AIMS Mathematics, 9(12): 36116–36139.
DOI: 10.3934/math.20241714
Received: 20 November 2024
Revised: 09 December 2024
Accepted: 13 December 2024
Published: 26 December 2024

http://www.aimspress.com/journal/Math

Research article

Cryptanalysis of hyperchaotic S-box generation and image encryption

Mohammad Mazyad Hazzazi[1], Gulraiz[2], Rashad Ali[3,*], Muhammad Kamran Jamil[4], Sameer Abdullah Nooh[5] and Fahad Alblehai[6]

[1] Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia

[2] Govt. High School Gulistan Colony Mustafa Abad (EX-MCL), Dharampura, 05478, Lahore, Pakistan

[3] Department of Mathematics, University of Trento, 38122 Trento, Italy

[4] Department of Mathematics, Riphah International University, 54660 Lahore, Pakistan

[5] Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University Jeddah 21589, Saudi Arabia

[6] Computer Science Department, Community College, King Saud University, Riyadh 11437, Saudia Arabia

* **Correspondence:** Email: rashadwattu@gmail.com.

Abstract: Cryptography serves as the cornerstone for safe communication and data security in today's digital environment. Because they feature substitution boxes, substitution-permutation networks (SPNs) are crucial for cryptographic algorithms such as the popular Advanced Encryption Standard (AES). The structure and properties of S-boxes have a significant impact on the overall security of cryptographic systems. This article aims to improve cryptographic security through unique S-box construction methodologies. The proposed S-boxes improve the security features by employing chaotic maps and Galois fields, which go beyond traditional design approaches. The S-boxes were analyzed and the weaknesses were removed to design strong candidate S-boxes. The efficiency of the proposed S-boxes in increasing cryptographic resilience is thoroughly explored thereby taking nonlinearity, strict avalanche requirements, bit independence constraints, linear approximation, and differential approximation into account. The dynamic S-boxes have average scores of nonlinearity, strict avalanche criteria(SAC), nonlinearity of Bit Independence Criteria (BIC Nonlinearity), SAC of Bit Independence Criteria (BIC SAC), Linear Approximation Probability (LAP) and Differential Approximation Probability (DAP) is 111.1025, 111.1022, 0.5014, 0.5024, 111.1082, 111.0964, 0.5024, 0.5022, 0.0726, 0.0729 and 0.0214, 0.0219, respectively. Furthermore, given the prevalence of images in modern communication and data storage, this work studies the seamless incorporation of advanced S-boxes into image

encryption systems. With its thorough research, the paper contributes to the current discussion on cryptographic security by providing theoretical understandings and practical solutions to improve digital communication and data security in an era of rising cyber dangers and ubiquitous connectivity.

Keywords: affine matrices; cryptanalysis; encryption; hyperchaos; S-box
Mathematics Subject Classification: 94A60, 68P25

1. Introduction

Personal information secrecy is something that many people want to keep private, and this requirement has always been present. There are several examples when it is necessary to protect sensitive data from prying eyes. It is crucial to stop enemies from listening in on conversations between military commanders or monarchs and their soldiers. Simple techniques have been previously used to obfuscate data. However, as society has developed and became more networked, there has been a significant rise in the dependence on electronic technologies [1]. As a result, there is now a greater need for electronic services, and sharing private information online is commonplace. As a result, the need for sophisticated data security methods has become more crucial in our day-to-day lives. The main goal of cryptography is to provide a safe network communication. Ensuring the security of information is often the main goal of cryptography [2]. Modern cryptography has evolved from a variety of fields, including computer science, mathematics, communication science, physics, and electrical engineering. Numerous real-world situations include the use of cryptography, such as safeguarding chip-based payment cards, enabling digital currencies, securing computer passwords, and expediting Internet commerce.

Cryptographic techniques play a pivotal role in safeguarding sensitive information from prying eyes, and their effectiveness hinges on the robustness of cryptographic components, such as substitution boxes (S-boxes). The need for robust S-boxes has led researchers to explore various techniques for their development. In the work referenced as [3], Cao Y. and Cui L. introduced a novel S-box structure known as Affine-Power-Affine (APA). The authors in [4] created an S-box using a chaotic map. Additionally, in the research conducted by X. Wang and Q. Wang, as documented in [5], dynamic S-boxes were crafted using chaos techniques. In another approach detailed in [6], Shah *et al*. harnessed the actions of the symmetric group S_8 on the Advanced Encryption Standard (AES) S-box to derive a substitution box. Another intriguing method, outlined in [7], employed a chaotic system to generate a series of S-boxes, where each was considered as a circular sequence with an initial pointer position. These S-boxes were selected to replace individual pixel values in images, and the selected S-boxes were dynamically updated by shifting the pointer forward based on the ciphered pixel and a randomly chosen integer. Furthermore, an alternative algorithm was proposed in [8], where the authors applied the group $PGL(2, GF(2^8))$ action on $GF(2^8)$ to design an S-box. Ali *et al.* [9] used the composition of a homomorphism of the group $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$ and inverse mapping of $GF(2^8)$ to design a large number of robust S-boxes with a minimal computation time. This scheme can have S-boxes with a nonlinearity less than 112.

Chaotic systems offer a viable strategy to design S-boxes. Chaotic systems are sensitive to starting circumstances, thus making them suitable to create pseudorandom sequences. This characteristic may

be utilized to generate encryption keys that are hard to predict. The authors in [10] studied how the unpredictability in chaotic maps is related to the Lyapunov exponent (LE). There were some drawbacks to using the newly created chaotic map in cryptography. These drawbacks included low randomness, a weak positive LE, and the absence of ergodicity in the phase space. In order to get over these restrictions and show how LE and randomness are related, the authors first built a generic n-dimensional non-degenerate hyper chaotic map (nD-NDCM) model with an adjustable LE using the Jacobian matrix's eigenvalues. Additionally, using this model as the basis, the authors instantiated 2D-NDCM and 3D-NDCM, and then examined their dynamic performance using the bifurcation diagrams, phase diagrams, and LE. Chaotic systems can develop diffusion procedures necessary for picture encryption. The authors in [11] designed a new strategy to design the fractional transformation of a finite field using the 2D Arnold map. The authors employed a chaotic logistic map for dynamically key dependent S-boxes. A new chaotic S-box was designed in [12] using the randomness of the LU Chen chaotic system. The authors designed two S-boxes with a substantial nonlinearity of 105–106 by employing row column permutations and a zigzag transformation. Ali *et al*. explored the applications of the Frobenius automorphism in [13]. The authors composed the linear fractional transformation with Frobenius map of the said field to design two new fractional transformations of degree 2. This mapping generates highly nonlinear and robust S-boxes. Additionally, the authors used a logistic map for dynamic generation. [14] proposed a unique picture encryption system based on an S-box formed by a mutation and crossover. [15] Lai and Hu introduced a revolutionary medical picture encryption strategy that blended compressive sensing techniques with a customised memristive hyperchaotic system. The suggested approach may swiftly encrypt a large quantity of medical photos into a custom-sized cypher image, thus significantly increasing the algorithm's efficiency. The S-box has a nonlinearity of 111.25, which is a good score on other aspects, with no fixed or reverse fixed points. The authors in [16] suggested a 4D memcapacitive hyperchaotic logistic map (4D-MHLM) that incorporated memcapacitors into the logistic map. The dynamical behavior of the 4D-MHLM was investigated using the Lyapunov exponent assessment, and the effects of various parameters on the system performance was examined. The complexity of producing pseudo-random sequences with the 4D-MHLM was explored using complexity analysis, which included spectral entropy and C0 complexity. The study in [17] suggested a method to improve the communication security through facial detection and chaotic partitioning. The system used an edge detection algorithm to identify facial details, which was subsequently encrypted. The hash value of the plaintext image was taken and used as the private key to the chaotic sequence produced by the system. The facial image underwent encryption processes to produce the final ciphertext. [18] used a genetic algorithm-based optimization model. The model employed chaotic sequences to construct initial S-boxes, and then nonlinearity was adjusted by treating it as an objective function. The average nonlinearity for the S-boxes was 110.25. The study [19] introduced an oscillatory term to discrete memristor (DM) models, thus creating four hyperchaotic maps with hidden attractors and diverse dynamical behaviors. These maps, validated through hardware implementation, generated highly random sequences, which were successfully applied in pseudorandom number generators (PRNGs). A non-degenerate 3D hyperchaotic map was designed for image encryption and an S-box in [20]. The authors eliminated the fixed, reverse fixed points ,and the short period rings in the designed S-box. The nonlinearity of the proposed scheme remained less than 112. Liu *et al.* [21] defined a new 2D hyperchaotic map to generate random affine invertible matrices over the binary field . They designed keyed S-boxes and introduced a mechanical

way to eradicate the existing weakness. The elimination process effected the nonlinearity, and its average was 110.60. The authors in [22,23] devised a similar methodology to eliminate the weaknesses in S-boxes, where the design was dependent upon a hyperchoatic map and algebraic transformations.

Based on the detailed analysis of existing literature, we have found that if an S-box is designed using Chaos, then its nonlinearity is very low and we have to use an optimization model as an extra layer to enhance the strength. The S-box designed based on algebraic transformations have other types of weaknesses, such as the existence of a fixed point, reverse fixed points, and short period cycles. A recent study in [12, 13] showed that employing chaotic mappings with algebraic transformations can be beneficial in terms of the nonlinearity, key dependence, complexity ,and the weaknesses. In this article, our primary goal is to bolster image security within cryptographic frameworks by advancing the state-of-the-art S-box design. To achieve this objective, we embark on a journey through the realm of mathematical structures, specifically the newly designed hybrid hyperchaotic map, 4×4 invertible matrices, and Galois fields. These mathematical constructs serve as the building blocks for the creation of novel S-boxes that exhibit remarkable security features. By harnessing the inherent properties of these structures, we enhance the resistance of S-boxes against a multitude of cryptographic attacks, thus ensuring that sensitive visual data remains protected. Our endeavor extends beyond theoretical development, as we rigorously assess the cryptographic performance of these newly devised S-boxes. Through a meticulous analysis that encompasses nonlinearity, strict avalanche criteria, bit independence criteria, linear approximation, and differential approximation, we provide empirical evidence of the enhanced security offered by these S-boxes. The designed S-boxes have no weaknesses such as fixed points, reverse fixed points, and short period cycles. Moreover, recognizing the practical significance of our research, we delve into the seamless integration of these sophisticated S-boxes into image encryption systems. This integration not only fortifies the security of visual data, but also paves the way for more resilient and reliable cryptographic practices in the realm of image security.

1.1. Motivations and contributions

The following are our motivations for this article:
(1) Developing new hybrid hyperchaotic maps with strong randomness and a large key space;
(2) Incorporating chaotic maps to generate dynamic S-boxes with Galois fields; and
(3) Designing highly nonlinear S-boxes without any weakness.

The contributions of the proposed study are as follows:
(1) A new 2D hybrid hyperchaotic map with a key space of 2.7378×10^{54} is designed;
(2) This scheme can generate millions of strong candidate S-boxes with any weakness; and
(3) The average scores of candidate S-boxes are better than existing schemes available in the literature.

The rest of the article is divided into four main sections: In Section 2, we introduce a new hybrid hyperchaotic map; in Section 3, we create some S-boxes using the action of matrices on the Galois fields; in Section 4 carefully analyzes the S-box generated in terms of statistics and compares it with other research in the field; the cryptanalysis is explained in Section 5 regarding the sensitivity; one of the S-boxes is used in Section 6 to encrypt different images; the results of this encryption are compared to the findings of previous studies in the literature; Section 7 sums up the article's main points and provides some ideas for future research in this area.

2. Construction of 2D hyperchaotic map

2.1. 2D hyperchaotic map

A chaotic map with ergodicity and excellent randomness can function as a pseudo random number generator. We created the 2D hyperchaotic map given in Eq (2.1) with three parameters using modular operations and represented it as follows:

$$\begin{aligned} x(i+1) &= r \cdot \left(1 - a^{\pi + y(i)}\right) + (r-a) \cdot (1 - x(i)) \pmod 1, \\ y(i+1) &= r \cdot \left(1 - b^{\pi + x(i)}\right) + (r-b) \cdot (1 - y(i)) \pmod 1. \end{aligned} \tag{2.1}$$

The parameter $r \in (0\ ,\ 1800]$, while a, b are real numbers in $[2\ ,\ 40]$. The bifurcation, phase diagrams, and Lyapunov exponents in Figures 1–3 indicate the ergodicity and randomness in the phase space for the time sequences created by 2D hyperchaotic map. We will use the 2D hyperchaotic map to generate a random affine transformation matrix and three index variables.

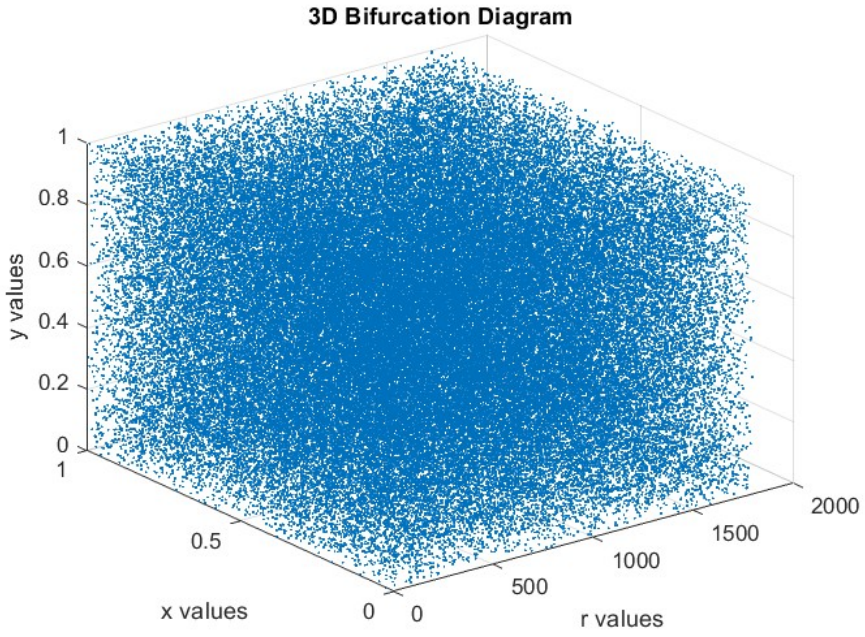


Figure 1. 3D Bifurcation diagram of Chaotic map with $a = 3.504946177477956, b = 19.835653902506410$.

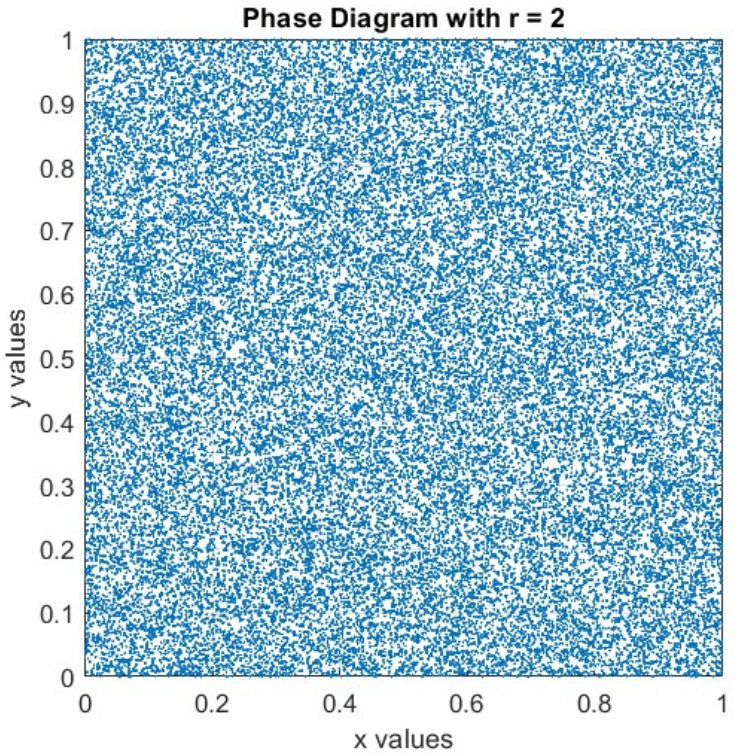


Figure 2. Phase diagram of Chaotic map with $a = 8.9958772224860656, b = 12.213067941059531$.

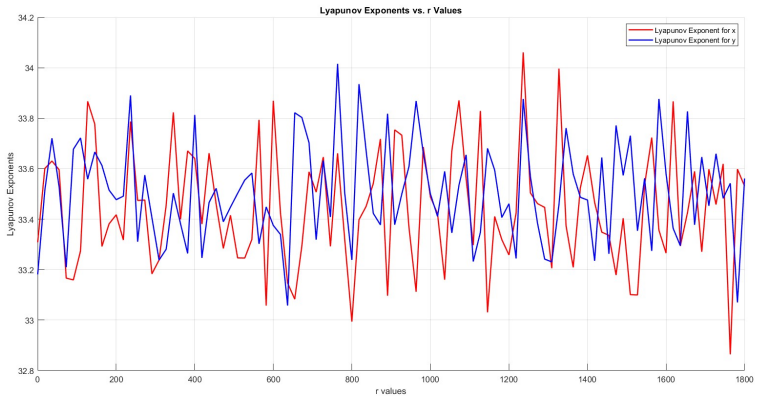


Figure 3. Lyapunov exponent.

2.2. *Generation of affine invertible matrices*

The most important step in the construction of the S-box in the proposed algorithm is the generation of affine invertible matrices over $\mathbb{F}_2$. For this, we iterated the 2D hyperchaotic for 1020 iterations. The two matrices are calculated as:

Discard the first 1000 iterations and define A and B by the following:

$$A = \text{reshape}\left(\left(\lfloor x_{1001:1016} \times 10^{16} \rfloor, 2\right), 4, 4\right) \pmod 2,$$

$$B = \text{reshape}\left(\left(\lfloor y_{1001:1016} \times 10^{16} \rfloor, 2\right), 4, 4\right) \pmod 2.$$

Calculate the determinant of both matrices, and if both are invertible over $GF(2)$, then we will proceed further; otherwise, we will modify both initial conditions. The two-column vectors are defined as follows:

$$b = \left(\left\lfloor x_{1017:1020} \times 10^{16} \right\rfloor\right) \pmod 2,$$

$$c = \left(\left\lfloor y_{1017:1020} \times 10^{16} \right\rfloor\right) \pmod 2.$$

Meanwhile, we also use the given new chaotic map for the selection of irreducible polynomials of degree 4 and 8 to generate finite fields with 16 and 256 elements. The three index variables are defined as follows:

$$\text{Index}_1 = \mod (\lfloor x_{1001} \times 256 \rfloor, 3) + 1,$$

$$\text{Index}_2 = \mod (\lfloor y_{1002} \times 256 \rfloor, 3) + 1,$$

$$\text{Index}_3 = \mod (\lfloor x_{1003} \times 256 \rfloor, 30) + 1.$$

The irreducible polynomials of degree 4 are as follows:

$$p(x) = x^4 + x + 1 \ (19),$$

$$q(x) = x^4 + x^3 + 1 \ (25),$$

$$r(x) = x^4 + x^3 + x^2 + x + 1 \ (31).$$

3. Generation of S-Box

Consider two finite fields $\mathbb{F}_1$ and $\mathbb{F}_2$ based on the irreducible polynomials $p(x)$, $q(x)$, and $r(x)$ then, the maps $\phi : \mathbb{F}_1 \to \mathbb{F}_1, \psi : \mathbb{F}_2 \to \mathbb{F}_2$ defined by $\phi(x) = Ax^{-1} + b$, $\psi(x) = Bx^{-1} + c$ are bijective iff A and B are invertible matrices over $\mathbb{F}_2$, whereas b, c are binary column vectors of size 4×1. Let $g(x)$ be the inversion map of the Galois field concerning irreducible polynomials of the list available in [13]. The algorithm to design the S-box is as follows:
(1) Convert each entry of $\mathbb{F}_1$ and $\mathbb{F}_2$ into binary.
(2) Apply the maps ϕ, ψ on binary entries of $\mathbb{F}_1$ and $\mathbb{F}_2$, and convert back to the decimal entries. Store the results in two sets C & D.
(3) Take the Cartesian product of the sets C and D and concatenate the bits to obtain a 16×16 matrix of entries $0 - 255$. Store the results in f.
(4) Define the S-boxes S_1 and S_2 by following two rules:

- $S_1 = f \circ g$.
- $S_2 = g \circ f$.

3.1. Elimination of weakness

There are some flaws in S-box designs, such as having fixed points, reverse fixed points, and short period cycles. The cryptographer aims to develop a highly nonlinear S-box that does not have a fixed point, reverse fixed point, or short-period cycles. For the elimination of weakness, we consider the method as developed in [21].

Two Sample candidate S-boxes are displayed in Tables 1 and 2, which were obtained by fixing $x_0 = 0.150591199468996, y_0 = 0.888238060843572, a = 6.401634045456396$, and $b = 19.376372433391815$.

Table 1. 1st Candidate S-box.

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

Table 2. 2nd Candidate S-box.

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

4. Statistical analysis and security evaluation of the S-boxes

In this context, we have presented the security assessment of our proposed S-boxes to confront potential cryptographic vulnerabilities. The S-boxes have been subjected to a series of evaluations. The obtained results have been compared against established S-boxes of repute. An explanation of the conducted tests is provided in the following section.

4.1. Nonlinearity (NL)

The concept of "nonlinearity" in this context was formally introduced by Pieprzyk and Finkelstein in 1988, as documented in [24]. Nonlinearity quantifies the disparity between an nth-variable Boolean function and the entire set of affine functions of n variables. The highest achievable nonlinearity for S-boxes constructed using $GF(2^8)$ is 120. The sample S-boxes of Tables 1 and 2 achieved the nonlinearity of 112 displayed in Table 3. Among randomly generated 1000 S-boxes, 239 and 223 are of the nonlinearity 112 by both composition functions. The average nonlinearity after removing the fixed, reverse fixed points, and short cycles stood at 111.1025 and 111.1022. The similar kind of scheme in [21] has the nonlinearity 110.60. However, our scheme produced better results as compared to the existing schemes. Meanwhile, most of the S-boxes have a nonlinearity greater than 110, as can be observed from the pie charts in Figures 4 and 5.

Table 3. Comparative Analysis of Candidate S-boxes 1 and 2.

S-boxes	Mathematical Structure	Nonlinearity	SAC	BIC Nonlinearity	BIC SAC	LAP	DAP
1st Candidate S-box	$GF(2^8)$	112	0.4971	112	0.4997	0.0625	0.0156
2nd Candidate S-box	$GF(2^8)$	112	0.4963	112	0.5015	0.0625	0.0156
Average Results 1st Composition	$GF(2^8)$	111.1025	0.5014	111.1082	0.5024	0.0726	0.0214
Average Results 2nd Composition	$GF(2^8)$	111.1022	0.5024	111.0964	0.5022	0.0729	0.0214
[11]	$GF(2^8)$	112	0.5066	111.28	0.5016	0.0703	0.0625
[12]	Chaos	105.75	0.4939	103.43	0.5032	0.1171	0.0390
[13]	$GF(2^8)$	112	0.5022	112	0.5008	0.0625	0.0156
[13]	$GF(2^8)$	112	0.5002	112	0.5054	0.0625	0.0156
[14]	Mutation	111.25	0.5022	103.78	0.5036	0.1328	0.0391
[18]	Genetic Algorithm	110.25	0.4953	104.07	0.5021	0.125	0.0391
[21]	Chaos	110.60	0.4966	109.67	0.5026	0.0790	0.0214
[25]	$GF(2^8)$	112	0.4988	112	0.5008	0.0625	0.0156
[26]	Chaos	107.25	0.4981	104.42	0.5008	0.1171	0.0391
[27]	Chaos	107	0.5012	103.07	0.4970	0.1250	0.04687
[28]	Chaos	103.75	0.4949	103.5	0.5036	0.0790	0.0391
[29]	Chaos	112	0.5829	104	0.5017	0.1406	0.0391
[30]	ECC	112	0.5032	112	0.5059	0.0625	0.0156
[31]	Neural Network	114.5	0.4975	107	0.5080	0.135	0.0391
[32]	Optimization	110.5	0.51	103	0.4998	-	0.0391
[33]	Quantum Oscillator	110	0.5000	108.5	0.5001	0.1250	0.04687
[34]	Sine Cosine optimization	112	0.5056	104	0.4991	0.1250	0.0391
[35]	ECC	107.75	0.5010	103.9286	0.5038	0.1250	0.0391
[36]	ECC	108	0.5068	103.3571	0.5018	0.070	0.015

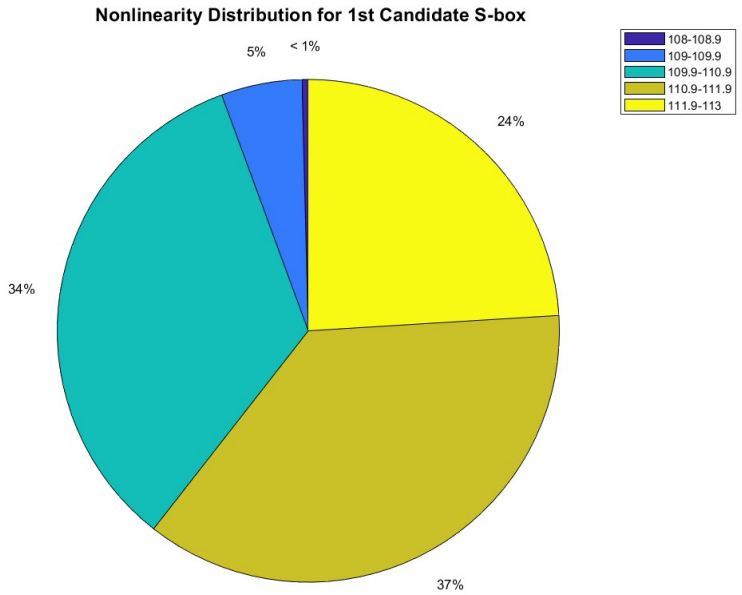


Figure 4. Nonlinearity Distribution for 1st Candidate S-box.

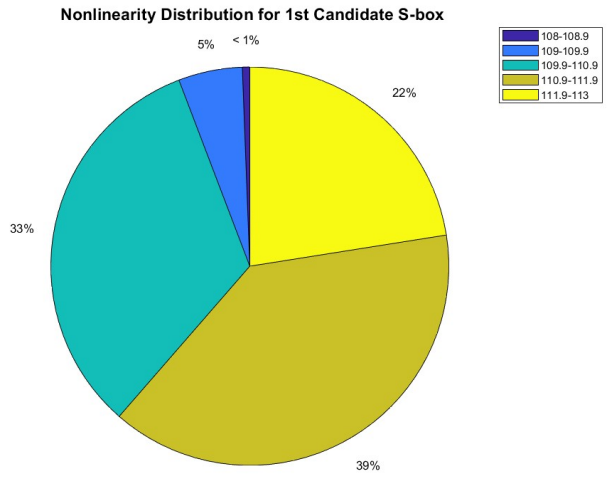


Figure 5. Nonlinearity Distribution for 2nd Candidate S-box.

4.2. Strict Avalanche Criteria (SAC)

This evaluation assesses the degree of fluctuation in the output resulting from a slight modification in the input value. The concept of Strict Avalanche Criteria (SAC) (i.e., Sensitivity to Input Changes) was pioneered by Tavares and Webster, as documented in their work [37]. According to the SAC

criterion, when a single input bit of the S-box is inverted, it is expected that exactly 50% of the output bits will, on average, undergo an inversion as well. The formula for the essential dependence matrix, denoted as "M," required for SAC is expressed as follows:

$$M(x) = \frac{\sum_{k=1}^{8} h(x) \oplus h(x \oplus y_j)}{256} \quad ; \quad HWT(y_j) = 1 \quad \forall \quad j = 1, 2, \ldots, 8. \tag{4.1}$$

The average SAC score in [21] was 0.4966 while, our scheme has $0.5014, 0.5024$ for both composition functions. The overall distribution of the SAC score can be observed in Figures 6 and 7.

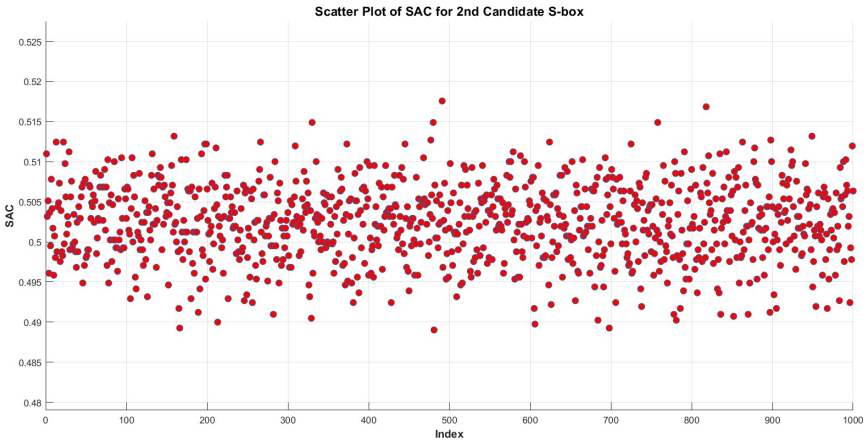


Figure 6. SAC Distribution for 2nd Candidate S-box.

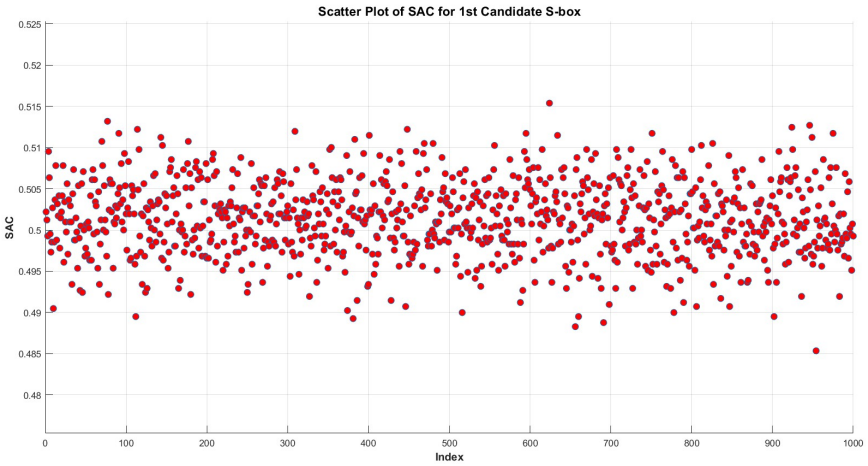


Figure 7. SAC Distribution for 1st Candidate S-box.

4.3. Bit Independence Criteria (BIC)

The Bit Independence Criteria (BIC) serves as a metric to gauge the cryptographic robustness of an S-box. It quantifies the level to which the output bits of an S-box exhibits independence from the input bits. A greater degree of autonomy between the input and output bits is sought after, as it

enhances the difficulty for potential attackers attempting to analyze and compromise the cryptographic system. The average values of the BIC Nonlinearity and the BIC SAC in [21] were 0.5026 and 109.67, while our proposed technique report values of $111.1082, 111.0964$, and $0.5024, 0.5022$. Thus, our technique outperforms the existing similar techniques in literature. The BIC Nonlinearity and SAC distribution can be observed in Figures 8–11.

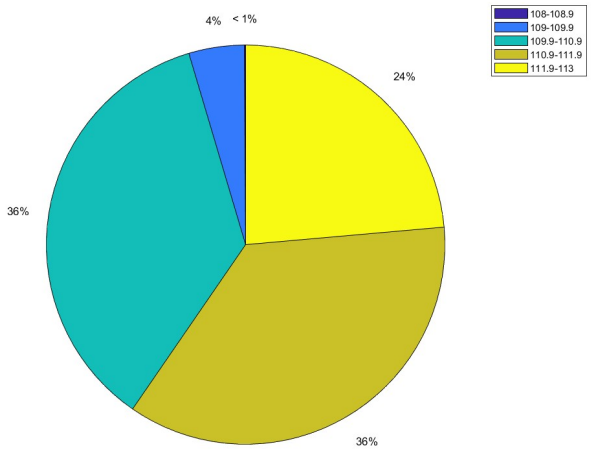


Figure 8. BIC Nonlinearity Distribution for 1st Candidate S-box.

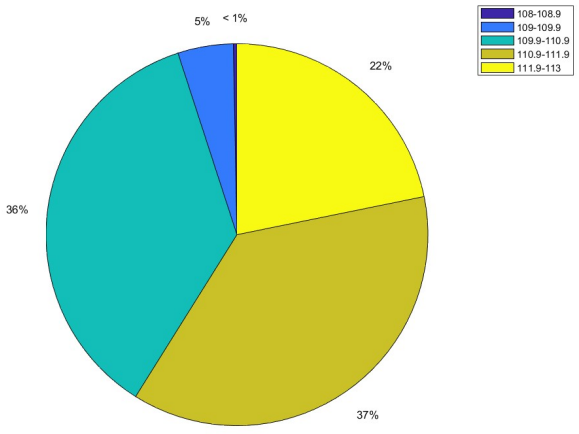


Figure 9. BIC Nonlinearity Distribution for 2nd Candidate S-box.

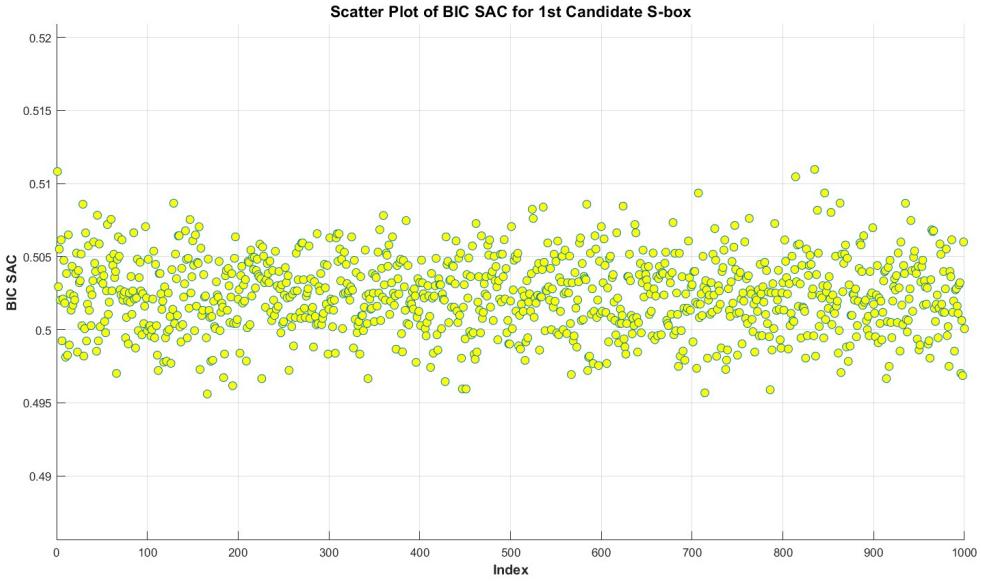


Figure 10. BIC SAC Distribution for 1st Candidate S-box.

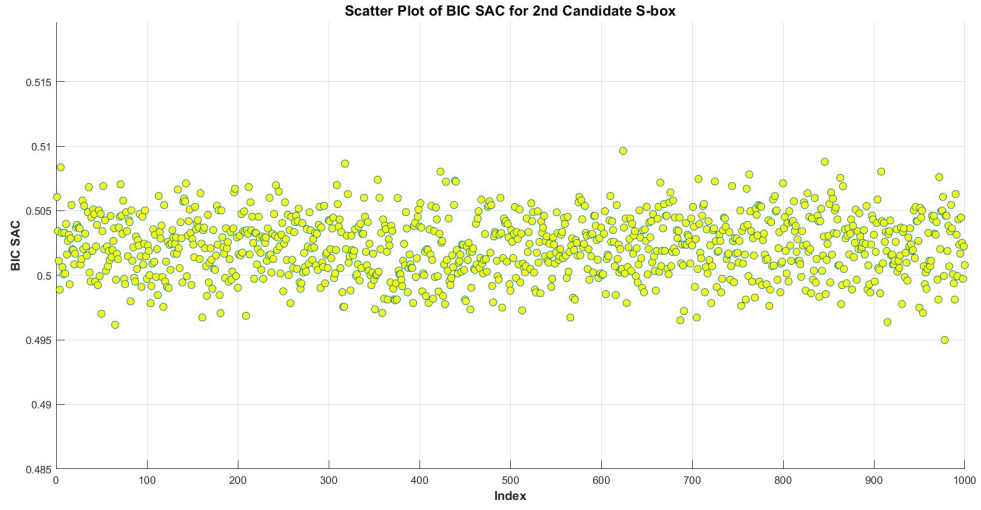


Figure 11. BIC SAC Distribution for 2nd Candidate S-box.

4.4. Linear Approximation Probability (LAP)

The Linear Approximation Probability (LAP) test is a powerful cryptanalysis tool designed to assess the robustness of an S-box in block ciphers. This test quantifies the probability of a linear connection between the input and output bits of an S-box. The LAP test operates by examining a set of input and output pairs linked with the S-box and calculating the correlation between these input and output bits using a statistical method. The correlation value indicates the level of linearity in the

relationship between the input and output bits of the S-box.

$$LAP = \max_{u,v\neq 0} \left| \frac{\left| \left\{ \alpha \in GF(2^8) \mid u \cdot \alpha = v \cdot S(\alpha) \right\} \right| - 128}{256} \right| \tag{4.2}$$

The average LP for 1000 S-boxes using both composition functions is 0.0726, 0.0729 (Figures 12 and 13), which is far good against the score of 0.0790 in [21]. The lowest value of 0.0625 is attained by 237 and 218 S-boxes produced by our scheme. This scheme has better scores of LP on the individual and collective levels.

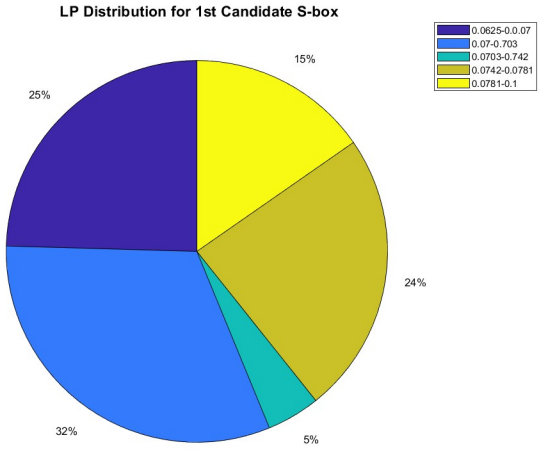


Figure 12. LP Distribution for 1st Candidate S-box.

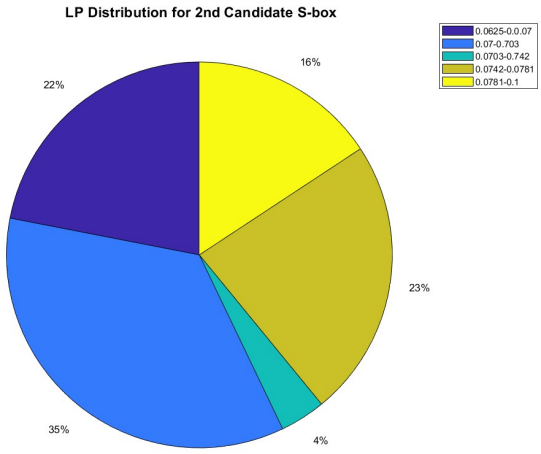


Figure 13. LP Distribution for 2nd Candidate S-box.

4.5. *Differential Approximation Probability (DAP)*

The Differential Approximation Probability (DAP) test employs a statistical methodology to gauge the likelihood of a differential relationship. Rather than analyzing all the possible input pairs, the DAP test selects a random groups of input pairs and computes the ratio of pairings that adhere to the defined differential relationship. A larger subset selection results in a more precise estimation of the differential probability. Typically, the DAP test is utilized alongside other statistical tests, such as the LAP test, to conduct a comprehensive assessment of an S-box's security properties as follows:

$$DP(\Delta u, \Delta v) = \frac{|\{u \in GF(2^8) \mid S(u) \oplus S(u \oplus \Delta u) = \Delta v\}|}{256}, \tag{4.3}$$

where Δu and Δv represents the input and output differential, respectively.

The DP values for both composition functions can be observed in Figures 14 and 15 with a sound score close to [21]. There are 216 and 223 S-boxes with a DP score of 0.0156.

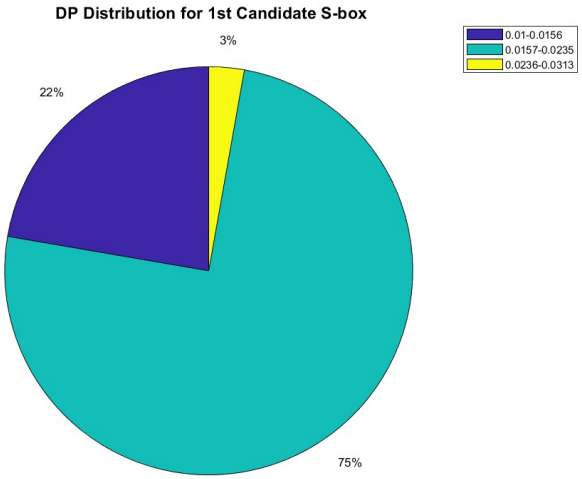


Figure 14. DP Distribution for 1st Candidate S-box.

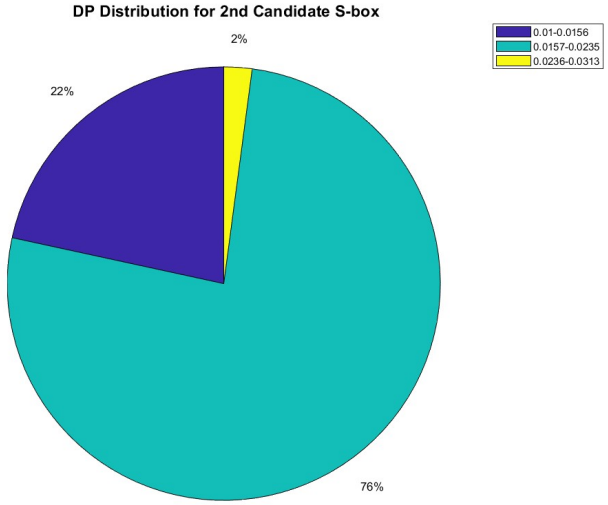


Figure 15. DP Distribution for 2nd Candidate S-box.

5. Cryptanalysis

5.1. Sensitivity analysis

5.2. Sensitivity with AES S-box

We randomly generated 1000 S-boxes from both composition functions and measured the hamming distances between each S-box and AES S-box. The average hamming distances were 1024.34 and 1023.64, which are very close to the ideal value of 1024. The distribution of hamming distances can be visualized in Figures 16 and 17.

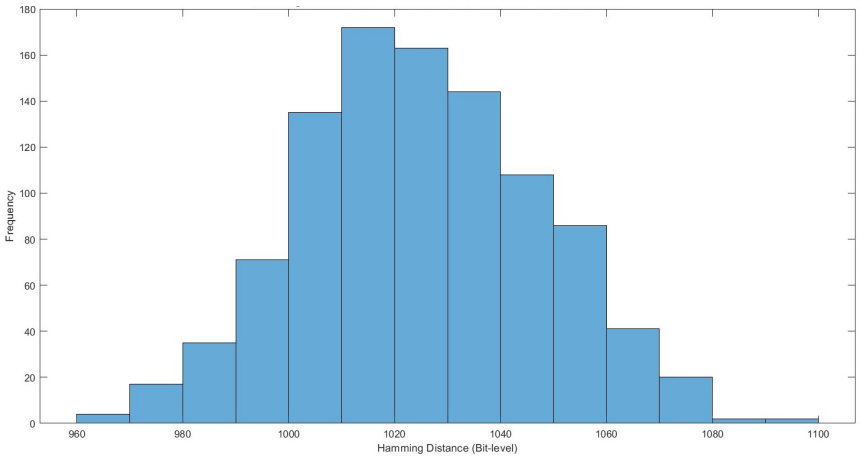


Figure 16. Hamming distance between 1st Candidate S-box and AES S-box.

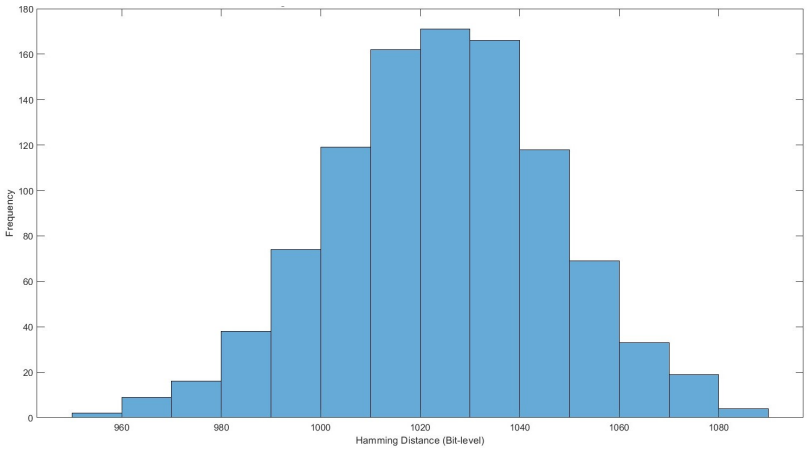


Figure 17. Hamming distance between 2nd Candidate S-box and AES S-box.

5.3. Initial key sensitivity

We measured the sensitivity of the proposed S-boxes by altering the initial keys. Consider $x_0 = 0.046414229568095, y_0 = 0.307869452852334$ and $x_0 + \epsilon = 0.046414229568105, y_0 + \epsilon = 0.307869452852344$, where $\epsilon = 10^{-14}$. The hamming distance between the candidate S-boxes of the 1st composition is 1024.8 and 1022.9 for 2nd composition. These results are very close to the ideal hamming distance of 1024 and surpass the results of [21]. The distribution can be observed in Figures 18 and 19.

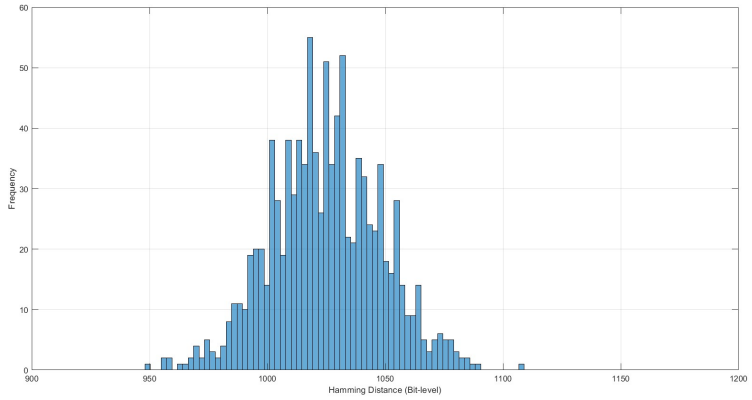


Figure 18. Hamming distance between 1st Candidate S-boxes.

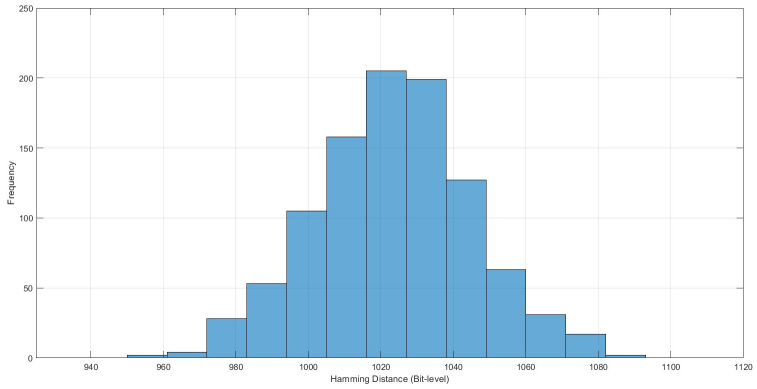


Figure 19. Hamming distance between 2nd Candidate S-boxes.

6. Utilization of the envisioned S-box in image encryption

In this section, we utilize our S-box to encrypt various images. We used the Cipher Block Chaining (CBC) mode of AES to encrypt digital photos using the best S box of Table 1 of our scheme. To assess the performance of the employed image encryption algorithm , we applied the majority logic criterion, which encompasses measures such as Contrast, Entropy, Correlation, Energy, and Homogeneity. The plane and corresponding cipher images are observed in Figures 20–23, while the results of the image encryption application are shown in Tables 4 and 5.

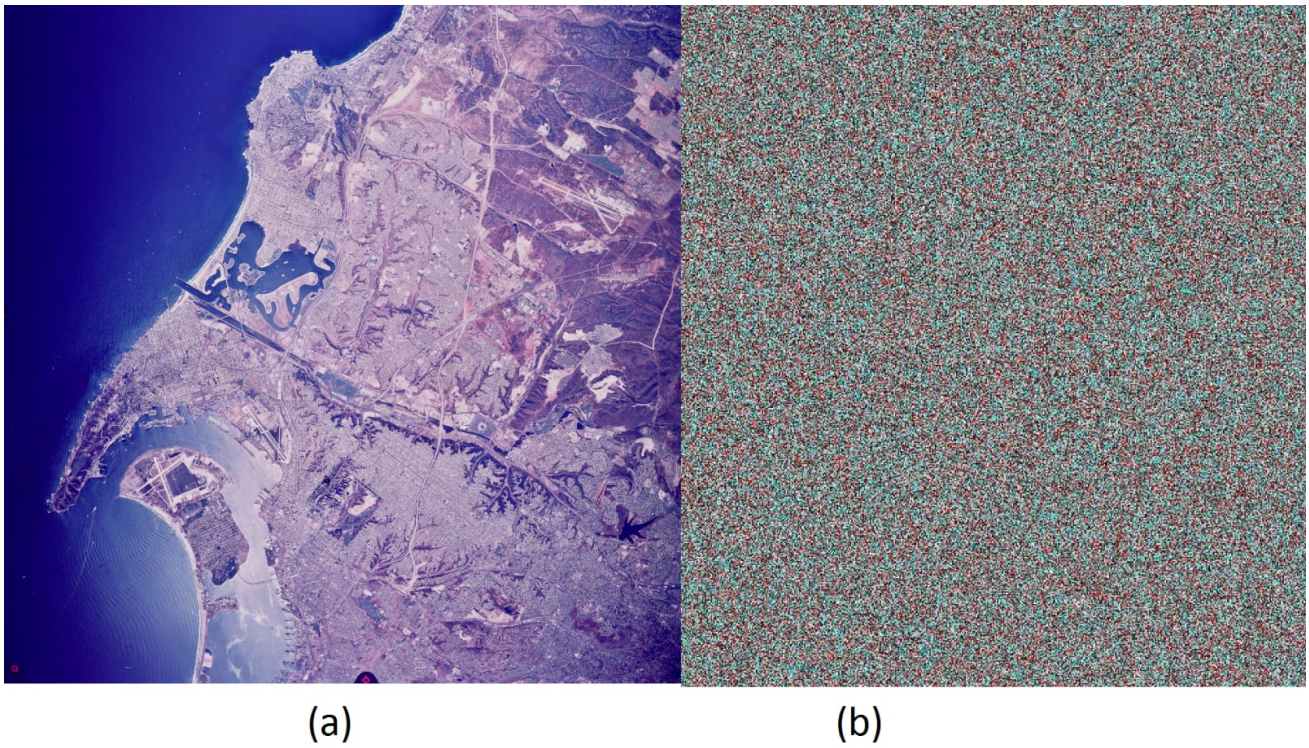


Figure 20. Original and encrypted aerial image.

Figure 21. Original and encrypted ECG image.

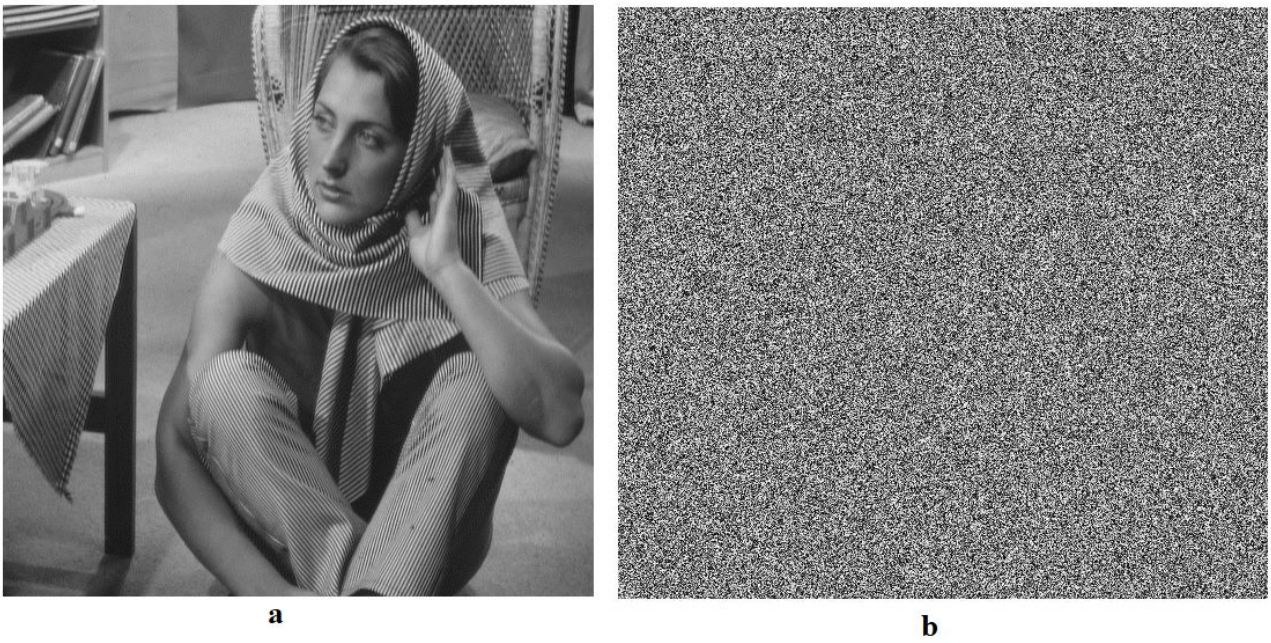
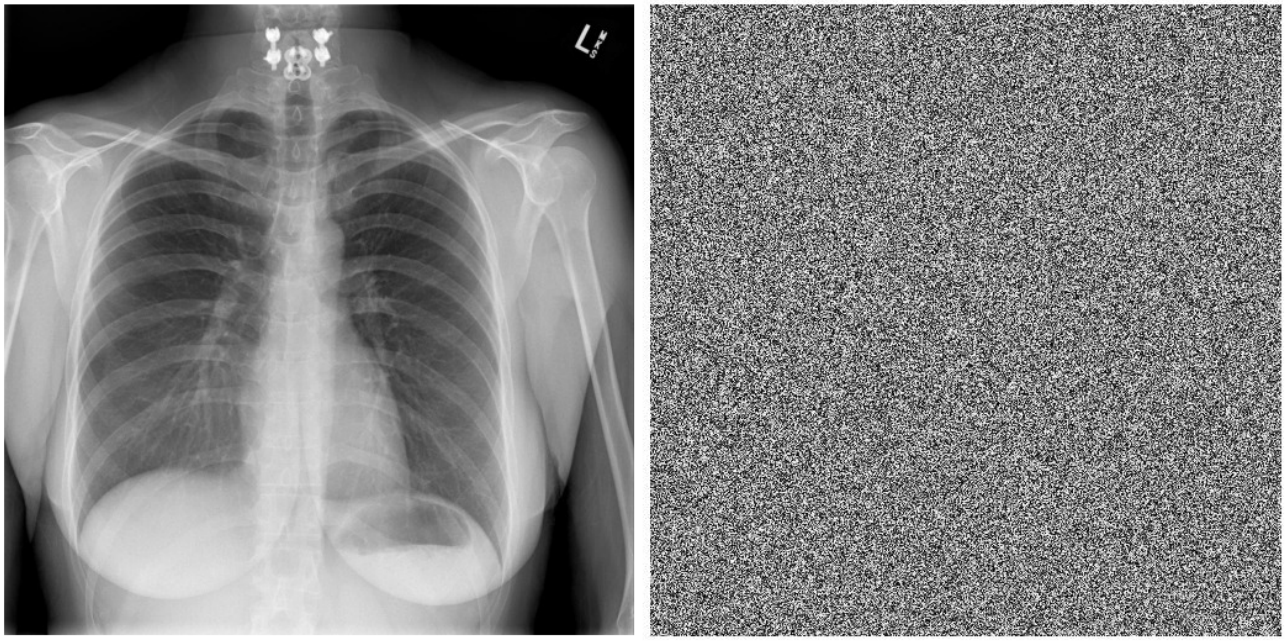


Figure 22. Original and encrypted barbra image.



a b

Figure 23. Original and encrypted X-Ray images.

Table 4. Results of different tests of image encryption

Image	S-Box	Entropy	Correlation	NPCR	UACI	MSE	PSNR
ECG	Table 1	7.9999	-0.0040	99.61	33.45	20051.2637	26.6200
	[38]	7.8	0.0121	99.6	33.63	5.3	708.3
	[39]	-	-0.0074	99.66	33.50	-	-
X-Ray	Table 1	7.9994	-0.0037	99.59	33.49	9669.0857	28.2038
	[38]	7.80	0.0194	99.8	33.29	5.7	780.12
	[39]	-	-0.0074	99.66	33.50	-	-
Barbara	Table 1	7.9994	-0.0044	99.59	33.43	16600.9376	27.0301
	[40]	7.9967	-0.0138	99.6090	33.4907	-	-
	[41]	7.9967	-0.0061	99.6002	33.8184	-	-
Aerial	Table 1	7.9998	-0.0051	99.60	33.44	8983.9332	28.3634
	[42]	7.9998	0.0016	-	-	-	-

Table 5. Comparison of time consumption for different algorithms and image types

Algorithm	**Size**	**Image Type**	**Time (s)**
Our Method	512×512	Barbara	1.04
Our Method	512×512	X-ray	1.01
Our Method	512×512	ECG	1.09
Our Method	1024×1024	Aerial	2.03
[43]	512×512	Lena	3.84
[44]	512×512	Lena	1.28

7. Conclusions

In symmetric cryptosystems, S-boxes are primarily used to create confusion and nonlinearity, which obscures the connection between the key and ciphertext and prevents hackers from obtaining the secret key. In this study, a 2D novel hyperchaotic map was designed with a large key space. The intrinsic nature of the proposed map was used to generate random affine invertible matrices over the binary field. A new approach that employed chaos and finite fields of degree 4 and 8 were introduced to design a large number of S-boxes with a nonlinearity of 112. The weaknesses were identified and removed to obtain candidate S-boxes with substantial nonlinearity in the range of $108 - 112$ with an average of 111.1025. A comparative study conducted against well-known S-boxes confirmed the effectiveness and robustness of our suggested method. Moreover, we employed a sample candidate S-boxes to encrypt digital images. In the future, we anticipate creating a diverse range of substitution boxes by employing new permutation polynomials of the Galois field along with new chaotic mappings, and optimization models. Furthermore, we are intrigued by the prospect of utilizing these substitution boxes to encrypt textual content, audio data, and video content.

Author contributions

Mohammad Mazyad Hazzazi: Methodology, Software, Data curation. Gulraiz: Conceptualization, Validation, Writing-original draft. Rashad Ali: Conceptualization, Methodology, Software, Writing, reviewing & editing. Muhammad Kamran Jamil: Data curation, Formal analysis, Investigation, Supervision. Sameer Nooh: Methodology, Visualization, Writing- review & editing. Fahad Alblehai: Conceptualization, Formal Analysis, Software. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors extend their gratitude to the deanship of scientific research of King Khalid University, for funding this work through a research project under grant R.G.P.2/34/45.

Conflict of interest

The authors declare no conflict of interest.

References

1. L. Zhang, Y. Lin, X. Yang, T. Chen, X. Cheng, W. Cheng, From sample poverty to rich feature learning: A new metric learning method for few-shot classification, *IEEE Access*, **12** (2024), 124990–125002. https://doi.org/10.1109/ACCESS.2024.3444483

2. Y. Lin, Z. Xie, T. Chen, X. Cheng, H. Wen, Image privacy protection scheme based on high-quality reconstruction DCT compression and nonlinear dynamics, *Expert Syst. Appl.*, **257** (2024), 124891. https://doi.org/10.1016/j.eswa.2024.124891
3. L. Cui, Y. Cao, A new S-box structure named affine-power-affine, *Int. J Innov. Comput. Info. Ctrl*, **3** (2007), 751–759. Available from: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=8044cda70fa8d0a18ff4708df185476bb92f3f7a
4. H. Liu, A. Kadir, P. Gong, A fast color image encryption scheme using one-time S-Boxes based on complex chaotic system and random noise, *Optics commun.*, **338** (2015), 340–347. https://doi.org/10.1016/j.optcom.2014.10.021
5. X. Wang, Q. Wang, A novel image encryption algorithm based on dynamic S-boxes constructed by chaos, *Nonlinear Dyn.*, **75** (2014), 567–576. https://doi.org/10.1007/s11071-013-1086-2
6. I. Hussain, T. Shah, H. Mahmood, A new algorithm to construct secure keys for AES, *Int. J. Contemp. Math. Sci.*, **5** (2010), 1263. Available from: https://m-hikari.com/ijcms-2010/25-28-2010/hussainIJCMS25-28-2010.pdf
7. X. Zhang, Y. Mao, Z. Zhao, An efficient chaotic image encryption based on alternate circular S-boxes, *Nonlinear Dyn.*, **78** (2014), 359–369. https://doi.org/10.1007/s11071-014-1445-7
8. I. Hussain, T. Shah, H. Mahmood, A projective general linear group based algorithm for the construction of substitution box for block ciphers, *Neural Comput. Appl.*, **22** (2013), 1085–1093. https://doi.org/10.1007/s00521-012-0870-0
9. R. Ali, M. K. Jamil, A. S. Alali, J. Ali, G. Afzal, A robust S-box design using cyclic groups and image encryption, *IEEE Access*, **11** (2023), 135880–135890. https://doi.org/10.1109/ACCESS.2023.3337443
10. R. Liu, H. Liu, M. Zhao, Reveal the correlation between randomness and Lyapunov exponent of n-dimensional non-degenerate hyper chaotic map, *Integration*, **93** (2023), 102071. https://doi.org/10.1016/j.vlsi.2023.102071
11. C. Luo, Y. Wang, Y. Fu, P. Zhou, M. Wang, Constructing dynamic S-boxes based on chaos and irreducible polynomials for image encryption, *Nonlinear Dyn.*, **112** (2024), 1–19. https://doi.org/10.1007/s11071-024-09353-w
12. B. M. Savadkouhi, A. M. Tootkaboni, S-Boxes design based on the Lu-Chen system and their application in image encryption, *Soft Comput.*, **28** (2024), 1–22. https://doi.org/10.1007/s00500-024-09912-8
13. R. Ali, J. Ali, P. Ping, M. K. Jamil, A novel S-box generator using Frobenius automorphism and its applications in image encryption, *Nonlinear Dyn.*, **1** (2024), 1–24. https://doi.org/10.1007/s11071-024-10003-4
14. D. Ustun, S. Sahinkaya, N. Atli, Developing a secure image encryption technique using a novel S-box constructed through real-coded genetic algorithm's crossover and mutation operators, *Expert Syst. Appl.*, **256** (2024), 124904. https://doi.org/10.1016/j.eswa.2024.124904
15. Q. Lai, G. Hu, A nonuniform pixel split encryption scheme integrated with compressive sensing and its application in IoMT, *IEEE Trans. Ind. Electron.*, **20** (2024), 11262–11272. https://doi.org/10.1109/TII.2024.3403266

16. S. Gao, H. H. C. Iu, U. Erkan, C. Şimşek, J. Mou, A. Toktas, Design, dynamical analysis, and hardware implementation of a novel memcapacitive hyperchaotic logistic map, *IEEE Internet Things J.*, **11** (2024), 30368–30375. Available from: https://ieeexplore.ieee.org/abstract/document/10552354
17. Z. Xie, Y. Lin, T. Liu, H. Wen, Face privacy protection scheme by security-enhanced encryption structure and nonlinear dynamics, *IScience*, **27** (2024), 110768. https://doi.org/10.1016/j.isci.2024.110768
18. Y. Wang, Z. Zhang, L. Y. Zhang, J. Feng, J. Gao, P. Lei, A genetic algorithm for constructing bijective substitution boxes with high nonlinearity, *Info. Sci.*, **523** (2020), 152–166. https://doi.org/10.1016/j.ins.2020.03.025
19. Q. Lai, L. Yang, G. Chen, Two-dimensional discrete memristive oscillatory hyperchaotic maps with diverse dynamics, *IEEE Trans. Ind. Electron.*, **72** (2024), 969–979. https://doi.org/10.1109/TIE.2024.3417974
20. M. Wang, H. Liu, M. Zhao, Construction of a non-degeneracy 3D chaotic map and application to image encryption with keyed S-box, *Multimed. Tools Appl.*, **82** (2023), 34541–34563. https://doi.org/10.1007/s11042-023-14988-9
21. R. Liu, H. Liu, M. Zhao, Cryptanalysis and construction of keyed strong S-Box based on random affine transformation matrix and 2D hyper chaotic map, *Expert Syst. Appl.*, **252** (2024), 124238. https://doi.org/10.1016/j.eswa.2024.124238
22. S. Yuanyuan, H. Liu, M. Zhao, Constructing keyed strong S-Box with higher nonlinearity based on 2D hyper chaotic map and algebraic operation, *Integration*, **88** (2023), 269–277. https://doi.org/10.1016/j.vlsi.2022.10.011
23. M. Zhao, H. Liu, Y. Niu, Batch generating keyed strong S-Boxes with high nonlinearity using 2D hyper chaotic map, *Integration*, **92** (2023), 91–98. https://doi.org/10.1016/j.vlsi.2023.05.006
24. J. Pieprzyk, G. Finkelstein, Towards effective nonlinear cryptosystem design, *IEEE Proc.-E: Comput. Digit. Tech.*, **135** (1988), 325–335.
25. J. Ali, M. K. Jamil, A. S. Alali, R. Ali, A medical image encryption scheme based on Mobius transformation and Galois field, *Heliyon*, **10** (2024), e23652. https://doi.org/10.1016/j.heliyon.2023.e23652
26. Y. Ma, Y. Tian, L. Zhang, P. Zuo, Two-dimensional hyperchaotic effect coupled mapping lattice and its application in dynamic S-box generation, *Nonlinear Dyn.*, **112** (2024), 1–32. https://doi.org/10.1007/s11071-024-09907-y
27. F. Artuger, F. Ozkaynak, A new chaotic system and its practical applications in substitution box and random number generator, *Multimed. Tools Appl.*, 2024, 1–15. https://doi.org/10.1007/s11042-024-19053-7
28. M. Vijayakumar, A. Ahilan, An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map, *Ain Shams Eng. J.*, **1** (2024), 102620. https://doi.org/10.1016/j.asej.2023.102620
29. S. Ullah, X. Liu, A. Waheed, S. Zhang, An efficient construction of S-box based on the fractional order Rabinovich Fabrikant chaotic system, *Integration*, **94** (2024), 102099. https://doi.org/10.1016/j.vlsi.2023.102099

30. A. S. Alali, R. Ali, M. K. Jamil, J. Ali, Gulraiz, Dynamic S-Box construction using mordell elliptic curves over galois field and its applications in image encryption, *Mathematics*, **12** (2024), 587. https://doi.org/10.3390/math12040587
31. A. Waheed, F. Subhan, S-box design based on logistic skewed chaotic map and modified Rabin-Karp algorithm: Applications to multimedia security, *Phys. Scr.*, **99** (2024), 055236. 10.1088/1402-4896/ad3991
32. F. Artuger, Strong S-box construction approach based on Josephus problem, *Soft Comput.*, **28** (2024), 1–13. https://doi.org/10.1007/s00500-024-09751-7
33. T. Shah, A. Elmoasry, S. I. Batool, M. Khan, Quantum harmonic oscillator and Schrödinger paradox based nonlinear confusion component, *Int. J. Theor. Phys.*, **59** (2020), 3558–3573. https://doi.org/10.1007/s10773-020-04616-9
34. F. Artuger, F. Ozkaynak, A new algorithm to generate AES-like substitution boxes based on sine cosine optimization algorithm, *Multimed. Tools Appl.*, **83** (2024), 38949–38964. https://doi.org/10.1007/s11042-023-17200-0
35. S. Ibrahim, A. M. Abbas, Efficient key-dependent dynamic S-boxes based on permuted elliptic curves, *Info. Sci*, **558** (2021), 246–264. https://doi.org/10.1016/j.ins.2021.01.014
36. T. Haider, N. A. Azam, U. Hayat, Substitution box generator with enhanced cryptographic properties and minimal computation time, *Expert Syst. Appl.*, **241** (2024), 122779. https://doi.org/10.1016/j.eswa.2023.122779
37. A. F. Weister, S. E. Tavares, On the design of S-boxes, *Adv. Crypt.-CRYPTO'85*, **1** (1986), 1–15. https://doi.org/10.1007/3-540-39799-X_41
38. P. T. Akkasaligar, S. Biradar, Selective medical image encryption using DNA cryptography, *Inf. Secur. J. Glob. Perspect.*, **29** (2020), 91–101. https://doi.org/10.1080/19393555.2020.1718248
39. W. Cao, Y. Zhou, C. L. P. Chen, L. Xia, Medical image encryption using edge maps, *Signal Process.*, **132** (2017), 96–109. https://doi.org/10.1016/j.sigpro.2016.10.003
40. A. H. Zahid, A. M. Iliyasu, M. Ahmad, M. M. U. Shaban, M. J. Arshad, H. S. Alhadawi, et al., A novel construction of dynamic S-box with high nonlinearity using heuristic evolution, *IEEE Access*, **9** (2021), 67797–67812. https://doi.org/10.1109/ACCESS.2021.3077194
41. B. Idrees, S. Zafar, T. Rashid, W. Gao, Image encryption algorithm using S-box and dynamic Hénon bit level permutation, *Multimed. Tools Appl.*, **79** (2020), 6135–6162. https://doi.org/10.1007/s11042-019-08282-w
42. P. Wang, Y. Wang, J. Xiang, X. Xiao, Fast image encryption algorithm for logistics-sine-cosine mapping, *Sensors*, **22** (2022), 9929. https://doi.org/10.3390/s22249929
43. A. Ur Rehman, X. Liaa, H. Wang, An innovative technique for image encryption using tri-partite graph and chaotic maps, *Multimed. Tools Appl.*, **80** (2021), 21979–22005. https://doi.org/10.1007/s11042-021-10692-8
44. X. Chai, X. Fu, Z. Gan, A color image cryptosystem based on dynamic DNA encryption and chaos, *Sign. Process.*, **155** (2019), 44–62. https://doi.org/10.1016/j.sigpro.2018.09.029

AIMS Press