

Article

Group-Action-Based S-box Generation Technique for Enhanced Block Cipher Security and Robust Image Encryption Scheme

Souad Ahmad Baowidan ^{1,*}, Ahmed Alamer ² , Mudassir Hassan ³ and Awais Yousaf ^{3,*} 

¹ Information Technology Department, Faculty of Computing and IT, King Abdulaziz University, Jeddah 21589, Saudi Arabia

² Department of Mathematics, Faculty of Science, University of Tabuk, Tabuk 71491, Saudi Arabia; aalamer@ut.edu.sa

³ Department of Mathematics, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan; mudassirhassan423@gmail.com

* Correspondence: sbaawidan@kau.edu.sa (S.A.B.); awais.yousaf@iub.edu.pk (A.Y.)

Abstract: Data security is one of the biggest concerns in the modern world due to advancements in technology, and cryptography ensures that the privacy, integrity, and authenticity of such information are safeguarded in today's digitally connected world. In this article, we introduce a new technique for the construction of non-linear components in block ciphers. The proposed S-box generation process is a transformational procedure through which the elements of a finite field are mapped onto highly nonlinear permutations. This transformation is achieved through a series of algebraic and combinatorial operations. It involves group actions on some pairs of two Galois fields to create an initial S-box P_r Sbox, which induces a rich algebraic structure. The post S-box P_o Sbox, which is derived from heuristic group-based optimization, leads to high nonlinearity and other important cryptographic parameters. The proposed S-box demonstrates resilience against various attacks, making the system resistant to statistical vulnerabilities. The investigation reveals remarkable attributes, including a nonlinearity score of 112, an average Strict Avalanche Criterion score of 0.504, and LAP (Linear Approximation Probability) score of 0.062, surpassing well-established S-boxes that exhibit desired cryptographic properties. This novel methodology suggests an encouraging approach for enhancing the security framework of block ciphers. In addition, we also proposed a three-step image encryption technique comprising of Row Permutation, Bitwise XOR, and block-wise substitution using P_o Sbox. These operations contribute to adding more levels of randomness, which improves the dispersion across the cipher image and makes it equally intense. Therefore, we were able to establish that the approach works to mitigate against statistical and cryptanalytic attacks. The PSNR, UACI, MSE, NCC, AD, SC, MD, and NAE data comparisons with existing methods are also provided to prove the efficiency of the encryption algorithm.

Keywords: group structure; block ciphers; Galois fields; group action; S-box

MSC: 11T71; 13B25



Citation: Baowidan, S.A.; Alamer, A.; Hassan, M.; Yousaf, A. Group-Action-Based S-box Generation Technique for Enhanced Block Cipher Security and Robust Image Encryption Scheme. *Symmetry* **2024**, *16*, 954. <https://doi.org/10.3390/sym16080954>

Academic Editor: Zhunga Liu

Received: 27 June 2024

Revised: 13 July 2024

Accepted: 17 July 2024

Published: 25 July 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Cryptography is a complicated mix of art and science that makes sure communication is safe. It has been around for a long time, evolving and altering as the requirements for information security have increased. From ancient times to the present day, this historical journey has seen many significant shifts that have formed the foundations on which current cryptographic systems are based. During this journey, important individuals and circumstances have left an indelible impression on the convoluted depiction of the cryptographic endeavor. The legendary Julius Caesar has been associated with founding cryptography. In “Commentarii de bello Gallico” [1], he used the Caesar cipher to protect messages. This was the first known use of encoding to ensure privacy. This basic scheme established the

groundwork for later evolutionary paths in cryptography techniques. Moving forward to the current day, the “Handbook of Applied Cryptography” [2], written by A. Menezes and colleagues, appears to be a comprehensive reference that summarizes the abundance of knowledge accumulated over centuries in the field of cryptography. This handbook is a solid foundation for both researchers and professionals working in the complex field of cryptography. It covers both basic theory and real-world uses. The seminal work “Communication Theory of Secrecy Systems” by Claude Shannon demonstrates the profound impact of information theory on the foundations of cryptography [3]. Shannon’s groundbreaking ideas carefully built the mathematical foundations for cryptography, highlighting how important entropy and information theory are. The era of standards in cryptography rose to prominence when digital communication became common. The National Institute of Standards and Technology (NIST) played a key part, which was made clear by the Data Encryption Standard (DES) in FIPS PUB 46-3 [4]. Even though DES is considered old-fashioned now, it was a huge step forward in the history of cryptographic methods. The Advanced Encryption Standard (AES) emerged at the turn of the millennium and was well documented in “The Design of Rijndael: AES-The Advanced Encryption Standard” [5] by J. Daemen and V. Rijmen. As a result of international competition and collaboration, AES became the standard for encryption, making it safer to communicate in a wide range of settings. Asymmetric key exchange was first proposed in Diffie and Hellman’s landmark work, “New Directions in Cryptography” [6], which introduced public-key cryptography and caused a paradigm shift. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems” [7] by R. Rivest et al. explains how this important work paved the way for later achievements, such as the creation of digital signatures and public-key cryptosystems. The development of elliptic curve cryptography (ECC) considerably broadened the field of encryption. The article “Use of Elliptic Curves in Cryptography” [8] by V. S. Miller and the in-depth look at elliptic curves in “Handbook of Elliptic and Hyperelliptic Curve Cryptography” [9] by Cohen H. et al. both highlighted their speed and safety benefits. Without recognizing the crucial function of cryptography machines, the historical tapestry would be incomplete. The books “The Enigma Machine” [10] by Smart, N. P., & Smart, N. P and “How Polish Mathematicians Deciphered the Enigma” [11] by M. Rejewski, tell interesting stories about the Enigma machine, which was a great piece of cryptography that played a big role in World War II. Differential cryptanalysis and timing attacks are two new threats that came up as encryption systems improved. The writings of E. Biham and A. Shamir on “Differential Cryptanalysis of the Data Encryption Standard” [12] and P. Kocher et al. on “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems” [13] are very helpful in understanding these holes. Recently, people have paid more attention to hash functions, like the Secure Hash Standard (SHS) described in FIPS PUB 180-4 [14]. This effort by NIST to standardize things shows that work is still being done to make secure basics stronger against new threats. Yousaf, Razaq, and Baig present a revolutionary lightweight picture encryption technique that takes cues from the Rubik’s Revenge cube [15]. Panchami and Mathews concentrate on protecting the Internet of Things by using customized replacement boxes for lightweight ciphers [16], whereas Das, Kar, Deb, and Singh introduce bFLEX- γ , a lightweight block cipher that uses a probability density function in conjunction with a key cross method [17]. Razaq, Ahmad, Yousaf, and associates investigate highly nonlinear substitute boxes for image encryption [18] and group theoretic designs of AES-like substitution boxes [19]. Besides, in relation to block ciphers, several approaches to generating S-boxes have been considered, such as chaos theory, optimization, and mathematical transformations. All of them have their own strengths and weaknesses. Cryptographic methods that employ chaotic systems rely on chaos’ stochasticity and sensitivity to initial conditions to generate highly non-linear and intricate S-boxes. These methods can help to achieve very good cryptographic characteristics including a high level of nonlinearity and protection against linear or differential cryptanalysis. But they also may exhibit implementation complexity and dependency on some pa-rameters [20]. Additional recent works of Liu et al. (2023) and

Zhang et al. (2024) have also extended to investigate more on the usage of chaotic systems in S-box generation and suggested that it offers great strength and effectiveness [21,22]. In this realm, some optimization techniques including genetic algorithm, particle swarm optimization, and heuristic optimization techniques help provide guidelines on how to generate sets of S-boxes that meet certain cryptographic requirements. These techniques may generate S-boxes with optimal traits, but their computational complexity is relatively high, and they are not always able to provide the best results [23]. Some notable works in this direction are by Kuznetsov et al. (2024) and Feng et al. (2024), where optimization methodologies for S-box design have been enhanced [24,25]. Symmetrical permutations associated with group theory and Galois fields offer a systematic and more formal way of achieving S-box generation. It can surely provide good algebraic properties and resilience to numerous cryptanalytic threats. However, they may involve the use of more advanced mathematical problems, which may be slightly difficult to solve and be able to implement when required [26]. Yousaf et al. in their latest work and Razaq et al. in their formal analysis targeted elaborate mathematical transformations that improve S-box security and performance [27,28]. In the recent past, various methods of generating the S-box have been generated using optimization techniques. These approaches are designed to improve the cryptographic characteristics of linear transformations, namely nonlinearity, avalanche effect, and immunity to differential and linear cryptanalysis attacks. For example, the Particle [29] Swarm Optimization (PSO) simulating the bird flocking process for the optimization of S-box parameters is associated with viewing the problem from other angles to reach a better solution that the conventional approach based solely on the mathematical analysis of Boolean functions could not achieve; thus, the introduction of new nonlinearity and immunity to attacks on S-box. Among specified meta-heuristic approaches [30], the Whale Optimization Algorithm (WOA), derived from the hunting pattern of humpback whales, exhibits both effective exploration and exploitation leading to the creation of highly non-linear S-boxes with desirable cryptographic characteristics. Genetic Algorithm (GA), inspired by natural selection and genetics, offers an evolution from a set of S-boxes with improved features by controlling crossover and mutations. Sine Cosine Algorithm (SCA) [31] which uses sine and cosine functions as a method to update solutions offers a good way of attaining the near-optimal S-boxes with the proposed security properties. However, as mentioned earlier, these optimization methods also have some drawbacks. They tend to use a lot of computational power and fine-tuning of the parameters to get the best outcome. In addition, these algorithms involve a stochastic approach for generating S-boxes and the quality of the generated S-boxes may vary as a result. On the other hand, the approach described in this paper uses group actions on Galois fields in combination with Heuristic Group-based Optimization which gives a more structured and deterministic S-boxes generation. This method guarantees high nonlinearity and resistance to various types of attacks and does not require significant computing resources. The S-boxes derived from our approach have better cryptographic characteristics, including a nonlinearity of 112 and an average of the Strict Avalanche Criterion (SAC) of 0.504, which is higher than that of the S-boxes obtained by using traditional optimization algorithms. Therefore, our method also solves the problems of computational complexity and variability and improves the overall security concept of block ciphers. The detailed analysis proves that the given S-box is more efficient than the data encryption standards for secure communication. This new idea is not only a great step forward in block ciphering security but also progress in the formation of cryptographically protected systems.

1.1. Motivation

This research is motivated by the need to constantly strengthen cryptographic techniques to protect against evolving cyber threats in today's digital world. The project aims to enhance cryptographic security by developing unique substitution boxes (S-boxes) that focus on non-linear components. This is motivated by the significant importance of block ciphers, such as AES, in various applications. This work aims to provide a new approach by

embracing abstract algebra, in particular Group theory, and using mathematical concepts like group actions and Galois fields. The pursuit is motivated by a desire to discover new and creative methods that go beyond traditional approaches, in order to tackle the ever-changing issues in cryptography design and improve the strength and reliability of cryptographic systems.

1.2. Contribution

This research significantly contributes to the academic discussion on cryptographic design by offering a novel method for creating non-linear components, notably substitution boxes, in block ciphers. The incorporation of abstract algebra, namely Group theory, in conjunction with mathematical structures such as Galois fields and group actions, represents a significant advancement in the foundational principles of cryptographic techniques. Implementing Heuristic Group-based Optimization enhances the practicality of the suggested methodology. The security study, evaluated using statistical tests such as SAC, LP, and DP, yields measurable numbers that confirm the effectiveness of the created substitution box according to sophisticated cryptographic standards. This research enhances the development of cryptographic design principles by combining theoretical depth and practical applicability to effectively tackle the current issues in safeguarding digital communication.

1.3. Preliminaries

As a preliminary, the study of this article consists of the concepts of polynomials, especially irreducible polynomials, and a finite field named Galois field. Particularly, the irreducible polynomials of degree 7 and the generated Galois field will be discussed so that we can easily understand the next section.

1.4. Irreducible Polynomials

Consider, $\mathbb{Z}_2[y]$, a ring of all polynomials with coefficients in $\mathbb{Z}_2$, under operation of polynomials addition and multiplication. Then a nonconstant polynomial $g(y) \in \mathbb{Z}_2[y]$ is an irreducible polynomial over $\mathbb{Z}_2$, if it cannot be written as product of two polynomials $f(y)$ and $h(y)$ in $\mathbb{Z}_2[y]$ where the degree of both polynomials $f(y)$ and $h(y)$ is less than that of $g(y)$ or if $g(y)$ is divisible by itself and constant only. The polynomial, $y^7 + y^3 + 1$, is an irreducible polynomial of degree 7 over field $\mathbb{Z}_2$, because it cannot be expressed as a product of two or more polynomials.

1.5. Galois Field

A Galois field, also known as a finite field, is a field which contains finite number of elements. Consider an irreducible polynomial $g(y)$ of degree n over $\mathbb{Z}_p$. The Galois field generated by this irreducible polynomial is denoted by $\text{GF}(p^n)$, for $n > 1$ and a prime p . The elements of this field are polynomials of degree less than n , whose coefficients belong to $\mathbb{Z}_p$. The order of this field is p^n . The addition and multiplication is the same as that of polynomials modulo $g(y)$. The Galois field generated by an irreducible polynomial of degree 7 over $\mathbb{Z}_2$ is denoted by $\text{GF}(2^7)$ and it contains 128 polynomials of degree less than or equal to $n - 1$.

2. Proposed Approach for S-box Design

Recently, many researchers have used Abstract Algebra and its application for construction of strong S-boxes, because many groups and fields have the capability to offer strong cryptographic-suited features. Fields possess the competence to generate randomness in output, distinctly and are non-periodic in nature. This helps in achieving some aspects of cryptographic system, i.e., confusion and diffusion. Due to these benefits, we design through unique composition of the elements of two Galois fields and its inverses, to generate cryptographically strong S-box and which further can be utilized by using group action. This work's primary goal is to strengthen the S-box's security by adding further security measures.

This process for generating dynamic S-box consists of five steps:

- Unique Compositions of two Galois fields.
- Induce an inverse map for two Galois fields.
- P_r S-box construction
- Heuristic Group-based Optimization.
- P_o S-box construction.

2.1. Unique Composition of Two Galois Fields

For any irreducible polynomial $p(y)$ of degree 7, the ring $\frac{\mathbb{Z}_2[y]}{\langle p(y) \rangle} = \{a_6y^6 + a_5y^5 + \dots + a_1y + a_0 | a_0, a_1, \dots, a_5, a_6 \in \mathbb{Z}_2\}$ is a finite field of order 128 and is denoted by $GF(2^7)$. For the construction of S-box, consider two Galois fields of order 128 evaluated through irreducible polynomials $p_1(y)$ & $p_2(y)$. The two sets of the elements of Galois field namely $\mathcal{E}p_1(y)$ and $\mathcal{E}p_2(y)$ are generated using $p_1(y)$ and $p_2(y)$, respectively.

2.2. Inducing Inverse Map

For the construction of the Proposed S-box, let us induce an inverse map $F_k : GF(2^7) \rightarrow GF(2^7)$ defined by

$$F_k(u) = \begin{cases} u^{-1} & , u \neq 0 \\ 0 & , u = 0 \end{cases} \quad (1)$$

where u^{-1} is the inverse of an element u by using irreducible polynomial $p_k(y)$, for $k = 1, 2$.

2.3. P_r S-box Construction

Algorithm 1 provides a comprehensive explanation of the process that was outlined for the development of the P_r S-box.

The comprehensive procedure for the construction of the Pre S-box is interpreted in the flowchart depicted in Figure 1. The resultant P_r Sbox, generated through the application of the algorithm described above, is presented in Table 1.

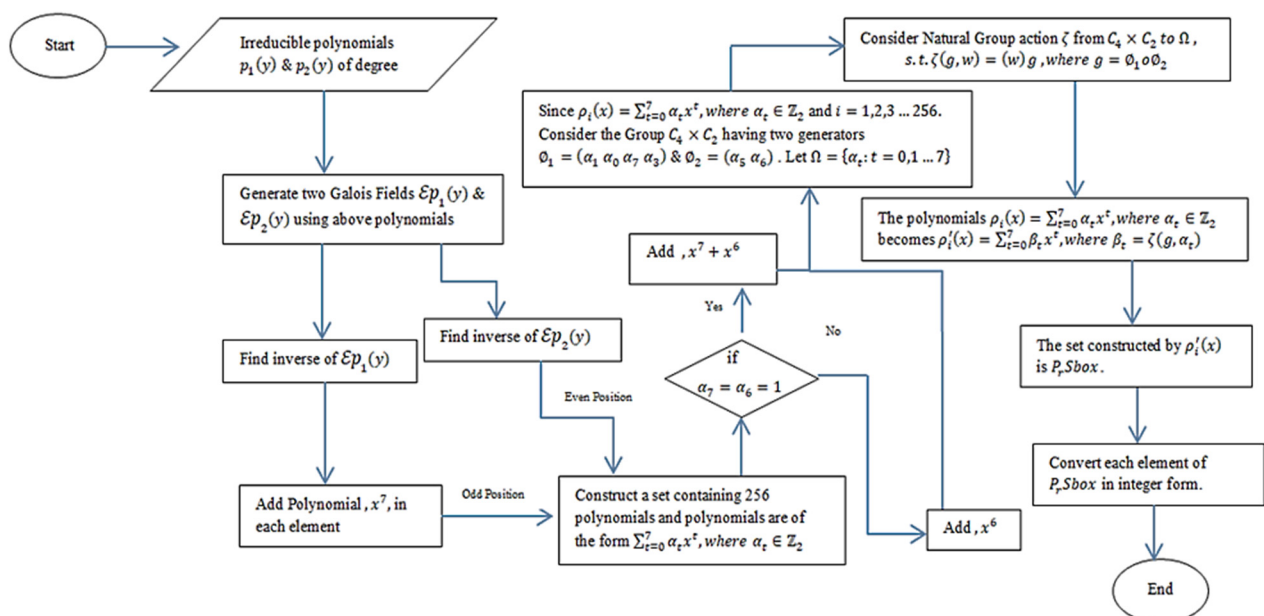


Figure 1. Flow Chart of Construction of P_r S-box.

Algorithm 1: PrS-box Construction

```

00  Initialization
01  Input:      Two irreducible polynomials  $p_1(y)$  and  $p_2(y)$  in  $\mathbb{Z}_2^7[y]$ .
02               $p_1(y) = y^7 + y^3 + 1$ 
03               $p_2(y) = y^7 + y^6 + y^5 + y^4 + y^2 + y + 1$ 
04  Output:    PrS-box
05
06  Compute Inverses:
07               $\mathcal{E}p_1(y^{-1}) = \text{InverseElements}(p_1(y))$ 
08               $\mathcal{E}p_2(y^{-1}) = \text{InverseElements}(p_2(y))$ 
09
10  Define  $\mathcal{E}p_3(y^{-1})$ :
11              Take  $\wp(y) = y^7$  of  $\text{GF}(2^8)$ 
12               $\mathcal{E}p_3(y^{-1}) = \wp(y) + \mathcal{E}p_1(y^{-1})$ .
13
14  Index Set and Element Representation:
15              For  $j = 1$  to 128:
16                   $g_j$  are the elements of  $\mathcal{E}p_3(y^{-1})$ 
17                   $h_j$  are the elements of  $\mathcal{E}p_2(y^{-1})$ 
18               $\text{In}_{\text{sbox}} = \begin{cases} I_{2j} = g_j \\ I_{2j-1} = h_j \end{cases}$ 
19
20  Define  $\rho_i(y)$ :
21              For each element in  $\text{In}_{\text{sbox}}$ 
22                   $\rho_i(y) = \sum_{t=0}^7 \alpha_t y^t$ , where  $\alpha_t$  is in  $\mathbb{Z}_2$ 
23              Update  $\text{In}_{\text{sbox}}$ :
24                   $\text{In}_{\text{sbox}} = \begin{cases} \rho_i(y) + y^6 + y^7 & \text{if } \alpha_7 = \alpha_6 = 1 \\ \rho_i(y) + y^6 & \text{otherwise} \end{cases}$ 
25
26  Define  $\Omega = \{\alpha_t : t = 0, 1, \dots, 7\}$  and group  $C_4 \times C_2$ :
27               $\Omega = \{\alpha_t : t = 0, 1, \dots, 7\}$ 
28               $C_4 \times C_2 = \langle \varphi_1, \varphi_2 \rangle$ , where
29                   $\varphi_1 = (\alpha_1 \alpha_0 \alpha_7 \alpha_3)$ 
30                   $\varphi_2 = (\alpha_5 \alpha_6)$ .
31              Natural group action  $\zeta$  from  $C_4 \times C_2$  to  $\Omega$ ,
32                   $\zeta(g, w) = (w)g$ , where  $g = \varphi_1 \circ \varphi_2$ 
33
34  Convert  $\rho_i(y)$  to  $\rho_i'(y)$  and PrS-box
35              For each term in  $\rho_i(y)$  compute  $\beta_t = \zeta(g, \alpha_t)$ .
36                  Construct  $\rho_i'(y)$  using the obtained  $\beta_t$  values
37                  PrS-box is the integer form of each polynomial of  $\rho_i'(y)$ .
38  End

```

Table 1. Constructed P_r S-box.

40	32	168	160	04	219	82	25	105	13	106	201	126	226	23	74
184	225	134	220	60	11	212	93	63	207	21	114	239	116	58	224
06	75	42	183	65	136	00	72	43	228	84	27	87	243	121	140
175	14	111	31	235	54	251	95	145	51	20	223	46	203	149	176
109	244	03	167	44	92	234	34	248	155	01	52	104	112	131	90
172	202	233	37	123	230	59	205	255	77	71	99	186	154	47	113
129	101	108	218	189	231	215	26	144	39	133	96	146	247	19	89
198	166	194	79	107	12	187	53	45	15	151	152	199	217	110	117
185	200	193	49	236	94	120	216	41	115	210	181	16	36	252	73
22	29	85	158	232	35	237	221	56	50	170	159	192	118	68	24
05	143	124	246	148	161	62	91	190	206	17	204	174	10	191	30
147	241	125	103	253	180	18	100	02	157	213	138	173	178	254	142
196	177	07	08	57	141	128	164	135	78	64	156	211	102	67	227
70	165	250	98	197	48	83	55	66	76	122	28	238	242	127	38

Table 1. Cont.

81	222	214	137	80	245	86	119	188	97	171	162	130	163	150	139
169	229	132	240	195	153	69	33	209	09	208	88	61	179	249	182

2.4. Enhancing S-box Non-Linearity through Heuristic Group-Based Optimization

The optimization of S-boxes is essential for developing strong and secure cryptographic systems. Recently, a strategy for carefully adjusting non-linearity based on a group's action on the P_r S-box has been developed because of a rigorous algorithmic search. Consider, the Abelian group $C_{24,483,888} \times C_{156} \times C_{78} \times C_2 \times C_2$, of order 1,191,679,796,736. This group is generated by nine generators $\langle u, v, w, x, y, z, s, t, r \rangle$, where the specific mappings for these generators are shown in Table 2.

Table 2. Group Generators in terms of Permutations.

u :	(1, 117, 102, 83, 106, 199, 254, 64, 53, 206, 119, 154, 18, 109, 90, 39, 85, 54, 27, 128, 160, 13, 153, 49, 237, 171, 62, 110, 2, 239, 236, 177, 6, 175, 107, 5, 162, 61, 42, 21, 253)
v :	(3, 105, 217, 226, 179, 19, 123, 189, 193, 47, 9, 235, 59, 135, 142, 230, 247, 234, 87, 66, 34, 74, 98, 93, 78, 214, 113, 185, 161, 24, 168, 97, 204, 28, 115, 223, 73, 29, 228, 208, 157, 225, 121, 150, 58, 146, 111, 20, 221, 75, 70, 57, 176, 229, 188, 156, 92, 167).
w :	(4, 116, 158, 12, 190, 255, 170, 186, 149, 129, 211, 205, 63).
x :	(7, 198, 103, 30, 52, 173, 183, 14, 218, 148, 191, 151, 114, 244, 224, 245).
y :	(8, 196, 71, 10, 11, 118, 169, 249, 68, 120, 212, 227, 133, 182, 108, 145, 233, 209, 174, 96, 202, 137, 55, 95, 192, 15, 94, 184, 130, 91, 81, 246, 203, 242, 134, 79, 37, 124, 232, 210, 104, 152, 45, 181, 248, 100, 132, 231, 26, 56, 195, 159).
z :	(16, 163, 240, 238, 88, 89, 50, 141, 51, 67, 136, 213, 80, 164, 143, 172, 243, 140, 17, 60, 147, 126, 241, 125, 84, 32, 69, 23, 250, 33, 38, 252, 166).
s :	(22, 43, 155, 178, 48, 99, 144, 216, 251, 165, 187, 131, 256, 219, 101, 122, 220, 139, 40, 197, 35, 65, 194, 112, 180, 31).
t :	(25, 127, 46, 44, 138, 86).
r :	(36, 200, 201, 41, 76, 222, 207, 82, 215).

The cyclic subgroup of $C_{24,483,888} \times C_{156} \times C_{78} \times C_2 \times C_2$, with an order of 24,483,888, has been determined to be relevant for the desired purpose after thorough experiments and simulations. The determined algebraic groups, along with their corresponding actions, are expressed as follows: This action can be defined as: $CSG \times I_{\Omega_i} \rightarrow I_{\Omega_i}$, where $i = 1, \dots, 256$; defined as, for fixed $g \in G$, $\mu(g, \omega) = (\omega)_{\varrho_g}$, $\omega \in I_{\Omega_i}$. The action of each element/permutation of the cyclic subgroup CSG on the index set of P_r S-box provides a distinct P_o S-box. It has been discovered via extensive investigation and analysis that the S-box associated with the constituent $g = u^{29}v^{43}w^8x^5y^{23}z^{16}s^3t^5r^8 \in CSG$ has the largest average non-linearity value. These specific powers were chosen after a thorough heuristic search, with an emphasis on their distinctive role in the non-linearity optimization. Hence, by establishing a bijection from I_{Ω_i} to P_r S-box, we obtain the S-box P_o S-box, as depicted in Algorithm 2, with its results presented in Table 3.

Table 3. Constructed P_o S-box.

225	61	245	249	179	233	237	71	48	64	229	232	191	215	234	181
139	130	75	125	187	89	197	51	110	23	162	238	30	38	177	03
246	127	210	164	180	252	247	15	52	102	103	115	113	27	112	84
04	199	224	195	24	150	68	154	196	144	02	163	235	228	178	117
72	194	44	152	216	173	153	34	145	248	151	242	104	227	236	06
209	83	00	111	32	63	114	217	169	203	190	120	137	13	25	207
19	239	170	251	193	77	240	70	69	123	128	253	17	60	222	42
81	226	01	206	146	94	56	119	62	182	155	96	16	255	243	147
79	12	208	47	221	214	05	212	07	230	189	124	37	93	88	241
33	66	205	31	160	168	18	10	133	175	58	20	159	157	200	219
35	176	184	136	73	132	36	29	131	211	46	161	82	86	39	121
231	11	244	109	78	87	141	106	45	149	55	171	101	185	174	08

Table 3. Cont.

186	57	100	172	28	166	54	135	43	95	53	220	201	126	202	138
49	188	118	165	09	192	183	140	97	116	213	122	134	67	92	158
99	59	26	80	105	91	142	22	218	156	198	107	143	85	40	223
14	98	74	76	254	167	129	41	65	90	108	204	50	21	250	148

Algorithm 2: Heuristic Group-based Optimization

```

00  Initialization:      P0S-box
01  Input:              Define generators: group_generators = < u, v, w, x, y, z, s, t, r >
02                    Construct group over group_generators: abelian_group
03  Heuristic Search:
04                    Loop through each generator and its powers
05                    For each power of the generator, generate the subgroup
06                    |   subgroup = CyclicSubgroup(Multiple of generator^power)
07                    |   Take the Action of Subgroup on PrS-box
08                    |   Calculate non-linearity of temp_S-box
09                    |   If the non-linearity > current maximum, update the maximum
10  Result Display:
11                    Display the highest non-linearity subgroup
12                    Display the P0S-box
13                    Display the mappings for generators:
14                    |   u : (1, 117, 102, 83, ...)
15                    |   v : (3, 105, 217, 226, ...)
16                    |   w : (4, 116, 158, 12, ...)
17                    |   x : (7, 198, 103, 30, ...)
18                    |   y : (8, 196, 71, 10, ...)
19                    |   z : (16, 163, 240, 238, ...)
20                    |   s : (22, 43, 155, 178, ...)
21                    |   t : (25, 127, 46, 44, ...)
22                    |   r : (36, 200, 201, 41, ...)
23                    Display the generator of CyclicSubgroup
24  End:

```

Algorithm 2 discussed earlier helps us to generate a Post S-box, which we refer to as P_0 S-box. The tabulated form of P_0 S-box can be found in Table 3. This algorithm precisely outlines the systematic process of generating and constructing the Post S-box, explaining the resulting cryptographic component in a logical and scientific way.

3. Analysis of Proposed S-box

The development of a new S-box constitutes a significant contribution to the field of data security. Here, we analyze the performance parameters of our proposed S-box to assess its strength and its efficacy in countering various algebraic attacks. The following are the criteria established for evaluating the strength of the S-box:

- NL—Nonlinearity
- SAC—Strict Avalanche Criterion
- BIC—Bit Independent Criterion
- Input/output XOR Distribution
- LP—Linear Approximation Probability
- DP—Differential Approximation Probability

3.1. Non-Linearity (NL)

One essential component in modern cryptographic methods for determining an S-box's effectiveness is nonlinearity. It guarantees that output is not a linear combination of input vectors. Furthermore, by adding complexity and resistance to assaults, nonlinearity plays a

critical role in improving security and secrecy in image encryption methods. Equation (2) is used to find the value of nonlinearity for a Boolean function φ .

$$N_L(\varphi) = 2^{m-1} - \frac{1}{2}(S_{max}(\varphi)) \quad (2)$$

where, $S_{max}(\varphi)$ = Walsh-Hadamard Spectrum of Boolean function φ having m bits.

The nonlinearity value for different Boolean functions of P_oS – box is given in Table 4.

Table 4. Nonlinearity score for P_oS – box.

Boolean function	f ₁	f ₂	f ₃	f ₄	f ₅	f ₆	f ₇	f ₈
NL Score	112	112	112	112	112	112	112	112

Table 5 displays P_oS – box’s minimum, maximum, and average nonlinearity ratings as well as those of more modern designs. Table 4 makes it evident that the Proposed S-box, with its Nonlinearity scores (min, max, and avg.) of 112, is greater than the bulk of the others. An analysis is conducted to contrast the suggested S-box with a few well-known S-boxes, such as AES [5], APA [32], and Gray [33]. It demonstrates how resilient the proposed S-box is to assaults such as linear cryptanalysis.

Table 5. Recent S-boxes and nonlinearity (NL) values.

S-box	Min. NL	Max. NL	Avg. NL
Proposed	112	112	112.00
Ref. [34]	98.0	106	102.75
Ref. [35]	110	112	110.25
Ref. [36]	110	112	111.50
Ref. [37]	108	111	110.00
Ref. [5]	112	112	112.00
Ref. [38]	112	114	112.25
Ref. [32]	112	112	112.00
Ref. [33]	112	112	112.00
Ref. [39]	106	108	106.50
Ref. [40]	106	108	106.50
Ref. [41]	106	108	106.75
Ref. [42]	106	108	106.80
Ref. [43]	106	110	108.00
Ref. [44]	108	110	109.75
Ref. [45]	98.0	106	103.75
Ref. [46]	110	112	110.75
Ref. [30]	112	112	112.00
Ref. [29]	110	112	110.50

3.2. Strict Avalanche Criterion (SAC)

Strict Avalanche Criterion plays a very significant role in the context of cryptographic functions like hash function and other block ciphers because it helps to ensure that the cryptographic function has a high level of diffusion and provides security against various attacks. This was first presented by Tavares and Webster [47]. It is the property that very small changes in input data result in significant and unpredictable changes in output. To comply with the criterion, that even a single bit of input change should result in a 50% of output bits changing. This criterion makes it highly sensitive to the input variations. To compute the SAC score of S-box, a dependency matrix is used. Its values for the Proposed S-box are calculated in Table 6. The ideal score of the SAC value for an S-box is considered as 0.5. The Proposed S-box has an average SAC value of 0.5049 which meets the required criterion.

Table 6. BIC – SAC Values for P_0S – box.

-	0.4844	0.4980	0.4648	0.5098	0.4941	0.5039	0.4941
0.4844	-	0.5098	0.4883	0.4980	0.5312	0.4922	0.4922
0.4980	0.5098	-	0.5273	0.4961	0.5215	0.4902	0.5000
0.4648	0.4883	0.5273	-	0.4668	0.5195	0.4883	0.5117
0.5098	0.4980	0.4961	0.4668	-	0.4785	0.5078	0.4980
0.4941	0.5312	0.5215	0.5195	0.4785	-	0.4961	0.5117
0.5039	0.4922	0.4902	0.4883	0.5078	0.4961	-	0.4805
0.4941	0.4922	0.5000	0.5117	0.4980	0.5117	0.4805	-

3.3. Bit Independence Criterion (BIC)

The Bit Independence Criterion (BIC) assesses the independence of bits in the output, providing a standardized measure for analyzing S-box strength as developed by Tavares and Webster [36]. The input bits that remain unaltered are investigated under the Bit Independence Criterion. BIC is concerned with how changes to individual bits in the encrypted image impact other bits, emphasizing the need for bits in the encrypted image to exhibit maximal independence. This means that the value of one bit should not disclose information about the values of other bits. A higher BIC value corresponds to enhanced security. The BIC-NL value of the proposed S-box is detailed in Table 7.

Table 7. BIC – NL Values for P_0S – box.

-	112	112	112	112	112	112	112
112	-	112	112	112	112	112	112
112	112	-	112	112	112	112	112
112	112	112	-	112	112	112	112
112	112	112	112	-	112	112	112
112	112	112	112	112	-	112	112
112	112	112	112	112	112	-	112
112	112	112	112	112	112	112	-

The results of the BIC analysis confirm that the suggested technique performs satisfactorily; the BIC-SAC values are nearly perfect, and the BIC-NL values are significantly higher, which is what is needed for strong security.

3.4. Input/Output XOR Distribution

Because some cryptographic attacks, such the differential attack described by Biham and Shamir [48], depend on imbalances in the input/output XOR distribution Table, the equiprobable input/output XOR distribution is essential. Every input XOR and every output XOR must occur with an equal probability in the setting of an S-box, where the information on the input changes determines the output changes. All entries equal to 4 are found in the input/output XOR distribution table for the proposed S-box.

3.5. Side Channel Attack

The proposed S-box is more resistant to side-channel than the other existing S-box structures in the literature. To test this hypothesis, attacks were launched on the standard AES algorithm for selected plaintext/ciphertext pairs and then the authors replaced the standard S-box with the above proposed S-box structure. The experiments revealed that because of the proposed S-box structures, it became more difficult to capture any part of the secret key, and as a result, provided better protection against side-channel attacks. When evaluating results from side-channel attacks, it was discovered that, employing 10 plaintext data, approximately six out of a hundred and sixty key parts could be accurately predicted for both the AES algorithm and the proposed approach, therefore suggesting the effectiveness of the group theoretic construction of S-box structures in fortification of security.

3.6. Linear Approximation Probability

The linear attack is a well-known method in modern cryptography, where the attacker attempts to identify linear calculations that depict a relationship between plaintext and ciphertext. In 1993, M. Matsui [49] employed linear cryptanalysis to assess the strengths and weaknesses of the Data Encryption Standard (DES). The approximation of the cipher's behavior with linear equations is determined through linear approximation probability. DES exhibited vulnerabilities against linear attacks, prompting the introduction of AES to mitigate such exploitable determinations by attackers. The calculation of linear approximation probability involves the following process:

$$LP = \max_{p_a, p_b \neq 0} \left| \frac{\#\{a \in T | a \cdot p_a = S(a) \cdot p_b\}}{2^n} - 0.5 \right|$$

where all input elements are 2^n , p_a and p_b are the masks applied on the equality of input and output bits and $T = \{0, 1, 2, \dots, 2^n - 1\}$.

The S-box under discussion is resilient against linear cryptanalysis if there is an insignificant linear relationship between the input and output. The Proposed S-box demonstrates its resistance to linear assaults with a very low LP value of 0.0625. Table 8 displays the average BIC-NL value as well as the scores for LP, DP, SAC, and other S-boxes. The Table makes it clear that our suggested S-box satisfies all the criteria for security.

Table 8. SAC, BIC-NL, LP and DP scores.

S-box	SAC	SAC-Offset	BIC-NL	LP	DP
Proposed	0.5040	0.004	112.00	0.062	0.039
Ref. [34]	0.4992	0.001	103.10	0.141	0.047
Ref. [50]	0.4976	0.002	102.85	0.132	0.039
Ref. [36]	0.5060	0.006	104.20	0.125	0.039
Ref. [48]	0.4977	0.002	104.10	0.132	0.046
Ref. [49]	0.4995	0.001	104.57	0.117	0.039
Ref. [38]	0.4995	0.001	106.35	0.128	0.039
Ref. [51]	0.5010	0.001	100.00	0.070	0.039
Ref. [52]	0.5101	0.010	106.25	0.105	0.039
Ref. [39]	0.4978	0.002	104.21	0.133	0.039
Ref. [40]	0.5034	0.003	103.80	0.133	0.039
Ref. [41]	0.5034	0.02441	103	0.071	0.039
Ref. [42]	0.5034	0.003	103.79	0.133	0.039
Ref. [43]	0.4990	0.001	104.29	0.125	0.039
Ref. [44]	0.5042	0.004	110.60	0.085	0.039
Ref. [45]	0.5022	0.002	112.40	0.156	0.039
Ref. [46]	0.4960	0.004	102.90	0.125	0.039
Ref. [5]	0.5040	0.004	112.00	0.062	0.015
Ref. [32]	0.5010	0.001	112.00	0.062	0.015
Ref. [33]	0.4999	0.001	112.00	0.062	0.015
Ref. [31]	0.5056	0.005	104.00	-	-
Ref. [28]	0.5058	0.005	106.86	-	-
Ref. [30]	0.5034	0.003	103.42	-	-

3.7. Differential Probability (DP)

Differential probability (DP) is employed to assess the strength of the S-box against differential attacks, as introduced by Biham and Shamir [48]. In this context, attackers scrutinize the disparities between input and output pairs. An S-box is deemed robust against differential cryptanalysis if it exhibits a low differential probability, indicating a uniform input/output distribution. Specifically, if all input elements are 2^n , and the set T

encompasses all potential input values, the measurement of the differential approximation is expressed as:

$$DP = \max_{\delta a \neq 0, \delta b} \left(\frac{\#\{a \in T | S(a) \oplus S(a \oplus \delta a) = \delta b\}}{2^n} \right)$$

Utilizing the above equation, it becomes evident that the proposed S-box exhibits robust resistance against differential attacks, as indicated by its notably low differential probability value of 0.039.

4. Proposed Technique for Image Processing

The following steps make up the proposed technique for image encryption: block substitution, XOR, and permutation. The first step is row-wise permutation of the 256×256 Original Image using the non-linear block cipher component produced by Algorithm 2, P_o Sbox. Following this permutation, the Enc_img_1 is built. Step two involves creating Enc_img_2 and updating Enc_img_1 with a bit-wise XOR operation. In the final stage, block-wise substitution is used to create the encrypted image. The steps of the suggested strategy are displayed in Figures 2–4, which highlights the importance of our approach.

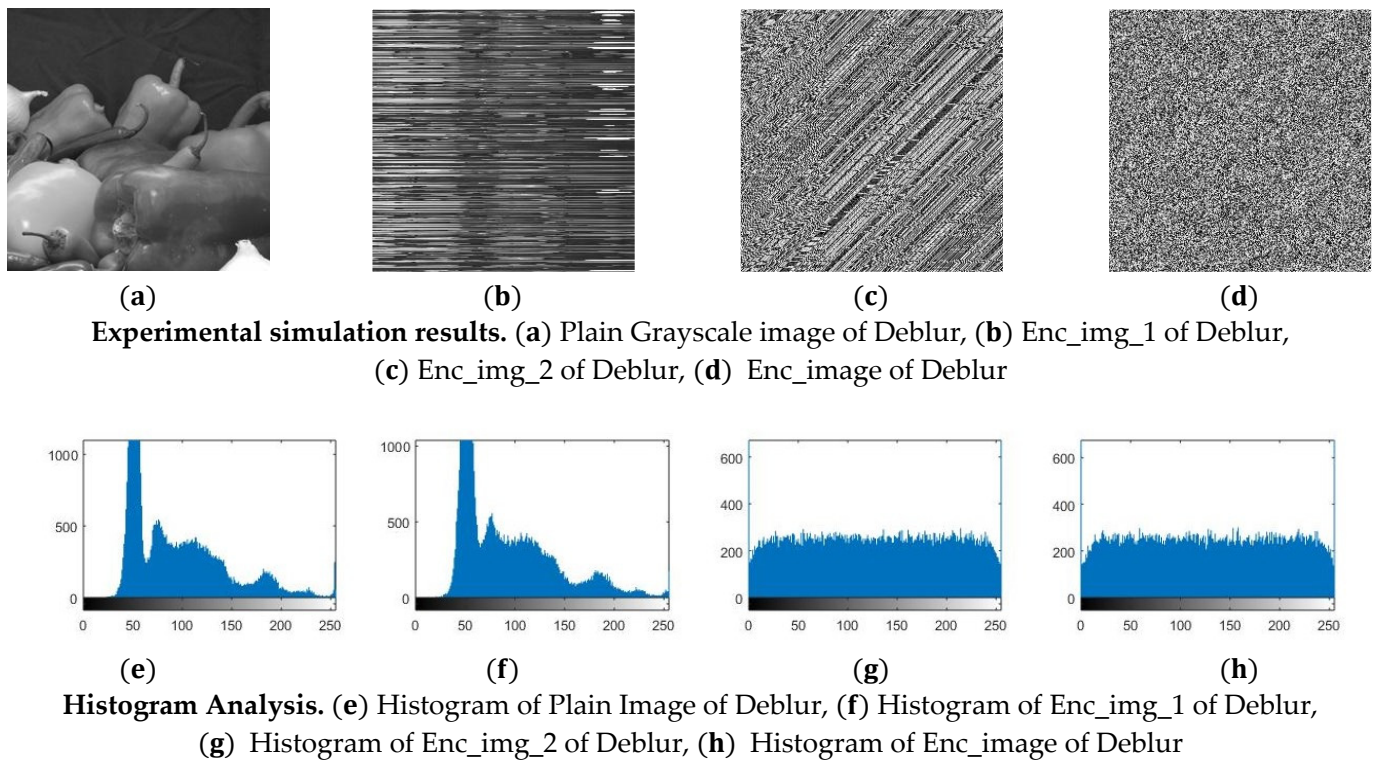


Figure 2. Experimental simulation results Deblur Images and Histogram Analysis.

The P_oS – box generated in Algorithm 2 is proved to be secure substitution box as it achieves a high security level and high efficiency against different well-known attacks. Its application in image encryption also makes it secure. The algorithm for image encryption is shown in Algorithm 3. Basically, this proposed technique consists of substitution, permutation, bit XOR and rotation which employ the typical confusion and diffusion structure.

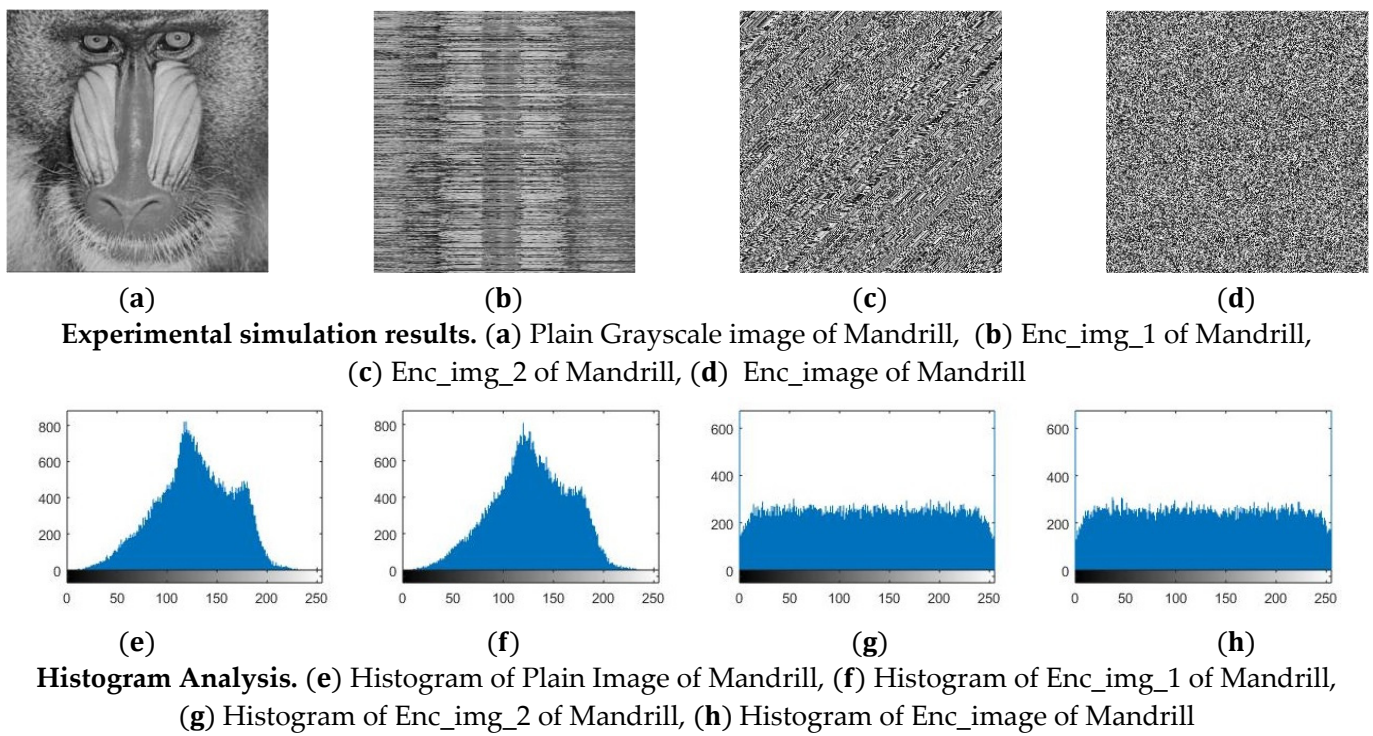


Figure 3. Experimental simulation results Mandrill Images and Histogram Analysis.

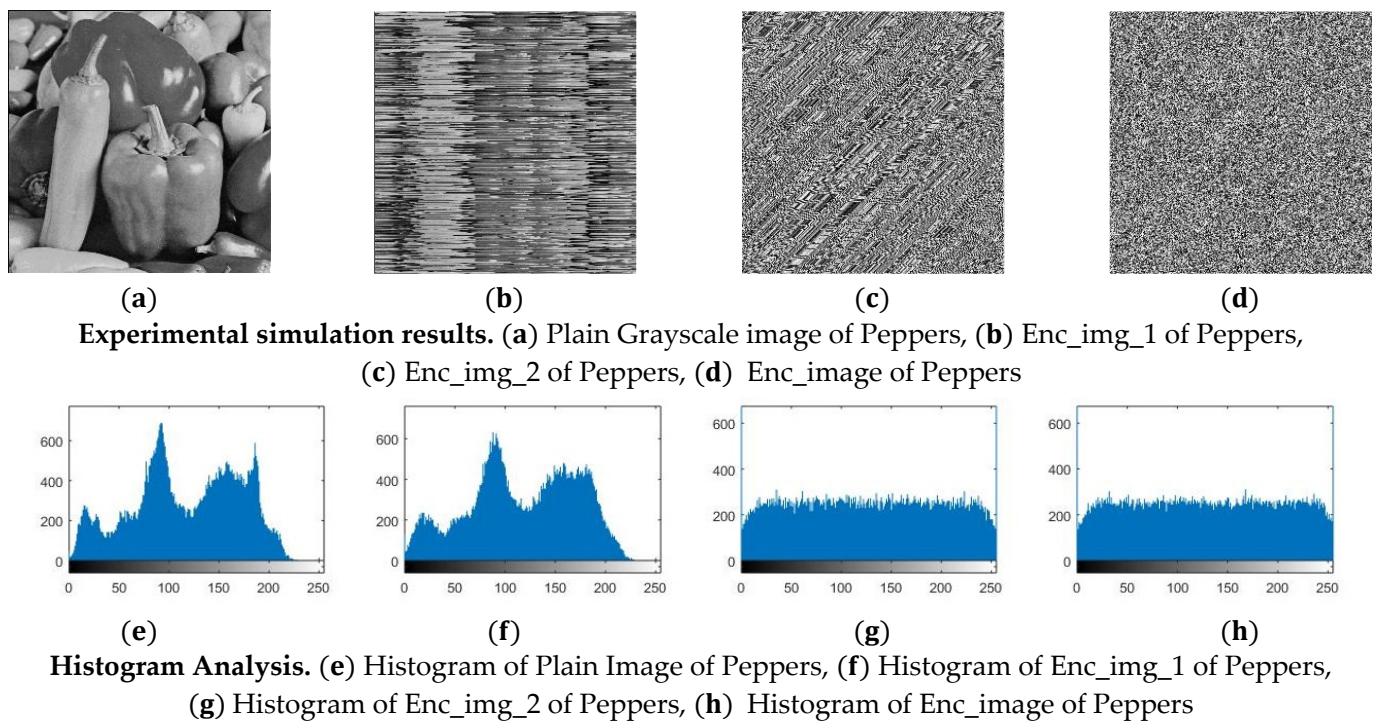


Figure 4. Experimental simulation results Peppers Images and Histogram Analysis.

Algorithm 3: Image Encryption Algorithm

```

00 Initialization
01 Input
02     Original Image, "Original_Image.jpg"
03     Permutation Key,  $P_0S - box$ 
04
05 Output
06     Enc_image
07 Load the input grayscale image
08     input_image = rgb2gray(imread('Original_Image.jpg'));
09
10 Encrypt the image using permutation and XOR encryption
11     Enc_img_1 = input_image( $P_0Sbox + 1, :$ ); % Rearrange pixel values
12     [height, width] = size(Enc_img_1);
13     for i = 1:height
14         for j = 1:width
15             | Enc_img_2(i, j) = bitxor(Enc_img_1(i, j),  $P_0Sbox (\text{mod}(i + j, \text{length}(P_0Sbox)) + 1)$ );
16         end
17     End
18 Block-wise substitution using permutation key
19     [height, width] = size(Enc_img_2);
20     for i = 1:block_size:height
21         for j = 1:block_size:width
22             block = Enc_img_3(i:i + block_size - 1, j:j + block_size - 1);
23             for x = 1:block_size
24                 for y = 1:block_size
25                     | block(x, y) =  $P_0Sbox (\text{block}(x, y) + 1)$ ;
26                 end
27             end
28             Enc_img_3(i:i + block_size - 1, j:j + block_size - 1) = block;
29         end
30     end
31 Construct Enc_image
32     Combine each substituted block
33 END

```

5. Performance Analysis of Proposed Technique

One top concern that needs to be considered is the encryption algorithm's security. This section employs a range of tests and studies to assess the security of the approach with respect to information entropy analysis, adjacent pixel correlation, and resistance to noise, cropping, and differential attacks. For testing, a range of photos of various sizes and kinds are employed.

5.1. Histogram

The frequency of each gray-level pixel in an image is described by the histogram, which also provides information on the image's lightness and darkness. The picture information must be concealed by the encryption technique from both the visual and statistical aspects of the data. For this reason, a good encryption method should have a smooth histogram of the cipher image. In Figures 3–5 are compared to the original images, the encrypted Deblur, Mandrill, and Peppers image's pixel values show a noticeably more uniform distribution. This finding highlights the efficacy of the suggested methodology in protecting the image and provides strong support for the idea that it offers robust security against statistical as well as differential assaults. From these, it is clear that the encryption technique that was created is quite effective in concealing the pixel distribution information of Plain images.

5.2. Majority Logical Criterion (MLC)

The several tests—Energy, Homogeneity, Correlation, Contrast, and Entropy—are employed to confirm the quality of the encryption [53]. These tests assess an S-box's suitability for use in the encryption process. These analyses calculate the encrypted image's unpredictability. Energy and homogeneity are used to determine the encrypted image's structures. The original and encrypted image's similarity is calculated using the correlation. The correlation analysis's lowest score indicates a significant modification in the encrypted image. The contrast of the host image is used to compute its brightness. A higher contrast indicates a better encryption technique. Plain images are distorted by the encryption system, and statistical analysis determines the suggested S-box's strength. Digital images are encrypted using the S-box that is produced. We have four 256×256 JPEG photographs (Deblur, Pepper and Mandrill) that we took in order to perform MLC. When compared to the original image, the encrypted image has completely transformed.

5.2.1. Adjacent Pixel Correlation

The independence of this relationship is demonstrated by correlation coefficient analysis [54], which is predicated on determining the correlation between two random variables. Strong pixel correlations in different directions are typically seen in plaintext image. An attacker often acquires information about a plaintext image by looking at the correlations between neighboring pixels. As a result, a secure encryption technique needs to minimize the correlations between adjacent pixels in an image [55]. The following formula is used to obtain the pixel correlation coefficient:

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2$$

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y))$$

where x_i and y_i are gray values of the adjacent pixels.

The cipher image's adjacent pixels are dispersed throughout the entire space in every direction, and their correlation coefficients are all very close to zero—much lower than those of the plain image. This indicates that the suggested encryption scheme effectively breaks the plain image's original statistical features and interferes with the correlation of adjacent pixels. The results of correlation analysis are presented in Table 9 and their comparison in Table 10. It is observed that the P_oSbox has the best confusion capability if evaluated in terms of correlation analysis parameters.

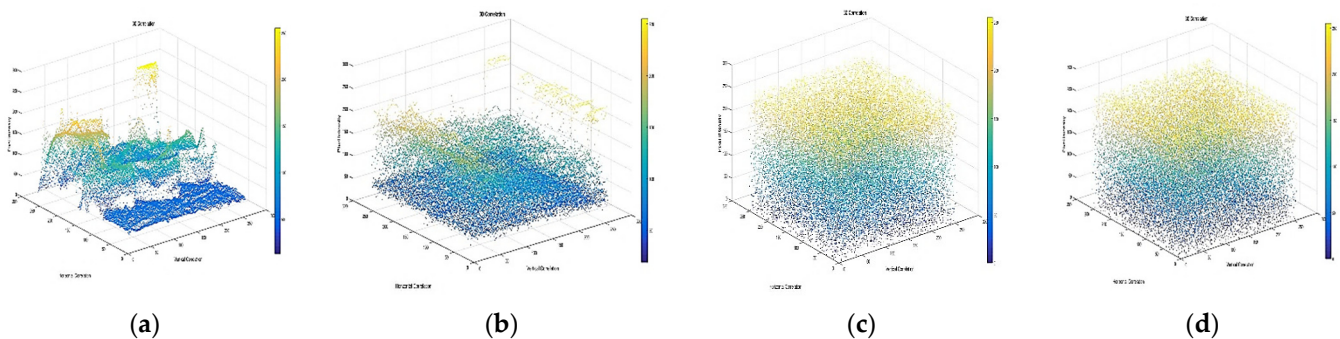
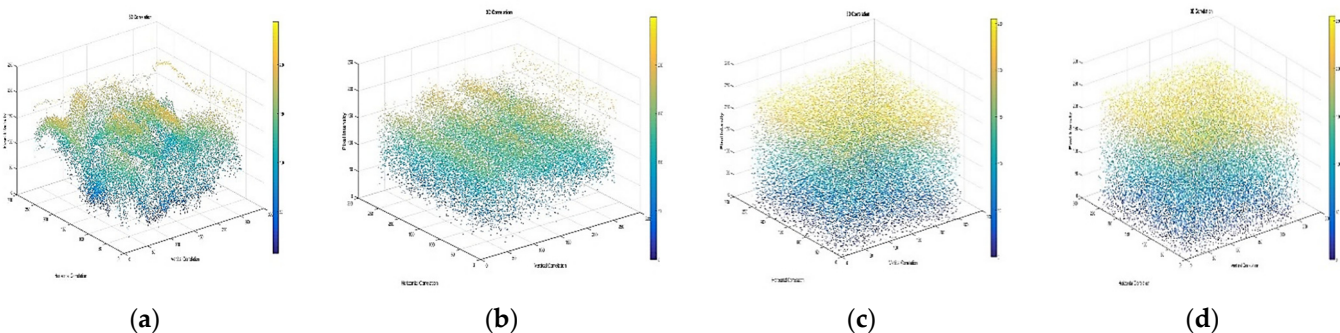
Table 9. Horizontal and Vertical Correlation of Encrypted Images.

Enc_Image	Vertical Correlation	Horizontal Correlation
Deblur	0.0031	0.0089
Mandrill	0.0025	−0.0019
Peppers	−0.0089	−0.0007

Table 10. Comparison of Correlations with different Approaches.

Approach	Images	Correlation	
		Horizontal	Vertical
Proposed	Deblur	−0.0098	−0.0054
Ref. [56]	-	−0.0005	0.0013
Ref. [57]	-	−0.0005	0.0598
Proposed	Mandrill	−0.0019	0.0025
Ref. [56]	-	0.0037	0.0027
Ref. [57]	-	0.0040	−0.0129
Proposed	Pepper	−0.0007	−0.0089
Ref. [57]	-	−0.0005	−0.0422
Ref. [58]	-	0.0662	0.0600

The Horizontal and Vertical correlations of original images and encrypted images of Mandrill, Deblur and Peppers are shown in Figures 5–7.

**Figure 5.** 3D Correlation Plot of Pixel Intensity with Vertical and Horizontal Positions in the images: (a) Plain Grayscale image of Deblur, (b) Enc_img_1 of Deblur, (c) Enc_img_2 of Deblur, (d) Enc_image of Deblur.**Figure 6.** 3D Correlation Plot of Pixel Intensity with Vertical and Horizontal Positions in the images: (a) Plain Grayscale image of Mandrill, (b) Enc_img_1 of Mandrill, (c) Enc_img_2 of Mandrill, (d) Enc_image of Mandrill.

5.2.2. Homogeneity Analysis

A method used to assess the arrangement of items next to the diagonal entries in the gray tone spatial dependency matrix (GTSDM) or the gray level co-occurrence matrix (GLCM) is called homogeneity analysis. In order to calculate statistical parameters and obtain insight into the frequency of gray level patterns in the GLCM data, the GLCM takes into account different combinations of pixel luminance values or gray levels. The following equation is used to divide the gray-level co-occurrence matrices within the GLCM in order to quantify homogeneity:

$$Hom = \sum_i \sum_j \frac{\gamma(i, j)}{1 + |i - j|}$$

where i, j are image pixel positions and $\gamma(i, j)$ represents the position of pixels in gray level co-occurrence matrix (GLCM).

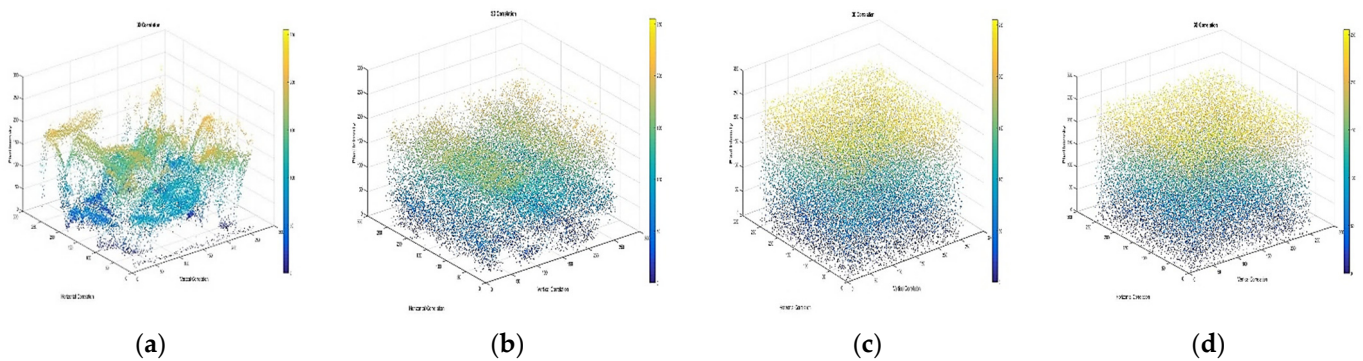


Figure 7. 3D Correlation Plot of Pixel Intensity with Vertical and Horizontal Positions in the images: (a) Plain Image of Peppers, (b) Enc_img_1 of Peppers, (c) Enc_img_2 of Peppers, (d) Enc_image of Peppers.

5.2.3. Energy

The energy of a picture is the pace at which its pixels change in brightness or color. Thus, the energy of an encrypted image should be low [59]. The gray-level co-occurrence matrix's sum of squared components is used to compute the energy metric:

$$Energy = \sum_{i,j} q(i,j)^2$$

5.2.4. Contrast

Contrast is connected with the intensity difference between neighboring pixels in an image. An image's contrast level makes it possible for the observer to distinguish the things that are in it. It enhances an image's appearance, making its constituent parts easier to recognize. An encrypted image has more unpredictability, which might result in a higher contrast level. Stronger encryption corresponds to a higher contrast level [60]. The following is a mathematical representation of contrast analysis:

$$Contrast = \sum_{i,j} q(i,j) |i - j|^2$$

5.2.5. Information Entropy

Information entropy is frequently used to quantify the content of information. Information entropy measures the amount of information included in an image; the higher the entropy, the less visual information the image contains. To effectively resist against entropy assaults, a safe encryption technique should uniformly distribute the image's pixels with high unpredictability. The information entropy of the encrypted image should be substantially greater than the plain image when compared; the theoretical information entropy of an entirely random 8-bit pixel image is 8 [61], which may be calculated as;

$$H(s) = \sum_{i=1}^{2^N-1} \rho(s_i) \log\left(\frac{1}{\rho(s_i)}\right)$$

where $\rho(s_i)$ represents the probability of the information source s_i , and N represents the number of bits of s_i . Table 11 displays the information entropy values for the encrypted images that our encryption technique determined. Table 11 displays the test results and reveals that the information entropy values are really rather near to the theoretical value of 8. Our suggested method's encryption image information entropy values are unquestionably closer to 8.

Table 11. MLC Comparison of Different Approaches.

Images	Approach		Contrast	Correlation	Energy	Homogeneity	Entropy
Pepper	Proposed	Original	0.3885	0.9320	0.1071	0.8809	7.5972
		Encrypted	10.6541	0.0054	0.0156	0.3870	7.9553
	Ref. [58], S-box I	Encrypted	9.3701	0.0449	0.0166	0.4166	7.9560
	Ref. [58], S-box II	Encrypted	9.4363	0.0639	0.0161	0.4235	7.9557
	Ref. [62]	Encrypted	10.7321	—	0.0157	0.3812	7.9975
		Original	0.4126	0.8607	0.1204	0.8393	7.2629
Mandrill	Proposed	Encrypted	10.5789	0.0021	0.0156	0.3884	7.9541
		Encrypted	10.3659	0.0404	0.0168	0.4136	7.9528
	Ref. [58], S-box I	Encrypted	9.6876	0.0258	0.0163	0.4141	7.9253
	Ref. [58], S-box II	Encrypted	9.4156	0.0267	0.0163	0.4088	7.3583
	Ref. [63]	Encrypted					
		Encrypted					

We used this set of statistical analyses to assess the applicability and stability of the performance of our created S-box-based picture encryption technique. The four test images are subjected to the MLC analysis and Table 11 displays the outcomes for both plain and encrypted images produced by our technique. We evaluate our S-box encryption performance against a few recently studied S-box-based image encryption techniques. The comparison of MLC findings with a conventional Mandrill and peppers images are presented in Table 11. It is evident that the performance of our S-box based image encryption technique is on level with that of several existing S-box based image encryption algorithms.

5.3. Image Encryption and Decryption Analysis

The simulations for Image encryption and Decryption analysis were performed using MATLAB, (R2015a) and to ensure unbiased data interpretation, they were run on a dedicated computer with a standardized configuration: 8 GB RAM, Intel Core i5 processor (2.60 GHz quad-core), and Windows 10 operating system. The following table shows the performance metrics for encryption and decryption three images (Deblur, Mandril, and Peppers) using different key bit complexities (128, 192, and 256 bits). These results demonstrate the superior performance of our encryption scheme, Table 12, showcasing its speed and high encryption throughput.

Table 12. Time, Storage Space and Memory Occupancy with rest to different Key bits.

Image	Key Bit Complexity	Time		Storage Space	Memory Occupancy
		Encryption	Decryption		
Peppers	128	0.1421 s	0.1349 s	65,552 bytes	332,336 bytes
	192	0.1416 s	0.1373 s	65,560 bytes	362,912 bytes
	256	0.1565 s	0.1434 s	65,568 bytes	364,406 bytes
Deblur	128	0.1355 s	0.1438 s	65,552 bytes	332,336 bytes
	192	0.1366 s	0.1405 s	65,560 bytes	362,912 bytes
	256	0.1324 s	0.1311 s	65,568 bytes	364,406 bytes
Mandrill	128	0.1287 s	0.1320 s	65,552 bytes	332,336 bytes
	192	0.1303 s	0.1424 s	65,560 bytes	362,912 bytes
	256	0.1492 s	0.1444 s	65,568 bytes	364,406 bytes

5.4. Keyspace and Key Sensitivity Analysis

The proposed encryption algorithm demonstrates substantial key space and high key sensitivity, which are crucial for ensuring robust security. The key space is defined by the permutation of 256 unique values, resulting in an astronomical number of possible keys. Specifically, the key space is $256!$, which is approximately $2^{1677.56}$. This vast key space effectively protects against brute-force attacks, as the number of potential keys is immensely large. Furthermore, the algorithm exhibits significant key sensitivity, meaning that even a slight alteration in the key results in a completely different encrypted output. This property

ensures that similar keys do not produce similar cipher texts, thereby enhancing the security of the encrypted data. The combination of a large key space and high key sensitivity ensures that the encryption method provides robust protection against unauthorized access and decryption attempts, making it highly suitable for securing sensitive medical images in telemedicine applications.

5.5. Encrypted Image Quality Measure

This section covers the experimental analysis of the proposed image encryption technique. For these experiments, four 256×256 JPEG images of Mandrill, Pepper and Deblur have been chosen. Table 13 displays the results of the various image quality tests that we ran using our *PoSbox*. The findings show that the modest *PoSbox* that was recommended is robust enough to resist a variety of attacks.

Table 13. Different image quality matrices of Deblur, Mandrill and Peppers.

Images	Deblur	Mandrill	Peppers
MSE	9067.40	7051.11	8537.08
PSNR	8.55597	9.64822	8.81771
NCC	1.0917	0.9168	0.9081
AD	−35.4257	0.0115	−11.3810
SC	0.4947	0.8119	0.7512
MD	255	228	251
NAE	0.8442	0.5526	0.6505
RMSE	95.2229	83.9709	92.3963
SSIM	0.0094	0.00963	0.01091
UQI	0.0027	−12.3962	0.0142

5.5.1. Mean Square Error (MSE)

The Mean Square Error (MSE) quantifies the average squared differences between corresponding elements of two images, typically the original and encrypted versions. It serves as a measure of the overall discrepancy between the two images [64]. A higher MSE score indicates a greater level of dissimilarity between the images, highlighting significant variations in their content or quality. Mathematically,

$$MSE = \frac{1}{N} \sum_{i=1}^N (X_i - X_i^*)^2$$

The mean square error (MSE) calculated by above formula for a different image is given in Table 14, which indicates the greater level of dissimilarity between original and encrypted images.

5.5.2. Root Mean Square Error (RMSE)

Another popular method of evaluating errors is called Root Mean square Error, which is used to quantify the variations between an estimator's anticipated value and the actual value. It assesses the magnitude of the error. The differences in forecasting errors from various estimators for a given variable are calculated using this ideal accuracy metric. The Root Mean Square Error may be defined as the square root of the Mean Square Error.

5.5.3. Peak Signal to Noise Ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) [65] is a metric utilized to assess the quality of reconstructed or compressed images by comparing them to the original. PSNR examines the variations between the two images and calculates the ratio of signal to noise. Essentially, PSNR quantifies how much noise is present relative to the signal strength, providing a more

nuanced evaluation than Mean Square Error (MSE) alone. Higher PSNR values signify better image quality, indicating a stronger signal relative to the noise level. Mathematically,

$$PSNR = 20 \log_{10} \left(\frac{MAXI}{MSE} \right) - 10 \log_{10}(MSE)$$

where MSE is mean square error and MAXI is the maximum possible pixel value of the image.

5.5.4. Structural Similarity Index Method (SSIM)

One approach that is based on perception is the Structural Similarity Index Method. This method considers the degradation of an image as a change in one's perception of structural information. It also functions with certain other important perception-based facts, such as luminance and contrast masking. Pixels that are highly interconnected or spatially limited are highlighted by the term "structural information". These intricately linked pixels provide further, important information about the visible items in the image domain.

The phenomenon known as "luminance masking" refers to the reduction in visibility of an image's distortion toward its borders. However, distortions in the texture of an image become less noticeable when contrast masking is applied. The perceived quality of images and videos is estimated by SSIM. It gauges how similar things are. In Table 14, the SSIM of Deblur, Mandrill and Peppers is given which shows that original and encrypted images have negligibly small similarity index and their comparison with already published articles is given in Table 14.

5.5.5. Average & Maximum Difference (AD & MD)

Calculating the average and maximum differences between the original $O(x, y)$ and encrypted $E(x, y)$ images is the aim of these tests. The AD value for the secure encryption procedure needs to be more than 3 and less than -3 [66]. The formulas listed below are used to determine the AD and MD scores:

$$AD = \frac{\sum_{y=1}^R \sum_{x=1}^S [O(x, y) - E(x, y)]}{R \times S}$$

$$MD = \max |O(x, y) - E(x, y)|$$

5.5.6. Structural Content (SC)

In essence, this test (SC) is a correlation-based metric. It is a measure to compare the structural similarity between the encrypted $E(x, y)$ and original $O(x, y)$ images. In terms of mathematical concepts,

$$SC = \frac{\sum_{y=1}^R \sum_{x=1}^S [O(x, y)]^2}{\sum_{y=1}^R \sum_{x=1}^S [E(x, y)]^2}$$

5.5.7. Normalized Absolute Error (NAE)

An indicator of performance called normalized absolute error (NAE) is the total absolute error normalized by the error in estimating the mean of the actual values. Because NAE is dependent on both minimum and maximum values, it can fluctuate somewhat. The following formula may be used to calculate the Normalized Absolute Error between the original $O(x, y)$ and encrypted $E(x, y)$ image:

$$NAE = \frac{\sum_{y=1}^R \sum_{x=1}^S [O(x, y) - E(x, y)]}{\sum_{y=1}^R \sum_{x=1}^S |O(x, y)|}$$

5.5.8. Mutual Information (MI)

Low mutual information (MI) values are always required for a good encryption method. It measures the total amount of original picture information that is extracted

from the deformed image. The mean differences between the original $O(x, y)$ and $E(x, y)$ images are found as a result of these studies. A strong encryption technique needs a low MI value [67] at all times. The values of MI and AD are calculated as

$$MI = \sum_{x \in E} \sum_{y \in O} \rho(x, y) \log_2 \frac{\rho(x, y)}{\rho(x) \rho(y)}$$

Table 14. Comparison of image Quality measure with various Approaches.

	Pepper				Mandrill			
	Proposed	Ref. [41]	Ref. [68]	Ref. [69]	Propose	Ref. [58], S-box I	Ref. [58], S-box II	Ref. [70]
MSE	8537.07	8234.45	7937.09	8002.87	7051.11	6548.04	6139.56	49.22
PSNR	8.8177	8.5390	8.1154	8.2496	9.64822	9.9697	10.249	31.209
NCC	0.9081	0.8299	0.8799	0.8125	0.9168	0.9021	0.9405	0.998
AD	−11.3810	−3.4583	−1.2214	−4.9927	0.0115	−2.6040	−1.2701	0.001
SC	0.7512	0.8011	0.7913	0.7714	0.8119	0.8520	0.8147	0.999
MD	251	222	231	209	228	235	243	-
NAE	0.6505	0.6021	0.6191	0.6548	0.5526	0.5329	0.4948	0.414
RMSE	92.3963	80.1984	83.9802	89.1031	83.9709	80.9199	78.3553	-
UQI	0.01428	0.0190	0.0867	0.0209	0.00963	0.0623	0.1369	-
SSIM	0.1090	0.8907	0.04921	0.0032	−12.39	−0.0214	0.0323	-

5.6. NPCR, UACI & BACI Analysis

Utilizing UACI (Unified Average Changing Intensity), NPCR (Number of Pixels Change Rate) [71] and blocked average changing intensity (BACI) are cryptanalysis techniques to determine how resilient encryption is against differentiating attacks. It is employed to identify how minor modifications to the source images impact encryption. The percentage of distinct pixel numbers in the original and encrypted images is provided by NPCR. The mathematical form of NPCR is as follows:

$$NPCR = \sum_{x=1}^n \sum_{y=1}^m C(x, y) \times \frac{100\%}{n \times m}$$

$$C(x, y) = \begin{cases} 0, & \text{if } A(x, y) = B(x, y) \\ 1, & \text{if } A(x, y) \neq B(x, y) \end{cases}$$

where $O(x, y)$ is the original image and the encrypted image is $E(x, y)$ and $C(x, y)$ is a specified array of the same size as A and B .

While Unified Average Changing Intensity (UACI) measures the changing in the intensity of original and encrypted images. Mathematically,

$$UACI = \sum_{i=1}^n \sum_{j=1}^m \left[\frac{|O(i, j) - E(i, j)|}{255} \right] \times \frac{100\%}{n \times m}$$

$$BACI = \frac{1}{(m-1)(n-1)} \sum_{i=1}^{(m-1)(n-1)} \frac{x_i}{255} \times 100\%$$

The image size is represented by $M \times N$ in these calculations, the and the average of the absolute values of the difference between the two elements is displayed by x_i . The image encryption algorithm's diffusion operation can maximize the impact of a slight alteration in the plaintext on the encrypted image's pixels. The anticipated value of NPCR is 99.6094% when the two images are entirely different from one another. The anticipated value of UACI was 33.4635% and 25% is the theoretical value of BACI [72]. Table 15 clears

that the NPCR of Encrypted images meets with anticipated value and same for UACI and BACI cases.

Table 15. NPCR and UACI score for Different Images.

Image	Approach	NPCR	UACI	BACI
Peppers	Proposed	99.6109%	29.8809%	22.3448%
	Ref. [58], S-box I	99.6200%	30.1971%	20.2427%
	Ref. [58], S-box II	97.1924%	26.3860%	21.5258%
	Ref. [58], S-box III	99.2142%	32.8705%	21.1537%
	Ref. [73]	99.6020%	33.4530%	-
	Ref. [74]	99.6300%	33.4100%	-
Mandrill	Proposed	99.6337%	27.6371%	19.9349%
	Ref. [58], S-box I	99.8400%	26.6469%	18.1314%
	Ref. [58], S-box II	99.7066%	24.5453%	20.0813%
	Ref. [58], S-box III	99.2935%	29.6113%	20.0984%
	Ref. [73]	99.5980%	33.3540%	-
	Ref. [74]	99.6048%	33.5547%	-

6. Conclusions

In the field of modern cryptography, where security is the most important factor, sophisticated block ciphers such as AES greatly depend on substitution boxes (S-boxes). This paper explores the use of abstract algebra, more precisely Group theory, as a distinctive design approach to developing S-boxes. Two distinct approaches are used to carry out the construction process: Heuristic Group-based Optimization and exploiting the special structure of Galois fields. When coupled with Algebraic Group action, the creative application of Galois fields in substitution box formulation proves to be a strong strategy that increases substitution box security. Initial tests of the produced S-box, that exceed the established standards for advanced S-boxes, reveal encouraging results. Interestingly, Table 5 demonstrates that the Post S-box has a far higher nonlinearity than other S-boxes described in the literature. A variety of statistical tests, including as the SAC (Strict Avalanche Criterion), LP (Linearity Property), and DP (Differential Property), were carefully carried out to determine its resistance to well-known attacks. The findings highlight the reliability of the built substitution box, with a DP evaluation demonstrating strong cryptographic characteristics, an LP measure of 0.062, DP score of 0.039 and a SAC value of 0.504. This work advances the field of secure cryptographic systems by offering a novel and successful method for building S-boxes that combines the theoretical breadth of abstract algebra with real-world cryptographic uses. We have provided a strong image encryption method that includes three critical steps: row permutations, bitwise XOR, and block-wise substitution. These methods effectively increased entropy and resulted in a more equal intensity distribution within the cipher. Our detailed assessment shows that this technique is very resistant to statistical and cryptanalytic attacks. Furthermore, our comparative analysis of existing techniques, which includes measurements such as PSNR, UACI, MSE, NCC, AD, SC, MD, and NAE, demonstrates its better efficacy in assuring image security. This demonstrates the effectiveness and dependability of our suggested encryption technique for protecting sensitive image data from various threats and attacks. Compared to traditional optimization techniques such as Particle Swarm Optimization (PSO), Whale Optimization Algorithm (WOA), Genetic Algorithm (GA), and Sine Cosine Algorithm (SCA), our method offers several advantages. Firstly, it provides a structured and deterministic approach, reducing the variability and computational overhead associated with stochastic optimization algorithms. This results in consistent and reliable cryptographic properties. Secondly, the incorporation of abstract algebra, specifically group actions on Galois fields, allows for a deeper mathematical foundation, enhancing the theoretical robustness of the generated S-boxes. However, there are also some limitations. The proposed method, while efficient, may require specialized mathematical knowledge to implement and understand, which could be a barrier for practitioners without a background in abstract algebra. Additionally, the

heuristic component of the optimization may still require some degree of parameter tuning, although to a lesser extent than purely stochastic methods. In contrast, optimization-based approaches like PSO, WOA, GA, and SCA are more accessible to implement and widely understood in the cryptographic community. These methods can also explore a broader search space, potentially discovering novel S-box configurations that might be missed by more deterministic methods. However, their stochastic nature often results in higher computational costs and less predictable outcomes, necessitating multiple runs to achieve optimal results.

Author Contributions: Methodology, A.A.; Software, S.A.B. and A.A.; Validation, A.Y.; Formal analysis, A.Y.; Investigation, M.H. and A.Y.; Resources, S.A.B.; Writing—original draft, M.H.; Writing—review & editing, S.A.B. and A.Y.; Supervision, A.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare that they have no conflicts of interests.

References

1. Caesar, G.I. *Commentarii de Bello Gallico*; Seidel: New Delhi, India, 1851.
2. Van Oorschot, P.C.; Menezes, A.J.; Vanstone, S.A. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1996.
3. Hannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
4. FIPS PUB. Data Encryption Standard (des). FIPS PUB; 1999; p. 3. Available online: <https://csrc.nist.gov/files/pubs/fips/46-3/final/docs/fips46-3.pdf> (accessed on 16 July 2024).
5. Joan, D.; Vincent, R. The Design of Rijndael: AES—the Advanced Encryption Standard. In *Information Security and Cryptography*; Springer: Berlin/Heidelberg, Germany, 2002.
6. Diffie, W.; Hellman, M.E. New directions in cryptography. In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*; ACM: New York, NY, USA, 2022; pp. 365–390.
7. Rivest, R.L. *A Method for Obtaining Digital Signature and Public-Key Cryptosystems*; ACM: New York, NY, USA, 1987; Volume 21.
8. Miller, V.S. Use of elliptic curves in cryptography. In *Proceedings of the Conference on the Theory and Application of Cryptographic Techniques*, Berlin, Germany, 18–22 August 1985.
9. Cohen, H.; Frey, G.; Avanzi, R.; Doche, C.; Lange, T.; Nguyen, K.; Vercauteren, F. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*; CRC Press: Boca Raton, FL, USA, 2005.
10. Smart, N.P. The Enigma machine. In *Cryptography Made Simple*; Springer International Publishing: Cham, Switzerland, 2016; pp. 133–161.
11. Rejewski, M. How Polish mathematicians deciphered the Enigma. *Ann. Hist. Comput.* **1981**, *3*, 213–234. [CrossRef]
12. Biham, E.; Shamir, A. *Differential Cryptanalysis of the Data Encryption Standard*; Springer Science & Business Media: Berlin, Germany, 2012.
13. Kocher, P.C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Proceedings of the Advances in Cryptology—CRYPTO’96: 16th Annual International Cryptology Conference*, Santa Barbara, CA, USA, 18–22 August 1996.
14. Fips Pub. Secure Hash Standard (shs). Fips Pub; 2012; Volume 180. Available online: <https://csrc.nist.gov/files/pubs/fips/180-4/upd1/final/docs/fips180-4-draft-aug2014.pdf> (accessed on 16 July 2024).
15. Yousaf, A.; Razaq, A.; Baig, H. A lightweight image encryption algorithm based on patterns in Rubik’s revenge cube. *Multimed. Tools Appl.* **2022**, *81*, 28987–28998. [CrossRef]
16. Panchami, V.; Mathews, M.M. A substitution box for lightweight ciphers to secure internet of things. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 75–89. [CrossRef]
17. Das, A.K.; Kar, N.; Deb, S.; Singh, M.P. A lightweight block cipher utilizing key cross approach via probability density function. *Arab. J. Sci. Eng.* **2022**, *47*, 10563–10578. [CrossRef]
18. Razaq, A.; Maghrabi, L.A.; Ahmad, M.; Aslam, F.; Feng, W. Fuzzy logic-based substitution-box for robust medical image encryption in telemedicine. *IEEE Access* **2024**, *12*, 7584–7608. [CrossRef]
19. Razaq, A.; Ahmad, M.; Yousaf, A.; Alawida, M.; Ullah, A.; Shuaib, U. A group theoretic construction of large number of AES-like substitution-boxes. *Wirel. Pers. Commun.* **2022**, *122*, 2057–2080. [CrossRef]
20. Hwang, J.; Kale, G.; Patel, P.P.; Vishwakarma, R.; Aliasgari, M.; Hedayatipour, A.; Rezaei, A.; Sayadi, H. Machine Learning in Chaos-Based Encryption: Theory, Implementations, and Applications. *IEEE Access* **2023**, *11*, 125749–125767. [CrossRef]
21. Liu, X.; Tong, X.; Zhang, M.; Wang, Z.; Fan, Y. Image compression and encryption algorithm based on uniform non-degeneracy chaotic system and fractal coding. *Nonlinear Dyn.* **2023**, *111*, 8771–8798. [CrossRef]
22. Ma, Y.; Tian, Y.; Zhang, L.; Zuo, P. Two-dimensional hyperchaotic effect coupled mapping lattice and its application in dynamic S-box generation. *Nonlinear Dyn.* **2024**, 1–32. [CrossRef]

23. Mishra; Rahul; Singh, B.; Delhibabu, R. *Searching for S-Boxes with Better Diffusion Using Evolutionary Algorithm*; Cryptology ePrint Archive, 2023. Available online: <https://eprint.iacr.org/2023/353> (accessed on 16 July 2024).
24. Kuznetsov, A.; Poluyanenko, N.; Frontoni, E.; Kandiy, S.; Peliukh, O. A new cost function for heuristic search of nonlinear substitutions. *Expert Syst. Appl.* **2024**, *237*, 121684. [\[CrossRef\]](#)
25. Feng, W.; Zhang, J.; Chen, Y.; Qin, Z.; Zhang, Y.; Ahmad, M.; Woźniak, M. Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption. *Expert Syst. Appl.* **2024**, *246*, 123190. [\[CrossRef\]](#)
26. Ahmad, M.; Al-Solami, E.; Alghamdi, A.M.; Yousaf, M.A. Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures. *IEEE Access* **2020**, *8*, 110397–110411. [\[CrossRef\]](#)
27. Yousaf, M.A.; Alolaiyan, H.; Ahmad, M.; Dilbar, M.; Razaq, A. Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes. *IEEE Access* **2020**, *8*, 39781–39792. [\[CrossRef\]](#)
28. Razaq; Abdul; Ahmad, M.; El-Latif, A.A.A. A novel algebraic construction of strong S-boxes over double GF (27) structures and image protection. *Comput. Appl. Math.* **2023**, *42*, 90. [\[CrossRef\]](#)
29. Ahmad, M.; Khaja, I.A.; Baz, A.; Alhakami, H.; Alhakami, W. Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications. *IEEE Access* **2020**, *8*, 116132–116147. [\[CrossRef\]](#)
30. Artuğer, F. A new S-box generator algorithm based on 3D chaotic maps and whale optimization algorithm. *Wirel. Pers. Commun.* **2023**, *131*, 835–853. [\[CrossRef\]](#)
31. Artuğer, F.; Özkaynak, F. A new algorithm to generate aes-like substitution boxes based on sine cosine optimization algorithm. *Multimed. Tools Appl.* **2024**, *83*, 38949–38964. [\[CrossRef\]](#)
32. Cui, L.; Cao, Y. A new S-box structure named affine-power-affine. *Int. J. Innov. Comput. Inf. Control* **2007**, *3*, 751–759.
33. Tran, M.T.; Bui, D.K.; Duong, A.D. Gray S-box for advanced encryption standard. In Proceedings of the International Conference on Computational Intelligence and Security, Suzhou, China, 13–17 December 2008.
34. Ali, T.; Ali, R. A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box. *Multimed. Tools Appl.* **2022**, *81*, 20585–20609. [\[CrossRef\]](#)
35. Artuğer, F. A novel algorithm based on DNA coding for substitution box generation problem. *Neural Comput. Appl.* **2024**, *36*, 1283–1294. [\[CrossRef\]](#)
36. Zahid, A.H.; Tawalbeh, L.O.A.I.; Member, S.; Ahmad, M.; Farhan, A.K. Efficient dynamic S-box generation using linear trigonometric transformation for security applications. *IEEE Access* **2021**, *9*, 98460–98475. [\[CrossRef\]](#)
37. Dougherty, S.T.; Klobusicky, J.; Şahinkaya, S.; Ustun, D. An S-Box construction from exponentiation in finite fields and its application in RGB color image encryption. *Multimed. Tools Appl.* **2024**, *83*, 41213–41241. [\[CrossRef\]](#)
38. Zhu, H.; Tong, X.; Wang, Z.; Ma, J. A novel method of dynamic S-box design based on combined chaotic map and fitness function. *Multimed. Tools Appl.* **2020**, *79*, 12329–12347. [\[CrossRef\]](#)
39. Lambic, D. S-Box design method based on improved one-dimensional discrete chaotic map. *J. Inf. Telecommun.* **2018**, *2*, 181–191. [\[CrossRef\]](#)
40. Lambic, D. A novel method of S-box design based on discrete chaotic map. *Nonlinear Dyn.* **2017**, *87*, 2407–2413. [\[CrossRef\]](#)
41. Alhadawi, H.S.; Majid, M.A.; Lambić, D.; Ahmad, M. A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm. *Multimed. Tools Appl.* **2020**, *80*, 7333–7350. [\[CrossRef\]](#)
42. Lambic, D. A novel method of S-box design based on chaotic map and composition method. *Chaos Solitons Fractals* **2014**, *58*, 16–21. [\[CrossRef\]](#)
43. Ibrahim, S.; Alhumyani, H.; Masud, M.; Alshamrani, S.S.; Cheikhrouhouet, O.; Muhammad, G.; Hossain, M.S.; Abbas, A.M. Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps. *IEEE Access* **2020**, *8*, 160433–160449. [\[CrossRef\]](#)
44. Long, M.; Wang, L. S-Box design based on discrete chaotic map and improved artificial bee colony algorithm. *IEEE Access* **2021**, *9*, 86144–86154. [\[CrossRef\]](#)
45. Masood, F.; Masood, J.; Zhang, L.; Jamal, S.S.; Boulila, W.; Rehman, S.U.; Khan, F.A.; Ahmad, J. A new color image encryption technique using DNA computing and chaos-based substitution box. *Soft Comput.* **2022**, *26*, 7461–7477. [\[CrossRef\]](#)
46. Zahid, A.H.; Arshad, M.J.; Ahmad, M.; Soliman, N.F.; El-Shafai, W. Dynamic S-Box Generation Using Novel Chaotic Map with Nonlinearity Tweaking. *Comput. Mater. Contin. CMC* **2023**, *75*, 3011–3026.
47. Webster, A.F.; Tavares, S.E. On the design of S-boxes. In Proceedings of the CRYPTO'85, Santa Barbara, CA, USA, 18–22 August 1985.
48. Liu, J.; Tong, X.; Zhang, M.; Wang, Z. The design of S-box based on combined chaotic map. In Proceedings of the AEMCSE, Shenzhen, China, 24–26 April 2020.
49. Farah, T.; Rhouma, R.; Belghith, S. A novel method for designing S-box based on chaotic map and teaching–learning-based optimization. *Nonlinear Dyn.* **2017**, *88*, 1059–1074. [\[CrossRef\]](#)
50. Jiang, Z.; Ding, Q. Construction of an S-box based on chaotic and bent functions. *Symmetry* **2021**, *13*, 671. [\[CrossRef\]](#)
51. Lambic, D. A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. *Nonlinear Dyn.* **2020**, *100*, 699–711. [\[CrossRef\]](#)
52. Shafique, A. A new algorithm for the construction of substitution box by using chaotic map. *Eur. Phys. J. Plus* **2020**, *135*, 194. [\[CrossRef\]](#)

53. Hussain, I.; Shah, T.; Gondal, M.A.; Mahmood, H. Generalized majority logic criterion to analyze the statistical strength of S-boxes. *Z. Naturforschung A* **2012**, *65*, 282–288. [\[CrossRef\]](#)
54. Pareek, N.K.; Patidar, V.; Sud, K.K. Image encryption using chaotic logistic map. *Image Vis. Comput.* **2006**, *24*, 926–934. [\[CrossRef\]](#)
55. Liu, H.; Kadir, A.; Xu, C. Color image encryption with cipher feedback and coupling chaotic map. *Int. J. Bifurc. Chaos* **2020**, *30*, 2050173. [\[CrossRef\]](#)
56. Zhang, X.-P.; Guo, R.; Chen, H.-W.; Zhao, Z.-M.; Wang, J.-Y. Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes. *Chin. Phys. B* **2018**, *27*, 080701. [\[CrossRef\]](#)
57. Razaq, A.; Akhter, S.; Yousaf, A.; Shuaib, U.; Ahmad, M. A group theoretic construction of highly nonlinear substitution box and its applications in image encryption. *Multimed. Tools Appl.* **2022**, *81*, 1–22. [\[CrossRef\]](#)
58. Razaq, A.; Iqra; Ahmad, M.; Yousaf, M.A.; Masood, S. A novel finite rings based algebraic scheme of evolving secure S-boxes for images encryption. *Multimed. Tools Appl.* **2021**, *80*, 20191–20215. [\[CrossRef\]](#)
59. Naseer, Y.; Shah, T.; Attaullah; Javeed, A. Advance image encryption technique utilizing compression, dynamical system and S-boxes. *Math. Comput. Simul.* **2020**, *178*, 207–217. [\[CrossRef\]](#)
60. Ahmad, J.; Hwang, S.O. Chaos-based diffusion for highly autocor related data in encryption algorithms. *Nonlinear Dyn.* **2015**, *82*, 1839–1850. [\[CrossRef\]](#)
61. Ahlswede, R. Remarks on Shannon's secrecy systems. *Probl. Contr. Inform. Theory* **1982**, *11*, 301–318.
62. Mahboob, A.; Nadeem, M.; Rasheed, M.W. A study of text-theoretical approach to S-box construction with image encryption applications. *Sci. Rep.* **2023**, *131*, 21081. [\[CrossRef\]](#) [\[PubMed\]](#)
63. Jamal, S.S.; Attaullah; Shah, T.; AlKhaldi, A.H.; Tufail, M.N. Construction of new substitution boxes using linear fractional transformation and enhanced chaos. *Chin. J. Phys.* **2019**, *60*, 564–572. [\[CrossRef\]](#)
64. Eskicioglu, A.M.; Fisher, P.S. Image quality measures and their performance. *IEEE Trans. Commun.* **1995**, *43*, 2959–2965. [\[CrossRef\]](#)
65. Khan, M.; Shah, T.; Mahmood, H.; Gondal, M.A. An efficient method for the construction of block cipher with multi-chaotic systems. *Nonlinear Dyn.* **2013**, *71*, 489–492. [\[CrossRef\]](#)
66. Huynh-Thu, Q.; Ghanbari, M. Scope of validity of PSNR in image/video quality assessment. *Electron. Lett.* **2008**, *44*, 800–801. [\[CrossRef\]](#)
67. Wu, X.; Kan, H.; Kurths, J. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. *Appl. Soft Comput.* **2015**, *37*, 24–39. [\[CrossRef\]](#)
68. Siddiqui, N.; Naseer, A.; Ehatisham-ul-Haq, M. A novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve. *Wirel. Pers. Commun.* **2020**, *116*, 3015–3030. [\[CrossRef\]](#)
69. Zahid, A.H.; Al-Solami, E.; Ahmad, M. A novel modular approach based substitution-box design for image encryption. *IEEE Access* **2020**, *8*, 150326–150340. [\[CrossRef\]](#)
70. Bhosale, A.G.; Bidkar, P.S. A Modified Image Template for FELICS Algorithm for Lossless Image Compression. *Int. J. Curr. Eng. Technol.* **2014**, *4*.
71. Biham, E.; Shamir, A. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptol.* **1991**, *4*, 3–72. [\[CrossRef\]](#)
72. Liang, H.; Zhang, G.; Hou, W.; Huang, P.; Liu, B.; Li, S. A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography. *Appl. Sci.* **2021**, *11*, 5691. [\[CrossRef\]](#)
73. 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* **2023**, *11*, 135880–135890. [\[CrossRef\]](#)
74. Li, Z.; Peng, C.; Tan, W.; Li, L. A novel chaos-based color image encryption scheme using bit-level permutation. *Symmetry* **2020**, *12*, 1497. [\[CrossRef\]](#)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.