Nonlinear Dyn (2024) 112:19463–19486
https://doi.org/10.1007/s11071-024-10003-4

RESEARCH

A novel S-box generator using Frobenius automorphism and its applications in image encryption

Rashad Ali · Javed Ali · Ping Ping · Muhammad Kamran Jamil

Received: 7 June 2024 / Accepted: 9 July 2024 / Published online: 31 July 2024

Abstract The goal of cryptography is to provide algorithms that safeguard sensitive information sent via unprotected networks. These methods encrypt the information, making it unintelligible even if adversaries manage to get it. The substitution box (S-box) structure is the most significant and nonlinear component of the Advanced Encryption Standard (AES) algorithm. In the algorithm, the S-box supplies the confusion or mixing process. A highly non-linearity-valued S-box significantly boosts defenses against a range of threats. Unfortunately, the achievable encryption throughput is constrained by the computationally costly nature of creating S-boxes. This emphasizes the necessity of creating new S-box generators with the best strength and minimum computing requirements to provide optimal security. We presented an efficient approach that uses the composition of Frobenius automorphism and Mobius transformation of $GF(2^8)$. In this way, we got two highly nonlinear permutations that can produce millions of S-boxes with very strong cryptographic strength. The dynamic behavior of the proposed generator is analyzed by clarifying the requirements for generating distinct S-boxes and ensuring that the produced S-boxes have a uniform probability distribution. Our generator can produce S-boxes with robust cryptographic features, according to a thorough security study. Our novel generation method for building S-boxes efficiently combines the benefits of both algebraic modeling and chaotic mapping, providing a solid basis for building robust S-boxes. Our approach can guarantee that the produced S-boxes have strong variety and outstanding comprehensive performance by using the ergodicity of the chaotic system. Additionally, the experimental findings presented in this study validate that the dynamic S-boxes generated by our technique not only satisfy the criteria for creating encryption methods but also provide enhanced security for picture encryption. Furthermore, our approach generates S-boxes with good efficiency. Our technique has a wide range of possible applications in cryptography, including the creation of dynamic S-boxes for encryption algorithms and high-performance S-boxes for image security. In light of current security risks and computing demands, our theoretical and computational evaluations indicate that our S-box generator is a good contender for real-world applications.

R. Ali
Government Associate College Haveli Lakha, 56020 Okara, Pakistan
e-mail: rashadwattu@gmail.com

J. Ali
Government Graduate College of Science Wahdat Road Lahore, Lahore, Pakistan
e-mail: javedaligcs@gmail.com

P. Ping
College of Computer and Information, Hohai University, Nanjing 210094, People's Republic of China
e-mail: pingpingnjust@163.com

M. K. Jamil (✉)
Department of Mathematics, Riphah International University, 54660 Lahore, Pakistan
e-mail: m.kamran.sms@gmail.com

Keywords Frobenius automorphism · Galois field · Logistic map · Nonlinearity · S-box

1 Introduction

The field of cryptology encompasses the study of codes, which is divided into two main branches: Cryptography and Cryptanalysis. Cryptography concerns itself with developing encryption algorithms, whereas Cryptanalysis focuses on breaking these algorithms. The two main sub-fields of cryptography are symmetric and asymmetric cryptography. The former explores block ciphers and stream ciphers whereas the latter, also known as public key cryptography, encrypts and decrypts communications using a pair of mathematically linked keys, one public and one private, to provide a secure method of exchanging information over an insecure network. Block ciphers operate on fixed-length groups of blocks and transform them into ciphertext. The size of a block varies according to the specific cipher being used. Block sizes commonly used are 64 bits, 128 bits, or 256 bits. A block cipher makes use of a secret key to encrypt the input. The key is utilized to generate a sequence of sub-keys that are applied to the plaintext blocks in a series of iterations or rounds. Each round involves multiple operations that transform the plaintext block into ciphertext. Nowadays, various contemporary cryptosystems are in use, which are data encryption standard (DES) [1], international data encryption algorithm (IDEA) [2], and advanced encryption standard (AES) [3]. One of the primary advantages of block ciphers is their speed and efficiency, making them ideal for use in applications that require fast encryption and decryption of large amounts of data. Yet, they are vulnerable to specific assault types, such as well-known plaintext assaults, which if the attacker has access to both the decrypted text and the encrypted text, can jeopardize the security of the cipher. Therefore the development of strong and secure block ciphers is an ongoing area of research in the field of cryptology. A Substitution-box is a non-linear constituent of a block cipher and its effectiveness determines the overall strength of the cipher. A well-designed S-box ought to have strong nonlinearity, resistance to differential and linear cryptanalysis, confusion, diffusion, bijectivity, algebraic complexity, and the absence of fixed points. As data traffic continues to grow, secure data transmission is becoming increasingly crucial, which is why the development of a robust S-box is the top priority of researchers.

1.1 Literature review

A range of methods, including the use of algebraic structures such as Galois fields, Galois rings, projective general and special linear groups, elliptic curves, coset diagrams, and Cayley graphs are being used to create effective S-boxes. The researchers used only primitive irreducible polynomials for the generation of the Galois field and then employed any bijective map for designing an S-box. The most used polynomial is $p(x) = x^8 + x^4 + x^3 + x^2 + 1$. There are 16 primitive and 14 non-primitive irreducible polynomials of degree 8 over $\mathbb{Z}_2$ which can be used to design an S-box. [4] proposed an image encryption scheme using S-boxes based on Mobius transformation. [5] designed a novel scheme of image encryption using Mobius transformation on $GF(2^8)$ and chaos. [6] used a novel irreducible polynomial to generate a robust S-box and used it to encrypt medical images. The authors used Mobius transformation to design a bijective S-box. A new S-box was proposed by [7] using I-Ching operators and the findings demonstrate that the S-box is well-suited for cryptography. A new S-box was proposed by [8] using cubic fractional transformation of the prime field to create a strong S-box. They used the composition of cubic polynomial and affine inversion map of $\mathbb{F}_{257}$. [9] examined the impact of nonlinearity on their findings by altering the basic irreducible polynomial that generates elements of the Galois field. They discovered that by selecting a specific irreducible polynomial could improve the effectiveness of S-boxes, developed based on the algebraic structure of the $GF(p^n)$. Unfortunately, it was determined that their suggested S-box was non-bijective. A new design was proposed by [10] by employing a direct product of cyclic groups and the Galois field to formulate a robust S-box. They used a highly nonlinear inversion map of the Galois field rather than a fractional transformation. [11] designed a novel S-box using a chaotic map. They also introduced a technique that can adaptively enhance the probability of differential approximation for the S-box. A new approach was employed by [12] that uses coset diagrams to show how $PSL(2, \mathbb{Z})$ acts on the projective lines of $GF(2^8)$. The Fibonacci sequence was additionally used by the authors to choose the coset diagram's vertex positions.

[13] describes a method for creating a useful S-box that combines the use of a logistic map with bacterial foraging optimization. [14] outlines a new algorithm that includes the composing of an inversion function with the action of the S_8 on the $GF(2^8)$. It was shown that the resulting S-box is highly nonlinear and bijective. A relatively new approach based on 2-D Arnold's Cat map was employed by [15] to generate dynamic S-boxes. The scheme produced efficient and nonlinear S-boxes but it does not provide any guarantee of bijectivity for every S-box. [16] developed a new chaotic system to formulate S-boxes, but the average nonlinearity of the proposed scheme was 107. A new chaotic sine map was designed by [17] to generate a highly nonlinear S-box. The author used an optimization model to enhance the nonlinearity of the S-box, but still, the average nonlinearity of the scheme was 110.25. An optimized S-box generator was designed by [18] based on elliptic curves with nonlinearity in the range 95–106. [19] introduced a new approach to designing robust S-box based on linear fractional transformation and a multi-layer perceptron architecture. They introduced a novel approach to enhance the nonlinearity of the initial S-box. A new approach based on a 2D hyperchaotic map was introduced by [20] to design S-boxes. They used affine transformations and boolean functions to design an S-box and then three possible weaknesses were removed by cryptanalyzing the dynamic approach. There are also existing schemes in literature that describe the techniques for safe storage, privacy, and integrity of data in cloud platforms ([21–27]).

The methods and techniques for building S-boxes that are described in the literature are either difficult and repetitive, or they are practical for static S-boxes. Due to their inherent flaws, static S-boxes may compromise the security of the cipher. Static S-boxes might aid an attacker in deciphering the intercepted ciphertext using cryptanalysis. Furthermore, the algorithms that create dynamic and key-dependent S-boxes are less effective and confusing. These methods also do not generate a large number of S-boxes with nonlinearity 112 and 4 differential uniformity. So, there is a continuous need for simple, efficient methods that can produce millions of S-boxes with nonlinearity 112 and differential uniformity 4.

1.2 Motivations and contributions

In this study, we have presented an efficient approach to generate a large number of S-boxes using the composition of an automorphism of a finite field of order 256 and a linear fractional transformation. The S-box created in this way has a high level of security and closely resembles the ideal values specified by the conventional S-box. The security strength of the proposed S-box is thoroughly tested and compared with other S-boxes, confirming its high level of security. We explore the complex world of finite fields, investigate the mathematics underlying Mobius transformations, and examine the characteristics that set apart the S-boxes produced by various classes of polynomials. The motivations of the proposed scheme are as follows;

1. Assessing the higher degree polynomials for generation of S-boxes.
2. Finding new nonlinear bijections of the Galois field with the lowest possible differential uniformity.
3. Proposing S-box generator scheme that can produce optimal S-boxes of high nonlinearity.
4. Analyzing the chaotic maps for generation of S-boxes.

The following are the contributions of said scheme;

1. We introduced another 4 differential uniformity permutation of $GF(2^8)$ by composing Frobenius automorphism and Mobius transformation.
2. Every S-box generated by this scheme has nonlinearity 112.
3. This scheme can produce 33553920 S-boxes with fixed irreducible polynomial and thus 30×33553920 total S-boxes.
4. A robust dynamic S-box generator is designed by modifying the control parameters in the generation formula using the chaotic logistic map. The suggested approach may effectively guarantee dynamic S-box diversity by exploiting the chaotic map's complexity and ergodicity.
5. For a fixed irreducible polynomial and fixed parameters of Mobius transformation, we can construct similar nonlinear permutations that generate optimal S-boxes of the same strength.

1.3 Structure of the article

The rest of the article is divided into seven sections. Section 2 provides an overview of the basic definition related to the Galois field and a list of irreducible polynomials. The algorithm for creating S-boxes is described in Sect. 3. The proposed S-boxes are analyzed in Sect. 4 for nonlinearity, strict avalanche criteria (SAC), bit independence criteria (BIC), probability of linear approximation (LP), probability of differential approximation (DP), fixed point analysis, and algebraic degree and compared to other S-boxes that are currently in use. Section 5 explains the algorithm of image encryption that employs the proposed S-box and provides the results of the majority logic criteria (MLC). We compared the results of our scheme in Sect. 6. Finally, Sect. 7 presents the conclusion of the study.

2 Preliminaries

In this section, we will present some basic definitions related to the Galois field and a list of all irreducible polynomials of degree 8.

2.1 Ideal

A non-empty subset I of a ring R is called an ideal of R if for every $a \in R, \forall h, k \in I, h-k, ah, ha \in I$.

2.2 Irreducible polynomial

If $(\mathbb{F}, +, .)$ is a field then a polynomial $p(x) \in \mathbb{F}[x]$ is called irreducible in $\mathbb{F}[x]$ if whenever $p(x) = q(x)r(x)$ for some $q(x), r(x) \in \mathbb{F}[x]$ then either $q(x)$ or $r(x)$ is a constant polynomial.

2.3 Maximal ideal

Let M be an ideal of R and $M \neq R$ then M is called maximal if no proper ideal of R contains M.

2.4 Galois field

For a prime number p and for an irreducible polynomial $f(x)$ of degree m in $\mathbb{Z}_p[x]$ the quotient ring $\frac{\mathbb{Z}_p[x]}{< f(x) >} = \{\sum_{k=0}^{m-1} a_k t^k | a_k \in \mathbb{Z}_p \ \forall\, 0 \leq k \leq m-1\}$ is a finite field of order p^m called Galois field and denoted by $GF(p^m)$, where t is a particular root of $f(x)$.

2.5 Primitive irreducible polynomial

A polynomial $f(x)$ of degree m over $\mathbb{Z}_p[x]$ is called primitive if x is the generator of cyclic group $(GF(p^m))^*$ otherwise $f(x)$ is called non-primitive. The following are primitive irreducible polynomials of degree 8 over $\mathbb{Z}_2[x]$;

1. $y^8 + y^4 + y^3 + y^2 + 1$ (285)
2. $y^8 + y^5 + y^3 + y + 1$ (299)
3. $y^8 + y^5 + y^3 + y^2 + 1$ (301)
4. $y^8 + y^6 + y^3 + y^2 + 1$ (333)
5. $y^8 + y^6 + y^4 + y^3 + y^2 + y + 1$ (351)
6. $y^8 + y^6 + y^5 + y + 1$ (355)
7. $y^8 + y^6 + y^5 + y^2 + 1$ (357)
8. $y^8 + y^6 + y^5 + y^3 + 1$ (361)
9. $y^8 + y^6 + y^5 + y^4 + 1$ (369)
10. $y^8 + y^7 + y^2 + y + 1$ (391)
11. $y^8 + y^7 + y^3 + y^2 + 1$ (397)
12. $y^8 + y^7 + y^5 + y^3 + 1$ (425)
13. $y^8 + y^7 + y^6 + y^5 + y^2 + y + 1$ (487)
14. $y^8 + y^7 + y^6 + y^3 + y^2 + y + 1$(463)
15. $y^8 + y^7 + y^6 + y^5 + y^4 + y^2 + 1$(501)
16. $y^8 + y^7 + y^6 + y + 1$ (451)

while the non-primitive irreducible polynomials are

1. $y^8 + y^4 + y^3 + y + 1$ (283)
2. $y^8 + y^7 + y^6 + y^5 + y^4 + y + 1$ (499)
3. $y^8 + y^5 + y^4 + y^3 + 1$ (313)
4. $y^8 + y^7 + y^5 + y^4 + y^3 + y^2 + 1$ (445)
5. $y^8 + y^6 + y^5 + y^4 + y^3 + y + 1$ (379)
6. $y^8 + y^7 + y^3 + y + 1$ (395)
7. $y^8 + y^7 + y^6 + y^5 + y^4 + y^3 + 1$ (505)
8. $y^8 + y^7 + y^6 + y^4 + y^2 + y + 1$ (471)
9. $y^8 + y^7 + y^6 + y^4 + y^3 + y^2 + 1$ (477)
10. $y^8 + y^7 + y^5 + y + 1$ (419)
11. $y^8 + y^7 + y^5 + y^4 + 1$ (433)
12. $y^8 + y^6 + y^5 + y^4 + y^2 + y + 1$ (375)
13. $y^8 + y^5 + y^4 + y^3 + y^2 + y + 1$ (319)
14. $y^8 + y^7 + y^4 + y^3 + y^2 + y + 1$ (415)

3 Proposed scheme

In this section, we will formulate the proposed mathematical model for S-box generation.

Theorem 3.1 *The map* $\psi : GF(2^8) \rightarrow GF(2^8)$ *defined by*

$$\psi(z) = \begin{cases} \dfrac{az+b}{cz+d} & : z \neq \dfrac{d}{c} \\ \dfrac{a}{c} & : z = \dfrac{d}{c} \end{cases}$$

$\forall\, a, b, c, d, z \in GF(2^8)$ *with* $ad-bc \neq 0$ *is a bijection on* $GF(2^8)$.

Proof In order to prove that ψ is one-one, we suppose that there are some $x, y \in GF(2^8)$ such that

$$\psi(x) = \psi(y). \tag{3.1}$$

Case -I If $x = y = \frac{d}{c}$ then we are done.

Case - II If $x \neq \frac{d}{c}, y \neq \frac{d}{c}$ then from 3.1, we have $\frac{ax+b}{cx+d} = \frac{ay+b}{cy+d}$ that yields to $(ad-bc)(x-y) = 0$. Since $GF(2^8)$ is an integral domain and $ad - bc \neq 0$, therefore we must have $x = y$.

Case III If $x \neq \frac{d}{c}, y = \frac{d}{c}$ then from 3.1, we have $\frac{ax+b}{cx+d} = \frac{a}{c}$ which leads to the contradiction that $ad - bc = 0$. Similarly, we can conclude that it is not possible that $x = \frac{d}{c}, y \neq \frac{d}{c}$.

Since $GF(2^8)$ is finite, therefore, being the $1-1$ function, $\psi : GF(2^8) \rightarrow GF(2^8)$ is a bijection.

Theorem 3.2 *The Frobenius map* $F : GF(2^8) \rightarrow GF(2^8)$ *defined by* $F(x) = x^2; \quad \forall x \in GF(2^8)$ *is an automorphism.*

Proof To show F is an automorphism, we need to show that F is a bijection and preserves the operations of $GF(2^8)$. Firstly, we will show that F is a bijection. Let $x_1, x_2 \in GF(2^8)$ such that

$$F(x_1) = F(x_2). \tag{3.2}$$

Case-I If one of x and y is zero. Without loss of generality, we assume that $x = 0$ then 3.3 implies that $y = 0$ and we are done.

Case-II If $x \neq 0$ &$y \neq 0$ then from 3.3 we have $x^2 = y^2$ which implies that $x^2 - y^2 = 0$ and $(x-y)^2 = 0$ which shows that $x = y$. As F is one-to-one it is a bijection being a one-to-one function between two same finite sets.

Now $F(x+y) = (x+y)^2 = x^2 + y^2 + 2xy = x^2 + y^2 = F(x) + F(y)$ and $F(xy) = (xy)^2 = x^2y^2 = F(x)F(y)$

Theorem 3.3 *The functions* $\psi, \zeta : GF(2^8) \rightarrow GF(2^8)$ *defined by* $\psi(t) = \begin{cases} \dfrac{ax^2+b}{cx^2+d} & : x \neq (\dfrac{d}{c})^{2^{-1}} \\ \dfrac{a}{c} & : x = (\dfrac{d}{c})^{2^{-1}} \end{cases}$ *and* $\zeta(t) = \begin{cases} (\dfrac{ax+b}{cx+d})^2 & : x \neq (\dfrac{d}{c})^{2^{-1}} \\ (\dfrac{a}{c})^2 & : x = (\dfrac{d}{c})^{2^{-1}} \end{cases}$ *are the bijections on* $GF(2^8)$.

Proof We know that the Mobius transformation $f : GF(2^8) \rightarrow GF(2^8)$ defined by $f(t) = \begin{cases} \dfrac{at+b}{ct+d} & : t \neq \dfrac{d}{c} \\ \dfrac{a}{c} & : t = \dfrac{d}{c} \end{cases}$ is a bijection, where $a, b, c, d \in GF(2^8)$ and $ad - bc \neq 0$. As the map $F(t) = t^2$ is an automorphism of $GF(2^8)$ so the functions $\psi(t) = (f \circ F)(t)$ and $\zeta(t) = (F \circ f)(t)$ are the bijections being the composition of bijective maps.

Note We can again compose the functions ψ, ζ with Frobenius automorphism to design new bijections.

3.1 Algorithm for construction of S-box

We used the chaotic logistic map as the starter of our proposed scheme. To choose irreducible polynomials and parameters of maps ψ and ζ, we iterate the logistic map. The procedure is described in the following steps;
Step 1: Set initial value $x_0 \in (0, 1)$ and parameter $r = 3.9999$ in

$$x(i+1) = rx(i)(1 - x(i)). \tag{3.3}$$

Iterate Eq. 3.3 for $K + 5$ times and discard the first K values, where K is a positive integer in the range 1000–2000.
Step 2: The index of irreducible polynomial is calculated using the formula:

$$\text{Index} = \quad \bmod\ (\lfloor x(K+1) \cdot 2^{10} \rfloor, 30) + 1$$

In this way, we will get the value of the index in the range 1–30. while the values of parameters a, b, c, d are selected in the following way,

Table 1 S-box ψ

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

Table 2 S-box ζ

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

$$\begin{aligned}
a &= \mod(\lfloor x(K+2)\cdot 10^{13}\rfloor, 255)+1,\\
b &= \mod(\lfloor x(K+3)\cdot 10^{14}\rfloor, 255)+1,\\
c &= \mod(\lfloor x(K+4)\cdot 10^{15}\rfloor, 255)+1,\\
d &= \mod(\lfloor x(K+5)\cdot 10^{16}\rfloor, 255)+1.
\end{aligned}$$

and we get the values a, b, c, d in range 1–255.

Step 3: Choose the degree of the irreducible polynomial and based on the index of the irreducible polynomial, calculate $ad - bc$ in the Galois field generated by the polynomial. If $ad - bc = 0$ then go to step 1 otherwise calculate the outputs of ψ and ζ.

Step 4; To generate dynamic S-boxes, include steps 1–3 in a for loop.

Two sample S-boxes are presented in Tables 1 and 2.

4 Security analysis of S-box

In this segment, we present the analysis of dynamic S-box generators against the cryptographic attacks. To ensure strong cryptographic resilience, the S-box needs to fulfill some prerequisites. The commonly employed criteria for evaluating the S-box typically include nonlinearity, strict avalanche criteria, bit independence criteria, linear approximation probability, differential approximation probability, fixed point analysis, and algebraic degree. The efficiency of the evaluations was then assessed by comparing the results to the standard S-boxes.

4.1 Bijectiveness and balanacedness

An S-box must ensure that each input value has a unique and exclusive output value, with each output value deriving from a separate input value, to satisfy the conditions of bijectivity. The decryption process in cryptographic algorithms requires the use of the inverse of the S-box, highlighting the significance of a bijective S-box in such algorithms.

If the same number of zeros and ones appear in the truth table of a boolean function then the S-box is considered to be balanced. An S-box is said to be balanced if and only if each of its component boolean functions exhibits equilibrium. If an S-box is unbalanced, favoring particular bit values for some or all of the input values, the security of cryptographic techniques may be compromised.

The S-boxes presented in Tables 1 and 2 are bijective, and satisfy the balance property.

4.2 Nonlinearity (NL)

An important factor in assessing the effectiveness of the S-box is the measurement of its unpredictability and nonlinearity (NL) is seen to be a key factor in this evaluation. The degree to which an S-box deviates from connecting its input and output bits in terms of their magnitudes linearly is referred to as its nonlinearity. Strong nonlinearity is necessary for an S-box used in cryptography because it increases system security by prohibiting attackers from inferring input bits from output bits.

4.3 Strict avalanche criteria (SAC)

The SAC (Strict Avalanche Criterion) predicts how an S-box will behave when its input is subjected to slight alterations, [34]. To pass the security criteria, an S-box must adhere to the strict avalanche criterion, which mandates that each output bit has an average probability of 0.5 of changing when a single bit is flipped in the input. With the use of this feature, attackers will have a difficult time extracting the original input data from the generated output.

4.4 Bit independence criteria (BIC)

The set of properties that make up the criterion for bit independence determines how statistically uncorrelated the input and output bits of an S-box are. The criteria specify the requirements that the S-box must fulfill for the output bits to show statistical independence from the input bits. We compute the BIC-Nonlinearity and BIC-SAC to assess the BIC performance of the S-box.

4.5 Linear approximation probability (LAP)

The likelihood that a linear function may resemble an S-box is measured by the Linear Approximation Probability (LAP). A measure of the S-box's fortitude or resistance to linear assaults is the linear approximation probability (LAP). The S-box's security strength increases as the LAP value decreases.

4.6 Differential approximation probability (DAP)

When all possible input differences are taken into account, the differential uniformity (DU) of an S-box is the maximum variation in frequency found between two distinct input differences that produce a specific output difference. This metric measures the largest probability difference between two input variations leading to a particular output variation. The differential approximation probability of an S-box is determined by dividing its differential uniformity by 256.

4.7 Fixed point analysis (FPA)

An S-box's design objective is to avoid having fixed points, which implies that no input value will map to itself as a result of the S-box transformation. Cryptographers rely on this study to evaluate the strength and resilience of cryptographic algorithms that use S-boxes against different types of cryptographic assaults, which is essential for understanding the security characteristics, weaknesses, and overall efficacy of these algorithms.

4.8 Algebraic degree (AD)

It is defined as the longest term in the algebraic normal form of an S-box. A stronger S-box can fend off higher-order differential attacks, hence higher algebraic degree is preferable. Based on the coordinate function g_i, the algebraic degree of an S-box S is determined.

$$AD(S) = max\{deg(g_i)|i = 1, 2, 3, , , 8\}$$

5 Applications in image encryption

The majority logic criteria (MLC) can be used to evaluate the encryption capabilities of S-boxes. MLC consists of several studies, including mean absolute deviation (MAD), contrast, energy, homogeneity, entropy, and correlation, which are used to determine the randomness in an encrypted image.

The properties of an encrypted image can be ascertained by an examination of homogeneity and energy. The correlation test looks for similarities or resemblances between encrypted images and plain images. The lower correlation value indicates a higher distortion brought on by encryption. The brightness loss of the original image is approximated by contrast. A more effective encryption method is one with a greater contrast score. The difference between the encrypted image and the original is measured using the MAD analysis. The quality of the S-box is determined by statistical characteristics, which are based on the distortions caused by the encryption process. We demonstrate the use of our dynamic S-boxes by using it in the proposed image encryption scheme presented by authors in [10]. The proposed scheme uses the CBC mode of AES for encryption of digital images. We used four-color images of Baboon, Cornfield, X-ray, and Pepper. The plain images with separate components are displayed in Figs. 1, 2, 3, 4, while the encrypted image and color components are presented in Figs. 5, 6, 7, 8. The decryption is just the reverse of these steps of AES CBC mode operation.

Algorithm 1: Encryption Algorithm for RGB Image

```
Input  : Original Image
Output: Encrypted Image
Initialization and Setup ;
Load the original image ;
Separate the image into its red, green, and blue channels ;
Generate a 256-bit random key ;
Define a custom S-box and MixColumns matrix ;
Preparation ;
Convert each channel into a 1D array of bytes ;
Pad each channel to make its length a multiple of 16 ;
Split the padded channel data into 128-bit blocks ;
Encryption ;
Initialize the previous block with random data ;
for each block in the channel do
    XOR the current block with the previous block (CBC mode) ;
    Add the round key to the block ;
    Substitute bytes using the S-box ;
    Perform row shifting ;
    Mix the columns ;
    Update the previous block with the current encrypted block ;
Post-processing ;
Concatenate the encrypted blocks ;
Reshape the encrypted data into image format for each channel ;
Combine the encrypted channels to form the final encrypted image ;
Output ;
Save the encrypted image ;
```

5.1 Key space analysis

Keyspace analysis establishes the number of distinct keys that may be developed and employed. A larger key space is preferred since it increases the number of keys that an attacker must attempt in a brute-force attack to successfully decrypt data. Brute force attacks consist of repeatedly trying every key until the right one is discovered. This increases the safety of the encryption technique since a wider key space makes brute force attacks more computationally expensive and time-consuming. An image encryption scheme can withstand brute force attacks if its key space is at least 2^{100}. The key space of our used scheme is 2^{256} with an extra layer of security by a 128 bit random vector.

Table 3 Comparative analysis of sample S-boxes ψ and ζ

S-boxes	Mathematical structure	Nonlinearity	SAC	BIC nonlinearity	BIC SAC	LAP	DAP
ψ	$GF(2^8)$	112	0.5022	112	0.5008	0.0625	0.0156
ζ	$GF(2^8)$	112	0.5002	112	0.5054	0.0625	0.0156
[10]	$GF(2^8)$	112	0.5066	112	0.5034	0.0625	0.0156
[6]	$GF(2^8)$	112	0.4988	112	0.5008	0.0625	0.0156
[15]	$GF(2^8)$	112	0.5066	111.28	0.5016	0.0703	0.0625
[17]	Chaos	110.25	0.5027	102.71	0.4936	0.1250	0.04687
[16]	Chaos	107	0.5012	103.07	0.4970	0.1250	0.04687
[20]	Chaos	110.60	0.4966	109.67	0.5026	0.0790	0.0214
[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]	Quantum oscillator	110	0.5000	108.5	0.5001	0.1250	0.04687
[19]	Neural network	114.5	0.4975	107	0.5080	0.135	0.0391
[18]	ECC	108	0.5068	103.3571	0.5018	0.070	0.015
[31]	ECC	112	0.5032	112	0.5059	0.0625	0.0156
[32]	ECC	107.75	0.5010	103.9286	0.5038	0.1250	0.0391
[33]	Sine cosine optimization	112	0.5056	104	0.4991	0.1250	0.0391

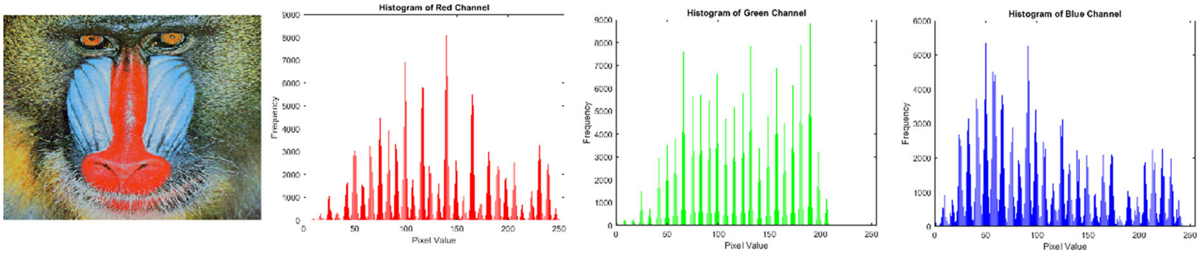


Fig. 1 Plain image of Baboon and histogram of its channels

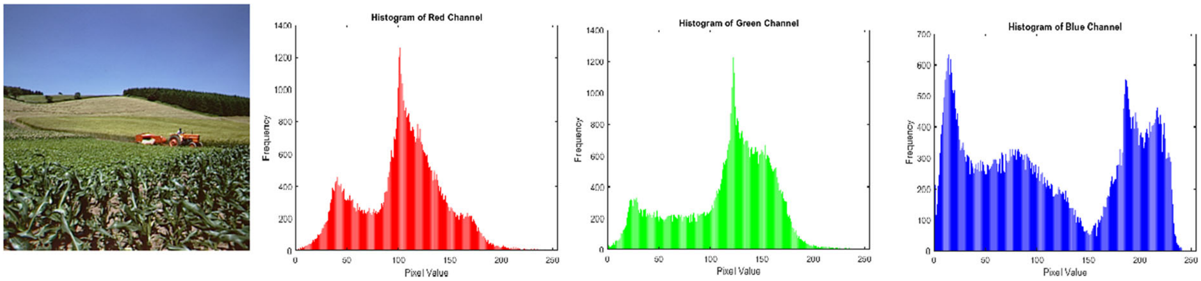


Fig. 2 Plain image of Cornfield and histogram of its channels

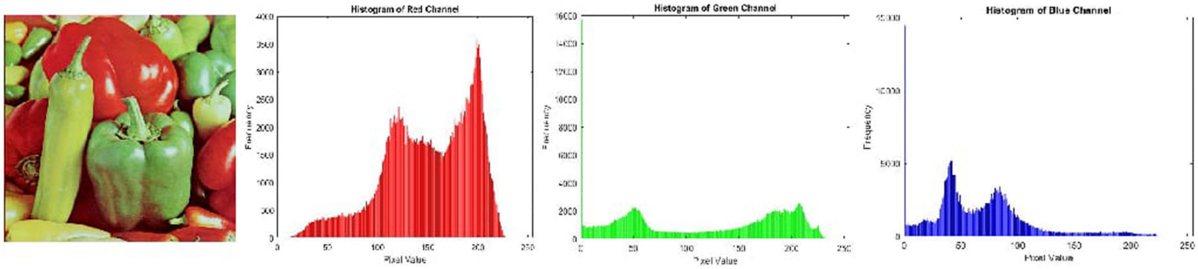


Fig. 3 Plain image of Pepper and histogram of its channels

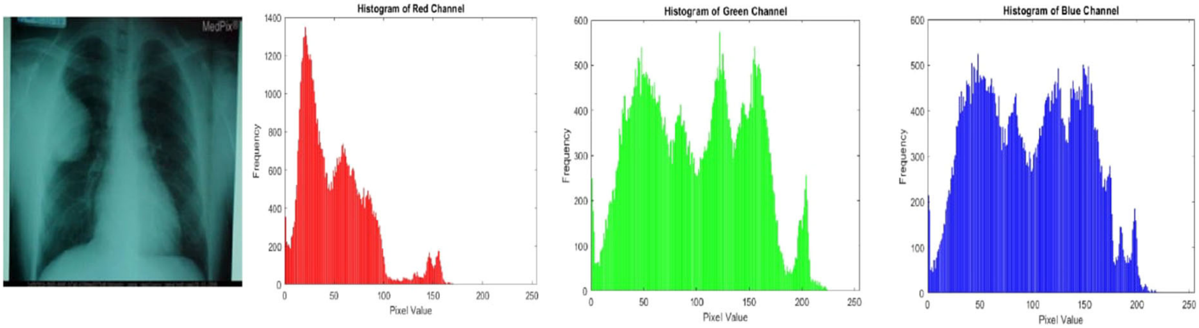


Fig. 4 Plain image of X-Ray and histogram of its channels

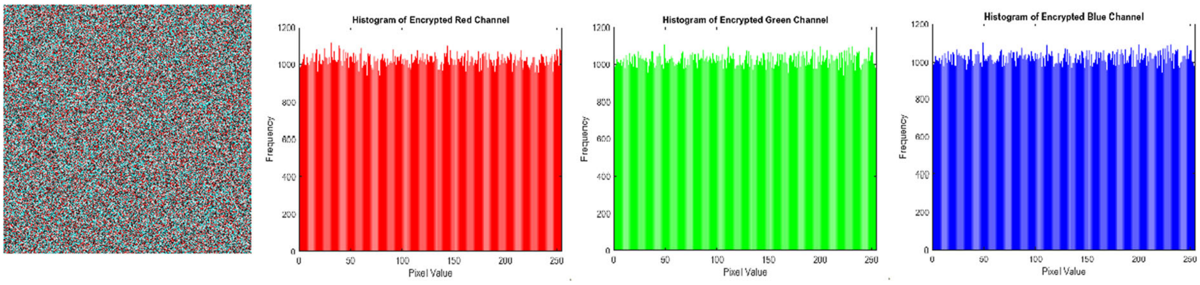


Fig. 5 Cipher image of Baboon and histogram of its channels

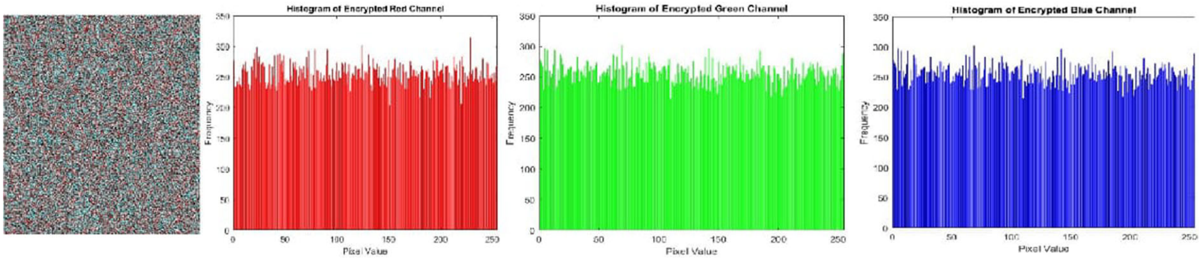


Fig. 6 Cipher image of Cornfield and histogram of its channels

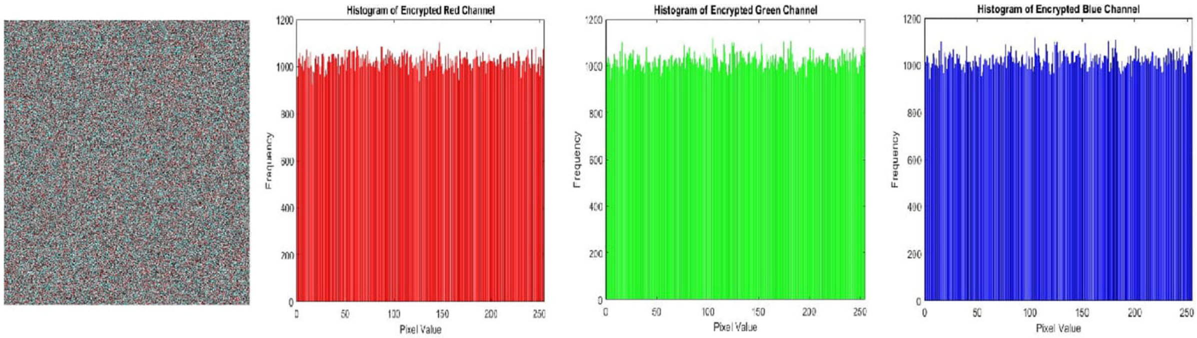


Fig. 7 Cipher image of Pepper and histogram of its channels

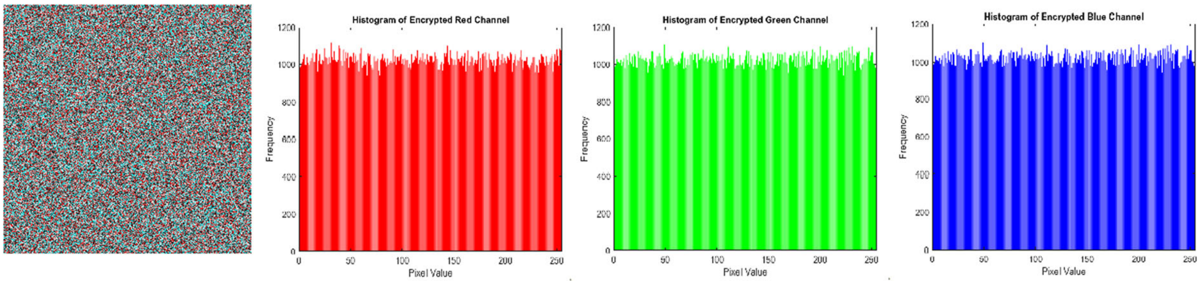


Fig. 8 Cipher image of X-Ray and histogram of its channels

5.2 Key sensitivity analysis

Key sensitivity analysis is a procedure used to assess how slight changes in the encryption key may affect the safety and effectiveness of the algorithm. The encryption key is subjected to minor modifications or disturbances. Individual bits may be changed, a minor value may be added or subtracted, or certain key generation settings may be altered. The same input image is then subjected to the image encryption process with the changed encryption keys being used in place of the original ones. As a result, various encrypted versions of the same image are produced. Images that were encrypted using the modified keys and the images that were encrypted using the original, unmodified key are contrasted. Considerations like image quality, security, resilience to attacks, and processing efficiency are evaluated during the comparison. Key sensitivity analysis is used to determine how resilient an image encryption technique is to changes in the encryption key. We used a gray image for the encryption process with the original key and modified key. The results can be seen in Figs. 9, 10, 11, and Table 10.

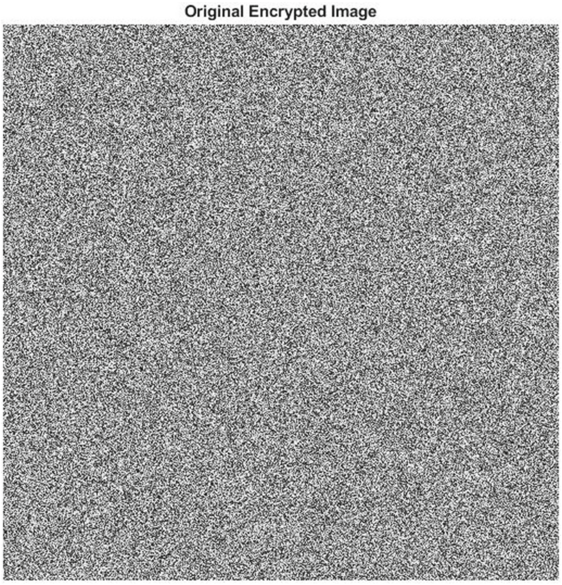


Fig. 9 Encrypted original image

6 Discussion

The following are the main findings of the scheme

Table 4 Comparison of AD and FP of ψ, and ζ

S-box	ψ	ζ	AES	[31]	[10]	[6]	[15]	[32]
FP	0	0	0	1	2	1	2	3
AD	7	7	7	7	7	7	7	6

Table 5 Experimental results of entropy

Images	Red	Green	Blue
Baboon	7.9995	7.9995	7.9995
Pepper	7.9995	7.9994	7.9995
Cornfield	7.9976	7.9978	7.9979
Chest X-Ray	7.9977	7.9978	7.9979

Table 6 Experimental results of correlation

Horizontal correlation	Red	Green	Blue
Baboon	−0.0011	−0.0004	−0.0032
Pepper	−0.0009	−0.0008	−0.0006
Cornfield	0.0023	0.0012	0.0019
Chest X-Ray	0.0010	−0.0002	−0.0053
Vertical correlation	Red	Green	Blue
Baboon	−0.0026	−0.0023	−0.0017
Pepper	−0.0006	−0.0016	0.0019
Cornfield	−0.0013	0.0071	−0.0027
Chest X−Ray	0.0031	0.0060	0.0089
Diagonal correlation	Red	Green	Blue
Baboon	−0.0025	−0.0022	−0.0006
Pepper	−0.00001	−0.0021	−0.0032
Cornfield	0.0034	0.0063	0.0042
Chest X−Ray	−0.0022	0.0042	−0.0003

1. S-box needs a high value of nonlinearity to fend against linear cryptanalysis. With a nonlinearity value of 112, our suggested sample S-boxes attain the optimal value (Table 3). Each S-box in our proposed scheme has nonlinearity 112, which too good as compared to other existing schemes [5,6,9,10,12,15,18,31,32,35–40]. The scheme proposed in [15] has a nonlinearity range in 110–112 with 2584 S-boxes of nonlinearity 110 and 5416 S-boxes with nonlinearity 112. The scheme in [18] has produced S-boxes with a nonlinearity range in 95–106. Our scheme produces better results with average nonlinearity 112 as confirmed by 1000 S-boxes in Fig. 12.
2. Regarding the satisfaction avalanche criteria, a SAC score close to the ideal value (0.50) is deemed acceptable. The SAC of our sample S-boxes is 0.5022 and 0.5002 which are very close to the ideal value of 0.5 and better than most of S-boxes as depicted in Table 3. We computed the average value of dependency matrices for each of generated S-box and displayed it in Fig. 13. The dependence matrices' mean values have upper and lower

Table 7 Experimental results of energy, contrast, homogeneity, MAD

Contrast	Red	Green	Blue
Baboon	110.5211	10.5148	10.4556
Pepper	10.5246	10.4809	10.4977
Cornfield	10.5014	10.4377	10.5251
Chest X-Ray	10.4947	10.58	10.5326
Energy	Red	Green	Blue
Baboon	0.0156	0.0156	0.0156
Pepper	0.0157	0.0156	0.0156
Cornfield	0.0156	0.157	0.0156
Chest X-Ray	0.0157	0.0156	0.0156
Homogeneity	Red	Green	Blue
Baboon	0.3887	0.3896	0.3894
Pepper	0.3891	0.3894	0.3889
Cornfield	0.3885	0.3883	0.3902
Chest X-Ray	0.3888	0.3881	0.3887
MAD	Red	Green	Blue
Baboon	76.1772	73.2125	80.965
Pepper	73.9228	86.4868	86.1352
Cornfield	72.6606	72.6679	86.9126
Chest X-Ray	92.44	77.8424	77.0528

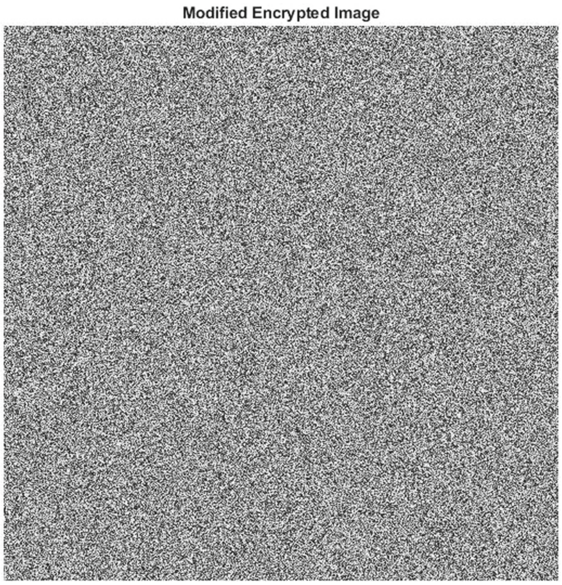


Fig. 10 Encrypted image with modified key

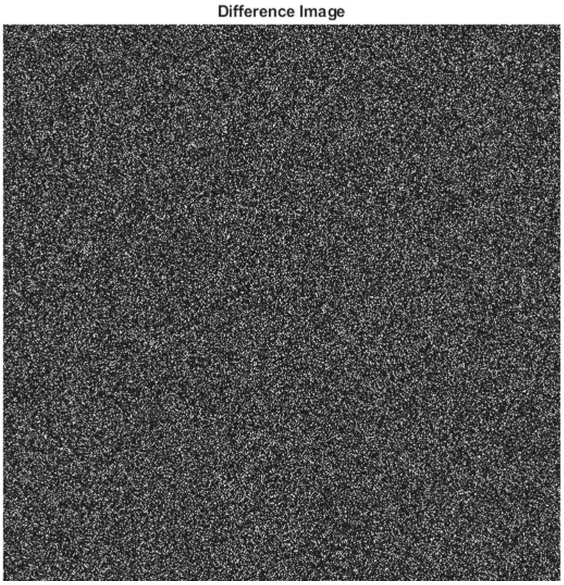


Fig. 11 Difference of images

Table 8 Experimental results of differential analysis

NPCR	Red	Green	Blue
Baboon	99.61	99.60	99.61
Pepper	99.64	99.59	99.59
Cornfield	99.59	99.57	99.59
Chest X-Ray	99.57	99.61	99.61
UACI	Red	Green	Blue
Baboon	33.47	33.49	33.39
Pepper	33.47	33.39	33.46
Cornfield	33.43	33.43	33.53
Chest X-Ray	33.62	33.63	33.51

Table 9 Comparative analysis of proposed image encryption scheme

Image	Algorithm	Entropy	Correlation	Contrast	NPCR	UACI	MAD
Baboon	Proposed	7.9995	−0.0011	10.5211	99.6050	33.45	76.7849
	[31]	7.9994	−0.0079	10.6137	99.5980	33.354	–
	[10]	7.9994	−0.0042	10.5556	99.59	33.48	–
	[29]	7.7536	−0.0025	75.2002	–	–	65.1942
Pepper	Proposed	7.9995	−0.0009	10.5246	99.62	33.43	73.9228
	[31]	7.9994	−0.0055	10.6004	99.60	33.45	–
	[29]	7.7517	−0.0016	75.2042	–	–	–

Table 10 NPCR and UACI results for key sensitivity analysis

S-box	NPCR	UACI
Gray image of Seashore		
Proposed	99.60	33.46

limits of 0.52 and 0.48, respectively, as can be seen. Since the majority of the dependence matrices' mean values are concentrated around 0.50, our technique produces S-boxes with excellent stringent avalanche criteria. We can confirm the average deviation of the SAC score of our S-boxes by Fig. 14, as most of the values are very close to 0.

3. Under the bits independence requirement, the pairwise disjoint Boolean functions have shown strong performance for both SAC and nonlinearity scores. The results for BIC Nonlinearity are depicted in Fig. 15 and confirm the efficacy of the proposed scheme as each S-box has BIC Nonlinearity 112, which is not found for each in schemes developed in [6,10,15,18,31,32]. The scores of BIC Nonlinearity and BIC SAC for sample S-boxes are presented in Table 3. In Fig. 16, BIC-SAC values of 1000 S-boxes are clustered in the range 0.48–0.52, which is quite near to the optimal value of 0.5 and most values are very close to 0.5. We calculated the deviation of BICSAC from 0.5, which is shown in Fig. 17. As a result, our technique produces S-boxes with excellent BIC-SAC performance. By combining these two assessment metrics, it is possible to determine that the S-box produced by our approach performs well in terms of BIC.
4. A lower DU score is indicative of a secure S-box. We can see the results of the DAP of our sample

Algorithm 2: Decryption Algorithm for RGB Image

```
Input  : Encrypted Image
Output: Decrypted Image
Initialization and Setup ;
Load the encrypted image ;
Separate the image into its red, green, and blue channels ;
Generate the 256-bit key used for encryption ;
Define the custom S-box and MixColumns matrix used for
encryption ;
Preparation ;
Convert each channel into a 1D array of bytes ;
Ensure the length of each channel is a multiple of 16 ;
Split the channel data into 128-bit blocks ;
Decryption ;
Initialize the previous block with the same random data
used during encryption ;
for each block in the channel do
    Store the current encrypted block ;
    Perform the inverse of MixColumns ;
    Perform the inverse of row shifting ;
    Substitute bytes using the inverse S-box ;
    Subtract the round key from the block ;
    XOR the block with the previous block (CBC mode) ;
    Update the previous block with the stored encrypted
    block ;
Post-processing ;
Concatenate the decrypted blocks ;
Reshape the decrypted data into image format for each
channel ;
Combine the decrypted channels to form the final
decrypted image ;
Output ;
Save the decrypted image ;
```

S-boxes in Table 3. We compute the DAP values of resultant S-boxes and display them in Fig. 18 to confirm their resistance to differential assault. The value of DAP is 0.0156 showing equality to AES S-box. The experimental findings demonstrate the remarkable performance of the S-boxes that our technique dynamically generates in withstanding differential assaults.

5. The resistance of S-box against linear cryptanalysis is likewise correlated with the likelihood of linear approximation. An S-box is considered more resilient against linear cryptanalysis if its LAP score is lower. Our sample S-boxes have the LAP value of 0.0625, which is quite low as compared to a single S-box presented in [31,40]. Figure 19 represents the LAP of 1000 S-boxes and this value is the same as of AES S-box and better than [6,10,15,18,31,32]. This suggests that our strategy produces S-boxes with strong resistance to linear assaults.
6. Our goal is to design S-boxes without any fixed points and our proposed S-boxes presented in Tables 1 and 2 satisfy this criteria as seen in Table 4. Our proposed scheme has the potential to design S-boxes with no fixed points. The sample S-boxes do not have fixed points while the 10000 randomly generated S-boxes have fixed points 0, 1, 2, 3, 4 as displayed in Figs. 20 and 21. The distribution of fixed points is displayed in Figs. 22 and 23. Among 1000 S-boxes, 33.1 % with no fixed points, 48.9 % with 1 fixed points, 17.9 % with 3 fixed points, and 0.1 % with 4 fixed points.
7. A higher value of the algebraic degree is needed for a strong S-box. For AES S-box, its value is 7. Our proposed S-boxes have the same value, which shows the efficiency of the proposed scheme. The algebraic degree of randomly generated 1000 S-boxes is calculated and displayed in Fig. 24. The algebraic degree of each S-box is 7, which is the same as of AES S-box.
8. Entropy analysis is used to determine the randomness in an encrypted image. We can observe that the entropy of the proposed cipher image is better than [6,10,31,41,42]. The contrast in an image refers to the variation in brightness. The viewer may discern the underlying information via contrast analysis by seeing items. The contrast of our scheme is better than [5,31,35,40,42, 43]. Correlation is used to determine how similar pixels are to each other so an encrypted image must have a low value of correlation. The average correlation values for the proposed scheme are -0.0003, -0.0010, -0.0003 and better than [5,31,35,40,42,43]. We can observe the efficiency of the encryption scheme by uniform histograms of each channel and from the results of MLC as depicted in Tables 5, 6, 8, 7, 9.
9. Single-bit variations in plain text should cause a strong cryptosystem to become very sensitive. NPCR and UACI assessments are used to gauge how sensitive the framework is. When a picture is encrypted using the recommended method, the NPCR (Number of Pixel Change Rate) statistic assesses the impact of a single-pixel change on the whole image. It calculates how often a pixel in the encrypted picture changes for every pixel that changes in the original image. The ideal value

Fig. 12 Results of nonlinearity of randomly generated 1000 S-boxes

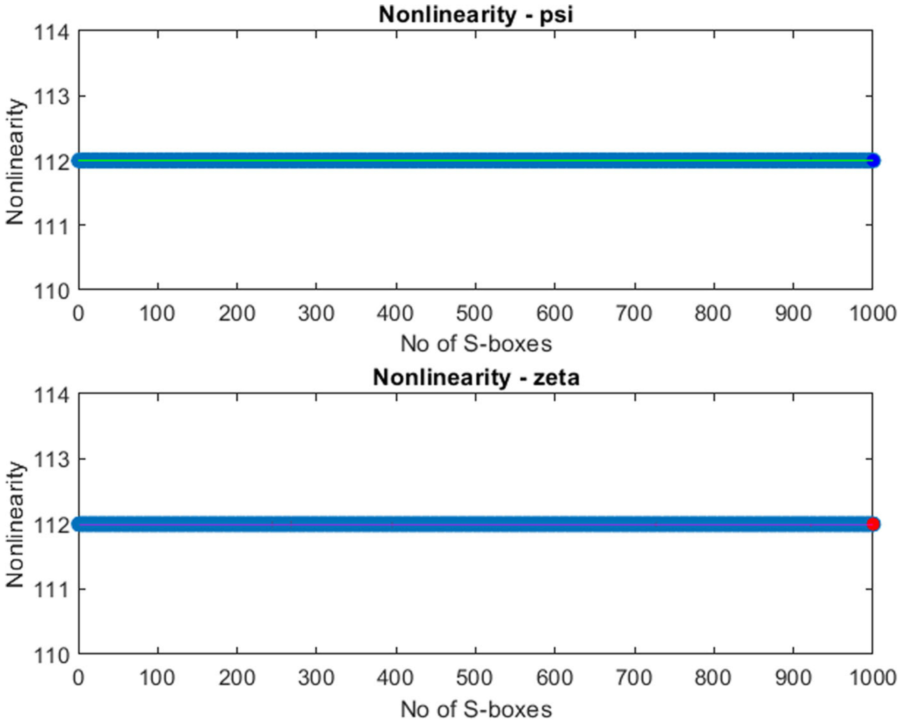
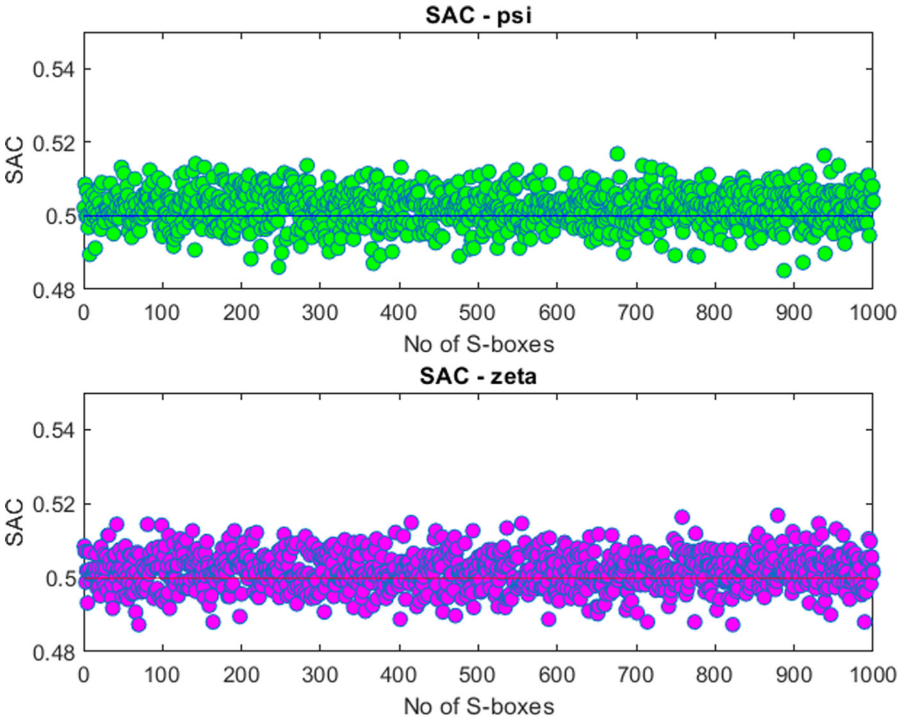


Fig. 13 Results of SAC of 1000 S-boxes generated randomly by proposed scheme



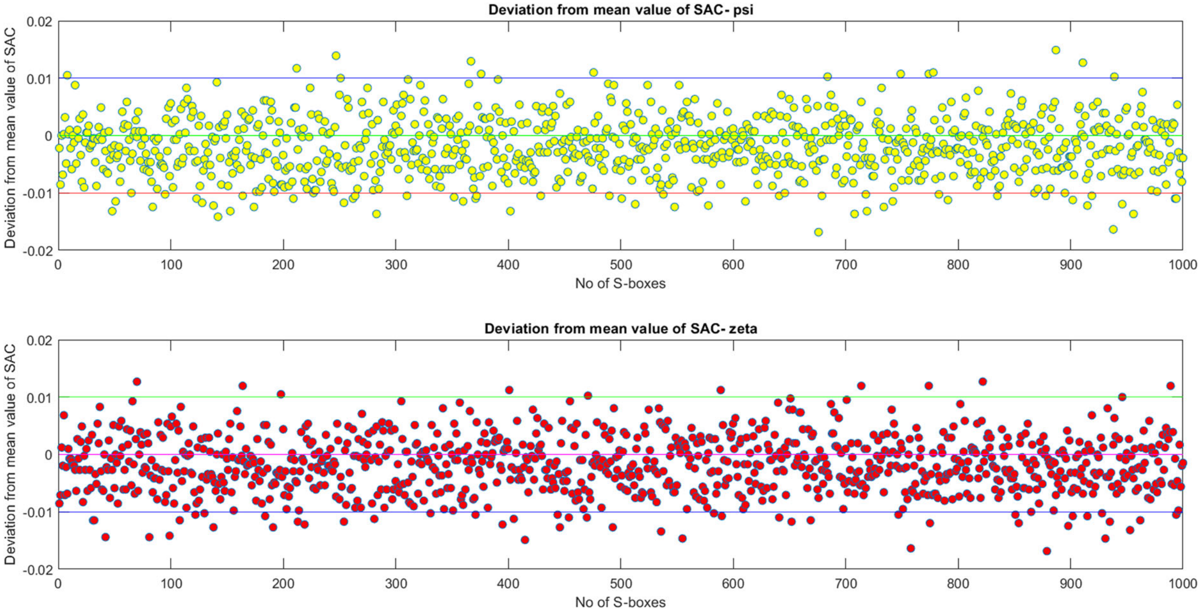
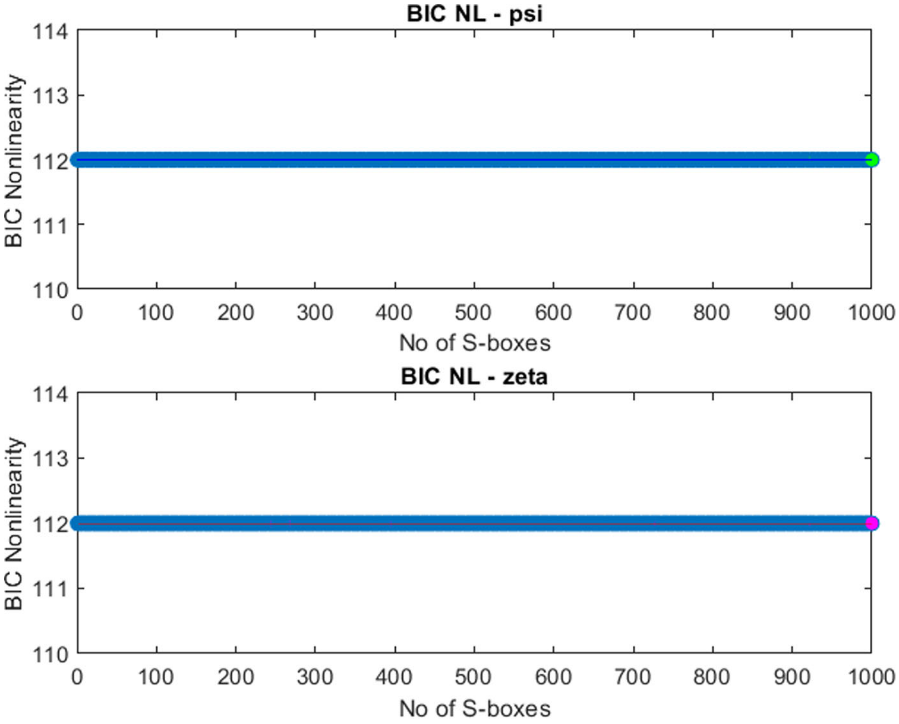


Fig. 14 Deviation of SAC from 0.5

Fig. 15 Results of BIC nonlinearity of 1000 S-boxes generated randomly by the proposed scheme



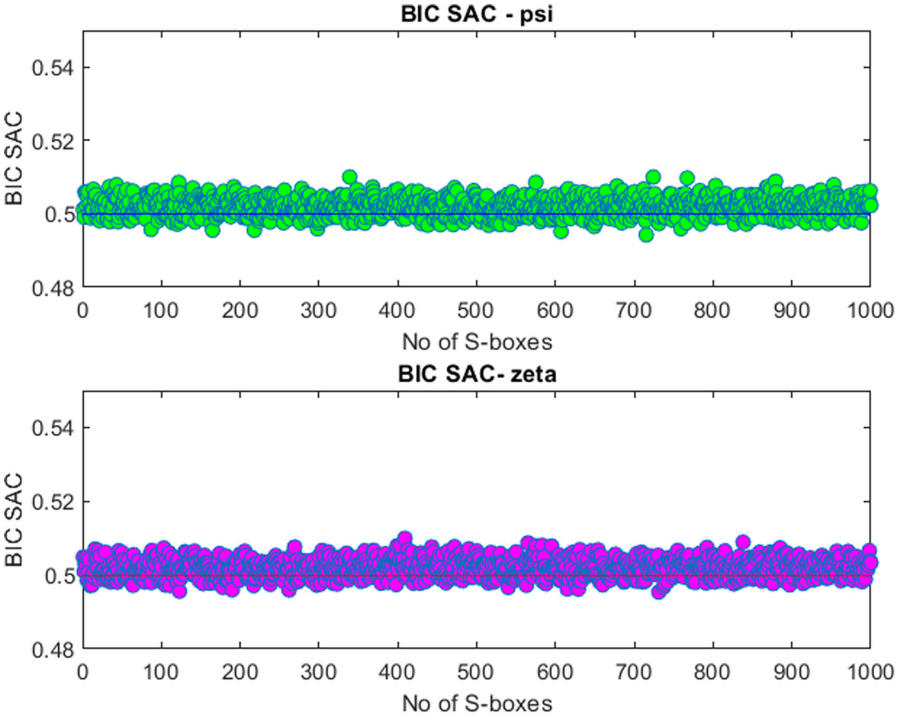


Fig. 16 Results of BIC SAC of 1000 S-boxes generated randomly by the proposed scheme

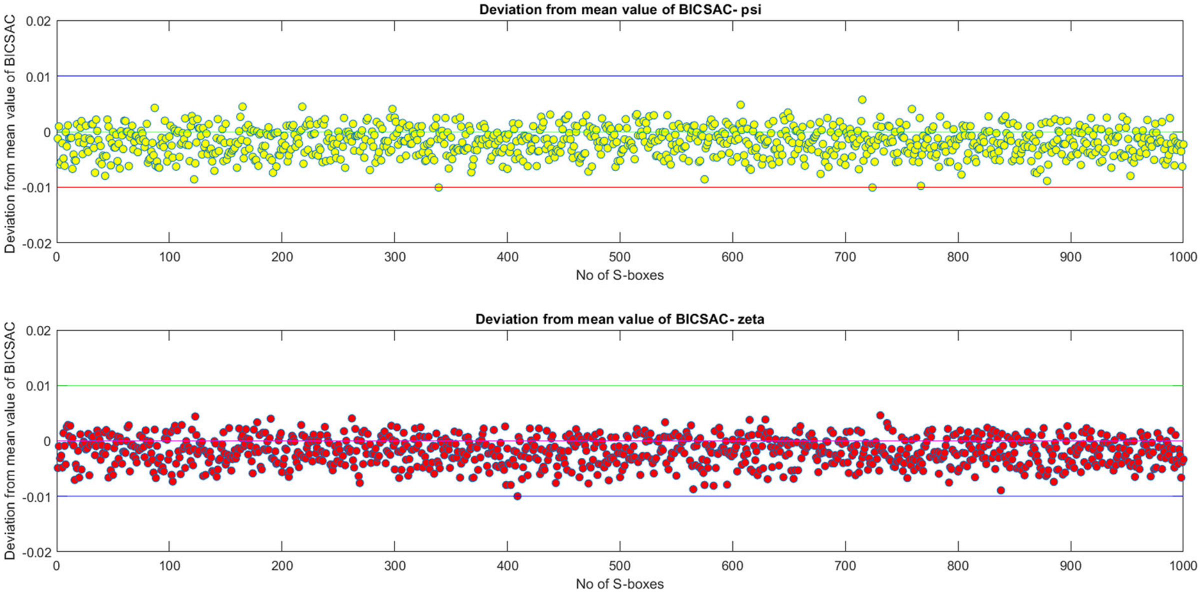


Fig. 17 Deviation of BIC SAC from 0.5

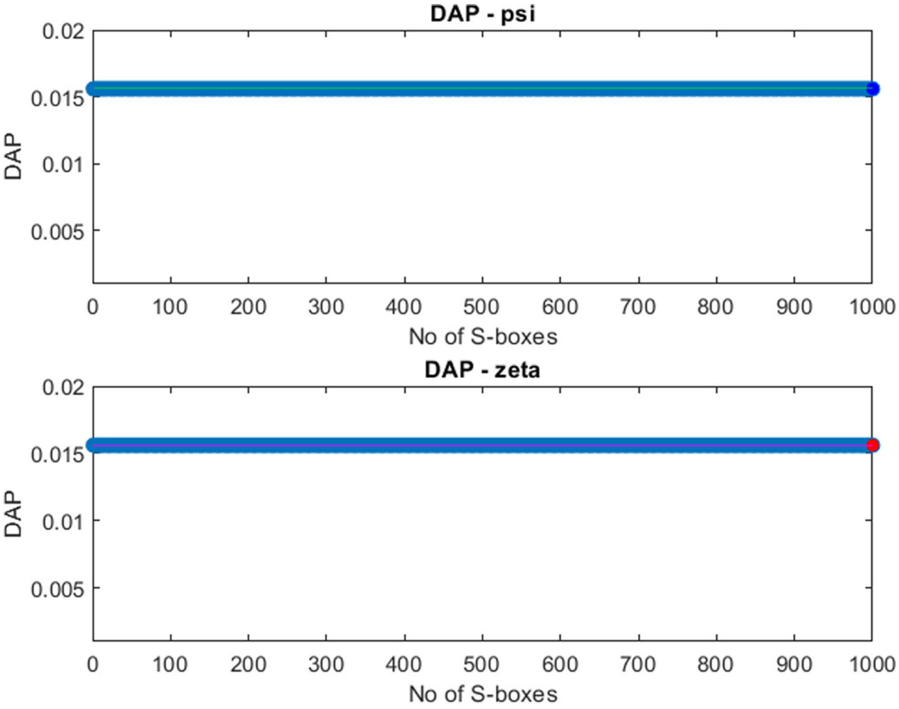


Fig. 18 DAP values of 1000 S-boxes

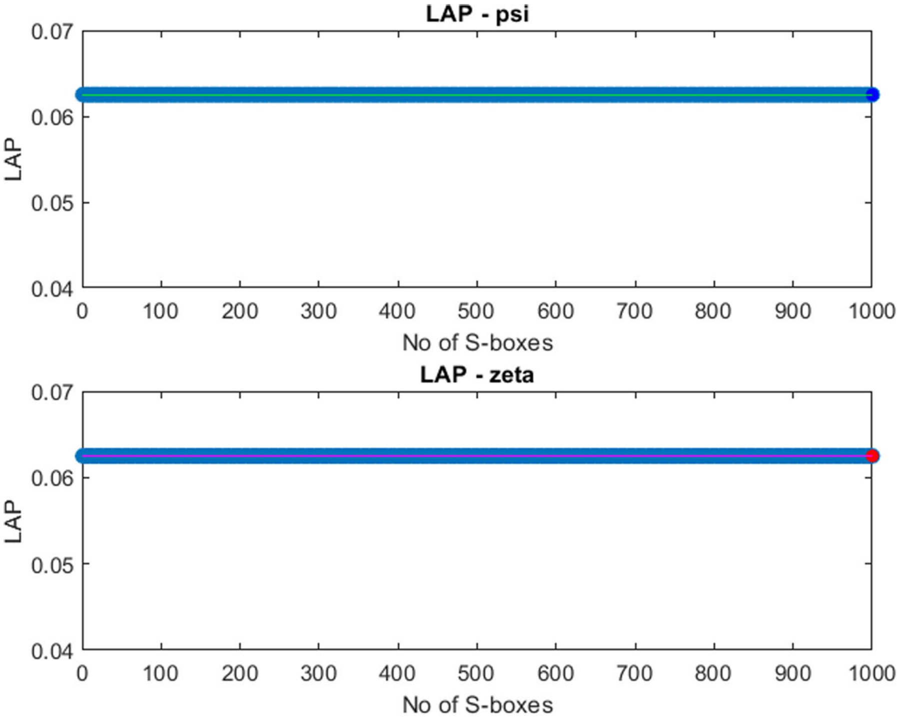


Fig. 19 LAP of 1000 S-boxes

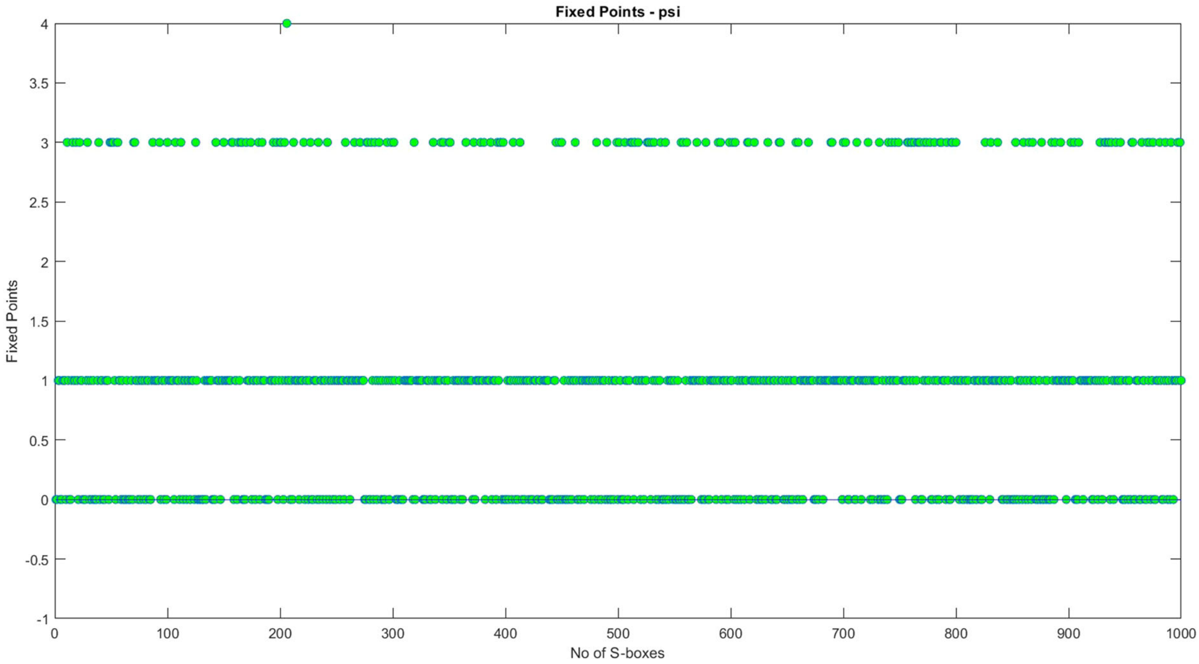


Fig. 20 Fixed points of 1000 S-boxes generated by function *psi*

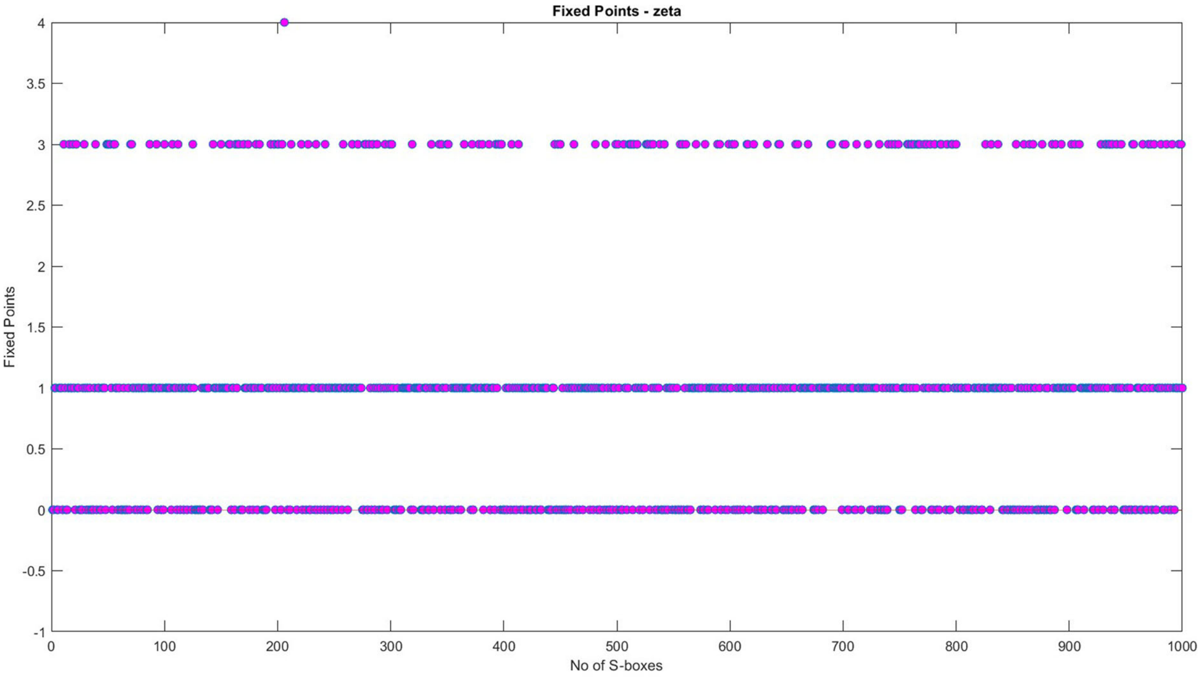


Fig. 21 Fixed points of 1000 S-boxes generated by function *zeta*

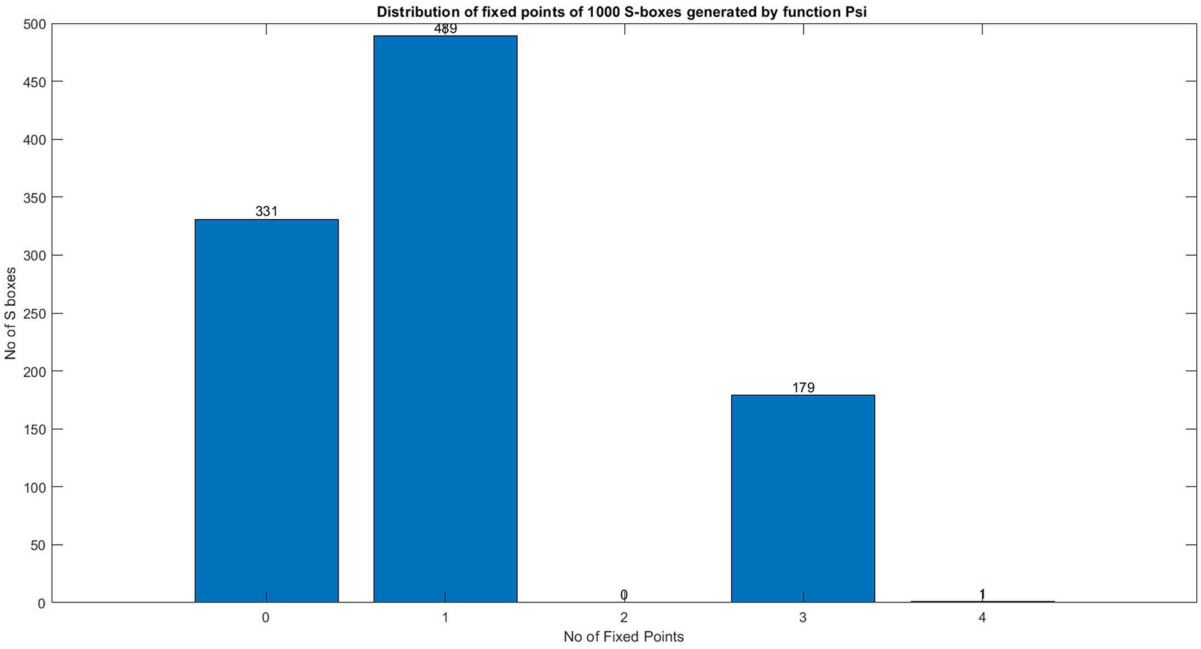


Fig. 22 Distribution of fixed points of S-boxes generated by function Psi

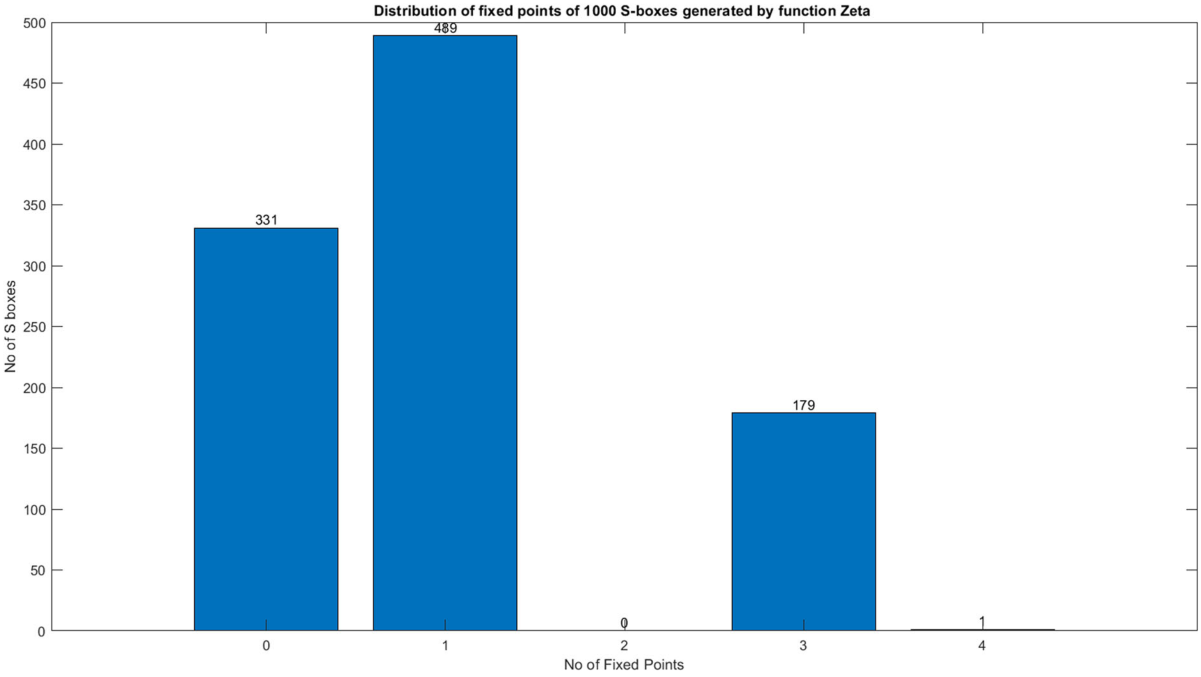


Fig. 23 Distribution of fixed points of S-boxes generated by function Zeta

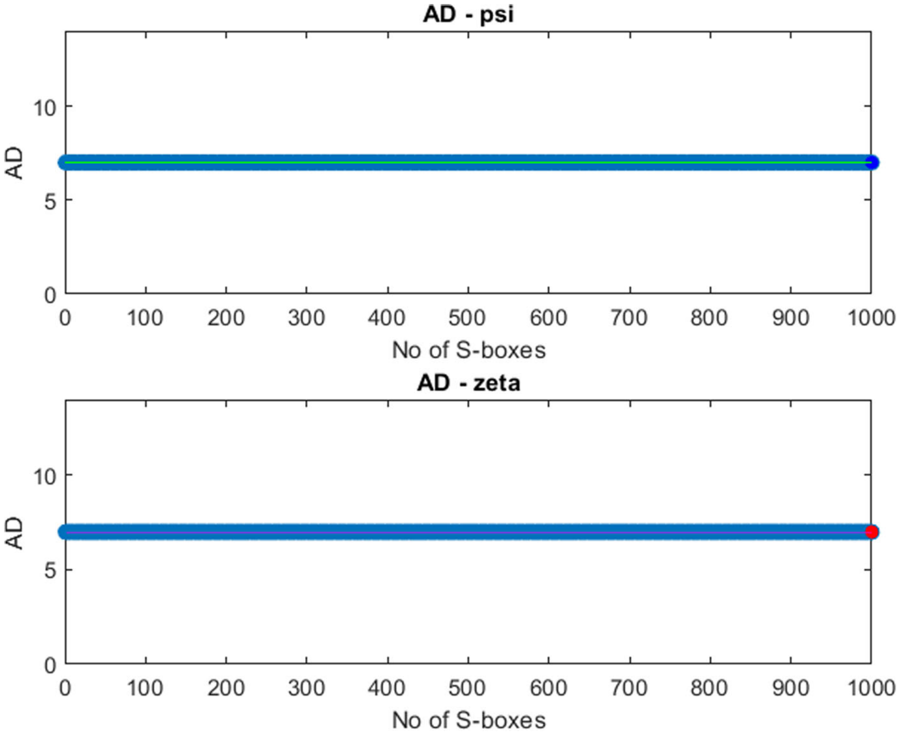


Fig. 24 Algebraic degree

of NPCR is 99.61, whereas the values in our proposed scheme are in the range 99.57–99.63 as seen in Table 7 and show the strong resistance to differential attacks on the image encryption algorithm. The UACI value indicates the average magnitude of the changes made to the pixel intensities during the encryption process. A lower UACI value indicates a smaller average change, suggesting better preservation of the original pixel intensities. Conversely, a higher UACI value indicates a greater average change, indicating a more significant alteration of the pixel intensities. The ideal value of UACI is 33.45 and our scheme shows great resistance to differential attacks with values in the range of 33.39–33.61 as seen in Table 7.

7 Conclusion

This article introduced a new approach to generating S-boxes, based on the Frobenius automorphism of the Galois field and a chaotic logistic map. Our generator is capable of producing S-boxes that are optimized and randomized, with strong cryptographic features such as minimum computing complexity and high nonlinearity. Through the demonstration of a prerequisite for our generator to produce different S-boxes, we were able to mathematically examine the dynamic behavior of our generator. We performed several thorough analyses on the performance of the S-boxes created by our system, looking at both single and batch S-box testing. Our S-box generation approach can effectively generate highly secure S-boxes in a short amount of time, according to the tests we conducted, which makes it a workable option for a variety of apps that need strong encryption infrastructure. By substituting our sample S-box for the scheme designed by [10], we presented the efficiency of our proposed S-box. The results of image encryption using the suggested S-box reveal a high degree of security for the image's cryptosystem. The proposed S-box generator shows remarkable efficiency by producing a large number of optimal S-boxes of nonlinearity 112, but it has just one limitation which is the term $ad - bc$ in Mobius transformation. Thus Our scheme shows great promise for creating encryption algorithms using dynamic S-boxes and providing various S-boxes for image security.

Acknowledgements We extend our sincere gratitude to the reviewers for their valuable comments and constructive suggestions, which have significantly improved the quality of our article.

We are also grateful to Prof. Mingyue Wang (College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, China) for insightful comments and suggestions, which significantly improved the quality of this work.

Author contributions All authors contributed equally.

Funding The authors declare that no external funding was received for this research.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no Conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
2. Chang, H. S.: International data encryption algorithm. jmu.edu, googleusercontent.com, Fall (2004)
3. Daeman, J., Rijmen, V.: The design of rijndael-AES: the advanced encryption standar. Springer (2002)
4. Gan, Z., Chai, X., Yuan, K., Lu, Y.: A novel image encryption algorithm based on LFT based S-boxes and chaos. Multimed. Tools Appl. **77**(7), 8759–8783 (2018)
5. Hussain, I., Shah, T., Gondal, M.A., Khan, W.A., Mahmood, H.: A group theoretic approach to construct cryptographically strong substitution boxes. Neural Comput. Appl. **23**(1), 97–104 (2013)
6. Ali, J., Jamil, M.K., Alali, A.S., Ali, R., Gulraiz: A medical image encryption scheme based on Mobius transformation and Galois field. Heliyon **10**(1), 23652–23652 (2023)
7. Zhang, T., Chen, C.L.P., Chen, L., Xu, X., Hu, B.: Design of highly nonlinear substitution boxes based on i-ching operators. IEEE Trans. Cybern. **48**(12), 3349–3358 (2018)
8. Zahid, A., Arshad, M., Ahmad, M.: A novel construction of efficient substitution-boxes using cubic fractional transformation. Entropy **21**(3), 245 (2019)
9. Mahmood, S., Farwa, S., Rafiq, M., Riaz, S.M.J., Shah, T., Jamal, S.S.: To study the effect of the generating polynomial on the quality of nonlinear components in block ciphers. Secur. Commun. Netw. **2018**, 1–8 (2018)
10. Ali, R., Jamil, M.K., Alali, A.S., Ali, J., Afzal, G.: A robust S box design using cyclic groups and image encryption. IEEE Access **11**, 135880–135890 (2023)
11. Bin Faheem, Z., Ali, A., Khan, M.A., Ul-Haq, M.E., Ahmad, W.: Highly dispersive substitution box (S-box) design using chaos. ETRI J. **42**(4), 619–632 (2020)
12. Shahzad, I., Mushtaq, Q., Razaq, A.: Construction of new S-box using action of quotient of the modular group for multimedia security. Secur. Commun. Netw. **2019**, 13 (2019)
13. Tian, Y., Lu, Z.: Chaotic S-box: intertwining logistic map and bacterial foraging optimization. Math. Probl. Eng. **2017**, 1–11 (2017)
14. Naseer, Y., Shah, T., Shah, D., Hussain, S.: A novel algorithm of constructing highly nonlinear S-p-boxes. Cryptography **3**(1), 6 (2019)
15. Luo, C., Wang, Y., Fu, Y., Zhou, P., Wang, M.: Constructing dynamic S-boxes based on chaos and irreducible polynomials for image encryption. Nonlinear Dyn. **112**(8), 6695–6713 (2024)
16. Artuger, F., Ozkaynak, F.: A new chaotic system and its practical applications in substitution box and random number generator. Multimed. Tools Appl. (2024). https://doi.org/10.1007/s11042-024-19053-7
17. Artuger, F.: A method for designing substitution boxes based on chaos with high nonlinearity. Wireless Pers. Commun. **135**, 1077–1092 (2024)
18. Haider, T., Azam, N.A., Hayat, U.: Substitution box generator with enhanced cryptographic properties and minimal computation time. Expert Syst. Appl. **241**, 122779 (2024)
19. Waheed, A., Subhan, F., Su'ud, M.M., Alam, M.M.: Molding robust S-box design based on linear fractional transformation and multilayer Perceptron: applications to multimedia security. Egypt. Inform. J. **26**, 100480 (2024)
20. Liu, R., Liu, H., Zhao, M.: Cryptanalysis and construction of keyed strong S-Box based on random affine transformation matrix and 2D hyper chaotic map. Expert Syst. Appl. **252**, 124238 (2024)
21. Zhang, M., Zhang, Y., Cen, Q., Wu, S.: Deep learning-based resource allocation for secure transmission in a non-orthogonal multiple access network. Int. J. Distrib. Sens. Netw. **18**(6), 15501329221104330 (2022)
22. Li, W., Susilo, W., Xia, C., Huang, L., Guo, F., Wang, T.: Secure data integrity check based on verified public key encryption with equality test for multi-cloud storage. IEEE Trans. Dependable Secure Comput. **01**, 1–15 (2024)
23. Bi, B., Huang, D., Mi, B., Deng, Z., Pan, H.: Efficient LBS security-preserving based on NTRU oblivious transfer. Wireless Pers. Commun. **108**(4), 2663–2674 (2019)
24. Liu, Q., Yuan, H., Hamzaoui, R., Su, H., Hou, J., Yang, H.: Reduced reference perceptual quality model with application to rate control for video-based point cloud compression. IEEE Trans. Image Process. **30**, 6623–6636 (2021)
25. Sun, G., Liao, D., Zhao, D., Xu, Z., Yu, H.: Live migration for multiple correlated virtual machines in cloud-based data centers. IEEE Trans. Serv. Comput. **11**(2), 279–291 (2015)
26. Cheng, D., Chen, L., Lv, C., Guo, L., Kou, Q.: Light-guided and cross-fusion U-Net for anti-illumination image super-resolution. IEEE Trans. Circuits Syst. Video Technol. **32**(12), 8436–8449 (2022)
27. Xuemin, Z., Haitao, D., Zenggang, X., Ying, R., Yanchao, L., Yuan, L., Delin, H.: Self-organizing key security management algorithm in socially aware networking. J. Signal Process. Syst. **96**, 369–383 (2024)
28. Vijayakumar, M., Ahilan, A.: An optimized chaotic S-box for real-time image encryption scheme based on 4-dimensional memristive hyperchaotic map. Ain Shams Eng. J. **15**(4), 102620 (2024)
29. Ullah, S., Liu, X., Waheed, A., Zhang, S.: An efficient construction of S box based on the fractional order Rabinovich Fabrikant chaotic system. Integration **94**, 102099 (2024)

30. Tariq, S., Elmoasry, A., Batool, S.I., Khan, M.: Quantum harmonic oscillator and schrodinger paradox based nonlinear confusion component. Int. J. Theor. Phys. **59**, 3558–3573 (2020)
31. Alali, A.S., Ali, R., Jamil, M.K., Ali, J., Gulraiz: Dynamic S-box construction using mordell elliptic curves over galois field and its applications in image encryption. Mathematics **12**(4), 587 (2024)
32. Ibrahim, S., Abbas, A.M.: Efficient key-dependent dynamic S-boxes based on permutated elliptic curves. Inf. Sci. **558**, 246–264 (2021)
33. Artuger, F., Ozkaynak, F.: A new algorithm to generate aes-like substitution boxes based on sine cosine optimization algorithm. Multimed. Tools Appl. **83**(13), 38949–38964 (2024)
34. Webster, A. F., Tavares, S. E.: On the design of S-boxes. In: Conference on the theory and application of cryptographic techniques, (pp. 523-534), Springer (1985)
35. Hussain, I., Shah, T., Gondal, M.A., Khan, M., Khan, W.A.: Construction of new S-box using a linear fractional transformation. World Appl. Sci. J. **14**(12), 1779–1785 (2011)
36. Hussain, I., Shah, T., Gondal, M.A., Mahmood, H.: An efficient approach for the construction of LFT S-boxes using chaotic logistic map. Nonlinear Dyn. **71**, 133–140 (2013)
37. Siddiqui, N., Afsar, U., Shah, T., Qureshi, A.: A novel construction of S16 AES S-box. Int. J. Comput. Sci. Inf. Secur. **14**(8), 810–818 (2016)
38. Razaq, A., Yousaf, A., Shuaib, U., Siddiqui, N., Ullah, A., Waheed, A.: A novel construction of substitution box involving coset diagram and a bijective map. Secur. Commun. Netw. **48**, 16 (2017)
39. Ullah, A., Jamal, S.S., Shah, T.: A novel algebraic technique for the construction of strong substitution box. Wireless Pers. Commun. **99**(1), 213–226 (2018)
40. Zahid, A., Arshad, M.: An innovative design of substitution-boxes using cubic polynomial mapping. Symmetry **11**(3), 437 (2019)
41. Siddiqui, N., Yousaf, F., Murtaza, F., Haq, M.E., Ashraf, M.U., Alghamdi, A.M., Alfakeeh, A.S.A.S.: A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field. PLoS ONE **15**(11), 1–16 (2020)
42. Zahid, A., Tawalbeh, L., Ahmad, M., Alkhayyat, A., Hassan, M.T., Manzoor, A., Farhan, A.K.: Efficient dynamic S-box generation using linear trigonometric transformation for security applications. IEEE Access **9**, 2–17 (2021)
43. Hussain, I., Shah, T., Gondal, M.A., Mahmood, H.: A projective general linear group based algorithm for the construction of substitution box for block ciphers. Neural Comput. Appl. **13**, 1085–1093 (2013)
44. Shannon, C.E.: Communication theory of secrecy systems. Bell Labs Tech. J. **28**, 656–715 (1949)
45. Younas, I., Khan, M.: A new efficient digital image encryption based on inverse left almost semi group and lorenz chaotic system. Entropy **20**(12), 913 (2018)
46. Naseer, Y., Shah, T., Shah, D., Hussain, S.: A novel algorithm of constructing highly nonlinear S-p-boxes. Cryptography **3**(1), 6 (2019)
47. Pieprzyk, J., Finkelstein, G.: Towards effective nonlinear cryptosystem design. IEEE Proc. Part E Comput. Digit. Tech. **135**(6), 325–335 (1988)
48. Arshad, B., Siddiqui, N.: Construction of highly nonlinear substitution boxes (S-boxes) based on connected regular graphs. Int. J. Comput. Sci. Inf. Secur. **18**(4), 105–122 (2020)
49. Wang, Y., Zhang, Z., Zhang, L.Y., Feng, J., Gao, J., Lei, P.: A genetic algorithm for constructing bijective substitution boxes with high nonlinearity. Inf. Sci. **523**, 152–166 (2020)
50. Xie, G., Hou, G., Pei, Q., Huang, H.: Lightweight privacy protection via adversarial sample. Electronics **13**, 1230 (2024)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.