Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.042777

ARTICLE

A New S-Box Design System for Data Encryption Using Artificial Bee Colony Algorithm

Yazeed Yasin Ghadi[1], Mohammed S. Alshehri[2], Sultan Almakdi[2], Oumaima Saidani[3,*], Nazik Alturki[3], Fawad Masood[4] and Muhammad Shahbaz Khan[5]

[1]Department of Computer Science, Al Ain University, Abu Dhabi, 112612, United Arab Emirates

[2]Department of Computer Science, College of Computer Science and Information Systems, Najran University, Najran, 61441, Saudi Arabia

[3]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia

[4]Department of Electrical Engineering, Institute of Space Technology, Islamabad, 4400, Pakistan

[5]School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh, EH10 5DT, UK

*Corresponding Author: Oumaima Saidani. Email: ocsaidani@pnu.edu.sa

Received: 11 June 2023 Accepted: 02 August 2023 Published: 31 October 2023

ABSTRACT

Securing digital image data is a key concern in today's information-driven society. Effective encryption techniques are required to protect sensitive image data, with the Substitution-box (S-box) often playing a pivotal role in many symmetric encryption systems. This study introduces an innovative approach to creating S-boxes for encryption algorithms. The proposed S-boxes are tested for validity and non-linearity by incorporating them into an image encryption scheme. The nonlinearity measure of the proposed S-boxes is 112. These qualities significantly enhance its resistance to common cryptographic attacks, ensuring high image data security. Furthermore, to assess the robustness of the S-boxes, an encryption system has also been proposed and the proposed S-boxes have been integrated into the designed encryption system. To validate the effectiveness of the proposed encryption system, a comprehensive security analysis including brute force attack and histogram analysis has been performed. In addition, to determine the level of security during the transmission and storage of digital content, the encryption system's Number of Pixel Change Rate (NPCR), and Unified Averaged Changed Intensity (UACI) are calculated. The results indicate a 99.71% NPCR and 33.51% UACI. These results demonstrate that the proposed S-boxes offer a significant level of security for digital content throughout its transmission and storage.

KEYWORDS

S-box; chaos; artificial bee colony; image encryption

1 Introduction

The rise of multimedia technology and information sharing via insecure channels necessitates robust security for sensitive data, including images of finances, personal information, and medical records [1]. As color images increasingly serve as digital communication mediums, securing them

against unauthorized access is vital. Image encryption is key to maintaining the confidentiality and integrity of such data. While traditional text encryption may not suffice for images, a blend of security techniques can protect information at different network communication layers. Physical layer protection may involve modulation systems and spread spectrum techniques, while cryptographic methods, including encryption, decryption, and digital signatures, safeguard the application layer [1,2]. Techniques like watermarking, steganography, and fingerprinting embed information within other data for proof of ownership or authenticity and content usage tracking [3]. Encryption systems typically fall into two categories: symmetric and asymmetric. Symmetric encryption uses one key for encryption and decryption, while asymmetric uses a public encryption key and a private decryption key. Enhancing encryption involves employing substitution boxes (S-boxes) that use mathematical functions to substitute one-bit sequences. This increases the complexity of the key-cipher text relationship, which determines the encryption strength, with the nonlinearity of S-boxes significantly intensifying this complexity.

This research focuses on creating highly nonlinear S-boxes [4,5] that are suitable for chaotic encryption systems. Chaotic maps have proven to be effective in encryption algorithms, for instance, a novel image encryption algorithm leveraging new fractional beta chaotic maps is proposed in [6]. The presented approach employs chaotic maps to generate pseudo-random sequences that reshuffle image pixels. The proposed scheme, characterized by a large key space and high key sensitivity, resulted in impressive entropy and low correlation coefficients, enhancing overall image encryption security. Similarly, in [7], the authors introduced a novel S-box generator using a deterministic algorithm over elliptic curves, resulting in dynamic, key-sensitive, and secure S-boxes. It was successfully applied in an image encryption scheme, demonstrating resistance against several types of cryptographic attacks. Besides, the authors [8] presented the use of chaotic systems for big data encryption, particularly image encryption, proposing a one-dimensional piece-wise quadratic polynomial chaotic map (PWQPCM). Coupled with a robust S-box construction method and a secure image encryption algorithm, the proposed model shows advantages in data loss resistance, time efficiency, and adjustable security strength. Moreover, the authors in [9] presented a new two-dimensional discrete hyperchaotic map, which possesses wider continuous chaotic intervals and larger Lyapunov exponents. This map is employed to generate S-boxes and pair them, resulting in a sophisticated encryption algorithm. Additionally, a two-dimensional chaotic map-based encryption method for images was discussed by Amina et al. [10], utilizing confusion and diffusion at the bit level. The analysis of this method demonstrates satisfactory and efficient encryption performance. Additionally, a four-dimensional chaotic system-based algorithm for color image encryption is presented by Li et al. [11] which exhibits good security, robustness, and efficiency through simulations and analysis. However, it is found that some existing encryption methods may lack sufficient security. Encryption involves two phases of confusion and diffusion. Confusion makes the relationship between plaintext and ciphertext complex through operations like substitution and permutation. Diffusion scatters the impact of each plaintext symbol across multiple ciphertext symbols, achieved through block ciphers and transformations. Substitution boxes contribute to confusion while scrambling algorithms aid diffusion [12]. Previous work in the field of application layer security has already been done by Kaur et al. [13], and chaos has been widely used in cryptography due to its sensitivity to initial conditions. One of the most critical characteristics of an efficient encryption system is its sensitivity to the key, the keyspace analysis, and the time analysis [14]. In the case of images, the correlation between neighboring pixels is high, making it challenging to provide security to them using traditional systems. Deoxyribonucleic Acid (DNA) and hyperchaos-based encryption discussed by Liu et al. [15] were proposed and the system works very well for the security of images. Hyperchaos-based encryption schemes are a type of cryptographic

algorithm that utilizes numerous chaotic systems with different initial conditions to achieve high encryption performance. These schemes offer several advantages, including strong security, efficient processing, and resistance to various attacks. Moreover, it employs multiple chaotic systems with distinct initial conditions which makes it challenging for attackers to reconstruct the encryption key. However, parallel processing techniques enable efficient handling of large amounts of data in real-time which is far better than Hyperchaos-based encryption schemes as it lacks flexibility due to their dependability on specific chaotic systems and initial conditions. It also limits their adaptability to different encryption scenarios. Basic requirements for efficient encryption systems are also discussed in related work [16]. Several similar works can be found in literature, such as the authors in [17] proposed a novel image encryption algorithm utilizing a two-dimensional spatiotemporal chaotic system that combines linear neighborhood coupling and nonlinear chaotic map coupling of lattices, offering enhanced cryptographic features compared to the traditional coupled map lattices system. Bit-level permutation further strengthens the cryptosystem security, with simulations illustrating a large key space, high key sensitivity, and resistance to attacks. Similarly, in [18] the authors introduced a unique image encryption scheme, exploiting DNA-based sequencing and chaotic sequencing. The image transforms DNA encoding, shuffling for diffusion, substitution for confusion, and repeated DNA fusion operations to disrupt pixel correlations. The ciphered image meets all standard benchmarks, proving the effectiveness of this innovative approach. Besides, the authors in [19] presented a hybrid image encryption method combining a logistic sine system, two-dimensional cellular automata, and Finite State Machines (FSM)-based DNA rule generator. Each of the three stages of encryption employs unique rules, delivering robust defense against various cryptographic attacks. The proposed method proves to be effective for secure encryption of classified grayscale images.

Encryption systems rely on key sensitivity, keyspace analysis, and time analysis. In images, pixel correlation can affect image quality; high correlation may lead to blurriness, while low correlation may result in noise. Effective encryption algorithms reduce this correlation, making histograms uniformly distributed, achieved by scrambling—shuffling pixel groups to diminish neighboring block correlation. This contributes to diffusion, vital for images with high neighborhood correlation. The S-box's properties, including non-linearity and the avalanche effect, determine encryption strength. A secure S-box exhibits significant output changes with input modifications and satisfies the strict avalanche criterion. The S-box's strength influences the confidentiality and integrity of encrypted data, with robust S-boxes enhancing security against unauthorized access. Therefore, this paper focuses on generating S-boxes exhibiting non-linearity, resilience, and compatibility with existing encryption algorithms. This work aims to develop highly nonlinear S-boxes for encryption, enhancing digital content security during transmission and storage. The focus is on incorporating these S-boxes in the encryption system's confusion phase and using various scrambling algorithms in the diffusion phase. The proposed system's effectiveness will be evaluated based on key sensitivity, keyspace analysis, time analysis, and the uniform distribution of encrypted image histograms.

The key contributions of this paper are:

1. Generation of highly nonlinear substitution boxes (S-boxes) using Artificial Bee Colony (ABC) algorithm that adheres to the key statistical security parameters such as Strict Avalanche Criteria (SAC), bijectivity, and Bit Independent Criteria (BIC). These highly nonlinear S-boxes enhance the security of digital content during transmission and storage.
2. Development of a novel encryption system for colored images, which innovatively incorporates the generated S-boxes into the confusion phase and employs different scrambling algorithms in the diffusion phase making it suitable for color image encryption.

3. A comprehensive and diverse security analysis has been presented for the proposed encryption system. This analysis includes brute force attack resistance, National Institute of Standards and Technology (NIST) statistical test, histogram analysis, differential analysis, time analysis, and key sensitivity analysis.

The rest of the paper is organized as follows: Section 2 introduces essential concepts used in S-box generation, outlines the process of generating and analyzing the S-boxes, and presents the proposed encryption system. Section 3 presents the extensive security analysis of the proposed encryption system followed by a concise and clear conclusion in Section 4.

2 Basic Theory and the Proposed S-Boxes-Based Encryption System

In this section of the paper, the basics of the algorithm used in the proposed encryption system are discussed.

2.1 Artificial Bee Colony Algorithm (ABC)

The ABC algorithm, introduced by Karaboga in 2005, mimics the foraging behavior of honey bee colonies to solve optimization problems [20]. It involves finding a vector that minimizes an objective function. The algorithm starts with a random population of solution vectors and iteratively searches for the best solution. In this study, the random search behavior of bee colonies is utilized to create S-boxes. The ABC algorithm is composed of four distinct phases, explained in detail in the following section.

2.1.1 Initialization Phase

All the possible vectors of the populations are initialized by the scout bee and the control parameters are set. The initialization is performed according to Eq. (1) [20].

$$y_{na} = j_a + rand\,(0,1) * (v_i - j_i) \tag{1}$$

Here is the population vector which holds $(a = 1, 2, 3, \ldots, n)$, this needs to be optimized to get a minimized objective function. v_i and j_i are the higher and lesser bounds of the y_{na}.

2.1.2 Employee Bee Phase

The task of the employee is to search for a new food source and determine its richness. Mathematically richness can be quantified through a fitness function. For finding the nearest food source the relation in Eq. (2) [20] can be used.

$$u_{ma} = y_{na} + \varnothing_{na}\,(y_{na} - y_{la}) \tag{2}$$

Here y_{na} is a randomly selected food source and is a randomly chosen number from $(-a,\ a)$. The fitness function for the solution might be figured using the relation as in Eq. (3) [20].

$$fit_n = \begin{Bmatrix} \dfrac{1}{1 + f_n\left(\vec{y_n}\right)} & if\ f_n\left(\vec{y_n}\right) \geq 0 \\ 1 + abs\left(f_n\left(\vec{y_n}\right)\right) & if\ f_n\left(\vec{y_n}\right) < 0 \end{Bmatrix} \tag{3}$$

where $f_n\left(\vec{y_n}\right)$ is the objective function value of the solution of y_{na}.

2.1.3 Onlooker Bee Phase

Apart from the employed bees there exist two other groups named onlooker bees and scout bees. Employer bees share the food source evidence with onlooker bees. The onlooker bees compute the fitness value of the food source and based on this evidence the food source is selected or rejected. If rejected, the same process goes iteratively. The probability with which a food source is chosen is given by Eq. (4) [20].

$$P_n = \frac{f_n\left(\vec{y_n}\right)}{\sum_{n=1}^{SN} f_n\left(\vec{y_n}\right)} \tag{4}$$

2.1.4 Scout Bees

Scouts are a group of bees who chooses their food sources randomly. After some predefined number of trials, employed bees whose solution is not improved become scouts. Scouts start the search process by choosing from a random location.

2.2 Logistic Chaotic Map

Owing to sensitivity to preliminary conditions, chaos has been commonly used in cryptography. The logistic chaotic map is given by Eq. (5) [21].

$$y_{n+1} = r y_n (1 - y_n) \tag{5}$$

Here y_n is the initial condition of the chaotic map, and its value is between zero and one. r $\in$ (0, 4). The map reveals chaotic behavior for $3.56 < r < 4$. Here is the initial condition y_n is calculated from the 32-length encryption key using the procedure in Eqs. (6) to (11) [21].

$$sum = [x(1,1) + x(1,2) + x(1,3) + x(1,4) + \cdots + x(1,32)] \tag{6}$$

$$y_1 = \left[\frac{x(1,19) + x(1,17) + sum}{2^8} + 0.01\right] \tag{7}$$

$$y_2 = \left[\frac{x(1,14) + x(1,12) + sum}{2^8} + 0.01\right] \tag{8}$$

$$y_3 = y_1 - floor(y_1 + 0.01) + 0.01 \tag{9}$$

$$y_4 = y_2 - floor(y_2 + 0.01) + 0.01 \tag{10}$$

$$y_n = [y_3, y_4] \tag{11}$$

2.3 Generation of Exclusive OR (XOR) Map

To decrease the association amongst the neighboring pixels first, we have to generate a chaos-based map of the same dimension of the image. The process of generating an XOR map is given below:

Step 1: The initial conditions for the logistic map are obtained using the technique discussed in the above section.

Step 2: The logistic chaotic map is iterated 10,000 times. The value for each iteration lies between 0 and 1. This value is multiplied by 1000000 and then the mode 256 operations are performed.

Step 3: The final values for each iteration are in the range 0 to 255.

Step 4: From these values, an N × N logistic map is calculated, which will be utilized in the proposed encryption system for the process of diffusion.

2.4 Shuffling Algorithm

The algorithm used for shuffling involves moving rows in a specific manner. In each channel, the first row remains unchanged, while the second row is shifted left circularly by one. The third row is shifted circularly to the right by two, and the n^{th} row is shifted circularly to the right by N-1. During decryption, the opposite of this process takes place, with circular left shifting being performed instead of circular right shifting. This shuffling technique generates diffusion in the cryptosystem, making it difficult to establish a relationship between the plaintext and ciphertext.

2.5 Proposed S-Box Generation

Three S-boxes have been proposed in this paper and are displayed in Tables 1–3, respectively. The proposed S-boxes are generated from the position vectors of the bees of the ABC algorithm. The S-boxes are designed and calculated as depicted in Fig. 1. The procedure is described as:

Step 1: The number of bees in the ABC along with their starting positions is initiated.

Step 2: The fitness function is calculated and based on the fitness function outcome the position is updated or terminated.

Step 3: All the position vectors of the bees are calculated and stored. In a vector, in each iteration, this process is carried out.

Step 4: Saved position vectors are loaded and multiplied by a large number and then mode 256 is performed.

Step 5: The outcome from step 4 is stored in a 1 × 256 vector. This vector contains unique values as no values should not be repeated.

Step 6: The proposed S-box is checked for non-linearity. If the nonlinearity is less than 110. The S-box is discarded otherwise it is saved.

Table 1: Proposed S-box 1

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

(Continued)

Table 1 (continued)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
14	165	120	61	134	92	196	51	80	233	247	169	253	82	38	126	193
15	60	9	242	13	200	50	151	173	234	172	226	207	88	66	21	187
16	4	250	69	77	40	26	192	6	221	201	45	30	149	14	11	232

Table 2: Proposed S-box 2

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

Table 3: Proposed S-box 3

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	98	145	184	199	107	178	165	15	131	29	247	91	55	215	43	167
2	104	86	126	70	113	179	49	195	189	205	146	88	18	217	76	254
3	8	16	187	117	197	40	33	226	35	67	54	232	139	208	42	53
4	64	125	241	239	72	233	80	14	253	180	135	108	175	142	148	2
5	169	186	114	39	122	111	112	95	192	166	144	219	99	84	228	11
6	71	246	109	183	231	9	120	65	74	210	61	56	110	224	0	79
7	155	248	216	13	119	102	81	194	223	207	19	118	161	137	227	25
8	97	77	26	154	93	230	5	92	121	90	1	182	147	213	4	220
9	163	209	193	116	100	157	173	174	51	75	236	188	203	22	151	127
10	130	83	238	38	57	133	196	171	58	243	234	141	201	138	20	62

(Continued)

Table 3 (continued)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
11	158	32	140	162	200	85	60	235	152	105	156	206	177	190	89	249
12	52	222	202	115	134	159	225	136	218	150	44	170	191	59	94	34
13	168	7	37	181	21	41	36	211	198	176	251	63	87	10	68	30
14	254	46	117	167	55	185	235	141	37	118	33	121	204	234	170	214
15	188	54	251	3	247	101	196	180	38	193	31	203	226	139	218	19
16	56	228	148	189	174	48	18	97	221	72	249	5	127	78	93	81

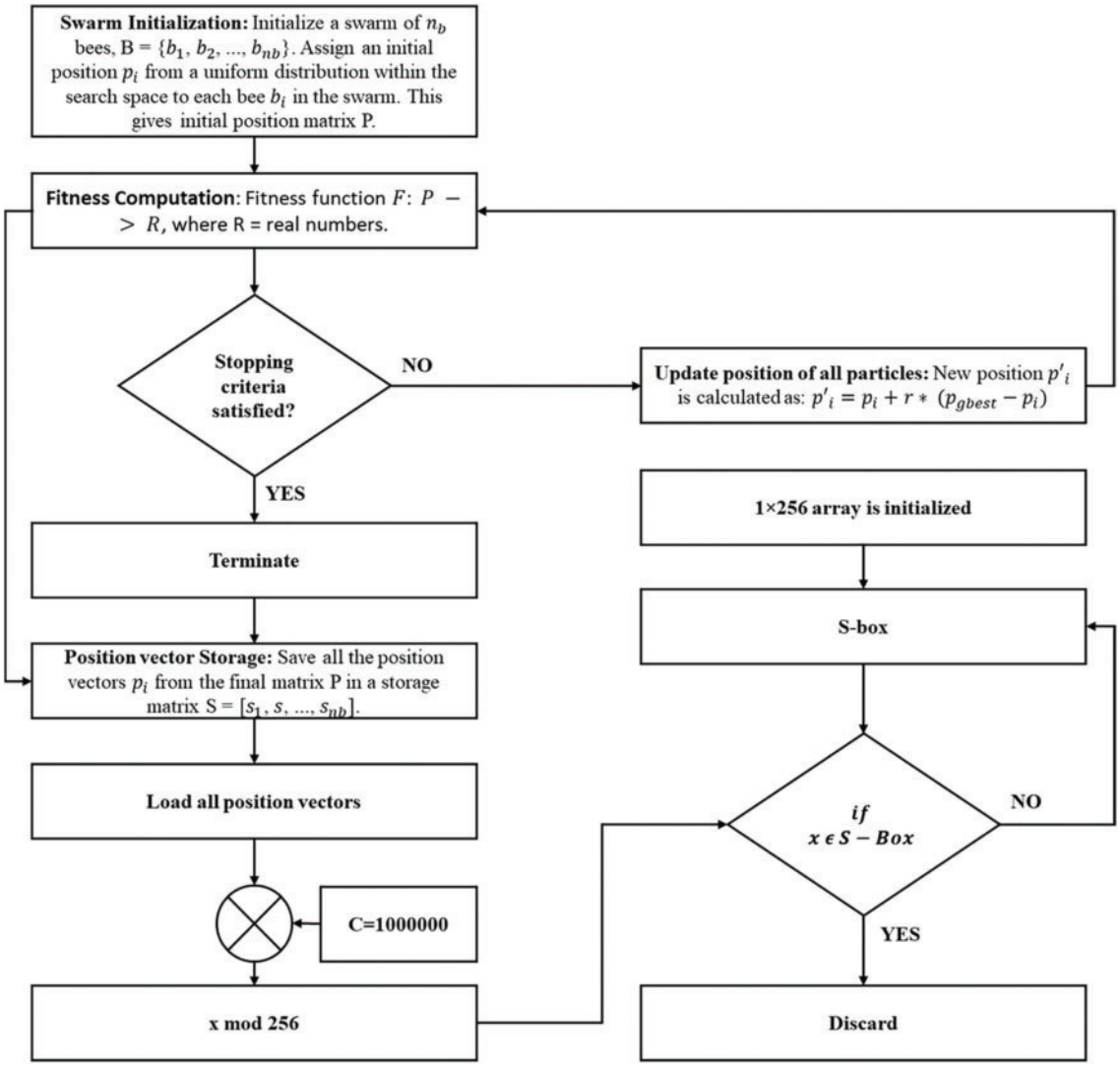

Figure 1: The proposed system for the generation of highly non-linear S-boxes

2.6 Non-Linearity

The nonlinearity of S-boxes is essential for ensuring the security of encryption systems. Randomness and unpredictability makes it challenging for intruders to decipher encrypted data. Linear S-boxes, on the other hand, are more vulnerable to intruding. Therefore, incorporating nonlinearity adds complexity and strengthens the security of the encryption system. It is crucial to assess and maintain sufficient degrees of nonlinearity in the S-boxes to ensure a high level of security. The nonlinearity of the S-boxes can be calculated using the relation in Eq. (12).

$$Non-linearity\ of\ Boolean\ function,\ f_b = \frac{1}{2}\left(2^x - W_{max}\left(f_b\right)\right) \tag{12}$$

Here x is the total of input bits, in our case $x = 8$. $W_{max}(f_b)$ is the Walsh-Hadamard transform of (f), and can be calculated in the relation in Eq. (13).

$$W_{max}\left(f_b\right) = H_{2^N}\left|(-1)^{f_b}\right| \tag{13}$$

The nonlinearity of the S-boxes is calculated and tabularized in Table 4. The comparison of the proposed S-box with the newly proposed S-boxes nonlinearity is given in Table 5. From the nonlinearity analysis, it is clear that the encryption system utilizing these S-boxes will possess a high degree of immunity to linear cryptographic attacks.

Table 4: Non-linearity outcomes of the proposed S-boxes

S-box	NL1	NL2	NL3	NL4	NL5	NL6	NL7	NL8	Average
S1	112	112	112	112	112	112	112	112	112
S2	112	112	112	112	112	112	112	112	112
S3	112	112	112	112	112	112	112	112	112

Table 5: Comparison of the proposed S-boxes and the newly proposed S-boxes

S-box	Non-linearity			BIC	BIC-non linearity	SAC		
	Min	Average	Max			Min	Average	Max
Ref. [22]	98	102.3	108	0.4992	100	0.3281	0.4836	0.6016
Ref. [23]	96	102.5	106	0.4026	102.5	0.3906	0.5178	0.6719
Ref. [24]	106	106.5	108	0.5003	104.2	0.4375	0.4978	0.5938
Ref. [25]	104	106.7	108	0.504	103.5	0.4062	0.4976	0.625
Ref. [26]	111	111.5	112	0.5068	110.28	0.4375	0.4978	0.5938
Ref. [27]	102	104.7	108	0.4972	103.3	0.4972	0.3906	0.5034
Ref. [28]	102	105.3	108	0.4971	104	0.4375	0.5056	0.5781
Ref. [29]	106	107.5	108	0.5001	104.3	0.4219	0.4944	0.5731
Proposed S3	112	112	112	0.5023	112	0.4219	0.5039	0.5938
Proposed S2	112	112	112	0.5134	112	0.4853	0.5431	0.5982
Proposed S1	112	112	112	0.5034	112	0.5493	0.5109	0.4721

2.7 Strict Avalanche Criteria (SAC)

SAC is the 50% modification in output when the input is altered by only one bit. In our case, the SAC of the proposed S-boxes is calculated and tabulated in Table 5. The calculated values of SAC come out to be approximately 0.5 which is near to the theoretical value. The SAC of the proposed S-boxes is compared with the recently proposed S-boxes in Table 5. The comparison reveals that the proposed S-boxes will provide a high degree of immunity to differential cryptanalysis.

2.8 Bijectivity

The bijectivity of S-boxes is crucial for the security of cryptographic systems, ensuring the confidentiality and integrity of information. Bijectivity means that each input has a unique output and vice versa, preventing duplication or repetition. Non-bijective S-boxes pose risks, as different inputs could yield the same output, potentially leading to information loss and security breaches. Designers employ techniques like using known bijective functions or nonlinear functions with proven bijectivity, such as the Advanced Encryption System (AES) S-box. Our S-boxes fulfill the criteria of bijectivity within the range of [0, 255], making them unique and secure.

2.9 Bit Independent Criteria (BIC)

In BIC we are checking the correlation of the two resultant vectors that are created by altering one bit in the input. Let vector A is obtained by altering bit 0 of the input vector and vector B be obtained by altering bit 2 of the input vector. The BIC can be calculated using the relation in Eq. (14).

$$BIC\left(A_i, B_j\right) = \max_{1<c\leq n} \left|correlation\ \left(A_i, B_j\right)\right| \tag{14}$$

The outcome of BIC lies in the [0, 1] range. The ideal value of BIC is 0.5. We have calculated the values of BIC and tabulated them in Table 5. The comparison reveals that the proposed S-boxes will provide a high degree of immunity to differential cryptanalysis.

2.10 Encryption Using the Proposed S-Boxes

To check the power of the Proposed S-boxes, here we present an encryption system. This encryption system utilizes the proposed S-boxes. The implemented encryption system, which is depicted in Fig. 2 comprises the following steps.

Step 1: Considerations for the logistic chaotic map are initiated from the encryption key as discussed in Section 2.2 of the article.

Step 2: The XOR map is generated as discussed in Section 2.2 and in parallel, the original image is split into R, G, and B channels, respectively.

Step 3: The three maps are XORed with the R, G, and B channels, respectively, by doing so the high correlation is smashed amongst the pixels.

Step 4: The process of shuffling as discussed in Section 2.4 is performed. Here the process of diffusion is completed.

Step 5: The S-box is generated from the ABC algorithm as discussed in Section 3. Here in this step utilizing these S-boxes, the process of substitution is performed.

Step 6: All three channels are joined to obtain the final encrypted Red-Green-Blue (RGB) Image.

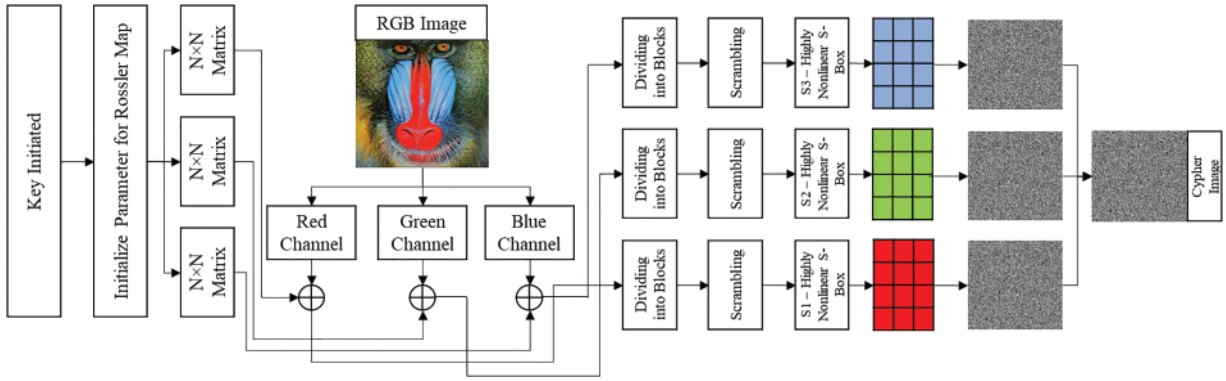

Figure 2: Encryption using the proposed S-boxes

3 Security Analysis

Conducting a thorough security analysis is essential for robust encryption systems. It identifies vulnerabilities, strengthens security, and safeguards sensitive data. Our research includes comprehensive security analyses to assess the resilience of our proposed encryption system, incorporating S-boxes, against diverse cryptographic attacks.

3.1 Brute Force Attack

The brute force attack is a technique used by hackers to discover passwords or encryption keys by systematically trying all possible combinations. Skilled attackers find this attack valuable because it does not rely on prior knowledge of the target password or key. Longer and more complex passwords or keys are harder to crack using brute force attacks due to the increasing number of combinations. Our research focuses on generating initial conditions that offer high resistance to brute force attacks in encryption systems, as explained in Section 2.2 of the paper.

3.2 Histogram Analysis

The histogram is a representation of the number of pixels in an image. For high-contrast images, the histogram is non-uniform and spread out over the x-axis. This can give intruders information about the image's contrast and brightness, which they can use to break the encryption. To prevent this, the encrypted image's histogram must be uniform. In Fig. 3, the histogram of the plain image is shown, and it can be seen that they are non-uniform. However, in Fig. 3, the histogram of the encrypted R, G, and B channels is shown to be uniform and devoid of any useful information for intruders. Our S-boxes-based system is thus claimed to be secure against histogram-based attacks based on this histogram analysis.

3.3 Differential Analysis

In differential analysis, the intruder takes an image, encrypts it, and then changes one pixel in the plain image and again encrypts that image and they try to find the function of the encryption system from these pairs of plain images and encrypted images to resist differential analysis. Any encryption system must have a 99% score for Number of Pixel Change Rate (NPCR) and a 33% score for Unified Averaged Changed Intensity (UACI). The NPCR and UACI are calculated and discussed in the following section. The NPCR of an image having dimension $X \times Y \times 3$ is calculated using the

relation in Eq. (15).

$$NPCR = \frac{1}{X \times Y \times 3} \sum_{i=1}^{X} \sum_{j=1}^{Y} \sum_{k=1}^{3} p(i,l,k) \times 100 \tag{15}$$

where,

$$p(i,j,k) = \begin{cases} 1 & I_1(i,j,k) = I_2(i,j,k) \\ 0 & elsewhere \end{cases} \tag{16}$$

where I1 is the result of encryption of the unchanged image and I2 is the result of encryption of one pixel changed image. The NPCR of the two images is calculated and tabulated in Table 6. The UACI of an image having dimension X × Y × 3 is calculated using the relation in Eq. (17).

$$UACI = \frac{1}{X \times Y \times 3} \sum_{i=1}^{X} \sum_{j=1}^{Y} \sum_{k=1}^{3} \frac{|I_1(i,j,k) - I_2(i,j,k)|}{255} \times 100 \tag{17}$$

where I1 is the result of encryption of the unchanged image and I2 is the result of encryption of one pixel changed image. The UACI of the two images is calculated and tabulated in Table 7.

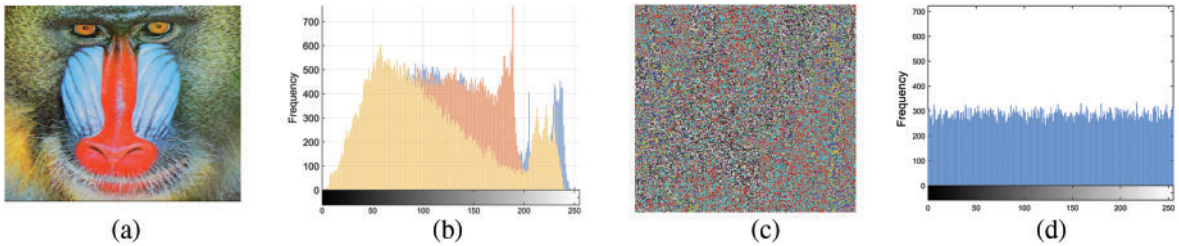

Figure 3: Histogram analysis; (a) plaintext image, (b) histogram of plaintext image, (c) encrypted image, and (d) histogram of encrypted image

Table 6: NPCR and UACI values

Image	NPCR	UACI
Lena	99.61	33.51
Airplane	99.66	33.46
Girl	99.68	32.33
Peppers	99.49	33.60
Baboon	99.71	33.51

3.4 Computational Complexity Analysis

The subjectivity of time analysis relies on the platform used for the encryption system. In the case of Field Programmable Gate arrays, a complex system can be encrypted in mere seconds. Our team implemented the encryption system in MATLAB, which was installed on a computer containing an Intel(R) Core(TM) i7-7700 processor @ 3.60 GHz processor and 8 GB of Random Access Memory (RAM). We compared the time analysis of our system with the AES by encrypting the same images using both systems and then we presented the results in Table 8.

Table 7: Comparison of NPCR and UACI values

Algorithm	NPCR	UACI
Ref. [17]	99.62	33.44
Ref. [18]	99.57	33.45
Ref. [19]	99.63	33.46
Proposed	99.71	33.51

Table 8: Computational complexity comparison of the proposed system with AES

Image	AES' time (sec)	Proposed system's time (sec)
Lena	99.61	33.51
Peppers	99.49	33.60
Baboon	99.71	33.51

3.5 National Institute of Standards and Technology (NIST) Statistical Test

To keep encrypted images safe from intruders, the randomness of the encryption key is of utmost importance. To test the efficacy of the proposed encryption system, tests based on NIST SP 800-22 criteria have also been conducted.

Each test produced a real number between 0 and 1, which was then compared with a pre-established significance degree α. If the value of p was greater than α, then it meant that the encryption system had passed the test successfully. In the proposed system, the value of α was set to 0.01. The results of the test were tabulated in Table 9, and it can be inferred that the proposed encryption system has excellent statistical properties and is a superior choice for image encryption.

Table 9: Results of NIST SP 800-22

Test	*p Value* for each layer of enciphering image				
	R	G	B	Gray	Qualified
Frequency	0.86727	0.88778	0.764164	0.641587	Yes
Universal	0.6447	0.67725	0.852215	0.676284	Yes
Runs (M = 10,000)	0.8442	0.67305	0.878779	0.704995	Yes
Non-overlapping	0.658972	0.67532	0.784813	0.741986	Yes
Rank	0.70549	0.84924	0.775579	0.764917	Yes
Spectral DFT	0.875153	0.68575	0.827160	0.826118	Yes
Block frequency	0.7141	0.77034	0.622756	0.61618	Yes
Overlapping test	0.7592	0.83375	0.880203	0.638971	Yes
Approximate entropy	0.7706	0.74081	0.60357	0.70113	Yes
Serial	0.6486	0.83828	0.69336	0.758559	Yes
Cumulative sums reverse	0.8067	0.82444	0.7351	0.625146	Yes
Cumulative sums forward	0.6686	0.87400	0.6457	0.84774	Yes

(Continued)

Table 9 (continued)

Test	*p Value* for each layer of enciphering image				
	R	G	B	Gray	Qualified
Long runs of ones	0.7615	0.89884	0.6234955	0.73263	Yes
Random excursions X = −4	0.6319	0.88856	0.601320	0.8324	Yes
Y = −3	0.845	0.86060	0.6253373	0.71993	Yes
Y = −2	0.6779	0.84002	0.729463	0.87318	Yes
Y = −1	0.654	0.67914	0.643665	0.640599	Yes
Y = 1	0.860	0.77391	0.764900	0.643418	Yes
Y = 2	0.8559	0.7866	0.70521	0.75397	Yes
Y = 3	0.7205	0.6227	0.67197	0.63699	Yes
Y = 4	0.6551	0.67198	0.72518	0.614896	Yes
Random excursions variant Y = −9	0.87081	0.883436	0.747259	0.74677	Yes
Y = −8	0.7013	0.87001	0.710774	0.63336	Yes
Y = −7	0.83407	0.71692	0.67250	0.72117	Yes
Y = −6	0.62893	0.6395	0.8826	0.88684	Yes
Y = −5	0.7725	0.617	0.67043	0.70594	Yes
Y = −4	0.8463	0.6046	0.61290	0.65069	Yes
Y = −3	0.2225	0.8472	0.0231	0.2225	Yes
Y = −2	0.4883	0.4343	0.0577	0.4883	Yes
Y = −1	0.7434	0.2422	0.9875	0.7434	Yes
Y = 1	0.4450	0.8055	0.9901	0.4450	Yes
Y = 2	0.9497	0.3555	0.3554	0.9497	Yes
Y = 3	0.5581	0.1166	0.0942	0.5581	Yes
Y = 4	0.9671	0.1084	0.1891	0.9671	Yes
Y = 5	0.6106	0.0848	0.0905	0.6106	Yes
Y = 6	0.5537	0.5596	0.0439	0.5537	Yes
Y = 7	0.6489	0.0677	0.1590	0.6489	Yes
Y = 8	0.6932	0.0983	0.1124	0.6932	Yes
Y = 9	0.4914	0.1205	0.0800	0.4914	Yes

3.6 Key Sensitivity Analysis

The employed technique demonstrates remarkable sensitivity to even a slight modification in the encryption key. The starting condition for the erratic and unpredictable logistic map is equivalent to the key for the encryption method. Upon encrypting an image, the same initial conditions are utilized at the decryption end for the formation of the S-box. After creating the S-box, inverse S-boxes are generated for decryption. By varying the key, i.e., initial conditions of the chaotic map, the produced S-box is entirely distinct, and the decrypted image does not reveal any essential information. Fig. 4 exhibits the decrypted image using the original key and the decrypted image with a marginally altered key. The chaotic map, which has been XORed in step 2, is responsible for this key sensitivity.

Figure 4: Key sensitivity analysis: (a) plain image; (b) encrypted image, (c) correctly decrypted image, (d) decrypted image through slightly changing the key

4 Conclusion

In conclusion, this research has proposed a unique and innovative method for generating substitution boxes (S-boxes) for encryption systems in the context of multimedia technology. As the strength of the entire encryption system depends on the cryptographic strength of the S-box, it is essential to ensure its reliability and robustness. By integrating the Proposed S-boxes into the encryption system's design and analyzing their nonlinearity, as well as other security parameters such as NPCR and UACI, we have demonstrated that the Proposed S-boxes provide a high degree of security to digital content during transmission and storage. This research provides valuable insights into enhancing the security of information sharing through insecure communication channels. Future studies could consider integrating multiple chaotic maps to enhance the robustness of the encryption scheme, optimizing the algorithm for better performance with large-scale real-world applications, and developing a dynamic key generation mechanism to increase security.

Acknowledgement: Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2023R333), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding Statement: This work was funded by Deanship of Scientific Research at Najran University under the Research Groups Funding Program Grant Code (NU/RG/SERC/12/3) and also by Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2023R333), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Author Contributions: The authors confirm their contribution to the paper as follows: study conception and design: Y. Y. Ghadi, M. S. Alshehri, S. Almakdi, O. Saidani, N. Alturki, F. Masood, M. S. Khan; data collection: Y. Y. Ghadi, M. S. Alshehri, S. Almakdi; analysis and interpretation of results: M. S. Alshehri, S. Almakdi, O. Saidani, N. Alturki, F. Masood; draft manuscript preparation: O. Saidani, N. Alturki, M. S. Khan. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data is available with the corresponding author upon appropriate request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] X. Wang and Q. Wang, "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos," *Nonlinear Dynamics*, vol. 75, no. 3, pp. 567–576, 2014.

[2] M. Khan, L. Khan, M. M. Hazzazi, S. S. Jamal and I. Hussain, "Image encryption scheme for multi-focus images for visual sensors network," *Multimedia Tools and Applications*, vol. 81, no. 12, pp. 16353–16370, 2022.

[3] A. Elmoasry, L. S. Khan, M. Khan and I. Hussain, "A dual layer security scheme for medical images using Hessenberg and singular value decompositions," *Multimedia Tools and Applications*, vol. 81, no. 10, pp. 14001–14022, 2022.

[4] E. Tanyildizi and F. Özkaynak, "A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps," *IEEE Access*, vol. 7, pp. 117829–117838, 2019.

[5] M. Khan and T. Shah, "A construction of novel chaos base nonlinear component of block cipher," *Nonlinear Dynamics*, vol. 76, no. 1, pp. 377–382, 2014.

[6] R. W. Ibrahim, H. Natiq, A. Alkhayyat, A. K. Farhan, N. M. G. Al-Saidi *et al.,* "Image encryption algorithm based on new fractional beta chaotic maps," *Computer Modeling in Engineering & Sciences*, vol. 132, no. 1, pp. 119–131, 2022.

[7] M. A. M. Khan, N. A. Azam, U. Hayat and H. Kamarulhaili, "A novel deterministic substitution box generator over elliptic curves for real-time applications," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 1, pp. 219–236, 2023.

[8] S. Zhu, X. Deng, W. Zhang and C. Zhu, "Secure image encryption scheme based on a new robust chaotic map and strong S-box," *Mathematics and Computers in Simulation*, vol. 207, pp. 322–346, 2023.

[9] S. Zhou, Y. Qiu, X. Wang and Y. Zhang, "Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box," *Nonlinear Dynamics*, vol. 111, no. 10, pp. 9571–9589, 2023.

[10] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," *Communications in Nonlinear Science and Numerical Simulation*, vol. 60, pp. 12–32, 2018.

[11] Z. Li, C. Peng, W. Tan and L. Li, "A novel chaos-based color image encryption scheme using bit-level permutation," *Symmetry*, vol. 12, no. 9, pp. 1497, 2020.

[12] X. Wang and R. Si, "A new chaotic image encryption scheme based on dynamic L-shaped scrambling and combined map diffusion," *Optik*, vol. 245, pp. 167658, 2021.

[13] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, 2020.

[14] M. Khan, A. S. Alanazi, L. S. Khan and I. Hussain, "An efficient image encryption scheme based on fractal Tromino and Chebyshev polynomial," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2751–2764, 2021.

[15] Z. Liu, C. Wu, J. Wang and Y. Hu, "A color image encryption using dynamic DNA and 4-D memristive hyper-chaos," *IEEE Access*, vol. 7, pp. 78367–78378, 2019.

[16] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[17] Y. He, Y. Q. Zhang and X. Y. Wang, "A new image encryption algorithm based on two-dimensional spatiotemporal chaotic system," *Neural Computing and Applications*, vol. 32, no. 1, pp. 247–260, 2020.

[18] A. Alghafis, F. Firdousi, M. Khan, S. I. Batool and M. Amin, "An efficient image encryption scheme based on chaotic and deoxyribonucleic acid sequencing," *Mathematics and Computers in Simulation*, vol. 177, pp. 441–466, 2020.

[19] S. Khan, L. Han, H. Lu, K. K. Butt, G. Bachira *et al.,* "A new hybrid image encryption algorithm based on 2D-CA, FSM-DNA rule generator, and FSBI," *IEEE Access*, vol. 7, pp. 81333–81350, 2019.

[20] D. Karaboga, "An idea based on honey bee swarm for numerical optimization," *Technical Report,* Erciyes University, Engineering Faculty, Computer Engineering Department, vol. 200, pp. 1–10, 2005.

[21] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.
[22] S. S. Jamal, M. U. Khan and T. Shah, "A watermarking technique with chaotic fractional S-box transformation," *Wireless Personal Communications*, vol. 90, no. 4, pp. 2033–2049, 2016.
[23] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and S8 permutation," *Neural Computing and Applications*, vol. 29, no. 4, pp. 993–999, 2018.
[24] D. Lambić, "S-box design method based on improved one-dimensional discrete chaotic map," *Journal of Information and Telecommunication*, vol. 2, no. 2, pp. 181–191, 2018.
[25] T. Ye and L. Zhimao, "Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling," *Nonlinear Dynamics*, vol. 94, no. 3, pp. 2115–2126, 2018.
[26] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami and W. Alhakami, "Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications," *IEEE Access*, vol. 8, pp. 116132–116147, 2020.
[27] F. Özkaynak, "Chaos based substitution boxes as a cryptographic primitives: Challenges and opportunities," *Chaotic Modeling Simulation*, vol. 1, pp. 49–57, 2019.
[28] A. Belazi, M. Khan, A. A. A. El-Latif and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 337–361, 2017.
[29] H. A. Ahmed, M. F. Zolkipli and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," *Neural Computing and Applications*, vol. 31, no. 11, pp. 7201–7210, 2019.