Hindawi
Security and Communication Networks
Volume 2023, Article ID 5767102, 19 pages
https://doi.org/10.1155/2023/5767102

Research Article

Fast Novel Efficient S-Boxes with Expanded DNA Codes

Abeer Tariq Maolood,[1] Alaa Kadhim Farhan,[1] Wageda I. El-Sobky,[2] Hany Nasry Zaky,[3] Hossam L. Zayed,[4] Hossam E. Ahmed,[4] and Tamer O. Diab[4]

[1]*Computer Sciences Department, University of Technology, Baghdad, Iraq*
[2]*Department of Basic Engineering Sciences, Benha Faculty of Engineering, Benha University, Benha 13511, Egypt*
[3]*Mathematics Department, Military Technical College, Cairo, Egypt*
[4]*Electrical Engineering Department, Benha Faculty of Engineering, Benha University, Benha 13511, Egypt*

Correspondence should be addressed to Alaa Kadhim Farhan; 110030@uotechnology.edu.iq

Received 28 September 2022; Revised 3 November 2022; Accepted 7 February 2023; Published 18 April 2023

Academic Editor: Je Sen Teh

IoT is one of the most popular technologies in recent years due to the interconnection of various infrastructures, physical devices, and software. To guarantee the security of Internet of Things (IoT) pervasiveness, lightweight cryptographic solutions are needed and this requires lightweight cryptographic primitives. The choice of S-box in light block ciphers plays an important role in characterizing the security-performance trade-off. The choice of the 4×4 S-box for the lightweight constructions results in compact hardware, speeding up the computational capability of the security algorithm unlike the 8×8 S-box. This work presents efficient algebraic S-boxes for a fast image cryptosystem based on a strong nonlinear function which is expanded by a biological technique depending on DNA. The robustness of the proposed S-boxes is analysed and tested against various standard attack criteria such as interpolation attacks, avalanche effect, and nonlinearity. The great advantage of introducing S-boxes is that its DSAC is the ideal value which is equal to zero. Also, other tests executed on these S-boxes guaranteed its robustness and excellent security performance. Moreover, the experiments are applied with full description in two different modes; RGB and gray images. The results of all tests proved to have fast and strong effective S-boxes.

1. Introduction

The general wireless communication protocols such as Bluetooth, Zigbee, Ethernet, Wi-Fi, and 4-G are majorly used for transferring data in IoT devices. However, power consumption, reliability, long communication, and security are primary aspects for IoT to obtain reliable communication between a transmitter and a receiver. Narrowband IoT (NB-IoT) of LTE is presented to obtain high throughput, low power consumption, and high battery life because it provided services to access the network through the physical layer [1]. To address the requirements of IoT, NB-IoT architecture is simplified from evolved packet core structure. The NB-IoT introduced many changes for medium access control to reduce power consumption thereby making the scheduling simple and flexible. HARQ is used for removing scheduling assignments hence reducing the number of control bits to enhance robustness and efficiency. A lightweight encryption system is popularly used for IoT implementation because of its bit permutation group operation. The rapid growth in computer networks and multimedia information technology attracts a lot of researchers towards the security and protection of digital data transmission via the Internet. The most important and widely used digital media are image information as it contains a huge amount of data with strong correlation and redundancy [2].

Many important and strategic applications such as geographical, medical, biological, communication satellites, and military applications are strongly dependent on digital images. Therefore, the significant development in these technologies and the security issues' complexity attracts researchers to introduce efficient algorithms for this attractive and critical field [1]. These algorithms can be used for hiding the data, watermarking, and for several techniques of encryption [3, 4].

The solution for these security complexities can be achieved by converting it into an unreadable form. Cryptography is the science which is responsible for fulfilling this process. It aims to protect these data from exploitation, alteration, or being missed and also to make sure that a specific receiver can read and comprehend these data. In any cryptographic algorithm, it is a principal factor to insert a confusion property in the ciphertext. Among these encryption techniques which are widely used to secure the color image content are Data Encryption Standard (DES) and Rivest F02D Shamir F02D Adelman (RSA). Nowadays, several techniques provide better image security than classical techniques. The idea behind the methodology of image encryption is to create a noise image out of the original one that uses both permutations and diffusion substitution box (S-box) or vice versa. There is a candid link between security and confusion, as the confusion level in ciphertext shows its robustness [5, 6]. This motivated the researchers to the DNA computing conversion concept. DNA cryptography, the arising path in information security considered as a promising technology for unbreakable algorithms, is the science of inheritance that has storage data based on DNA biology [7–9].

The National Institute of Standards and Technology (NIST) published several criteria to measure the S-box strength, such as strict avalanche criterion, nonlinearity, and bit independence criterion [10, 11]. This work provides a simple novel fast way to image encryption based on a highly nonlinear algebraic function expanded by a DNA conversion algorithm to expand the number of S-boxes. The produced S-boxes have excellent properties, especially it has a distance strict avalanche criterion that equals to zero [12–14].

This study is organized as follows: Section 2 presents the proposed novel fast S-box. Section 3 presents the performance of the proposed S-box, while Section 4 describes the different schemes of the proposed S-box. Finally, the conclusion of this work is presented in Section 5.

2. Proposed Novel Fast S-Box

There are many methods used to construct S-boxes such as the chaos system which has many defects: the computer implementation of the chaos has limited precision; the simple chaotic system time series output generally cannot reach the theoretical complete randomness [7, 12], resulting in the problem that the pseudorandom sequence appears periodically. So, our main idea depends on algebraic construction for novel S-box evaluation. We are sure from all the values of all tests and plus in IOT applications they depend on lightweight encryption based on (4×4)S-boxes because they are very fast, accurate, and secure and all of these conditions were found in our work as well.

This section is divided into two parts. Part one, presented in 2.1, explains the basic novel idea of the proposed S-box. Part 2, presented in 2.2, describes how to expand the proposed S-box using biological techniques depending on DNA codes.

2.1. The Novel Proposed S-Box in GF $(\mathbf{2^4})$. A very new secure simple construction high nonlinear S-box is generated by the following steps:

First, we apply affine transformation which is defined by the following equation:

$$k = T\left(aX^2 + b\right) = \begin{bmatrix} a_3\, a_2\, a_1\, a_0 \\ a_0\, a_3\, a_2\, a_1 \\ a_1\, a_0\, a_3\, a_2 \\ a_2\, a_1\, a_0\, a_3 \end{bmatrix} \begin{bmatrix} X_3 \\ X_2 \\ X_1 \\ X_0 \end{bmatrix}^2 + \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix}, \quad (1)$$
$$a = 0x7, 0xD,$$
$$b = 0x3, 0x1, 0x6,$$

the multiplicative inverse is computed from the result k: $k = k^{-1}$ in $\mathrm{GF}(2^8)$, which can be defined as

$$k = k^{-1} = \begin{cases} k^{14} & Y \neq 0, \\ 0 & Y = 0, \end{cases} \quad (2)$$

affine transformation is applied twice

$$k = T\left(ak^2 + b\right) = \begin{bmatrix} a_3\, a_2\, a_1\, a_0 \\ a_0\, a_3\, a_2\, a_1 \\ a_1\, a_0\, a_3\, a_2 \\ a_2\, a_1\, a_0\, a_3 \end{bmatrix} \begin{bmatrix} k_3 \\ k_2 \\ k_1 \\ k_0 \end{bmatrix}^2 + \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix}, \quad (3)$$
$$a = 0x7, 0xD,$$
$$b = 0x3, 0x1, 0x6.$$

The family of generated S-boxes is shown in Tables 1–3.

Now, the values are converted into the binary form, and its length must be a multiple of 8. If not, zeros will be added to the left to adjust the number. The next step is to replace each double bit with one a DNA code, i.e., in code 8, 00 is substituted by *T*, 01 by *G*, 10 by *C*, and 11 by *A*.

Using the eight codes that are mentioned, we can obtain for each S-box different eight-S-boxes shown in appendices' of Tables 4–30. The algorithm1 that is used to generate the proposed S-box is shown in the following steps:

The three S-boxes presented in Tables 1–3 were generated based on 3 irreducible polynomials $x^4 + x + 1$, $x^4 + x^3 + 1$, and $x^4 + x^3 + x^2 + 1$.

2.2. Deoxyribonucleic Acid (DNA) Image Conversion. DNA is the genetic pattern which is responsible for the distinction among living creatures, and adenine, cytosine, guanine, and thymine are the DNA computing bases which are used for representing the data as A, T, C, and G, respectively, as shown in Figure 1. All the creature's cosmetic cells contain a full set of DNA data that makes this distinction. The benefit of these characteristics in security is that the image pixels are converted to 8-bit binary and uses 00, 01,

Table 1: The 1st proposed S-box (HEX).

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3	e	D	F	8	B	1	5	C	6	9	0	a	7	2	4

Table 2: The 2nd proposed S-box (HEX).

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	6	A	2	F	3	9	8	E	4	b	D	7	0	5	c

Table 3: The 3rd proposed S-box (HEX).

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
6	b	8	A	D	E	4	0	9	3	c	5	f	2	7	1

Table 4: The ANF for the 1st proposed S-box.

F1 equation
$\mathbf{X_1 + X_2 + X_3 + X_4 + X_1X_2 + X_1X_3 + X_2X_4 + X_3X_4 + X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4}$
F2 equation
$\mathbf{X_1 + X_3 + X_4 + X_1X_2 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 + X_1X_3X_4}$
F3 equation
$\mathbf{1 + X_1 + X_2 + X_3 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 + X_1X_2X_3}$
F4 equation
$\mathbf{1 + X_1 + X_2 + X_4 + X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_3X_4 + X_1X_2X_4}$

Table 5: The 1st proposed S-box using rule 1.

AA	AG	AC	AT	GA	GG	GC	GT	CA	CG	CC	CT	TA	TG	TC	TT
AT	TC	TG	TT	CA	CT	AG	GG	TA	GC	CG	AA	CC	GT	AC	GA

Table 6: The 1st proposed S-box using rule 2.

AA	AC	AG	AT	CA	CC	CG	CT	GA	GC	GG	GT	TA	TC	TG	TT
AT	TG	TC	TT	GA	GT	AC	CC	TA	CG	GC	AA	GG	CT	AG	CA

Table 7: The 1st proposed S-box using rule 3.

GG	GA	GT	GC	AG	AA	AT	AC	TG	TA	TT	TC	CG	CA	CT	CC
GC	CT	CA	CC	TG	TC	GA	AA	CG	AT	TA	GG	TT	AC	GT	AG

Table 8: The 1st proposed S-box using rule 4.

CC	CA	CT	CG	AC	AA	AT	AG	TC	TA	TT	TG	GC	GA	GT	GG
CG	GT	GA	GG	TC	TG	CA	AA	GC	AT	TA	CC	TT	AG	CT	AC

Table 9: The 1st proposed S-box using rule 5.

GG	GT	GA	GC	TG	TT	TA	TC	AG	AT	AA	AC	CG	CT	CA	CC
GC	CA	CT	CC	AG	AC	GT	TT	CG	TA	AT	GG	AA	TC	GA	TG

Table 10: The 1st proposed S-box using rule 6.

CC	CT	CA	CG	TC	TT	TA	TG	AC	AT	AA	AG	GC	GT	GA	GG
CG	GA	GT	GG	AC	AG	CT	TT	GC	TA	AT	CC	AA	TG	CA	TC

Table 11: The 1st proposed S-box using rule 7.

TT	TC	TG	TA	CT	CC	CG	CA	GT	GC	GG	GA	AT	AC	AG	AA
TA	AG	AC	AA	GT	GA	TC	CC	AT	CG	GC	TT	GG	CA	TG	CT

Table 12: The 1st proposed S-box using rule 8.

TT	TG	TC	TA	GT	GG	GC	GA	CT	CG	CC	CA	AT	AG	AC	AA
TA	AC	AG	AA	CT	CA	TG	GG	AT	GC	CG	TT	CC	GA	TC	GT

Table 13: The ANF for 2nd proposed S-box.

F1 equation
$\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{X}_3 + \mathbf{X}_1\mathbf{X}_3 + \mathbf{X}_1\mathbf{X}_4 + \mathbf{X}_2\mathbf{X}_3 + \mathbf{X}_2\mathbf{X}_4 + \mathbf{X}_3\mathbf{X}_4 + \mathbf{X}_1\mathbf{X}_2\mathbf{X}_3$
F2 equation
$\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{X}_4 + \mathbf{X}_1\mathbf{X}_2 + \mathbf{X}_1\mathbf{X}_3 + \mathbf{X}_1\mathbf{X}_4 + \mathbf{X}_2\mathbf{X}_3 + \mathbf{X}_3\mathbf{X}_4 + \mathbf{X}_1\mathbf{X}_2\mathbf{X}_4$
F3 equation
$\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{X}_3 + \mathbf{X}_4 + \mathbf{X}_1\mathbf{X}_2 + \mathbf{X}_1\mathbf{X}_3 + \mathbf{X}_2\mathbf{X}_4 + \mathbf{X}_3\mathbf{X}_4 + \mathbf{X}_1\mathbf{X}_2\mathbf{X}_3 + \mathbf{X}_1\mathbf{X}_2\mathbf{X}_4 + \mathbf{X}_1\mathbf{X}_3\mathbf{X}_4 + \mathbf{X}_2\mathbf{X}_3\mathbf{X}_4$
F4 equation
$\mathbf{1} + \mathbf{X}_1 + \mathbf{X}_3 + \mathbf{X}_4 + \mathbf{X}_1\mathbf{X}_2 + \mathbf{X}_1\mathbf{X}_4 + \mathbf{X}_2\mathbf{X}_3 + \mathbf{X}_2\mathbf{X}_4 + \mathbf{X}_3\mathbf{X}_4 + \mathbf{X}_1\mathbf{X}_3\mathbf{X}_4$

Table 14: The 2nd proposed S-box using rule 1.

AA	AG	AC	AT	GA	GG	GC	GT	CA	CG	CC	CT	TA	TG	TC	TT
AG	GC	CC	AC	TT	AT	CG	CA	TC	GA	CT	TG	GT	AA	GG	TA

Table 15: The 2nd proposed S-box using rule 2.

AA	AC	AG	AT	CA	CC	CG	CT	GA	GC	GG	GT	TA	TC	TG	TT
AC	CG	GG	AG	TT	AT	GC	GA	TG	CA	GT	TC	CT	AA	CC	TA

Table 16: The 2nd proposed S-box using rule 3.

GG	GA	GT	GC	AG	AA	AT	AC	TG	TA	TT	TC	CG	CA	CT	CC
GA	AT	TT	GT	CC	GC	TA	TG	CT	AG	TC	CA	AC	GG	AA	CG

Table 17: The 2nd proposed S-box using rule 4.

CC	CA	CT	CG	AC	AA	AT	AG	TC	TA	TT	TG	GC	GA	GT	GG
CA	AT	TT	CT	GG	CG	TA	TC	GT	AC	TG	GA	AG	CC	AA	GC

Table 18: The 2nd proposed S-box using rule 5.

GG	GT	GA	GC	TG	TT	TA	TC	AG	AT	AA	AC	CG	CT	CA	CC
GT	TA	AA	GA	CC	GC	AT	AG	CA	TG	AC	CT	TC	GG	TT	CG

Table 19: The 2nd proposed S-box using rule 6.

CC	CT	CA	CG	TC	TT	TA	TG	AC	AT	AA	AG	GC	GT	GA	GG
CG	GA	GT	GG	AC	AG	CT	TT	GC	TA	AT	CC	AA	TG	CA	TC

Table 20: The 2nd proposed S-box using rule 7.

TT	TC	TG	TA	CT	CC	CG	CA	GT	GC	GG	GA	AT	AC	AG	AA
TC	CG	GG	TG	AA	TA	GC	GT	AG	CT	GA	AC	CA	TT	CC	AT

Table 21: The 2nd proposed S-box using rule 8.

TT	TG	TC	TA	GT	GG	GC	GA	CT	CG	CC	CA	AT	AG	AC	AA
TG	GC	CC	TC	AA	TA	CG	CT	AC	GT	CA	AG	GA	TT	GG	AT

Table 22: The ANF for the 3rd proposed S-box.

F1 equation
$\mathbf{X_1 + X_2 + X_3 + X_4 + X_1X_2 + X_1X_3 + X_2X_4 + X_3X_4 + X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4}$
F2 equation
$\mathbf{1 + X_1 + X_3 + X_4 + X_1X_2 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 + X_1X_3X_4}$
F3 equation
$\mathbf{1 + X_1 + X_2 + X_3 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 + X_1X_2X_3}$
F4 equation
$\mathbf{X_1 + X_2 + X_4 + X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_3X_4 + X_1X_2X_4}$

Table 23: The 3rd proposed S-box using rule 1.

AA	AG	AC	AT	GA	GG	GC	GT	CA	CG	CC	CT	TA	TG	TC	TT
GC	CT	CA	CC	TG	TC	GA	AA	CG	AT	TA	GG	TT	AC	GT	AG

Table 24: The 3rd proposed S-box using rule 2.

AA	AC	AG	AT	CA	CC	CG	CT	GA	GC	GG	GT	TA	TC	TG	TT
CG	GT	GA	GG	TC	TG	CA	AA	GC	AT	TA	CC	TT	AG	CT	AC

Table 25: The 3rd proposed S-box using rule 3.

GG	GA	GT	GC	AG	AA	AT	AC	TG	TA	TT	TC	CG	CA	CT	CC
AT	TC	TG	TT	CA	CT	AG	GG	TA	GC	CG	AA	CC	GT	AC	GA

Table 26: The 3rd proposed S-box using rule 4.

CC	CA	CT	CG	AC	AA	AT	AG	TC	TA	TT	TG	GC	GA	GT	GG
AT	TG	TC	TT	GA	GT	AC	CC	TA	CG	GC	AA	GG	CT	AG	CA

Table 27: The 3rd proposed S-box using rule 5.

GG	GT	GA	GC	TG	TT	TA	TC	AG	AT	AA	AC	CG	CT	CA	CC
TA	AC	AG	AA	CT	CA	TG	GG	AT	GC	CG	TT	CC	GA	TC	GT

Table 28: The 3rd proposed S-box using rule 6.

CC	CT	CA	CG	TC	TT	TA	TG	AC	AT	AA	AG	GC	GT	GA	GG
TA	AG	AC	AA	GT	GA	TC	CC	AT	CG	GC	TT	GG	CA	TG	CT

Table 29: The 3rd proposed S-box using rule 7.

TT	TC	TG	TA	CT	CC	CG	CA	GT	GC	GG	GA	AT	AC	AG	AA
CG	GA	GT	GG	AC	AG	CT	TT	GC	TA	AT	CC	AA	TG	CA	TC

Table 30: The 3rd proposed S-box using rule 8.

TT	TG	TC	TA	GT	GG	GC	GA	CT	CG	CC	CA	AT	AG	AC	AA
GC	CA	CT	CC	AG	AC	GT	TT	CG	TA	AT	GG	AA	TC	GA	TG

Input
Input a, b and irreducible polynomial
Output
S-box of size = 4 × 4.
1. For i = 0: 3
2. Apply affine to i
3. Substitute in Equation1:
4. $K = T(aX^2 + b)$Irredu cible polynomial
5. $K \longleftarrow K^{-1}$mod Irredu cible polynomial
6. Repeat step 3 to get a new Y value using the same values of *a* and *b*.
7. S-box[i] = K
8. End for 9. Return S-box.

Algorithm 1: Create new S-box.

10, and 11 to represent A, *T*, C, and *G*, respectively, corresponding to a total of 24 encoding rules. However, in order to retain the biological nature of DNA, only 8 encoding rules are valid as shown in Table 31. Also, the same technique is used as a decoding rule in the decryption process [7, 8, 13].

In image processing, the pixel is considered as the basic unit. The gray value of the pixel point is expressed as an 8-bit binary sequence. For example, if the pixel value is 211 using encoding rule-1 in Table 31, the binary sequence is represented as [11010011] and the corresponding DNA sequence is represented as [C A *G* C]. Similarly, if the DNA sequence is given as TGAT using coding rule-2 in Table 31, a decoded binary sequence of 00110110 is obtained with the decimal number as "134." This is how the DNA sequence is decoded.

The eight convention rules are shown in Table 31.

DNA nucleotides XOR, addition, and subtraction rules are shown in Table 32, Table 33, and Table 34, respectively.

In this work, these rules are used for expanding the S-box process. Section 2 explains the steps followed to get the proposed S-box, and then the analysis of its performance using NIST tests is illustrated in Section 3. Section 0 presents this scheme based on the proposed S-box to protect multimedia data.

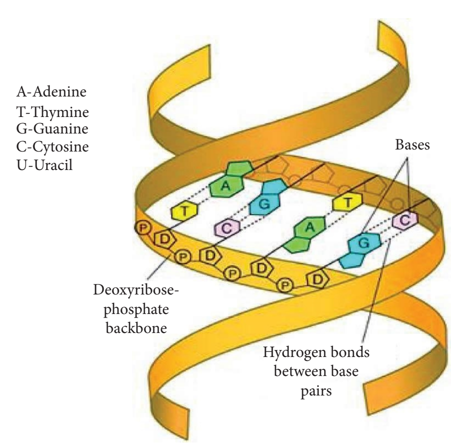


Figure 1: DNA structure.

Table 31: DNA eight rules.

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
00	G	T	T	A	C	A	G	C
01	A	G	C	C	A	G	T	T
10	T	C	G	G	T	C	A	A
11	C	A	A	T	G	T	C	G

Table 32: XOR operation.

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

Table 33: Addition operation.

+	A	T	C	G
A	T	G	A	C
T	G	C	T	A
C	A	T	C	G
G	C	A	G	T

Table 34: Subtraction operation.

−	A	T	C	G
A	C	G	A	T
T	A	C	T	G
C	G	T	C	A
G	T	A	G	C

3. The Proposed S-Box Performance Analysis

NL, SAC, and BIC tests are used for analyzing the S-box. The dynamic properties of these tests have a great advantage in dealing with the relationship between plaintext and ciphertext changes. The algebraic normal form (ANF) method is used to get a polynomial in n -variables as a Boolean function, the input binary bits, with terms of its input bits, and the bitwise sum of these terms. These tests, based on the Boolean function, will be illustrated in brief.

3.1. The Lagrange Interpolation Form. The standard AES (S-box) has a low complexity due to the weakness of these simple algebraic expressions. The new S-boxes of this work are dependent on the multiple steps of transformation to overcome the weakness reason [1, 7]. In this, multiple-step S-box depends on the irreducible polynomial $P(x) = x^4 + x^3 + x^2 + x + 1$ in which the complexity of the algebraic expression is increased to 5 terms which is able to resist differential cryptanalysis. These S-boxes can be formulated using Lagrange interpolation to compute the value of the algebraic resistance attack which is defined as follows:

$$G_k(x) = \frac{(m-m_0)\dots(m-m_{k-1})(m-m_{k+1})\dots(m-m_n)}{(m_k-m_0)\dots(m_k-m_{k-1})(m_k-m_{k+1})\dots(m_k-m_n)}, (k = 0, 1\dots, n-1 = 15), \quad (4)$$

$G_k(x)$ is the coefficient of the Lagrange polynomial

$$S_{x_i} = \sum_{i=0}^{m-1} y_k G_k(x_i) = y_i, (i = 0, 1\dots, m-1 = 15). \quad (5)$$

The algebraic complexity of these generated S-boxes reinforces the security and complexity as it has multiple terms (up to 5) which is shownin the following Tables 35–37.

4. The S-Box Algebraic Performance

The nonlinearity of any block cipher depends on the efficiency of its S-box performance which meets a number of criteria [15, 16], such as the measure of the algebraic attack resistance; this quantity measures the resistance of the S-box against the algebraic attacks.

Theorem 1 (see [10, 11]). *Given m equations in n terms in* GF(2^4)*, the algebraic attack resistance* (AAR) *which is called Γ can be expressed as*

$$\Gamma = \left(\frac{n-m}{k}\right)^{\lceil n-m/k \rceil}. \quad (6)$$

The ideal value of Γ should be greater than 2^6 as proposed in previous research studies [17] to avoid the S-box weakness. The novel family of the S-box, $m = 5$, $n = 30$ terms, and $k = 4$, gets a new result for (AAR) $\Gamma = 2^{6.575}$. This (AAR) $\Gamma = 2^{6.575}$ reflects the strength of these S-boxes against algebraic attacks. In GF(2^8), K = 8, $m = 81$, and $n = 24$ and $\Gamma = 2^{22.9}$.

4.1. S-Box Iteration Period. The S-box iteration period is defined by the following theorem:

Theorem 2 (see [17, 18]). *We assume that S-box bent function is denoted by $P(n)$. $P(n)$ fulfills the periodicity if $P^m(n) = n$ such that m is any positive. For every $n \in$ GF(2^4), the equation $P^m(n) = n$, for the novel S-boxes, the iterative period is increased to the highest value which is 16 for any positive number of* GF(2^4).

Table 35: Coefficients of algebraic expression of the 1st proposed S-box (HEX).

E(X)	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	0	11	6	0	3	0	0	0	3	0	0	0	0	0	0	3

Table 36: Coefficients of algebraic expression of the 2nd proposed S-box (HEX).

E(X)	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
	0	5	7	0	6	0	0	0	3	0	0	0	0	0	0	1

Table 37: Coefficients of algebraic expression of the 3rd proposed S-box (HEX).

E(X)	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
	0	b	6	0	3	0	0	0	3	0	0	0	0	0	0	6

Example 1 (Example 1 Table 38).

The maximum period evaluated for this example is only 2.

EX: 1 ⟶ 1 Period = 1

2 ⟶ C ⟶ 2 Period = 2

3 ⟶ 8 ⟶3 Period = 2

Example 2 (Example 2 Table 39).

One of the proposed S-box periods is mentioned through the following three examples.

EX: 0 ⟶3 ⟶ F ⟶4 ⟶ 8 ⟶*C* ⟶ A ⟶ 9 ⟶ 6 ⟶ 1 ⟶*E*⟶ 2 ⟶*D*⟶ 7 ⟶ 5 ⟶ B ⟶ 0 Period = 16

9 ⟶ 6 ⟶ 1 ⟶*E*⟶ 2 ⟶*D*⟶ 7 ⟶ 5 ⟶ B ⟶ 0 ⟶3 ⟶ F ⟶4 ⟶ 8 ⟶*C* ⟶ A ⟶ 9

Period = 16.

E ⟶ 2 ⟶*D*⟶ 7 ⟶ 5 ⟶ B ⟶ 0 ⟶3 ⟶ F ⟶4 ⟶ 8 ⟶*C* ⟶ A ⟶ 9 ⟶ 6 ⟶ 1 ⟶ E

Period = 16.

4.2. Strict Avalanche Criterion (SAC). The SAC represents the distinction in the output bits according to any input bit change. The theoretical value states that half of the output bits are changed with the change of only one input bit.

Theorem 3 (see [19]). *If* $E(x) = (e_1(x), \ldots, e_m(x))$ *from* $GF(2)^m$ *to* $GF(2)^m$ *is a Boolean function of many outputs,* $\forall \rho = (\rho_m, \rho_{m-1}, \ldots, \rho_1) \epsilon\, GF(2)^m$, $w(\rho) = 1$, *if* $w(e_l(x+a) + e_l(x)) = 2^{n-1}$, $(1 \le l \le m)$, *then* $E(x)$ *satisfies* (SAC).

Theorem 4 (see [7, 19]). *If* $E(x) = (e_1(x), \ldots, e_m(x))$ *from* $GF(2)^m$ *to* $GF(2)^m$ *is a Boolean function of many outputs, the distance to SAC is symbolled by DSAC(F) and its theorem is*

$$\mathrm{DSAC}(\mathrm{E}) = \sum_{l=1}^{n} \sum_{\substack{\rho \in GF(2)^m \\ w(\rho)=1.}} \left| w\left(e_l(x+\rho) + e_l(x) - 2^{m-1}\right) \right|, \tag{7}$$

Table 38: Maximum period.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	C	8	6	F	4	E	3	D	6	A	2	9	7	5

Table 39: Maximum period.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3	e	d	F	8	B	1	5	C	6	9	0	a	7	2	4

If DSAC = 0 that means $E(x)$ fulfills SAC. For the time being, there is no existing S-box that satisfies SAC. Table 40 illustrates the SAC of the new S-box function $E(x) = e_1(x), e_2(x), \ldots, e_m(x))$, and its DSAC is equal to zero.

DSAC (new S-boxes) = 0.

Accordingly, the SAC is satisfied with the rate of change in output bits which is $0.5 * 2^m$ = 8-bit.

In Table 41, there is a comparison between our S-boxes and other boxes which proves that our S-boxes have an ideal value.

From the previous table, we compare by sketching the strict avalanche criterion of the proposed S-box and other S-boxes in Figure 2.

4.3. Bit Independence Criterion (BIC). The BIC parameter is used as a standard to represent the level of security of S-boxes against different attacks [34–36].

Theorem 5 (see [17]). *If* $E(x) = (e_1(x), \ldots, e_m(x))$ *from* $GF(2)^m$ *to* $GF(2)^m$ *is a Boolean function of many outputs, then BIC is made by getting* $m \times m-$ *dimensional matrix* $\mathrm{BIC}(E) = b_{lk}$ *such that* l, k *and* b_{lk} *is defined to be*

$$\mathrm{BIC}(\mathrm{E}) = \sum_{l=1}^{n} \sum_{\substack{\rho \in GF(2)^m \\ w(\rho)=1.}} \left| w\left(e_l(x) + e_k(x) - 2^{m-1}\right) \right|. \tag{8}$$

Our result of 3 S-boxes of BIC is shown in Table 42.

4.4. Nonlinearity (NL). Nonlinearity has a great effect on cryptosystem efficiency. As the value of nonlinearity increases, the resistance against both differential and linear attacks also increases.

$$\mathrm{NL}(e) = 2^{m-1} - \frac{1}{2}\left(\max_{u \in \{0,1\}^m} \left| W_e(u) \right| \right), \tag{9}$$

where $u \in e_2^m$,

$$W_e(u) = \sum_{t \in \{0,1\}^m} (-1)^{e(t) \oplus t.u},$$
$$\mathrm{NL}(e) = \min_{\substack{0 \ne v \in GF(2)^m \\ l(x) \in L_m[X].}} d(v.E(x), l(x)), \tag{10}$$

Mathematically, Walsh's spectrum measures the nonlinearity of the S-boxes.

Table 40: SAC of the proposed S-box.

SAC	f_1	f_2	f_3	f_4
1	8	8	8	8
2	8	8	8	8
4	8	8	8	8
8	8	8	8	8

Table 41: Comparison of the proposed S-boxes and other S-boxes in SAC values.

S-box SAC	Max	Avg.	Min
1st proposed S-box	0.5	0.5	0.5
2nd proposed S-box	0.5	0.5	0.5
3rd proposed S-box	0.5	0.5	0.5
Reference [7]	0.53125	0.50122	0.4375
Reference [3]	0.5625	0.4956	0.4531
Reference [20]	0.625	0.507	0.421
Reference [21]	0.5938	0.5049	0.4219
Reference [22]	0.5938	0.4971	0.4063
Reference [23]	0.5781	0.5017	0.3906
Reference [24]	0.5625	0.4978	0.4375
Reference [25]	0.5781	0.5010	0.4219
Reference [26]	0.6094	0.5037	0.4062
Reference [27]	0.5938	0.5029	0.4219
Reference [28]	0.5938	0.5046	0.4375
Reference [29]	0.5625	0.5017	0.4375
Reference [30]	0.5781	0.4990	0.4063
Reference [31]	0.6094	0.5037	0.3594
Reference [32]	0.5625	0.5049	0.4531
Reference [33]	0.594	0.507	0.406

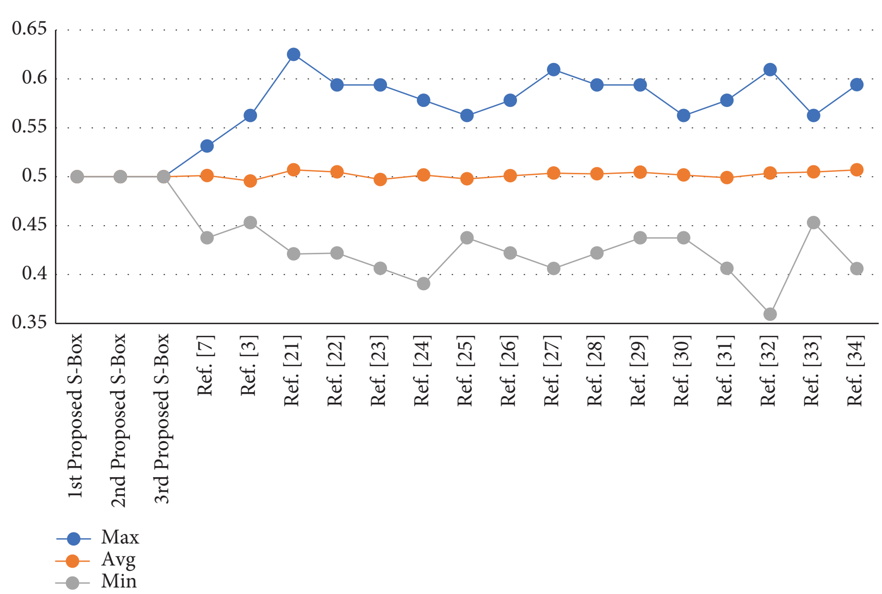


Figure 2: Strict avalanche criterion of the proposed S-box and other S-boxes.

Theorem 6 (see [17]). *We suppose* $E(x) = (e_1(x), \ldots, e_m(x))$ *from* $GF(2)^m$ *to* $GF(2)^m$ *is a Boolean function of many outputs, the nonlinearity computed for* m-bit *Boolean functions* $NL(E)$ *is as follows:*

$L_n[x]$ *is the linear function set from* $GF(2)^m$ *to* $GF(2)^m$, $NL(e)$ *measures the resistance of the S-box against linear attacks. The ideal nonlinear function* $NL(e)$ *should have* $NL(e) = 2^{m-1} - 2^{(m/2)-1} = 6NL(e) = 4$ *for the new S-boxes,*

Table 42: BIC of the new S-boxes.

BIC	β_1	β_2	β_3	β_4
1	—	8	8	8
2	14	—	16	16
4	8	10	—	0
8	8	10	0	—

which is very close to the ideal value of NL(e) *as shown in Tables 43 and 44–45.*

The best value of the nonlinearity can be found in Table 44.

5. Image Encryption Algorithm Based on the Proposed S-BOX

The algorithm is used to encrypt the two modes of the image (RGB and Gray). The encrypted image is generated based on the following steps:

(1) We divide the colored image into three $n \times m$ components
(2) NewKey = OldKey(K_r, K_g, K_b)
(3) We encrypt each pixel by using NewPixel = OldPixel ⊕OldKey(K_r, K_g, K_b)
(4) We save the NewPixel in NewKey (K_r, K_g, K_b)
(5) We collect all components to get the ciphered image

6. Statistical Attack Analysis

The validation of the encryption algorithm strengths toward statistical attacks is based on the following two criteria: correlation coefficients (CC) and histogram analysis as shown in the following sections.

6.1. Correlation Coefficient Analysis. The correlation coefficient is the mirror of image recognition. When the correlation coefficient is high, the visual image is considered understood/recognized. It expresses the relationship between any neighbouring pixels; horizontal, vertical, or diagonal [37]. For the recognized images, they are almost the same. On the other hand, our target is to have a poor/low correlation coefficient for enciphered images [38]. These coefficients are computed using the following expression:

$$\text{Co} = \frac{\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}\left(P_{ij} - \overline{P}\right)\left(C_{ij} - \overline{C}\right)}{\sqrt{\left(\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}\left(P_{ij} - \overline{P}\right)^2\right)\left(\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}\left(C_{ij} - \overline{C}\right)^2\right)}}, \quad (11)$$

where α and β are the image width and height, respectively. Here, C_{ij} and P_{ij} are the pixel positions in the cipher image, and it corresponds in the plain image with coordinates i^{th} column and j^{th} row, respectively. $\overline{P}$ and $\overline{C}$ are the mean values of P and C, respectively. The correlation coefficients of 7-RGB photos of different sizes are calculated in Table 46.

Table 43: Nonlinearity of Boolean functions of the 1st proposed S-box.

B_{e_i}	e_1	e_2	e_3	e_3
NL (B_{e_i})	6	6	4	4

Table 44: Nonlinearity of Boolean functions of the 2nd proposed S-box.

B_{e_i}	e_1	e_2	e_3	e_3
NL (B_{e_i})	6	6	6	4

Table 45: Nonlinearity of Boolean functions of the 3rd proposed S-box.

B_{e_i}	e_1	e_2	e_3	e_3
NL (B_{e_i})	6	4	4	6

The three types of correlation coefficients of 4-RGB photos are shown in detail in Figure 3.

6.2. Information Entropy. The basic concept of information theory is information entropy. It was developed in 1948 by Claude *E.* Shannon at Bell laboratories [39]. The information entropy is a measure of the degree of uncertainty state of the physical system [40]. It is defined mathematically as

$$\text{IE}(m) = \sum_{i=0}^{L-1} p(m_i)\log\frac{1}{p(m_i)}, \quad (12)$$

$$L = 2^m - 1, \quad (13)$$

where $\log(1/p(m_i))$ is the information content associated with the pixel intensity value m_i. Thus, the average amount of the intensity value information in the image is provided by the information entropy as shown in (12). The value of entropy is tested for both plain and ciphered images in Table 47.

From the previous results, it is deduced that the information entropy value of the encrypted image is very close to 8 as expected.

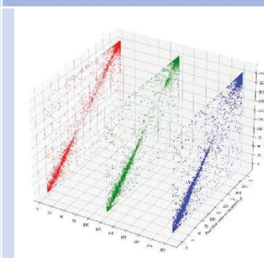
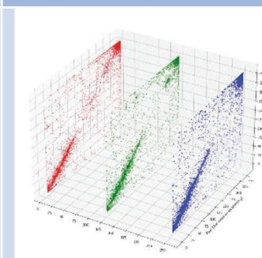
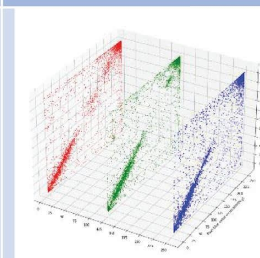
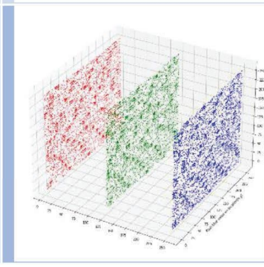
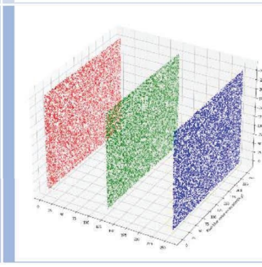
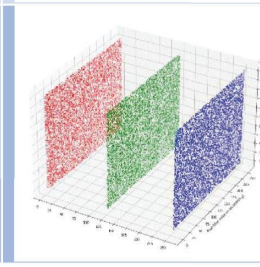
6.3. Histogram Analysis. To show the distribution intensity color levels of the pixels in the image, we refer to the important histogram analysis. This test reflects the value of image resistance against static attacks [41]. Plain images and their related ciphered histogram are shown in Figure 4. A secure image encryption has a uniform distribution of pixel intensity between 0 and 255. The histogram for images in the RGB mode is shown in Figure 4.

7. Differential Attacks

In order to discover more about the enciphering scheme, differential cryptanalysis looks for statistical distributions and trends in the ciphertext. This procedure is necessary

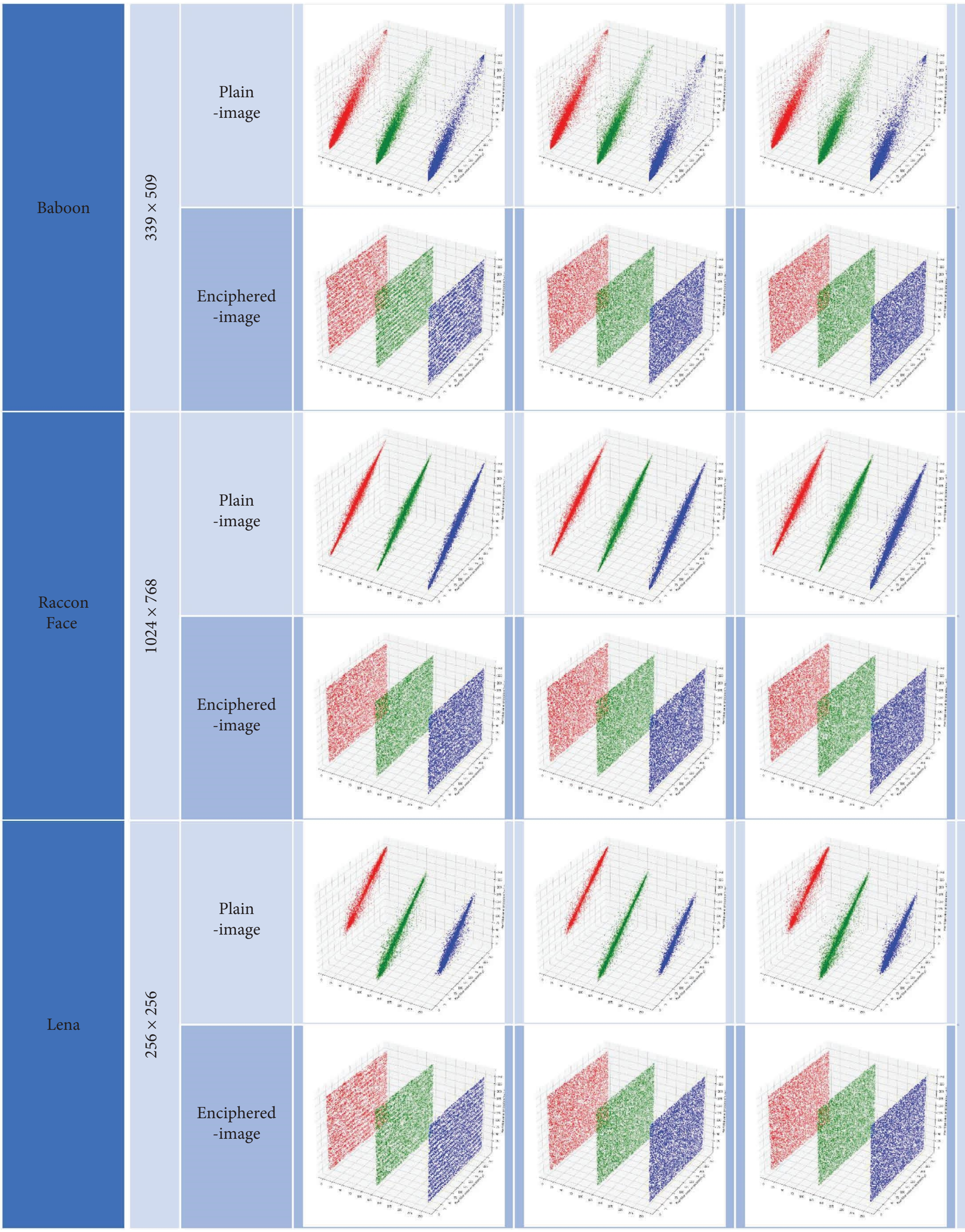
Table 46: The correlation coefficients of the RGB plain images and the corresponding enciphered ones.

	Image	BFOE		Baboon		Raccoon face		Lena		Swirling		Tower		Peppers	
	Size	256 × 256		339 × 509		1024 × 768		256 × 256		728 × 455		648 × 1080		225 × 225	
		Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain
Horizontal	Red	0.7807199	−0.0093272	0.8969669	0.0103413	0.9728871	−0.0088674	0.9523122	0.0044871	0.7797366	0.0263331	0.9733448	0.0442772	0.9360438	−0.0153272
	Green	0.7961294	−0.0392933	0.8709259	0.0124111	0.9729532	−0.0010644	0.94109705	0.0029018	0.7653249	0.0333426	0.8789268	0.0468484	0.9619039	−0.0247432
	Blue	0.8446289	−0.0357815	0.8611989	0.0010846	0.9795084	−0.00579499	0.9089592	0.002322	0.8385775	0.0174346	0.8450444	0.0240907	0.9160306	−0.0003187
Vertical	Red	0.7066377	−0.000255	0.8439172	0.0056568	0.9624684	−0.0107386	0.9733594	0.0059123	0.8576381	0.0099237	0.9774625	−0.0056336	0.9424194	−0.0008091
	Green	0.7308941	−0.0018005	0.8108648	−0.017974	0.9632355	0.0019626	0.9714832	0.0158106	0.8454462	0.0010768	0.8967948	0.0073807	0.9677748	−0.0055361
	Blue	0.7938528	0.0019882	0.8345863	0.0001316	0.9710014	0.0073319	0.9477644	−0.0051086	0.8871041	0.0023223	0.8623912	0.0034202	0.9323405	0.0099321
Diagonal	Red	0.6974984	0.00065899	0.8303537	0.0143824	0.9421205	0.0021898	0.9275691	0.0004557	0.7378458	0.00782	0.9639886	−0.0036234	0.8934853	0.0021819
	Green	0.720062	0.0011495	0.7893617	0.0088829	0.9432355	−0.0008645	0.9182886	−0.0244704	0.7166576	−0.0086022	0.8493233	0.0058216	0.9364671	$-2.883149e-05$
	Blue	0.77231684	0.0052565	0.804431	−0.0192258	0.9564989	−0.0111759	0.87731749	0.013558056	0.77035625	0.00883396	0.8065287	0.0012412	0.861544	0.0063233

Image	Size	Image type	Correlation		
			Horizontal	Vertical	Diagonal
Benha Faculty of Engineering slogan (BFOE)	350 × 306	Plain-image			
		Enciphered -image			

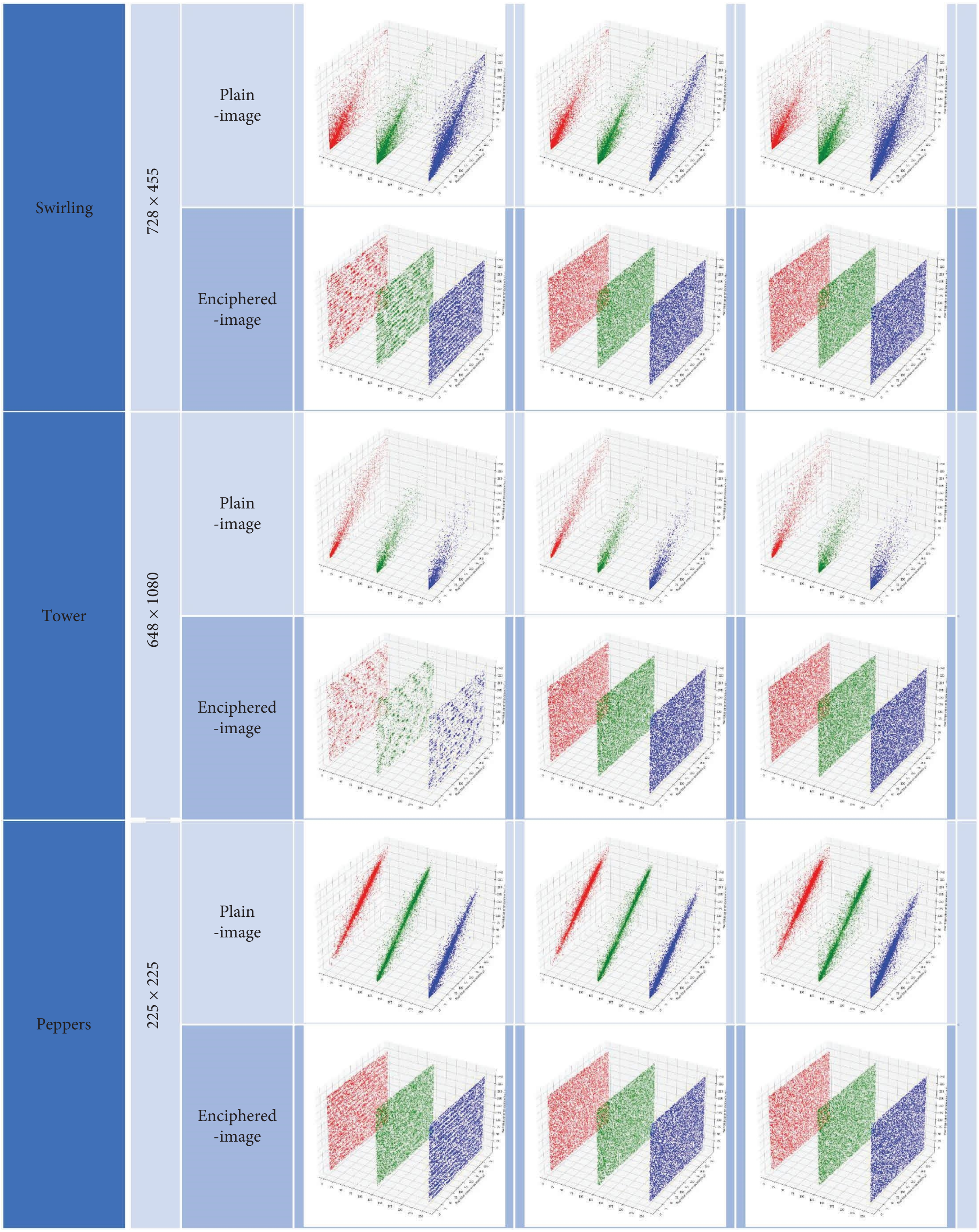
(a)

Figure 3: Continued.



(b)

Figure 3: Continued.



(c)

Figure 3: The correlation of the RGB plain images and their corresponding enciphered ones.

because ciphertext changes that are not random may point to a flaw in the encryption algorithm. By observing information changes, an unauthorized third party can discover what was encrypted or how it was encrypted. In this manner, it is vital to ensure that this strategy is not used. This will be accomplished when the scheme is dependent on minor data

Table 47: Information entropies of the RGB plain images and their corresponding enciphered ones.

Image	Size	Plain image				Enciphered image			
		Red	Green	Blue	Image	Red	Green	Blue	Image
BFOE	350 × 306	4.498424	4.532627	4.72979	4.601032	7.991048	7.991136	7.99298	7.9969
Baboon	339 × 509	7.511691	7.273655	7.01323	7.324211	7.998883	7.998709	7.998993	7.999655
Raccoon face	1024 × 768	7.733968	7.768381	7.802693	7.792045	7.999763	7.99981	7.999749	7.999927
Lena	256 × 256	7.268828	7.597630	6.971601	7.750769	7.996912	7.99725	7.997555	7.999139
Swirling	728 × 455	5.480604	6.026812	7.415581	6.513926	7.999409	7.999413	7.999429	7.999778
Tower	648 × 1080	3.130693	2.516498	2.395896	2.70175	7.995063	7.998601	7.997481	7.998854
Peppers	225 × 225	7.446196	7.700623	7.226196	7.79589	7.996319	7.996243	7.996663	7.99884

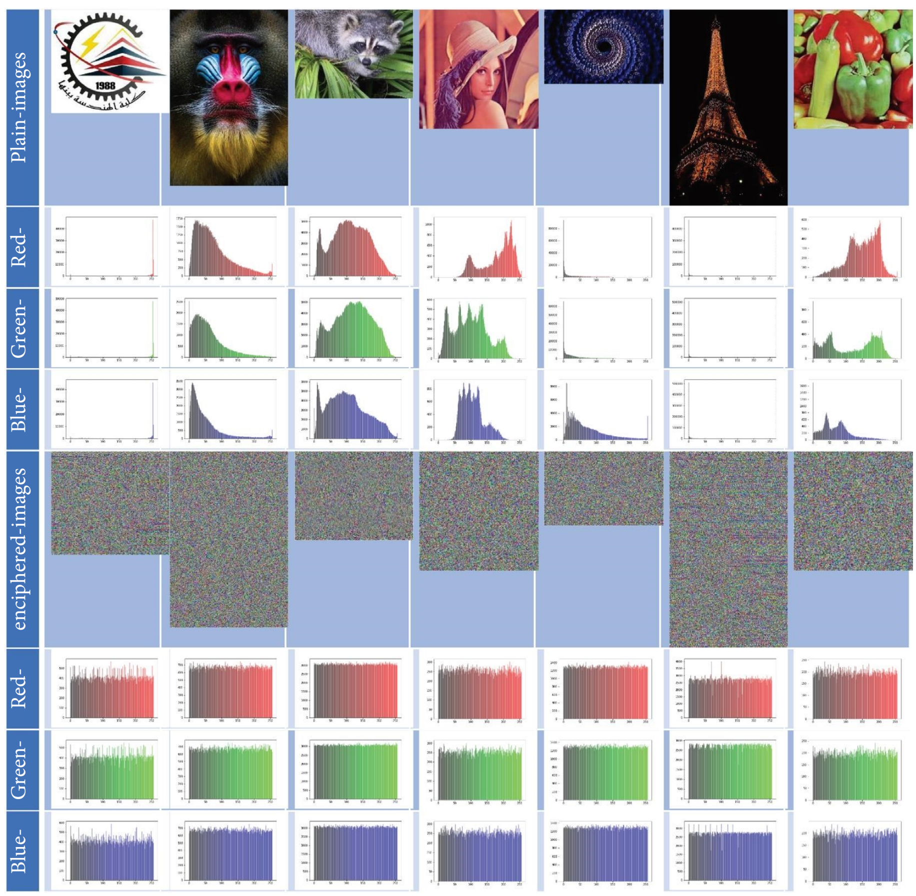


Figure 4: RGB mode plain images and enciphered images using the proposed enciphering scheme based on the proposed S-box with their corresponding histograms.

existing in the image. In order to decide whether our scheme has this feature or not, a number of tests should be executed [42].

7.1. UACI and NPCR. The quality of the image encryption schemes can be estimated by the two estimators. The first of them is the unified average changing intensity UACI which is used to estimate the average difference in intensity between the two ciphered images [42]. The expected theoretical value of UACI is 33.4635%. The UACI is defined as follows:

$$\mathrm{UACI}_{R,G,B} = \frac{1}{\alpha * \beta}\left[\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}\frac{\left|C_1(i,j) - C_2(i,j)\right|}{255}\right], \quad (14)$$

where $C_1(i, j)$ and $C_2(i, j)$ are the enciphered images and their corresponding plain images are the same but a bit changed.

The second is the number of pixels' change rate NPCR which is defined as the percentage of different pixels between two encrypted images [43]. The expected theoretical value of NPCR is 99.6094% and can be calculated by using the

Table 48: Theoretical acceptance interval for the parameter of differential analysis.

Parameters	Size	0.05-Level	0.01-Level	0.001-Level
NPCR	256 × 256	[99.5693, 100]	[99.5527, 100]	[99.5341, 100]
	512 × 512	[99.5893, 100]	[99.5810, 100]	[99.5717, 100]
	1024 × 1024	[99.5994, 100]	[99.5952, 100]	[99.5906, 100]
UACI	256 × 256	[33.2824, 33.6447]	[33.2255, 33.7016]	[33.1594, 33.7677]
	512 × 512	[33.3730, 33.5541]	[33.3445, 33.5826]	[33.3115, 33.6156]
	1024 × 1024	[33.4183, 33.5088]	[33.4040, 33.5231]	[33.3875, 33.5396]

Table 49: UACI and NPCR of the plain and enciphered RGB images.

Images	Size	Plain image				Enciphered image			
		Red	Green	Blue	Image	Red	Green	Blue	Image
BFOE	350 × 306	33.841497	33.721796	33.5271343	33.69681	100	100	100	100
Baboon	339 × 509	33.544424	33.613048	33.510647	33.55604	100	100	100	100
Raccoon face	1024 × 768	33.618098	33.5890617	33.599216	33.602125	100	100	100	100
Lena	256 × 256	33.454524	33.527114	33.6516676	33.544435	100	100	100	100
Swirling	728 × 455	33.591145	33.6105685	33.5981517	33.599955	100	100	100	100
Tower	648 × 1080	33.654057	33.5376276	33.6155911	33.602425	100	100	100	100
Peppers	225 × 225	33.333341	33.4958354	33.6709484	33.500042	100	100	100	100

Table 50: MSE and PSNR of the enciphered RGB images.

Images	Size	The plain-image				PSNR (DB)
		Red	Green	Blue	Image	
BFOE	350 × 306	18747.811363	18325.3397	18478.7679178	18517.306327	5.4550254980815
Baboon	339 × 509	11282.5009418	12295.632845	14148.52294104	12575.55224253	7.135532951228
Raccoon face	1024 × 768	8780.6692822	8737.5787099	9693.97708637	9070.74169283	8.554375611358
Lena	256 × 256	10722.7294464	9053.0839386	7081.427185058	8952.413523356	8.6114022627033
Swirling	728 × 455	17373.16782394	16541.386303	12225.02848692	15379.86087128	6.2612795408327
Tower	648 × 1080	19474.15869913	20223.676083	20464.60989654	20054.14822626	5.108761402491
Peppers	225 × 225	8121.168217284	10953.2516543	10978.60104691	10017.67363951	8.1231348193428

following equation, and all parameters of differential analysis are shown in Table 48.

$$\mathrm{NPCR}_{R,G,B} = \frac{1}{\alpha * \beta}\left[\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta} D(i,j)\right],$$
$$D(i,j) = \begin{cases} 1 & \text{if } C_1(i,j) \neq C_2(i,j), \\ 0 & \text{if } C_1(i,j) = C_2(i,j). \end{cases} \quad (15)$$

The calculated values of both tests are shown in Table 49.

7.2. Data Loss. Data loss occurs when all elements that store the information are damaged, and the redundancy of the record cannot cover this loss. The main causes of data loss are human error, hardware destruction, software damage, and viruses.

7.2.1. MSE and PSNR. Mean squared error (MSE) or mean squared deviation (MSD) measure the deviation of the predicted enciphered image from the actual original Palin image values. As the difference between them increases, the MSE increases. It is defined as follows:

$$\mathrm{MSE}_{R,G,B} = \frac{1}{\alpha * \beta}\left[\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}\left(C_{ij} - P_{ij}\right)^2\right]. \quad (16)$$

The peak signal-to-noise ratio (PSNR) measures the quality of how an image can be represented, by comparing its maximum power to the corrupting noisy power. PSNR is calculated as follows:

$$\mathrm{PSNR} = 20 * \log\left(\frac{P_{\mathrm{MAX}}}{\sqrt{\mathrm{MSE}}}\right), \quad (17)$$

where P_{MAX} is the pixel expected maximum value.

The MSE and PSNR for seven enciphered images are shown in Table 50.

It is deduced that the smaller the PSNR value is, the higher the difference between the images occurs.

7.2.2. Mean Absolute Error (MAE). MAE is defined as the mean difference between the original image and the ciphered image according to the following equation. The MAE of the enciphered RGB images is shown in Table 51.

Table 51: MAE of the enciphered RGB images.

Images	Size	The plain-image			
		Blue	Red	Blue	Image
BFOE	350 × 306	114.83536881421	115.95080298787	114.83536881421	115.03702147527
Baboon	339 × 509	97.972668950047	86.716252006647	97.972668950047	91.811821818859
Raccoon face	1024 × 768	80.54194132487	76.953487396242	80.54194132487	78.088364071317
Lena	256 × 256	70.332916259766	84.708786010742	70.332916259766	77.655649820964
Swirling	728 × 455	90.480346576541	110.51264943851	90.480346576541	102.76645232061
Tower	648 × 1080	122.58593106999	118.76022233658	122.58593106999	121.00813709805
Peppers	225 × 225	85.542083950626	74.443753086428	85.542083950626	81.821655967087

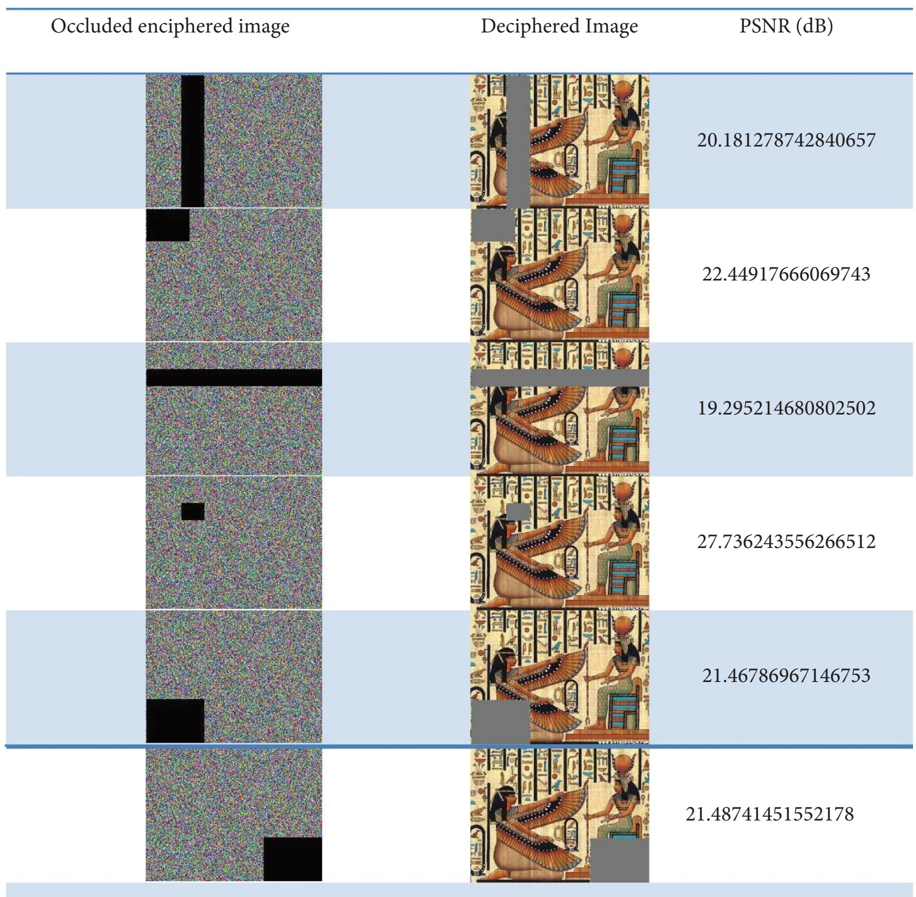


Figure 5: Experimental results of occlusion attacks.

$$\mathrm{MAE}_{R,G,B} = \frac{1}{\tau * \mu}\left[\sum_{i=1}^{\tau}\sum_{j=1}^{\mu}\left|C(i,j) - P(i,j)\right|\right]. \quad (18)$$

7.2.3. Occlusion Attack. This section shows how any change in the intensity value of the cipher image has small effects on the intensity of the encrypted image (plain text) which can be defined by the occlusion attack [44]. The importance of this property comes from the plain image that can be recovered although of the existence of any distortion or losses of the cipher image. Digital images are highly sensitive to noise existing in the digital transmission process. Pharaohs' picture image was chosen as the plain image, and our S-box can recover this plain image from noisy or deteriorated images. The experimental result of the occlusion attack is shown in Figure 5.

8. Conclusion

The presented work consists of three light weight S-boxes suitable for real-time cryptographic purposes and is compared with other existing S-boxes' performance, and, as a result of this comparison, the following advantages are found in these new S-boxes:

(1) Very fast as it depends on 4 bits only
(2) Provide DSAC ideal value equals to zero
(3) Provide a maximum period equals to 16
(4) Provide high-security performance when compared to other S-boxes
(5) DNA coding is applied to extend each S-box into eight S-boxes to generate twenty-four S-boxes which improves the efficiency of the encrypted image

The system demonstrates its robust ability to defend the encrypted image from statistical, differential, data loss, and occlusion attacks.

Data Availability

The data used to support the findings of the study are included within the article.

Disclosure

The second author in this study is the editor in this journal and he has a waiver for fee-free.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to express their deep and sincere gratitude to post student Hend Ali for her cooperation to finish this study.

References

[1] L. Jinomeiq, W. Baoduui, and W. Xinmei, "One AES S-box to increase complexity and its cryptanalysis," *Journal of Systems Engineering and Electronics*, vol. 18, no. 2, pp. 427–433, 2007.
[2] H. R. Yassein, N. M. G. Al-Saidi, and A. K. Farhan, "A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 2, pp. 523–542, 2020.
[3] M. S. Mahmood Malik, M. A. Ali, M. A. Khan et al., "Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices," *IEEE Access*, vol. 8, pp. 35682–35695, 2020.
[4] J. M. Cheung, "The design of s-boxes," in *Proceedings of the Lecture notes in computer sciences; 218 on Advances in cryptology CRYPTO 85*, Berlin, Heidelberg, February 2010.
[5] M. Mansour∗, W. Elsobky, A. Hasan, and W. Anis, "Appraisal of multiple AES modes behavior using traditional and enhanced substitution boxes," *International Journal of Recent Technology and Engineering*, vol. 8, no. 5, pp. 530–539, 2020.
[6] A. Kumar and S. S.-B. O. X. A. Tejani, "S-BOX architecture," *Communications in Computer and Information Science*, pp. 17–27, 2019.
[7] H. A. M. A. Basha, A. S. S. Mohra, T. O. M. Diab, and W. I. E. Sobky, "Efficient image encryption based on new substitution box using DNA coding and bent function," *IEEE Access*, vol. 10, pp. 66409–66429, 2022.
[8] A. H. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. I. Udzir, "A new DNA-based S-box," *International Journal of Engineering and Technology (IJET)*, vol. 15, pp. 1–9, 2015.
[9] A. Majumdar, A. Biswas, A. Majumder, S. K. Sood, and K. L. Baishnab, "A novel DNA-inspired encryption strategy for concealing cloud storage," *Frontiers of Computer Science*, vol. 15, no. 3, Article ID 153807, 2020.
[10] W. Hafez, H. Saeed, and A. N. Elwakeil, "Different types of attacks on block ciphers," *International Journal of Recent Technology and Engineering*, vol. 9, no. 3, pp. 28–31, 2020.
[11] E. W. Afify, W. I. E. sobky, A. Twakol, and R. A. Alez, "Performance analysis of advanced encryption standard (AES) S-boxes," *International Journal of Recent Technology and Engineering*, vol. 9, no. 1, pp. 2214–2218, 2020.
[12] N. E. El-Meligy, T. O. Diab, A. S. S. Mohra, A. Y. Hassan, and W. I. El-Sobky, "A novel dynamic mathematical model applied in hash function based on DNA algorithm and chaotic maps," *Mathematics*, vol. 10, no. 8, Article ID 10081333, 2022.
[13] A. K. Farhan, R. S. Ali, and G. H. Abdul-Majeed, "Proposal new s-box depending on DNA computing and mathematical operations," in *Proceedings of the 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, Baghdad, Iraq, May 2016.
[14] A. K. Farhan, R. S. Ali, H. R. Yassein, N. M. G. Al-Saidi, and G. H. Abdul-Majeed, "A new approach to generate multi S-boxes based on RNA computing," *International Journal of Innovative Computing, Information and Control (IJICIC)*, vol. 16, pp. 331–348, 2020.
[15] K. Mohamed, M. N. M. Pauzi, F. H. H. M. Ali, S. Ariffin, and N. H. N. Zulkipli, "Study of s-box properties in block cipher," in *Proceedings of the 2014 International Conference on Computer, Communications, and Control Technology (I4CT)*, Langkawi, Malaysia, October 2014.
[16] A. A. Abdel-Hafez, R. Elbarkouky, and W. Hafez, "Comparative study of algebraic attacks," *Wageda Comparative Study of Algebraic Attacks*, vol. 3, no. 5, pp. 85–90, 2016.
[17] J. Cui, L. Huang, H. Zhong, C. Chang, and W. Yang, "An improved AES S-box and its performance analysis," *International Journal of Innovative Computing, Information and Control (IJICIC)*, vol. 7, pp. 2291–2302, 2011.
[18] E. w. afify∗, W. I. E. sobky, A. Twakol, and R. A. Alez, "Algebraic construction of powerful substitution box," *International Journal of Recent Technology and Engineering*, vol. 8, no. 6, pp. 405–409, 2020.
[19] W. I. E. Sobky, A. R. Mahmoud, A. S. Mohra, and T. El-Garf, "Enhancing hierocrypt-3 performance by modifying its S-box and modes of operations," *Journal of Communications*, pp. 905–912, 2020.
[20] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, "A projective general linear group based algorithm for the construction of substitution box for block ciphers," *Neural Computing & Applications*, vol. 22, no. 6, pp. 1085–1093, 2013.
[21] F. Özkaynak and A. B. Özer, "A method for designing strong S-boxes based on chaotic lorenz system," *Physics Letters A*, vol. 374, no. 36, pp. 3733–3738, 2010.
[22] R. Guesmi, M. A. Ben Farah, A. Kachouri, and M. Samet, "A novel design of chaos based S-boxes using genetic algorithm techniques," in *Proceedings of the 2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*, pp. 678–684, Doha, Qatar, November 2014.
[23] G. Ivanov, N. Nikolov, and S. Nikova, "Cryptographically strong S-boxes generated by modified immune algorithm," in

Proceedings of the Cryptography and Information Security in the Balkans, E. Pasalic and L. R. Knudsen, Eds., pp. 31–42, Springer International Publishing, Cham, Champa, 2016.
[24] M. Ahmad, E. Al-Solami, A. M. Alghamdi, and M. A. Yousaf, "Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures," *IEEE Access*, vol. 8, pp. 110397–110411, 2020.
[25] D. A. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlinear Dynamics*, vol. 100, no. 1, pp. 699–711, 2020.
[26] F. Özkaynak, "On the effect of chaotic system in performance characteristics of chaos based S-box designs," *Physica A: Statistical Mechanics and Its Applications*, vol. 550, Article ID 124072, 2020.
[27] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.
[28] M. Rodinko, R. Oliynykov, and Y. Gorbenko, "Optimization of the high nonlinear S-boxes generation method," *Tatra Mountains Mathematical Publications*, vol. 70, no. 1, pp. 93–105, 2017.
[29] A. Razaq, H. Alolaiyan, M. Ahmad et al., "A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups," *IEEE Access*, vol. 8, pp. 75473–75490, 2020.
[30] S. Ibrahim, H. Alhumyani, M. Masud et al., "Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps," *IEEE Access*, vol. 8, pp. 160433–160449, 2020.
[31] A. A. Abd El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics & Laser Technology*, vol. 116, pp. 92–102, 2019.
[32] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of cryptographic S-boxes based on mobius transformation and chaotic tent-sine system," *IEEE Access*, vol. 7, pp. 173273–173285, 2019.
[33] A. H. Zahid and M. J. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, Article ID 11030437, 2019.
[34] A. H. Zahid, M. J. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Entropy*, vol. 21, no. 3, Article ID 21030245, 2019.
[35] S. RoyChatterjee, K. Sur, and M. Chakraborty, "Study on S-box properties of convolution coder," in *Proceedings of the Proceedings of International Ethical Hacking Conference 2019*, M. Chakraborty, S. Chakrabarti, and V. E. Balas, Eds., pp. 119–128, Springer, Singapore, 2020.
[36] N. A. Azam, U. Hayat, and M. Ayub, "A substitution box generator, its analysis, and applications in image encryption," *Signal Processing*, vol. 187, Article ID 108144, 2021.
[37] M. Khan and H. M. Waseem, "A novel image encryption scheme based on quantum dynamical spinning and rotations," *PLoS One*, vol. 13, no. 11, Article ID 206460, 2018.
[38] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24–39, 2015.
[39] J. x. Chen, Z. l. Zhu, C. Fu, L. b. Zhang, and Y. Zhang, "An efficient image encryption scheme using lookup table-based confusion and diffusion," *Nonlinear Dynamics*, vol. 81, no. 3, pp. 1151–1166, 2015.
[40] Y. Zhang, X. Li, and W. Hou, "A fast image encryption scheme based on AES," in *Proceedings of the 2017 2nd International Conference on Image, Vision and Computing (ICIVC)*, Chengdu, China, July 2017.
[41] Y. Kang, L. Huang, Y. He, X. Xiong, S. Cai, and H. Zhang, "On a symmetric image encryption algorithm based on the peculiarity of plaintext DNA coding," *Symmetry*, vol. 12, no. 9, Article ID 12091393, 2020.
[42] A. H. Zahid, L. Tawalbeh, M. Ahmad et al., "Efficient dynamic S-box generation using linear trigonometric transformation for security applications," *IEEE Access*, vol. 9, pp. 98460–98475, 2021.
[43] A. A. Shah, S. A. Parah, M. Rashid, and M. Elhoseny, "Efficient image encryption scheme based on generalized logistic map for real time image processing," *Journal of Real-Time Image Processing*, vol. 17, no. 6, pp. 2139–2151, 2020.
[44] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A novel color image encryption algorithm based on three-dimensionalchaotic maps and reconstructiontechniques," *IEEE Access*, vol. 9, pp. 61334–61345, 2021.