: International workshop on cryptographic hardware and embedded systems. Berlin: Springer; 2007:450–66 pp.