Computational and Applied Mathematics (2023) 42:90
https://doi.org/10.1007/s40314-023-02215-y

A novel algebraic construction of strong S-boxes over double $GF(2^7)$ structures and image protection

Abdul Razaq[1] · **Musheer Ahmad**[2] · **Ahmed A. Abd El-Latif**[3,4]

Received: 2 September 2022 / Revised: 17 January 2023 / Accepted: 22 January 2023

Abstract

To provide safe data communication, substitution boxes are employed in a variety of frameworks and cryptosystems. The acceptance of the AES encryption standard posed a challenge for security experts to develop sustainable substitution boxes utilizing various underlying techniques. It is because they are solely responsible to determine whether a cryptosystem is resistant to differential and linear cryptanalyses. The present study revealed a novel algebraic scheme of designing S-boxes with almost optimal characteristics to satisfy the robustness criteria. In literature, many S-box generation techniques based on Galois field of order 256 have been developed. Unlike existing Galois fields-based S-box methods, we utilized two Galois fields $GF(2^7)$ of order 128 with different structures for the construction of initial seed S-box, that forms a solid foundation for further optimization of the proposed technique. Then, for the merit of non-linearity optimization, we consider the action of the permutation group $C_{6888} \times C_4 \times C_4$ on initial S-box to enhance the proficiency of generated S-box. The quality of anticipated S-box is examined through various well-known performance parameters. The encouraging outcomes of standard performance analyses confirm that the generated S-box fulfills all the requirements for secure communication and image encryption.

Communicated by Somphong Jitman.

✉ Musheer Ahmad
musheer.cse@gmail.com; mahmad9@jmi.ac.in

✉ Ahmed A. Abd El-Latif
a.rahiem@gmail.com

Abdul Razaq
makenqau@gmail.com

1 Division of Science and Technology, Department of Mathematics, University of Education, Lahore 54770, Pakistan

2 Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India

3 EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia

4 Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Al Minufiyah 32511, Egypt

Published online: 22 February 2023

Keywords Block ciphers · Substitution-box (S-box) · Galois fields $GF(2^7)$ · Permutation group · Image protection

Mathematics Subject Classification 11T71 · 94A60 · 20B35

1 Introduction

Cryptography assists people and associations to keep safe their secret data. Various symmetric and asymmetric ciphers were developed for this purpose. Symmetric ciphers are simple and efficient unlike asymmetric ciphers, consume less computing resources. Symmetric ciphers have been categorized into block and stream ciphers (Bhanot and Hans 2015). The block cipher encodes a plaintext block of a certain length that contains several bits at a time. On the other hand, a stream cipher enciphers the messages in bit-by-bit manner. The block ciphers are actively utilized in Internet correspondence while stream ciphers are valuable in the circumstance where computing assets are minimal or proficiency is not the primary issue.

A block cipher helps to accomplish information privacy, which is one of the objectives of cryptography. It is one of the most broadly utilized tools for ensuring the security of information (Paar and Pelzl 2009). The present-day mainstream symmetric ciphers, such as AES, IDEA, Blowfish, and DES, are all block ciphers. Block ciphers are easy to implement and secure than the stream ciphers (Shamir 2004). Many of the block ciphers based on substitution and permutation operations or the Feistel structure. Block ciphers depending upon the Feistel structure split the plaintext block into two or more sections and execute various operations. DES, Kasumi, Blowfish, Camellia are some examples of Feistel Cipher. In substitution–permutation ciphers, (Lambić and Živković 2013) used sub-keys and multiple sets of rounds to transform plaintext into ciphertext. In addition to various tasks, substitutions and permutations are carried out on the input bits in each round,. AES, SQUARE, PRESENT and SHARK are among the famous block ciphers that use substitution and permutation operations.

Let $\mathbb{Z}_2 = \{0, 1\}$, it is well known that $\mathbb{Z}_2$ is a field under multiplication modulo 2 and a function $\beta : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is called Boolean mapping. A vectorial Boolean mapping $\gamma : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ is defined as; $\gamma(z) = (\beta_1(z), \beta_2(z), \ldots, \beta_m(z))$, where $z = (z_1, z_2, \ldots, z_n) \in \mathbb{Z}_2^n$ and β_i is Boolean mapping, for all $i = 1,2,\ldots,m$. A substitution box of size $n \times n$ is precisely defined as a vectorial Boolean mapping $\psi : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$. In other words, an $n \times n$ substitution box picks an n bits block and converts it to an n bits output. It behaves like a non-linear mapping ψ from $\{0, 1\}^n$ to $\{0, 1\}^n$ (Makarim and Tezcan 2014). A Boolean map β_i is considered to be balanced if there is a balanced distribution of 1's and 0's in its outputs (Picek et al. 2015). The $n \times n$ S-boxes have great importance in several cryptographic systems and S-P network-based ciphers. Many well-known ciphers, including KASUMI, AES, KECCAK, ARIA, PRESENT, hash function, etc. use them (Knudsen and Robshaw 2011). Recently, the use of S-boxes has also been explored for image/video encryption schemes, pseudo-random sequence design and watermarking etc.

The extraordinary importance of substitution boxes in various cryptographic schemes inspires cryptographers to construct S-boxes possessing adequate strength to counter different attacks. In the recent past, many researchers have developed a number of methods for S-box generation. An innovative method to develop key dependent substitution box is proposed in Kazlauskas and Kazlauskas (2009). The authors announced to enhance the safety level of AES block encryption. In (Usama et al. 2019), Usama et al. proposed a systematic method of S-box

generation based on mixing properties of the chaotic sine map. Jamal et al. combined chaotic Tent-Sine function and linear transformations to evolve reliable S-boxes (Jamal et al. 2019). In (Zhang et al. 2018), the authors presented a new algorithm based on I-Ching operators to generate their S-box. The strength of S-box was determined by various analyses. The results showed that it has very good cryptographic qualities. Javeed et al. (Javeed and Shah 2020) proposed a strong substitution box using Rabinovich–Fabrikant equations. A graphical method for S-box generation has been presented in Shahzad et al. (2019). The authors used coset graphs for the alternating group A_4 and suggested a high-quality S-box. Razaq et al. (2020) presented an innovative method to improve the quality of already developed S-boxes while preserving their actual mathematical structure. In (Özkaynak 2019a), a secure S-box based on Rössler hyper-chaotic system of equation has been designed by Özkaynak. The new scheme for generating a large number of different S-boxes based on different permutations was presented in Roslan et al. (2019). According to the authors, more than 50% of the generated S-boxes have NL scores greater than 100, while the NL value of the best S-box is 110.

The present research reveals a new approach to design robust S-boxes for block ciphers. The accompanying contemplations were taken into account while constructing our S-box:

- The generated S-box should be cryptographically strong and meet the required standard of information security.
- The S-box must possess a sufficient level of confusion and perplexity, but the method of its construction remains simple and computationally low.
- The S-box should maintain a decent score when examined through modern cryptographic performance evaluation parameters.
- The S-box must be suitable for multimedia image encryption.

The S-box design technique introduced in this work is neoteric and proves to be more efficient as compared to other algebraic techniques displayed in the literature. Many 8×8 S-box generation techniques based on Galois field of order 256, denoted by $GF(2^8)$, have been presented in the literature. As far as we know, it is the first endeavor to create 8×8 S-boxes using two Galois fields of order 128. Furthermore, we consider the action of the permutation group $C_{6888} \times C_4 \times C_4$ on the initial S-box for further enhancement of its strength and stiffness. After the S-box was developed, performance evaluation was carried out to measure its cryptographic strength. It is found that the generated S-box has excellent cryptographic qualities compared to other recently developed S-boxes. The outcomes showed that our S-box is a decent choice for image encryption.

The remainder of the article is divided into the following sections. The suggested algebraic technique for S-box construction is described in Sect. 2. By performing different renowned cryptographic tests, the security of the generated S-box is evaluated in Sect. 3. Majority Logic Criterion is presented in Sect. 4. Section 5 deals with differential analyses for the generated cryptosystem. Section 6 concludes this study.

2 Algebraic construction of S-box

This section is devoted to the structure of our generated S-box. Before we explore the existing algorithm, it is important to reiterate some facts regarding Galois fields $GF(2^n)$. Before the turn of the 19th century, algebraists believed that every finite field is of prime order. It was Évariste Galois (1811–1832) who constructed finite fields of order p^n, where p is a prime number and n is a positive integer, know as Galois fields, denoted by $GF(p^n)$. Galois showed

that $GF(p^n) = \mathbb{Z}_p[X]/f(\alpha) = \left\{0, \alpha, \alpha^2, \alpha^3, \ldots, (\alpha)^{p^n-1} = 1\right\}$, where $\mathbb{Z}_p[X]$ is the field extension of finite field of order p, denoted by $\mathbb{Z}_p$ and $f(\alpha)$ denotes an irreducible polynomial of degree n over $\mathbb{Z}_p$. In simple words, every irreducible polynomial of degree n over $\mathbb{Z}_p$ generates a Galois field $GF(p^n)$. Note that, for fixed n and p, there are several irreducible polynomials of degree n over $\mathbb{Z}_p$, so we can develop more than one Galois fields $GF(p^n)$. Since an 8×8 S-box has 256 elements and $2^8 = 256$, therefore Galois field $GF(2^8)$ becomes important in the generation of 8×8 S-boxes. In the literature, numerous techniques of S-box construction based on $GF((2^8)$ have been presented. In AES (Daemen and Rijmen 1999), the construction of S-box is based on irreducible polynomial $f(\alpha) = 1+\alpha+\alpha^3+\alpha^4+\alpha^8$. In (Altaleb et al. 2017; Hussain et al. 2013), Hussain et al. used $f(\alpha) = 1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^8$ in their S-box construction schemes. Farwa et al. (2016) proposed an S-box using $f(\alpha) = 1 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^8$. In this work, we have developed a novel scheme for the formation of 8×8 S-box using two Galois fields of order 128, namely $GF_1(2^7)$ and $GF_2(2^7)$, for the first time. The following irreducible polynomials

$$f(\alpha) = 1 + \alpha^4 + \alpha^7$$

$$g(\omega) = 1 + \omega + \omega^2 + \omega^3 + \omega^7$$

are used to generate the elements of $GF_1(2^7)$ and $GF_2(2^7)$ respectively (see Tables 1,2).

2.1 Proposed scheme

Step A: First, we write the elements of both the fields $GF_1(2^7)$ and $GF_2(2^7)$ in a 16×16 matrix M_1 (see Table 3) in the following way. The elements 0, α^1,α^2,α^3, … of $GF_1(2^7)$ are set at 1st, 3rd 5th, 7th, … position of the 1st row of M_1, whereas, the elements 0, ω^1,ω^2, ω^3, … of $GF_2(2^7)$ are placed at 2nd, 4th, 6th and 8th, … position of the 1st row. Similarly, all other elements of both the field are arranged in M_1.

Let $a_{i,j}$ denote the element of 16×16 matrix which is lying in the ith row and jth column, $\mu = n(\text{mod}8)$ and $\kappa = \begin{cases} \frac{n+8}{8} & \text{if } 8 \text{ divides } n \\ \lceil \frac{n}{8} \rceil & \text{otherwise} \end{cases}$

Mathematically, M_1 can be constructed by the following rule;

$$0 \in GF_1(2^7) \rightarrow a_{1,1}$$

$$0 \in GF_2(2^7) \rightarrow a_{1,2}$$

$$\alpha^n \in GF_1(2^7) \rightarrow a_{\kappa,2\mu+1}$$

$$\omega^n \in GF_2(2^7) \rightarrow a_{\kappa,2\mu+2}$$

Step B: In this step, we create intricacy in the data. For this purpose, the following mapping is applied on M_1 and a new matrix M_2 is generated (see Table 4).

$$\alpha^n \rightarrow \alpha^{77n+13(\text{mod})127}$$

$$\omega^n \rightarrow \omega^{101n+17(\text{mod})127}$$

Table 1 Structure description of $GF_1(2^7)$

Binary values	$GF_1(2^7)$	Decimal	Binary values	$GF_1(2^7)$	Decimal	Binary values	$GF_1(2^7)$	Decimal	Binary values	$GF_1(2^7)$	Decimal
0,000,000	0	0	0,000,001	1	1	0,000,010	α^1	2	0,000,100	α^2	4
0,001,000	α^3	8	0,010,000	α^4	16	0,100,000	α^5	32	1,000,000	α^6	64
0,001,001	α^7	9	0,010,010	α^8	18	0,100,100	α^9	36	1,001,000	α^{10}	72
0,011,001	α^{11}	25	0,110,010	α^{12}	50	1,100,100	α^{13}	100	1,000,001	α^{14}	65
0,001,011	α^{15}	11	0,010,110	α^{16}	22	0,101,100	α^{17}	44	1,011,000	α^{18}	88
0,111,001	α^{19}	57	1,110,010	α^{20}	114	1,101,101	α^{21}	109	1,010,011	α^{22}	83
0,101,111	α^{23}	47	1,011,110	α^{24}	94	0,110,101	α^{25}	53	1,101,010	α^{26}	106
1,011,101	α^{27}	93	0,110,011	α^{28}	51	1,100,110	α^{29}	102	1,000,101	α^{30}	69
0,000,011	α^{31}	03	0,000,110	α^{32}	06	0,001,100	α^{33}	12	0,011,000	α^{34}	24
0,110,000	α^{35}	48	1,100,000	α^{36}	96	1,001,001	α^{37}	73	0,011,011	α^{38}	27
0,110,110	α^{39}	54	1,101,100	α^{40}	108	1,010,001	α^{41}	81	0,101,011	α^{42}	43
1,010,110	α^{43}	86	0,100,101	α^{44}	37	1,001,010	α^{45}	74	0,011,101	α^{46}	29
0,111,010	α^{47}	58	1,110,100	α^{48}	116	1,100,001	α^{49}	97	1,001,011	α^{50}	75
0,011,111	α^{51}	31	0,111,110	α^{52}	62	1,111,100	α^{53}	124	1,110,001	α^{54}	113
1,101,011	α^{55}	107	1,011,111	α^{56}	95	0,110,111	α^{57}	55	1,101,110	α^{58}	110
1,010,101	α^{59}	85	0,100,011	α^{60}	35	1,000,110	α^{61}	70	0,000,101	α^{62}	05
0,001,010	α^{63}	10	0,010,100	α^{64}	20	0,101,000	α^{65}	40	1,010,000	α^{66}	80
0,101,001	α^{67}	41	1,010,010	α^{68}	82	0,101,101	α^{69}	45	1,011,010	α^{70}	90
0,111,101	α^{71}	61	1,111,010	α^{72}	122	1,111,101	α^{73}	125	1,110,011	α^{74}	115
1,101,111	α^{75}	111	1,010,111	α^{76}	87	0,100,111	α^{77}	39	1,001,110	α^{78}	78

Table 1 (continued)

Binary values	$GF_1(2^7)$	Decimal	Binary values	$GF_1(2^7)$	Decimal	Binary values	$GF_1(2^7)$	Decimal	Binary values	$GF_1(2^7)$	Decimal
0,010,101	α^{79}	21	0,101,010	α^{80}	42	1,010,100	α^{81}	84	0,100,001	α^{82}	33
1,000,010	α^{83}	66	0,001,101	α^{84}	13	0,011,010	α^{85}	26	0,110,100	α^{86}	52
1,101,000	α^{87}	104	1,011,001	α^{88}	89	0,111,011	α^{89}	59	1,110,110	α^{90}	118
1,100,101	α^{91}	101	1,000,011	α^{92}	67	0,001,111	α^{93}	15	0,011,110	α^{94}	30
0,111,100	α^{95}	60	1,111,000	α^{96}	120	1,111,001	α^{97}	121	1,111,011	α^{98}	123
1,111,111	α^{99}	127	1,110,111	α^{100}	119	1,100,111	α^{101}	103	1,000,111	α^{102}	71
0,000,111	α^{103}	07	0,001,110	α^{104}	14	0,011,100	α^{105}	28	0,111,000	α^{106}	56
1,110,000	α^{107}	112	1,101,001	α^{108}	105	1,011,011	α^{109}	91	0,111,111	α^{110}	63
1,111,110	α^{111}	126	1,110,101	α^{112}	117	1,100,011	α^{113}	99	1,001,111	α^{114}	79
0,010,111	α^{115}	23	0,101,110	α^{116}	46	1,011,100	α^{117}	92	0,110,001	α^{118}	49
1,100,010	α^{119}	98	1,001,101	α^{120}	77	0,010,011	α^{121}	19	0,100,110	α^{122}	38
1,001,100	α^{123}	76	0,010,001	α^{124}	17	0,100,010	α^{125}	34	1,000,100	α^{126}	68

Table 2 Structure description of $GF_2(2^7)$

Binary values	$GF_2(2^7)$	Decimal	Binary values	$GF_2(2^7)$	Decimal	Binary values	$GF_2(2^7)$	Decimal	Binary values	$GF_2(2^7)$	Decimal
0,000,000	0	0	0,000,001	1	1	0,000,010	ω^1	2	0,000,100	ω^2	4
0,001,000	ω^3	8	0,010,000	ω^4	16	0,100,000	ω^5	32	1,000,000	ω^6	64
1,110,001	ω^7	113	0,010,011	ω^8	19	0,100,110	ω^9	38	1,001,100	ω^{10}	76
1,101,001	ω^{11}	105	0,100,011	ω^{12}	35	1,000,110	ω^{13}	70	1,111,101	ω^{14}	125
0,001,011	ω^{15}	11	0,010,110	v^{16}	22	0,101,100	ω^{17}	44	1,011,000	ω^{18}	88
1,000,001	ω^{19}	65	1,110,011	ω^{20}	115	0,010,111	ω^{21}	23	0,101,110	ω^{22}	46
1,011,100	ω^{23}	92	1,001,001	ω^{24}	73	1,100,011	ω^{25}	99	0,110,111	ω^{26}	55
1,101,110	ω^{27}	110	0,101,101	ω^{28}	45	1,011,010	ω^{29}	90	1,000,101	ω^{30}	69
1,111,011	ω^{31}	123	0,000,111	ω^{32}	07	0,001,110	ω^{33}	14	0,011,100	ω^{34}	28
0,111,000	ω^{35}	56	1,110,000	ω^{36}	112	0,010,001	ω^{37}	17	0,100,010	ω^{38}	34
1,000,100	ω^{39}	68	1,111,001	ω^{40}	121	0,000,011	ω^{41}	03	0,000,110	ω^{42}	06
0,001,100	ω^{43}	12	0,011,000	ω^{44}	24	0,110,000	ω^{45}	48	1,100,000	ω^{46}	96
0,110,001	ω^{47}	49	1,100,010	ω^{48}	98	0,110,101	ω^{49}	53	1,101,010	ω^{50}	106
0,100,101	ω^{51}	37	1,001,010	ω^{52}	74	1,100,101	ω^{53}	101	0,111,011	ω^{54}	59
1,110,110	ω^{55}	118	0,011,101	ω^{56}	29	0,111,010	ω^{57}	58	1,110,100	ω^{58}	116
0,011,001	ω^{59}	25	0,110,010	ω^{60}	50	1,100,100	ω^{61}	100	0,111,001	ω^{62}	57
1,110,010	ω^{63}	114	0,010,101	ω^{64}	21	0,101,010	ω^{65}	42	1,010,100	ω^{66}	84
1,011,001	ω^{67}	89	1,000,011	ω^{68}	67	1,110,111	ω^{69}	119	0,011,111	ω^{70}	31
0,111,110	ω^{71}	62	1,111,100	ω^{72}	124	0,001,001	ω^{73}	09	0,010,010	ω^{74}	18
0,100,100	ω^{75}	36	1,001,000	ω^{76}	72	1,100,001	ω^{77}	97	0,110,011	ω^{78}	51

Table 2 (continued)

Binary values	$GF_2(2^7)$	Decimal	Binary values	$GF_2(2^7)$	Decimal	Binary values	$GF_2(2^7)$	Decimal	Binary values	$GF_2(2^7)$	Decimal
1,100,110	ω^{79}	102	0,111,101	ω^{80}	61	1,111,010	ω^{81}	122	0,000,101	ω^{82}	05
0,001,010	ω^{83}	10	0,010,100	ω^{84}	20	0,101,000	ω^{85}	40	1,010,000	ω^{86}	80
1,010,001	ω^{87}	81	1,010,011	ω^{88}	83	1,010,111	ω^{89}	87	1,011,111	ω^{90}	95
1,001,111	ω^{91}	79	1,101,111	ω^{92}	111	0,101,111	ω^{93}	47	1,011,110	ω^{94}	94
1,001,101	ω^{95}	77	1,101,011	ω^{96}	107	0,100,111	ω^{97}	39	1,001,110	ω^{98}	78
1,101,101	ω^{99}	109	0,101,011	ω^{100}	43	1,010,110	ω^{101}	86	1,011,101	ω^{102}	93
1,001,011	ω^{103}	75	1,100,111	ω^{104}	103	0,111,111	ω^{105}	63	1,111,110	ω^{106}	126
0,001,101	ω^{107}	13	0,011,010	ω^{108}	26	0,110,100	ω^{109}	52	1,101,000	ω^{110}	104
0,100,001	ω^{111}	33	1,000,010	ω^{112}	66	1,110,101	ω^{113}	117	0,011,011	ω^{114}	27
0,110,110	ω^{115}	54	1,101,100	ω^{116}	108	0,101,001	ω^{117}	41	1,010,010	ω^{118}	82
1,010,101	ω^{119}	85	1,011,011	ω^{120}	91	1,000,111	ω^{121}	71	1,111,111	ω^{122}	127
0,001,111	ω^{123}	15	0,011,110	ω^{124}	30	0,111,100	ω^{125}	60	1,111,000	ω^{126}	120

Table 3 Matrix M_1, the initial presentation of Galois fields $GF_1(2^7)$ and $GF_2(2^7)$

0	0	α^1	ω^1	α^2	ω^2	α^3	ω^3	α^4	ω^4	α^5	ω^5	α^6	ω^6	α^7	ω^7
α^8	ω^8	α^9	ω^9	α^{10}	ω^{10}	α^{11}	ω^{11}	α^{12}	ω^{12}	α^{13}	ω^{13}	α^{14}	ω^{14}	α^{15}	ω^{15}
α^{16}	ω^{16}	α^{17}	ω^{17}	α^{18}	ω^{18}	α^{19}	ω^{19}	α^{20}	ω^{20}	α^{21}	ω^{21}	α^{22}	ω^{22}	α^{23}	ω^{23}
α^{24}	ω^{24}	α^{25}	ω^{25}	α^{26}	ω^{26}	α^{27}	ω^{27}	α^{28}	ω^{28}	α^{29}	ω^{29}	α^{30}	ω^{30}	α^{31}	ω^{31}
α^{32}	ω^{32}	α^{33}	ω^{33}	α^{34}	ω^{34}	α^{35}	ω^{35}	α^{36}	ω^{36}	α^{37}	ω^{37}	α^{38}	ω^{38}	α^{39}	ω^{39}
α^{40}	ω^{40}	α^{41}	ω^{41}	α^{42}	ω^{42}	α^{43}	ω^{43}	α^{44}	ω^{44}	α^{45}	ω^{45}	α^{46}	ω^{46}	α^{47}	ω^{47}
α^{48}	ω^{48}	α^{49}	ω^{49}	α^{50}	ω^{50}	α^{51}	ω^{51}	α^{52}	ω^{52}	α^{53}	ω^{53}	α^{54}	ω^{54}	α^{55}	ω^{55}
α^{56}	ω^{56}	α^{57}	ω^{57}	α^{58}	ω^{58}	α^{59}	ω^{59}	α^{60}	ω^{60}	α^{61}	ω^{61}	α^{62}	ω^{62}	α^{63}	ω^{63}
α^{64}	ω^{64}	α^{65}	ω^{65}	α^{66}	ω^{66}	α^{67}	ω^{67}	α^{68}	ω^{68}	α^{69}	ω^{69}	α^{70}	ω^{70}	α^{71}	ω^{71}
α^{72}	ω^{72}	α^{73}	ω^{73}	α^{74}	ω^{74}	α^{75}	ω^{75}	α^{76}	ω^{76}	α^{77}	ω^{77}	α^{78}	ω^{78}	α^{79}	ω^{79}
α^{80}	ω^{80}	α^{81}	ω^{81}	α^{82}	ω^{82}	α^{83}	ω^{83}	α^{84}	ω^{84}	α^{85}	ω^{85}	α^{86}	ω^{86}	α^{87}	ω^{87}
α^{88}	ω^{88}	α^{89}	ω^{89}	α^{90}	ω^{90}	α^{91}	ω^{91}	α^{92}	ω^{92}	α^{93}	ω^{93}	α^{94}	ω^{94}	α^{95}	ω^{95}
α^{96}	ω^{96}	α^{97}	ω^{97}	α^{98}	ω^{98}	α^{99}	ω^{99}	α^{100}	ω^{100}	α^{101}	ω^{101}	α^{102}	ω^{102}	α^{103}	ω^{103}
α^{104}	ω^{104}	α^{105}	ω^{105}	α^{106}	ω^{106}	α^{107}	ω^{107}	α^{108}	ω^{108}	α^{109}	ω^{109}	α^{110}	ω^{110}	α^{111}	ω^{111}
α^{112}	ω^{112}	α^{113}	ω^{113}	α^{114}	ω^{114}	α^{115}	ω^{115}	α^{116}	ω^{116}	α^{117}	ω^{117}	α^{118}	ω^{118}	α^{119}	ω^{119}
α^{120}	ω^{120}	α^{121}	ω^{121}	α^{122}	ω^{122}	α^{123}	ω^{123}	α^{124}	ω^{124}	α^{125}	ω^{125}	α^{126}	ω^{126}	α^{127}	ω^{127}

Table 4 Matrix M_2 evolved after step B

0	0	α^{90}	ω^{118}	α^{40}	ω^{92}	α^{117}	ω^{66}	α^{67}	ω^{40}	α^{17}	ω^{14}	α^{94}	ω^{115}	α^{44}	ω^{89}
α^{121}	ω^{63}	α^{71}	ω^{37}	α^{21}	ω^{11}	α^{98}	ω^{112}	α^{48}	ω^{86}	α^{125}	ω^{60}	α^{75}	ω^{34}	α^{25}	ω^{8}
α^{102}	ω^{109}	α^{52}	ω^{83}	α^{02}	ω^{57}	α^{79}	ω^{31}	α^{29}	ω^{5}	α^{106}	ω^{106}	α^{56}	ω^{80}	α^{6}	ω^{54}
α^{83}	ω^{28}	α^{33}	ω^{2}	α^{110}	ω^{103}	α^{60}	ω^{77}	α^{10}	ω^{51}	α^{87}	ω^{25}	α^{37}	ω^{126}	α^{114}	ω^{100}
α^{64}	ω^{74}	α^{14}	ω^{48}	α^{91}	ω^{22}	α^{41}	ω^{123}	α^{118}	ω^{97}	α^{68}	ω^{71}	α^{18}	ω^{45}	α^{95}	ω^{19}
α^{45}	ω^{120}	α^{122}	ω^{94}	α^{72}	ω^{68}	α^{22}	ω^{42}	α^{99}	ω^{16}	α^{49}	ω^{117}	α^{126}	ω^{91}	α^{76}	ω^{65}
α^{26}	ω^{39}	α^{103}	ω^{13}	α^{53}	ω^{114}	α^{3}	ω^{88}	α^{80}	ω^{62}	α^{30}	ω^{36}	α^{107}	ω^{10}	α^{57}	ω^{111}
α^{7}	ω^{85}	α^{84}	ω^{59}	α^{34}	ω^{33}	α^{111}	ω^{7}	α^{61}	ω^{108}	α^{11}	ω^{82}	α^{88}	ω^{56}	α^{38}	ω^{30}
α^{115}	ω^{4}	α^{65}	ω^{105}	α^{15}	ω^{79}	α^{92}	ω^{53}	α^{42}	ω^{27}	α^{119}	ω^{1}	α^{69}	ω^{102}	α^{19}	ω^{76}
α^{96}	ω^{50}	α^{46}	ω^{24}	α^{123}	ω^{125}	α^{73}	ω^{99}	α^{23}	ω^{73}	α^{100}	ω^{47}	α^{50}	ω^{21}	α^{127}	ω^{122}
α^{77}	ω^{96}	α^{27}	ω^{70}	α^{104}	ω^{44}	α^{54}	ω^{18}	α^{4}	ω^{119}	α^{81}	ω^{93}	α^{31}	ω^{67}	α^{108}	ω^{41}
α^{58}	ω^{15}	α^{8}	ω^{116}	α^{85}	ω^{90}	α^{35}	ω^{64}	α^{112}	ω^{38}	α^{62}	ω^{12}	α^{12}	ω^{113}	α^{89}	ω^{87}
α^{39}	ω^{61}	α^{116}	ω^{35}	α^{66}	ω^{9}	α^{16}	ω^{110}	α^{93}	ω^{84}	α^{43}	ω^{58}	α^{120}	ω^{32}	α^{70}	ω^{6}
α^{20}	ω^{107}	α^{97}	ω^{81}	α^{47}	ω^{55}	α^{124}	ω^{29}	α^{74}	ω^{3}	α^{24}	ω^{104}	α^{101}	ω^{78}	α^{51}	ω^{52}
α^{1}	ω^{26}	α^{78}	ω^{127}	α^{28}	ω^{101}	α^{105}	ω^{75}	α^{55}	ω^{49}	α^{5}	ω^{23}	α^{82}	ω^{124}	α^{32}	ω^{98}
α^{109}	ω^{72}	α^{59}	ω^{46}	α^{9}	ω^{20}	α^{86}	ω^{121}	α^{36}	ω^{95}	α^{113}	ω^{69}	α^{63}	ω^{43}	α^{13}	ω^{17}

Table 5 Matrix M_3, the initial S-box generated after step C

0	128	118	210	108	111	92	212	169	121	44	125	30	182	165	87
147	242	189	17	237	105	251	194	116	208	34	178	239	156	181	19
199	180	62	138	4	186	149	123	102	160	56	254	223	61	64	59
66	45	12	132	191	75	163	97	72	37	104	99	201	248	207	43
20	146	193	226	229	174	209	15	177	39	82	190	88	176	60	65
74	91	38	222	122	67	211	134	255	150	225	41	68	79	215	170
106	196	135	198	124	27	08	83	42	57	197	240	112	204	183	33
137	168	141	25	24	142	126	113	70	154	153	05	217	29	155	69
151	144	40	63	139	230	195	101	171	238	98	130	173	93	185	200
120	234	157	73	76	188	253	109	175	09	247	49	203	23	129	127
167	107	221	31	14	152	241	216	16	85	84	47	131	89	233	03
110	11	18	236	26	95	48	21	245	162	133	35	50	117	187	81
54	228	46	184	80	166	22	232	143	148	86	244	205	07	90	192
114	13	249	250	58	246	145	218	243	136	94	103	231	51	159	202
02	55	78	1	179	214	28	164	235	53	32	220	161	158	06	206
219	252	213	224	36	115	52	71	96	77	227	119	10	140	100	172

Step C: Both the matrices M_1 and M_2 are not bijective. This issue is resolved by applying the following rule on M_2:

$$\mu^n \to \begin{cases} \mu^n & \text{if } \mu^n = \alpha^n \text{ and is even or } \mu^n = \omega^n \text{ and is odd} \\ \mu^n + 128 & \text{if } \mu^n = \alpha^n \text{ and is odd or } \mu^n = \omega^n \text{ and is even} \end{cases}$$

This will generate our initial proposed S-box M_3 (see Table 5). We found that M_3 has adequate cryptographic strength. Its average non-linearity score is 104.75.

The last procedural step **D** is carried out to improve the cryptographic quality of the initial S-box using the action of a permutation group $C_{6888} \times C_4 \times C_4$ of order 110,208.

Step D: Each permutation defined on a set $\{1, 2, 3, \ldots, 256\}$ of 256 elements reshuffles the entries of S-box. In this step, we consider the action of a group of permutations $C_{6888} \times C_4 \times C_4$ on M_3. The group $C_{6888} \times C_4 \times C_4$ is generated by 3 elements a,b, and c, where

a = (1,207,60,187,67,224,26,161,220,68,17,199,190,25,253,106,76,216,120,41,182,94, 39,200,123,112,252,131,95,219,236,212,158,256,29,107,97,111,99,130,167,217,166,247, 231,163,177,153,210,52,178,89,14,96,133,28,221,132,108,186,98,75,250,145,127,198,35, 30,141,19,232,121,113,159,116,79,214,230,58,59,244,4,9,110,78,191,18,246,82,180,203, 175,208,5,228,53,20,118,189,74,245,64,115,45,72,240,205,126,114,188,197,109,56,90,69, 184,149,211,237,124,24,65,117,248,209,238,249,15,49,2,148,242,85,93,73,33,233,57,105, 218,8,165,46,122,51,157,227,143,234,32,170,22,6,134,169,7,71,139,202,23,13,81,255,204).

b = (3,44,16,125,223,91,12,152,136,50,83,54,88,213,241,87,43,171,103,42,147,137,201, 146,70,251,47,34,31,101,229,40,62,239,55,77,36,86,63,104,142,235,162,192,254, 48,27,37,80,206,129,84,21,225,119,181,168,11,185,154,195,150,61,176,66,128,183,164, 196,160,140,92,102,173,172,174,10,151,135,193,38,144,194,155).

c = (100,179,243,222,138,156,226,215).

We have found the finite presentation

$$\langle a, b, c : a^{164} = b^{84} = c^8 = aba^{-1}b^{-1} = aca^{-1}c^{-1} = bcb^{-1}c^{-1} = 1 \rangle$$

of $C_{6888} \times C_4 \times C_4$ using GAP, a software to compute many group theoretic components.

It has 110,208 elements, written in the form of product its generators a,b, and c. A GAP structural description of $C_{6888} \times C_4 \times C_4$ is displayed in Fig. 1. The action of each element of $C_{6888} \times C_4 \times C_4$ on M_3 evolves an S-box. Following extensive analysis and investigation, it was discovered that the S-box related to $a^{47}b^7c^5 \in C_{6888} \times C_4 \times C_4$ has the highest NL score. This S-box is marked as our suggested S-box. (See Table 6). An overview of all S-boxes generated by group action is presented in Table 7 which indicates the strength of the action of $C_{6888} \times C_4 \times C_4$ on M_3.

3 Performance analyses

To assess the cryptographic quality of generated S-box, some widespread performance parameters, such as non-linearity, bit independence criterion, differential and linear approximation probabilities, and strict avalanche criterion, have been exploited. In this section, a brief discussion about these security analyses and their outcomes for proposed S-box has been present.

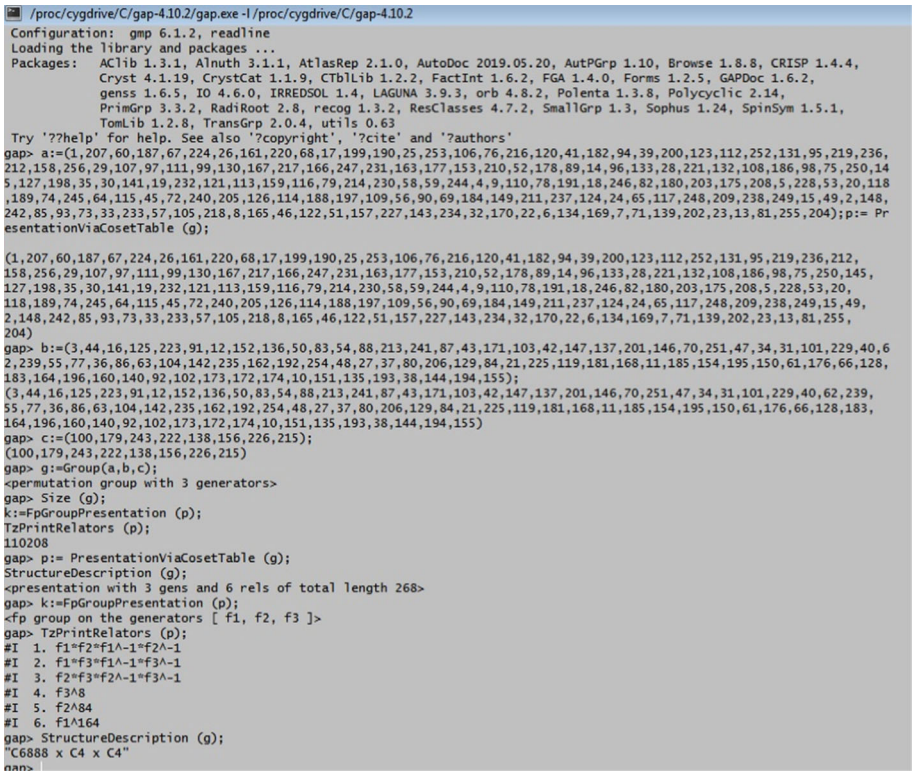

Fig. 1 A screenshot image of the GAP describing algebraic structure of $C_{6888} \times C_4 \times C_4$

3.1 Nonlinearity

An S-box is required to create a certain degree of disorder in the information to protect the data from various security attacks by unauthorized persons. The non-linearity analysis is utilized to test the ability of an S-box ψ to create confusion (Pieprzyk and Finkelstein 1988). Mathematically, it is defined as:

$$N(\psi) = {}_{a,b,c}{}^{min}\left\{y \in GF\left(2^8\right) : a, \psi(y) \neq b, y \oplus z\right\}$$

where $a \in GF\left(2^8\right), b \in GF\left(2^8\right)\backslash\{0\}$ and $c \in GF(2)$. A highly non-linear S-box can produce disarray in the Information. The average non-linearity of suggested S-box is 110.75, which is good enough to create confusion in the data. The NL of the proposed S-box is shown in Table 8 and comparison is done with recently developed S-boxes is in Table 9.

3.2 Strict avalanche criterion

To develop a secure cryptographic system, adequate avalanche effects are compulsory. Websters and Tavares originated the idea of strict avalanche criterion (Webster and Tavares 1985). Let $\alpha(z) : GF(2^n) \rightarrow GF(2)$ be a Boolean function. SAC is said to be satisfied, if by switching a single input bit the likelihood of a change in output bit is 50%. SAC is an important

Table 6 Proposed S-box generated after step D

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

Table 7 Analysis of Nonlinearity scores of all S-boxes generated by applying $C_{6888} \times C_4 \times C_4$ on M_3

Nonlinearity	< 100	≥ 100	≥ 105	≥ 106	≥ 107	≥ 108	≥ 109	≥ 110
Number of S-boxes	20,388	89,820	12,123	7899	1556	144	19	5

Table 8 Nonlinearity values of all Boolean functions of generated S-box

Boolean function	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
Score	112	110	110	112	112	110	110	112

Table 9 Performance comparison of different S-boxes

S-box	Nonlinearity			SAC	BIC-NL	DU	LP
	min	max	Mean				
Proposed S-box	110	112	110.75	0.5012	110.64	6	0.0781
AES (Daemen and Rijmen 1999)	112	112	112	0.5058	112	4	0.0625
Zhang et al. (2018)	108	110	108.75	0.4946	94	10	0.1328
Alzaidi et al. (2018b)	110	112	110.25	0.50	104	10	0.125
Khan et al. (2016)	84	106	100	0.4812	96	16	0.1796
Yong and Peng (2012)	108	110	109	0.5026	102	10	0.1406
Guesmi et al. (2014)	106	110	107.5	0.4971	196	10	0.125
Ahmad et al. (2015)	106	110	107	0.5015	98	10	0.1484
Tian and Lu (2016)	106	110	108	0 .5073	100	10	0.1523
Ahmad et al. (2016)	106	110	107.5	0 .5036	90	10	0.1484
Farah et al. (2017)	104	110	106.5	0.4995	98	10	0.1172
Ahmed et al. (2019)	106	108	107.5	0.4943	98	10	0.125
Khan et al. (2013)	100	106	105.5	0.4946	96	10	0.1328
Lambić (2014)	108	112	109.25	0.5012	104	8	0.0937
Lambić (2017)	106	108	106.75	0.5034	100	10	0.1328
Ullah et al. (2017)	106	108	106.75	0.4939	102	16	0.125
Jamal and Shah (2018)	106	108	107.25	0.5034	98	12	0.1328
Hussain et al. (2022)	110	112	11.50	0.4878	111.64	6	0.070
Özkaynak (2019b)	106	108	106.75	0.4941	98	10	0.125
Ye and Zhimao (2018)	104	108	106.75	0.4076	98	10	0.1328
Silva-García et al. (2018)	102	108	106	0.5066	96	12	0.1445
Yi et al. (2019)	106	110	107.75	0.4976	100	10	0.125
Alzaidi et al. (2018a)	108	110	109.5	0.4985	98	10	0.1328
Solami et al. (2018)	106	110	108.5	0.5017	100	10	0.1328
Hussain et al. (2020)	104	110	106.87	0.509	106.11	8	0.113

Table 10 SAC outcomes of generated S-box

0.5156	0.4844	0.5312	0.5156	0.5	0.5156	050	0.5312
0.4375	0.5	0.5156	0.4531	0.5469	0.5156	0.4688	0.4844
0.5	0.5469	0.5781	0.5312	0.5156	0.5469	0.5312	0.4844
0.4844	0.4531	0.4531	0.5625	0.5	0.5469	0.4531	0.5156
0.5625	0.5	0.5156	0.4219	0.5156	0.4844	0.5	0.5312
0.4531	0.5625	0.4375	0.5625	0.4531	0.5156	0.5469	0.4688
0.5156	0.4688	0.5156	0.4531	0.4688	0.4688	0.5312	0.4844
0.4375	0.4688	0.5	0.5156	0.4844	0.4688	0.5312	0.5156

characteristic of an S-box to counter various cryptographic attacks. A dependency matrix is utilized to compute value of SAC. The dependency matrix for the newly generated S-box is provided in Table 10. A substitution box is considered to fulfill the requirements of SAC if the average of all entries of the matrix is close to the ideal estimation of 0.5. The average score of SAC for our S-box is 0.5012. A comparison of the SAC values between generated S-boxes and different recently developed S-boxes is given in Table 9.

3.3 Output bits independent criteria

It is another important characteristic to determine the quality of S-boxes, which was presented in Webster and Tavares (1985). The close to the optimal score of BIC means that, for a given set of avalanche vectors generated by changing only one bit, the avalanche variables are pairwise autonomous. In (Webster and Tavares 1985), it is stated that for a Boolean mapping h_i and two bits output bit h_j, $h_i \oplus h_j$ should possess high value of non-linearity to guarantee the value of correlation coefficient of each output bit approximately zero when a single input bit is changed. The outcomes of BIC Test for non-linearity and SAC of generated S-box are presented in Tables 11 and 12 respectively. The average BIC non-linearity score our S-box is 110.64. The average of BIC-SAC is 0.4987, that is nearly equal to the optimal value 0.5. Thus, the generated S-box met the requirements of the BIC.

Table 11 BIC non-linearity values of suggested S-box

–	110	110	112	112	110	110	112
110	–	112	110	112	110	110	108
110	112	–	112	110	110	110	110
112	110	112	–	112	112	110	110
112	112	110	112	–	108	108	112
110	110	110	112	108	–	112	112
110	110	110	110	108	112	–	112
112	108	110	110	112	112	112	–

Table 12 BIC outcomes for SAC

–	0.4648	0.4961	0.5039	0.5137	0.5254	0.4883	0.4863
0.4648	–	0.4902	0.4961	0.5215	0.5273	0.4902	0.5
0.4961	0.4902	–	0.4863	0.4961	0.4863	0.4941	0.4805
0.5039	0.4961	0.4863	–	0.4883	0.4844	0.5195	0.5059
0.5137	0.5215	0.4961	0.4883	–	0.5078	0.5156	0.5176
0.5254	0.5273	0.4863	0.4844	0.5078	–	0.4688	0.5039
0.4883	0.4902	0.4941	0.5195	0.5156	0.4688	–	0.5039
0.4863	.5	0.4805	0.5059	0.5176	0.5039	0.5039	–

3.4 Differential uniformity

This important analysis was introduced by Biham and Shamir (Biham and Shamir 1991). The mapping from the input bits to the output bits is examined to calculate Differential Uniformity score. The focus of this test is on ensuring the different homogeneity. The input differential Δh should be uniquely associated with an output differential Δk. The mathematical formula to compute differential uniformity score is given as

$$DU = {}_{\Delta h \neq 0, \Delta k}{}^{\max}[\neq \{h \in I : S(h) \oplus S(h + \Delta h) = \Delta k\}]$$

The differential uniformity of newly constructed (See Table) is 4 which confirm its immense resistance ability to work against differential attacks.

3.5 Linear approximation probability

The purpose of this analysis is to determine the performance of an S-box to neutralize linear cryptanalysis (Matsui 1994). In this test, an imbalance of an event is examined and the maximum score is computed. Let γ be the set of all possible inputs, then the Linear approximation probability of an S-box is calculated by the following formula:

$$\mathrm{LP} = \max_{\beta_x, \beta_y \neq 0} \left| \frac{\#\{\gamma / \gamma \cdot \beta_x = S(\gamma) \cdot \beta_y\}}{2^n} - \frac{1}{2} \right|.$$

In the above expression, β_x and β_y denote input and output masks respectively. The maximum score of LP of the generated S-box is only 0.0781, which indicates its ability to counter different linear attacks.

4 Majority logic criterion for image protection assessment

The majority logic criterion (MLC) (Hussain et al. 2012) is the set of various analyses which include contrast, energy, entropy, correlation and homogeneity. The key motive of MLC is the examination of the statistical characteristics of substitution boxes during the process of encryption. We applied our S-box to encrypt digital images and validate its effective utilization in multimedia security and image encryption. During encryption process, the host image is altered and such alternations fix the quality of proposed technique. The similarity between both the images is determined in Correlation test. Notice, the smaller value of

Table 13 MLC outcomes of generated S-box

Criteria	Lena		Pepper		Baboon	
	Plain image	After encryption	Plain image	After encryption	Plain image	After encryption
Homogeneity	0.8817	0.4627	0.8659	0.4294	0.8403	0.4159
Correlation	0.9220	0.1093	0.9243	0.0600	0.8621	0.0426
Energy	0.1227	0.0184	0.1012	0.0168	0.1208	0.0175
Contrast	0.3563	9.2275	0.4359	9.6996	0.4089	10.5710
Entropy	7.4467	7.9564	7.5553	7.9566	7.2636	7.9553

Table 14 Vertical and Horizontal Correlation Matrices

Direction/image	Lena	Pepper	Baboon
Vertical			
Org	0.9073	0.9028	org: 0.8817
Enc	0.1192	0.0429	0.0307
Horizontal			
Org	0.9700	0.9315	0.8761
Enc	0.1760	0.0361	0.0493

correlation minimizes the likelihood of decrypting secret information. In host image, the loss of brightness can be assessed by contrast value. A secure encryption process demands its large value in an encrypted image. Entropy finds the measure of randomness in the encrypted image. The behavior and features of the enciphered image can be depicted by homogeneity and energy analysis. The plain images are encrypted using proposed S-box. We have chosen three standard gray images of *Lena*, Baboon, and Pepper with size 256×256 to perform MLC analysis. The outcomes of all MLC Tests are presented in Table 13. The computed correlation coefficients for images in Fig. 4 are given in Table 14. Figure 2 shows the outcomes of image encryption with the generated S-box. In Fig. 3, histograms of the original and encrypted images of *Lena*, Baboon, and Pepper are shown. The correlation plots for vertically and horizontally neighboring pixels in original and encrypted images are shown in Fig. 4. These outcomes certify that the generated S-box can be used for encryption applications effectively and is satisfactory enough to be included in the protocols meant for the safe communication of the confidential information.

5 Differential analysis of image protection

A robust cryptosystem is extremely sensitive to modifications in one bit of the plaintext. Through UACI and NPCR testing, the sensitivity of the system is assessed. UACI indicates the unified mean intensity change between original and encrypted image while NPCR calculates the number of pixels change rate of the encrypted image if a single pixel is altered in the

Fig. 2 Original and encrypted images

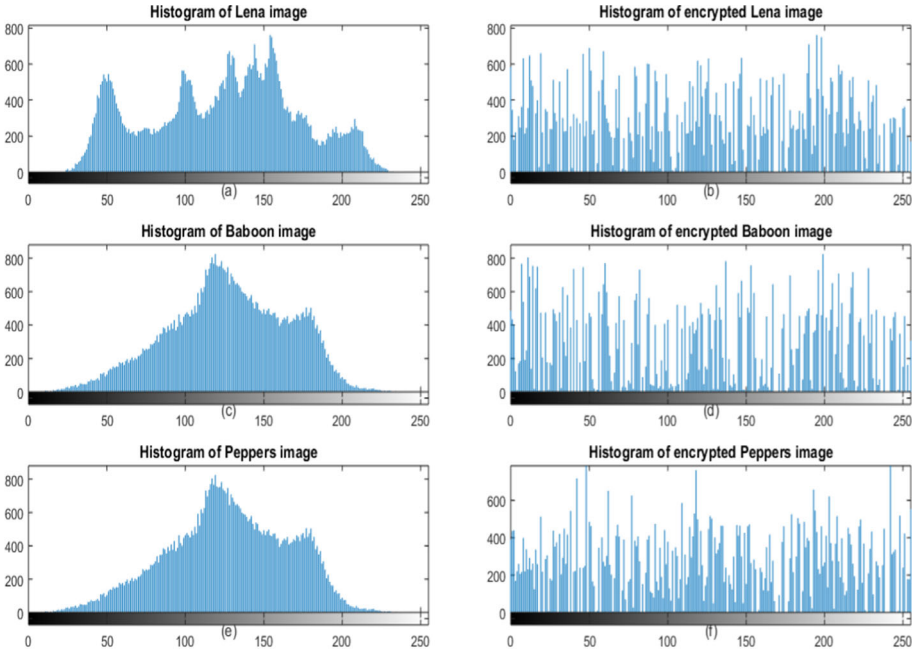

Fig. 3 Histogram analysis

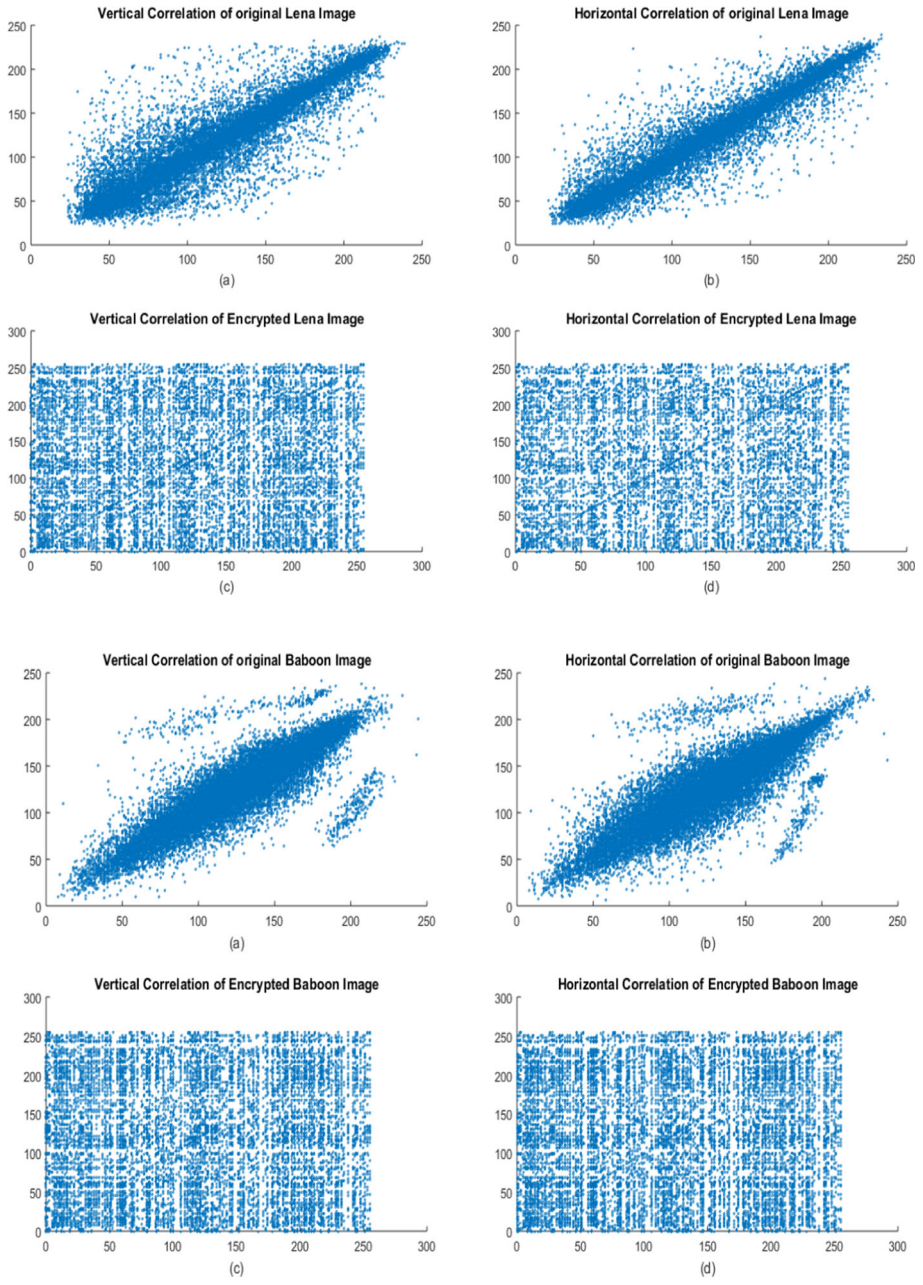

Fig. 4 Pixel correlation plots

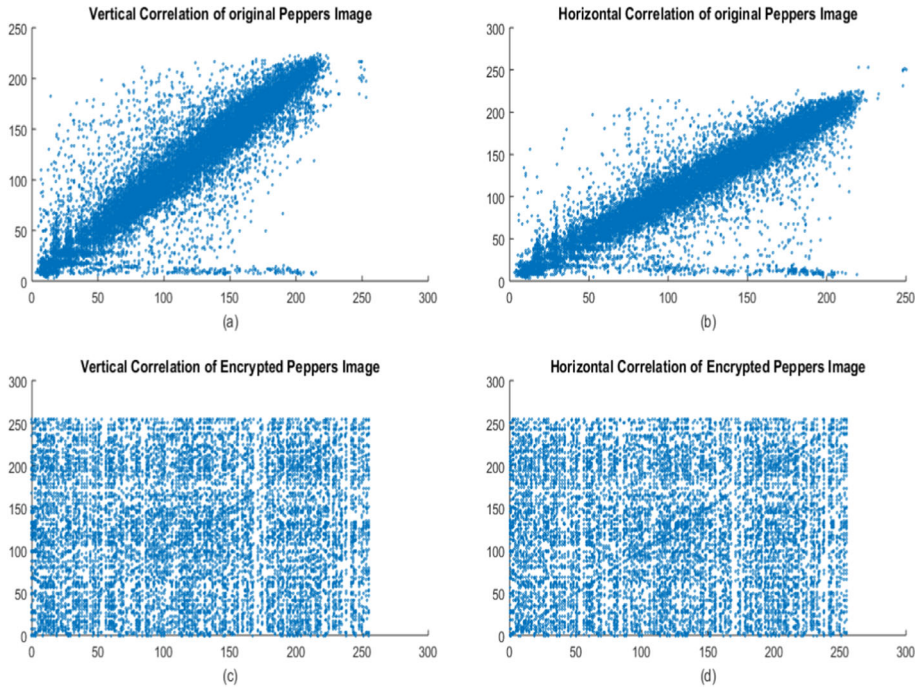

Fig. 4 continued

Table 15 NPCR, UACI and BACI outcomes

Image	NPCR (%)	UACI (%)	BACI (%)
Lena	99.87	28.83	17.57
Pepper	99.90	29.76	19.91
Baboon	99.81	27.53	18.03

original image. The following formulae are used to compute the values of UACI and NPCR:

$$\text{UACI} = \frac{1}{JK}\sum_{j,k}\frac{E_1(j,k) - E_2(j,k)}{255} \times 100\%$$

$$\text{NPCR} = \frac{\sum_{jk} D(j,k)}{JK} \times 100\%$$

where $E_1(j,k)$ and $E_2(j,k)$ denote the grayscale values of pixels obtained (j,k) th position and

$$D(j,k) = \begin{cases} 0 & \text{if } E_1(j,k) \text{ and } E_2(j,k) \text{ are equal} \\ 1 & \text{otherwise} \end{cases}.$$

The percentage score of UACI and NPCR, presented in Table 15, shows the quality of our S-box.

6 Conclusion

In this work, we have demonstrated a novel method to generate strong 8×8 S-boxes. In the literature, there are many 8×8 S-box generation proposals based on Galois field GF(2^8) of order 256. As far as we know, no one has applied a pair of Galois fields of order 128 to construct 8×8 S-box. In the 1st phase, we have generated an initial seed S-box with sufficient cryptographic strength with the help of two Galois fields of order 128. In 2nd phase, we consider the action of the permutation group $C_{6888} \times C_4 \times C_4$ on underlying S-box for additional improvement of its tensile strength and rigidity. After the S-box was developed, execution assessment is done to quantify its cryptographic quality. It is found that the generated S-box has excellent cryptographic qualities in comparison to other recent S-boxes. The results of various analyses showed that the generated S-box is suitable for cryptographic use, and proposed method is very effective to generate highly non-linear S-boxes. Thus, we conclude that our S-box is quite useful for information hiding schemes and various encryption approaches. In comparison to a single Galois field, the combination of two Galois fields produces more complexity and randomness. In future, we intend to use these robust S-boxes, developed by the proposed scheme, in multimedia security application including image encryption, audio and video steganography and watermarking.

Acknowledgements This work was supported by the EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia.

Data availability The data that support the findings of this study are openly available upon your request.

Declarations

Conflict of interest No conflict of interest exits in the submission of this work.

References

Ahmad M, Bhatia D, Hassan Y (2015) A novel ant colony optimization based scheme for substitution box design. Proc Comput Sci 57:572–580

Ahmad M, Mittal N, Garg P, Khan MM (2016) Efficient cryptographic substitution box design using travelling salesman problem and chaos. Perspect Sci 8:465–468

Ahmed HA, Zolkipli MF, Ahmad M (2019) A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. Neural Comput Appl 31(11):7201–7210

Altaleb A, Saeed MS, Hussain I, Aslam M (2017) An algorithm for the construction of substitution box for block ciphers based on projective general linear group. AIP Adv 7(3):035116

Alzaidi AA, Ahmad M, Doja MN, Al Solami E, Beg MS (2018b) A new 1D chaotic map and β-hill climbing for generating substitution-boxes. IEEE Access 6:55405–55418

Alzaidi, A. A., Ahmad, M., Ahmed, H. S., & Solami, E. A. (2018a). Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map. Complexity 2018a

Bhanot R, Hans R (2015) A review and comparative analysis of various encryption algorithms. Int J Secur Appl 9(4):289–306

Biham E, Shamir A (1991) Differential cryptanalysis of DES-like cryptosystems. J Cryptol 4(1):3–72

Daemen J, Rijmen V (1999) The Rijndael block cipher: AES proposal. In: First candidate conference (AeS1), pp 343–348

Farah T, Rhouma R, Belghith S (2017) A novel method for designing S-box based on chaotic map and teaching–learning-based optimization. Nonlinear Dyn 88(2):1059–1074

Farwa S, Shah T, Idrees L (2016) A highly nonlinear S-box based on a fractional linear transformation. Springerplus 5(1):1–12

Guesmi R, Farah MAB, Kachouri A, Samet M (2014) A novel design of Chaos based S-Boxes using genetic algorithm techniques. In: 2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA), IEEE, pp 678–684
Hussain I, Shah T, Gondal MA, Mahmood H (2012) Generalized majority logic criterion to analyze the statistical strength of S-boxes. Zeitschrift Für Naturforschung A 67(5):282–288
Hussain I, Shah T, Mahmood H, Gondal MA (2013) A projective general linear group based algorithm for the construction of substitution box for block ciphers. Neural Comput Appl 22(6):1085–1093
Hussain S, Jamal SS, Shah T, Hussain I (2020) A power associative loop structure for the construction of non-linear components of block cipher. IEEE Access 8:123492–123506
Hussain S, Shah T, Javeed A (2022) Modified advanced encryption standard (MAES) based on non-associative inverse property loop. Multimed Tools Appl 1–20
Jamal SS, Shah T (2018) A novel algebraic technique for the construction of strong substitution box. Wireless Pers Commun 99(1):213–226
Jamal SS, Anees A, Ahmad M, Khan MF, Hussain I (2019) Construction of cryptographic S-boxes based on mobius transformation and chaotic tent-sine system. IEEE Access 7:173273–173285
Javeed A, Shah T (2020) Design of an S-box using Rabinovich–Fabrikant system of differential equations perceiving third order nonlinearity. Multimed Tools Appl 79(9):6649–6660
Kazlauskas K, Kazlauskas J (2009) Key-dependent S-box generation in AES block cipher system. Informatica 20(1):23–34
Khan M, Shah T, Mahmood H, Gondal MA (2013) An efficient method for the construction of block cipher with multi-chaotic systems. Nonlinear Dyn 71(3):489–492
Khan M, Shah T, Batool SI (2016) Construction of S-box based on chaotic Boolean functions and its application in image encryption. Neural Comput Appl 27(3):677–685
Knudsen LR, Robshaw M (2011) The block cipher companion. Springer, Berlin
Lambić D (2014) A novel method of S-box design based on chaotic map and composition method. Chaos, Solitons Fractals 58:16–21
Lambić D (2017) A novel method of S-box design based on discrete chaotic map. Nonlinear Dyn 87(4):2407–2413
Lambić D, Živković M (2013) Comparison of random S-box generation methods. Publications De L'institut Mathematique 93(107):109–115
Makarim RH, Tezcan C (2014) Relating undisturbed bits to other properties of substitution boxes. International workshop on lightweight cryptography for security and privacy. Springer, Cham, pp 109–125
Matsui M (1994) Linear cryptanalysis method for DES cipher. Workshop on the theory and application of of cryptographic techniques. Springer, Berlin, pp 386–397
Özkaynak F (2019a) Chaos based substitution boxes as a cryptographic primitives: challenges and opportunities. Chaotic Model Simul 1:49–57
Özkaynak F (2019b) Construction of robust substitution boxes based on chaotic systems. Neural Comput Appl 31(8):3317–3326
Paar C, Pelzl J (2009) Understanding cryptography: a textbook for students and practitioners. Springer, Berlin
Picek S, Jakobovic D, Miller JF, Marchiori E, Batina L (2015) Evolutionary methods for the construction of cryptographic Boolean functions. European Conference on Genetic Programming. Springer, Cham, pp 192–204
Pieprzyk J, Finkelstein G (1988) Towards effective nonlinear cryptosystem design. IEE Proc E-Comput Digital Techn 135(6):325–335
Razaq A, Ullah A, Waheed A (2020) A novel technique to improve nonlinearity of substitution box without disturbing its mathematical properties. Wireless Pers Commun 111(4):2091–2105
Roslan MFB, Seman K, Ab Halim AH, Sayuti MNASM (2019) Substitution box design based from symmetric group composition. J Phys Confer Ser 1366(1):012001
Shahzad I, Mushtaq Q, Razaq A (2019) Construction of new S-box using action of quotient of the modular group for multimedia security. Secur Commun Netw 2019
Shamir A (2004) Stream ciphers: dead or alive?. In: ASIACRYPT
Silva-García VM, Flores-Carapia R, Rentería-Márquez C, Luna-Benoso B, Aldape-Pérez M (2018) Substitution box generation using Chaos: An image encryption application. Appl Math Comput 332:123–135
Solami AE, Ahmad M, Volos C, Doja MN, Beg MMS (2018) A new hyperchaotic system-based design for efficient bijective substitution-boxes. Entropy 20(7):525
Tian Y, Lu Z (2016) S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm. J Syst Eng Electron 27(1):232–241
Ullah A, Jamal SS, Shah T (2017) A novel construction of substitution box using a combination of chaotic maps with improved chaotic range. Nonlinear Dyn 88(4):2757–2769

Usama M, Rehman O, Memon I, Rizvi S (2019) An efficient construction of key-dependent substitution box based on chaotic sine map. Int J Distrib Sens Netw 15(12):1550147719895957

Webster AF, Tavares SE (1985) On the design of S-boxes. Conference on the theory and application of cryptographic techniques. Springer, Berlin, pp 523–534

Ye T, Zhimao L (2018) Chaotic S-box: six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. Nonlinear Dyn 94(3):2115–2126

Yi L, Tong X, Wang Z, Zhang M, Zhu H, Liu J (2019) A novel block encryption algorithm based on chaotic S-box for wireless sensor network. IEEE Access 7:53079–53090

Yong W, Peng L (2012) An improved method to obtaining S-box based on chaos and genetic algorithm. HKIE Trans 19(4):53–58

Zhang T, Chen CP, Chen L, Xu X, Hu B (2018) Design of highly nonlinear substitution boxes based on I-Ching operators. IEEE Trans Cybern 48(12):3349–3358