

# Security and Communication Networks

## Fast Novel Efficient S-Boxes with Expanded DNA Codes

Abeer Tariq Maalood<sup>1</sup>, Alaa Kadhim Farhan<sup>2\*</sup>, Wageda I. El-Sobky<sup>3</sup>, Hany Nasry Zaky<sup>4</sup>, Hossam L. Zayed<sup>5</sup>, Hossam E. Ahmed<sup>6,7</sup>, Tamer O. Diab<sup>7</sup>

<sup>1</sup>Computer sciences Department, University of Technology, Iraq, [abeer.t.maalood@uotechnology.edu.iq](mailto:abeer.t.maalood@uotechnology.edu.iq)

<sup>2</sup>Computer sciences Department, University of Technology, Iraq, [Alaa.k.farhan@uotechnology.edu.iq](mailto:Alaa.k.farhan@uotechnology.edu.iq)

<sup>3</sup>Department of Basic Engineering Sciences, Benha Faculty of Engineering, Benha University, Benha 13511, Egypt; [wageda.alsobky@bhit.bu.edu.eg](mailto:wageda.alsobky@bhit.bu.edu.eg)

<sup>4</sup>Mathematics Department, Military Technical College, Cairo, Egypt; [hanynasry@mtc.edu.eg](mailto:hanynasry@mtc.edu.eg)

<sup>5</sup>Electrical Engineering Department, Benha Faculty of Engineering, Benha University, Benha 13511, Egypt; [hossam.zayed@bhit.bu.edu.eg](mailto:hossam.zayed@bhit.bu.edu.eg)

<sup>6</sup>Electrical Engineering Department, Benha Faculty of Engineering, Benha University, Benha 13511, Egypt [hossameldin.ibrahim@bhit.bu.edu.eg](mailto:hossameldin.ibrahim@bhit.bu.edu.eg);

<sup>7</sup>Electrical Engineering Department, Benha Faculty of Engineering, Benha University, Benha 13511, Egypt [tamer.almarsafawy@bhit.bu.edu.eg](mailto:tamer.almarsafawy@bhit.bu.edu.eg)

\*Correspondence: [Alaa.k.farhan@uotechnology.edu.iq](mailto:Alaa.k.farhan@uotechnology.edu.iq);

### Abstract

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  $4 \times 4$  S-box for the lightweight constructions results in compact hardware, speed up the computational capability of the security algorithm unlike the  $8 \times 8$  S-box. This work presents an 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 attacks criteria such as interpolation attacks, avalanche effect, nonlinearity...etc. The great advantage of the introduce S-Boxes is that its DSAC is the ideal value which is equal to zero. Also, other tests are executed on these S-Boxes that guaranteed its robustness and excellent security performance. Moreover, the experiments have 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.

**Keywords:** S-Box; DNA code; Algebraic attack; DSAC

### 1. Introduction

The general wireless communication protocols like 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 transmitter and receiver. Narrow band IoT (NB-IoT) of LTE is presented to obtain high throughput, low power consumption and high battery life because it is provided services form access to network through

physical layer [2]. To address the requirements of IoT, NB-IoT architecture is simplified from evolved packet core structure. The NB-IoT is 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 number of control bits to enhance robustness and efficiency. A light weight encryption system is popular used for IoT implementation because of bit permutation group operation. The rapid growth in computer network and multimedia information technology attracts a lot of researchers towards the security and protection of digital data transmission via internet. The most important and widely used digital media are the image information as it contains a huge amount of data with strong correlation and redundancy [1].

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 [2]. From these algorithms are hiding of data, water marking and 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 this data from exploitation, alteration or being missed and also to make sure that a specific receiver can read and comprehend this data. In any cryptographic algorithms, 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), Rivest-Shamir-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 and uses both permutations and diffusion Substitution Box (S-Box) or vice versa. There's a candid link between security and confusion; as 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].

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

This paper is organized as follows: Section 2 presents the proposed novel fast S-Box. Section 3 presents the performance of the proposed S-Box while in 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 [45-46], resulting in the problem that the pseudorandom sequence appears periodically. So, our main idea depends on algebraic construction for novel S-box evaluation. We sure from all the values of all testes plus in IOT applications they depends on light weight encryption based on (4x4)s-boxes because they very fast, accurate and secure all these conditions were found in our work

This section is divided into two parts. Part one, presented in 2.1, explains the basic novel idea of the proposed S-Box. And 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(2<sup>4</sup>).

A new very secure simple construction high non-linear S-Box is generated by the following steps. Apply firstly affine transformation which is defined by:

$$k = T(aX^2 + b) = \begin{bmatrix} a_3 & a_2 & a_1 & a_0 \\ a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \end{bmatrix} \begin{bmatrix} X_3 \\ X_2 \\ X_1 \\ X_0 \end{bmatrix}^2 + \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} \quad (1)$$

$$a = 0x7, 0xD \quad \text{and} \quad b = 0x3, 0x1, 0x6$$

the multiplicative inverse is Computed of the result  $k: k = k^{-1}$  in GF(2<sup>8</sup>), that 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:

$$k = T(ak^2 + b) = \begin{bmatrix} a_3 & a_2 & a_1 & a_0 \\ a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \end{bmatrix} \begin{bmatrix} k_3 \\ k_2 \\ k_1 \\ k_0 \end{bmatrix}^2 + \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} \quad (3)$$

$$a = 0x7 \text{ and } 0xD \quad \text{and} \quad b = 0x3, 0x1 \text{ and } 0x6$$

The family of generated S-boxes are shown in Table 1, Table 2 and Table 3.

Now, the values are converted into the binary form, and its length must be 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 will be mentioned, we can obtain for each S-Box different eight-S-boxes written in appendices' tables. The algorithm used to generate the proposed S-Box can be presented in the following steps:

Input	Input a, b and Irreducible polynomial
Output	S-Box of size =4 × 4.
	<ol style="list-style-type: none"> <li>1. For i = 0: 3</li> <li>2. Apply affine to i</li> <li>3. Substitute in Equ.1:</li> <li>4. <math>K = T(aX^2 + b) \text{ mod Irreducible polynomial}</math></li> <li>5. <math>K \leftarrow K^{-1} \text{ mod Irreducible polynomial}</math></li> <li>6. Repeat step 3 to get new Y value using the same values of a, b.</li> <li>7. <math>S\text{-Box}[i] = K</math></li> <li>8. End For</li> <li>9. Return S-Box</li> </ol>

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

The three S-Boxes presented in Tables 1,2 and 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 the living creatures. In figure 1, the Adenine, Cytosine, Guanine and Thymine are the DNA computing bases used for data representation 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 are that the image pixels are converted to 8-bit binary and use 00, 01, 10, 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 4. 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 pixel point is expressed as 8-bit binary sequence. For example, if the pixel value is 211 using encoding rule-1 in Table 4, 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 4 a decoded binary sequence of 00110110 is obtained with the decimal number is "134". And, this is how the DNA sequence is decoded.

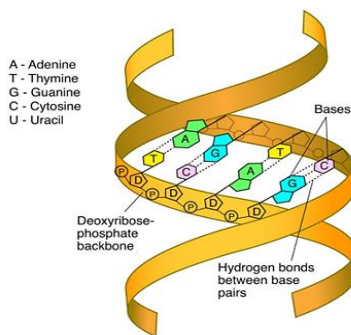


Figure 1. DNA Structure

The eight convention rules are shown in Table 4.

Table 4. DNA eight rules

	C <sub>1</sub>	C <sub>2</sub>	C <sub>3</sub>	C <sub>4</sub>	C <sub>5</sub>	C <sub>6</sub>	C <sub>7</sub>	C <sub>8</sub>
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

DNA nucleotides XOR, addition, and subtraction rules are shown in Table 5, Table 6, and Table 7 respectively.

Table 5. 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 6. 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 7. 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

In this work, these rules are used during 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. In Section 0 presents this scheme based on proposed S-Box to protect multimedia data.

### 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 then 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 low complexity due to the weakness of these simple algebraic expressions. The new S-boxes of this work are depending on multiple steps of transformation to overcome the weakness reason [2,7]. 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 and 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:

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

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

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

The algebraic complexity of these generated S-Boxes reinforces the security and complexity as it has multiple terms (up to be 5) is written in the following tables (8-10)

Table 8. 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 9. 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 10. 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

#### 4. The S-Box algebraic performance

The non-linearity of the 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 attacks resistance; this quantity measures the resistance of the S-Box against the algebraic attacks.

##### Theorem 1 [10,11].

Given  $m$  equations in  $n$  terms in  $GF(2^4)$ , the algebraic attacks resistance (AAR) which is called  $\Gamma$ :

$$\Gamma = \left( \frac{n-m}{k} \right)^{\lfloor \frac{n-m}{k} \rfloor} \quad (6)$$

The ideal value of  $\Gamma$  should be greater than  $2^6$  as proposed in previous researches [17] to avoid the S-box weakness. The novel family of the S-box,  $m = 5$ ,  $n = 30$  terms, and  $k = 4$ , gets 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  $n=24$ ,  $\Gamma = 2^{22.9}$ .

##### 4.1 S-Box Iteration period

The S-Box iteration period is defined in the following theorem.

**Theorem 2 [17,18]:** Assume S-box bent function is donated by  $P(n)$ .  $P(n)$  fullfills 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  $GF(2^4)$ .

Example 4.1

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

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 4.2

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

One of the proposed S-Box period 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 [19].** If  $E(x) = (e_1(x), \dots, e_m(x))$  from  $GF(2)^m$  to  $GF(2)^m$  is a Boolean function of many outputs,  $\forall \rho = (\rho_m, \rho_{m-1}, \dots, \rho_1) \in GF(2)^m$ ,  $w(\rho) = 1$ , if  $w(e_l(x + \rho) + e_l(x)) = 2^{n-1}$ , ( $1 \leq l \leq m$ ), then  $E(x)$  satisfies (SAC).

**Theorem 4 [7,19]:** If  $E(x) = (e_1(x), \dots, e_m(x))$  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

$$DSAC(E) = \sum_{l=1}^n \sum_{\substack{\rho \in GF(2)^m \\ w(\rho)=1}} |w(e_l(x + \rho) + e_l(x) - 2^{m-1})| \quad (7)$$

If DSAC = 0 that means  $E(x)$  fulfills SAC. For the time being there is no existing S-box satisfies SAC. Table 11 illustrates the SAC of the new S-box function  $E(x) = (e_1(x), e_2(x), \dots, e_m(x))$ , and its DSAC equals to zero.

DSAC (new S-Boxes) = 0

Table 11. SAC of the proposed S-Box

SAC	f <sub>1</sub>	f <sub>2</sub>	f <sub>3</sub>	f <sub>4</sub>
<b>1</b>	8	8	8	8
<b>2</b>	8	8	8	8
<b>4</b>	8	8	8	8
<b>8</b>	8	8	8	8

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

In Table 12 there's Comparison between our S-Boxes and other boxes which prove that's our S-Boxes have ideal value.

Table 12. Comparison of proposed S-Boxes and other S-Boxes in SAC values

S-Box SAC	Max	Avg.	Min
1 <sup>st</sup> Proposed S-Box	0.5	0.5	0.5
2 <sup>nd</sup> Proposed S-Box	0.5	0.5	0.5
3 <sup>rd</sup> Proposed S-Box	0.5	0.5	0.5
Ref. [7]	0.53125	0.50122	0.4375
Ref. [3]	0.5625	0.4956	0.4531
Ref. [23]	0.625	0.507	0.421
Ref. [24]	0.5938	0.5049	0.4219
Ref. [25]	0.5938	0.4971	0.4063
Ref. [26]	0.5781	0.5017	0.3906
Ref. [27]	0.5625	0.4978	0.4375
Ref. [28]	0.5781	0.5010	0.4219
Ref. [29]	0.6094	0.5037	0.4062
Ref. [30]	0.5938	0.5029	0.4219
Ref. [31]	0.5938	0.5046	0.4375
Ref. [32]	0.5625	0.5017	0.4375
Ref. [33]	0.5781	0.4990	0.4063
Ref. [34]	0.6094	0.5037	0.3594
Ref. [35]	0.5625	0.5049	0.4531
Ref. [36]	0.594	0.507	0.406

From the previous table we compare by sketch Strict Avalanche Criterion of the proposed S-Box and other S-Boxes in Figure 2.

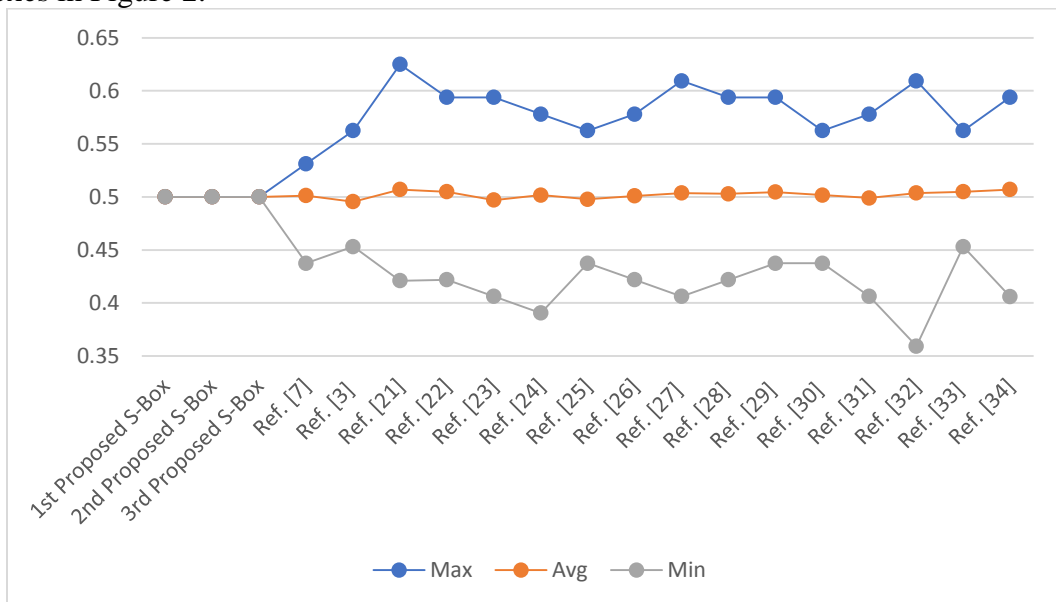


Figure 2. Strict Avalanche Criterion of the proposed S-Box and other S-Boxes



### 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 [20–22].

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

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

Our result of 3 S-Boxes of BIC is shown in Table 13.

Table 13. BIC of the new S-Boxes

BIC	$\beta_1$	$\beta_2$	$\beta_3$	$\beta_4$
1	-	8	8	8
2	14	-	16	16
4	8	10	-	0
8	8	10	0	-

### 4.4 Non-Linearity (NL)

Nonlinearity has a great effect in the cryptosystem efficiency. As the value of non-linearity increases, the more resistance against both differential and linear attacks.

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

Where  $u \in e_2^m$ ,

$$W_e(u) = \sum_{t \in \{0,1\}^m} (-1)^{e(t) \oplus t \cdot u} \quad (10)$$

$$NL(e) = \min_{\substack{0 \neq v \in GF(2)^m \\ l(x) \in L_m[X]}} d(v \cdot E(x), l(x)) \quad (11)$$

Mathematically, Walsh's spectrum measures the Non-linearity of the S-Boxes.

**Theorem 6 [17]:** Suppose  $E(x) = (e_1(x), \dots, e_m(x))$  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:

$L_n[x]$  is the linear functions set from  $GF(2)^m$  to  $GF(2)^m$ .

$NL(e)$  measures the resistance of the S-Box against linear attacks. The ideal Non-Linear function  $NL(e)$  should have  $NL(e) = 2^{m-1} - 2^{\frac{m}{2}-1} = 6$ .  $NL(e) = 4$  for the new S-boxes, which is very close to the ideal value of  $NL(e)$  as shown in the Tables 14, 15 and 16.

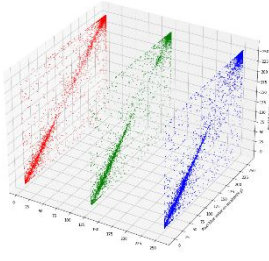
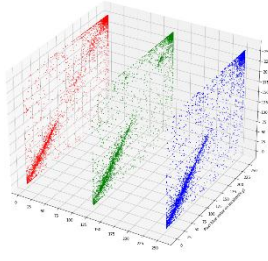
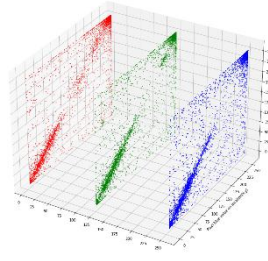
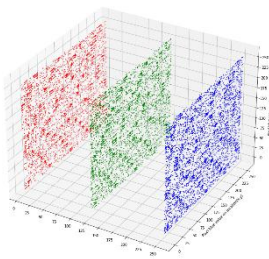
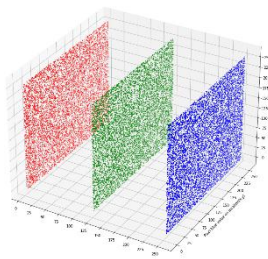
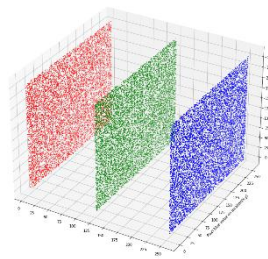
Table 14. Non-Linearity of Boolean functions of the 1st proposed S-Box

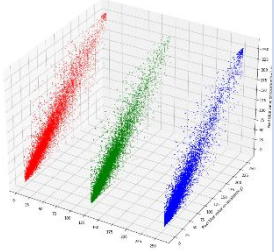
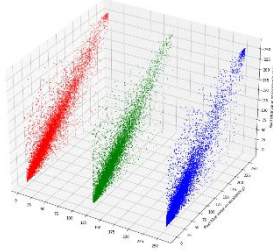
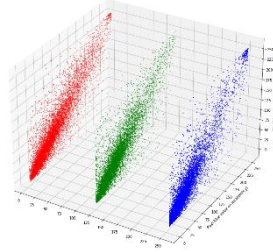
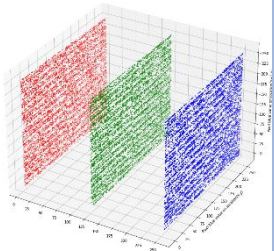
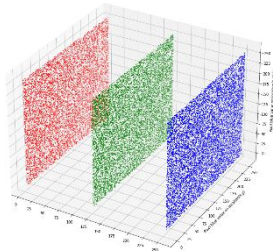
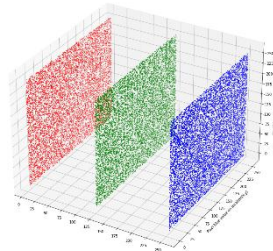
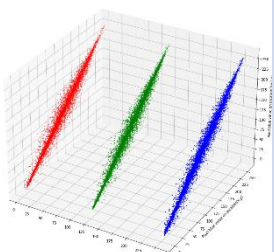
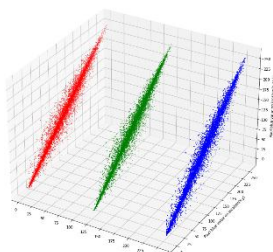
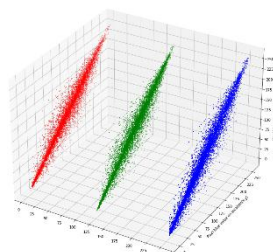
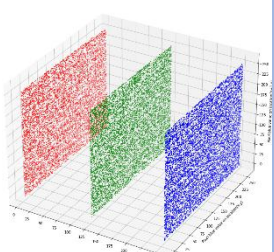
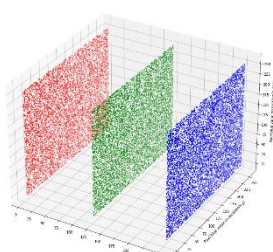
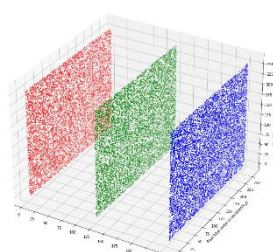
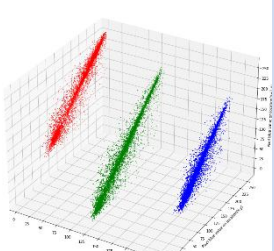
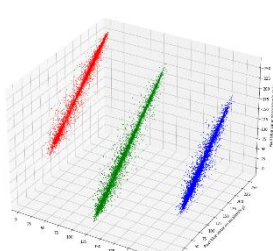
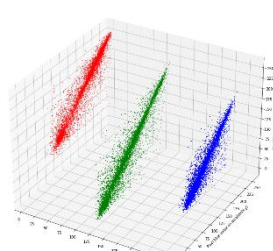
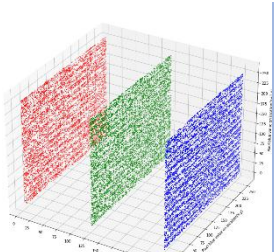
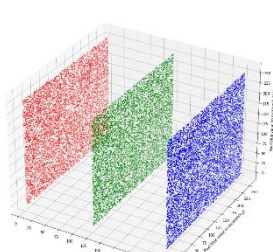
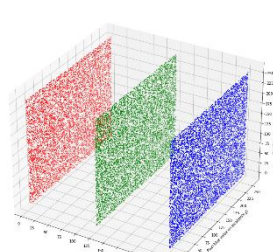
$B_{e_i}$	$e_1$	$e_2$	$e_3$	$e_3$
$NL(B_{e_i})$	6	6	4	4



<b>Horizontal</b>	Red	0.780 7199	- 0.009 3272	0.896 9669	0.010 3413	0.972 8871	- 0.008 8674	0.952 3122	0.004 4871	0.779 7366	0.026 3331	0.973 3448	0.044 2772	0.936 0438	- 0.015 3272
	Green	0.796 1294	- 0.039 2933	0.870 9259	0.012 4111	0.972 9532	- 0.001 0644	0.941 09705	0.002 9018	0.765 3249	0.033 3426	0.878 9268	0.046 8484	0.961 9039	- 0.024 7432
	Blue	0.844 6289	- 0.035 7815	0.861 1989	0.001 0846	0.979 5084	- 0.005 79499	0.908 9592	0.002 322	0.838 5775	0.017 4346	0.845 0444	0.024 0907	0.916 0306	- 0.000 3187
<b>Vertical</b>	Red	0.706 6377	- 0.000 255	0.843 9172	0.005 6568	0.962 4684	- 0.010 7386	0.973 3594	0.005 9123	0.857 6381	0.009 9237	0.977 4625	- 0.005 6336	0.942 4194	- 0.000 8091
	Green	0.730 8941	- 0.001 8005	0.810 8648	- 0.017 974	0.963 2355	0.001 9626	0.971 4832	0.015 8106	0.845 4462	0.001 0768	0.896 7948	0.007 3807	0.967 7748	- 0.005 5361
	Blue	0.793 8528	0.001 9882	0.834 5863	0.000 1316	0.971 0014	0.007 3319	0.947 7644	- 0.005 1086	0.887 1041	0.002 3223	0.862 3912	0.003 4202	0.932 3405	0.009 9321
<b>Diagonal</b>	Red	0.697 4984	0.000 65899	0.830 3537	0.014 3824	0.942 1205	0.002 1898	0.927 5691	0.000 4557	0.737 8458	0.007 82	0.963 9886	- 0.003 6234	0.893 4853	0.002 1819
	Green	0.720 062	0.001 1495	0.789 3617	0.008 8829	0.943 2355	- 0.000 8645	0.918 2886	- 0.024 4704	0.716 6576	- 0.008 6022	0.849 3233	0.005 8216	0.936 4671	- 2.883 149e- 05
	Blue	0.772 31684	0.005 2565	0.804 431	- 0.019 2258	0.956 4989	- 0.011 1759	0.877 31749	0.013 55805 6	0.770 35625	0.008 83396	0.806 5287	0.001 2412	0.861 544	0.006 3233

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

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

<b>Baboon</b>	339 × 509	Plain-image			
		Enciphered-image			
<b>Racoon Face</b>	1024 × 768	Plain-image			
		Enciphered-image			
<b>Lena</b>	256 × 256	Plain-image			
		Enciphered-image			

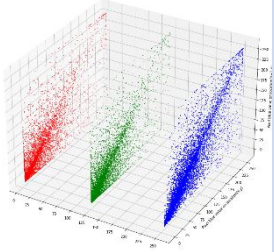
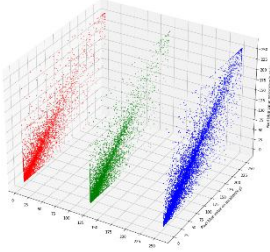
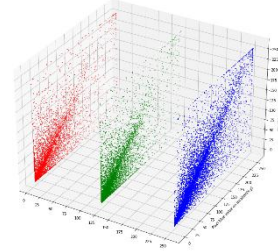
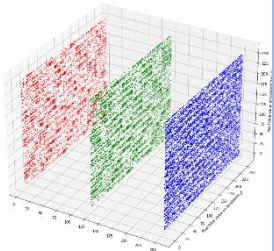
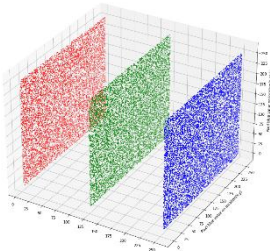
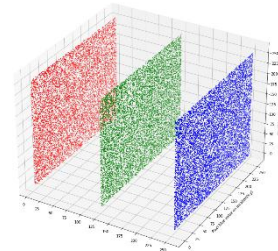
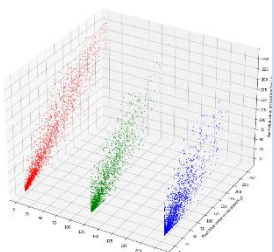
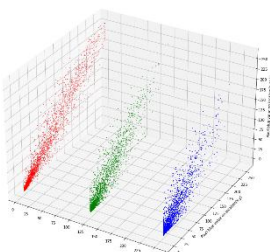
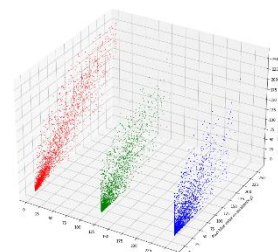
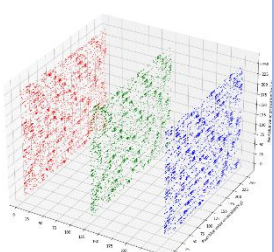
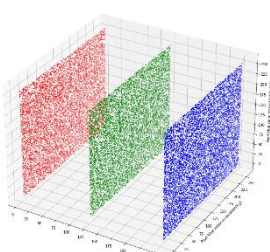
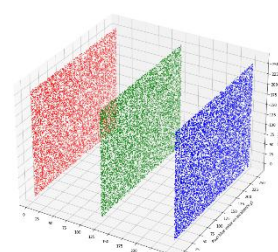
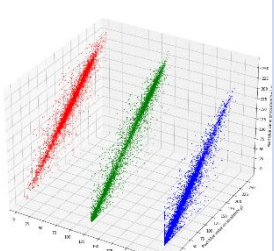
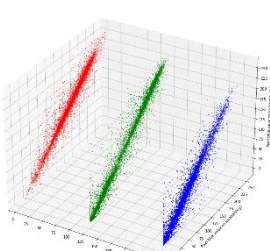
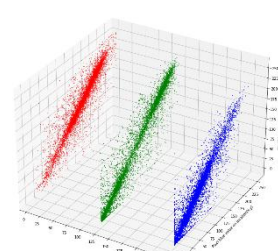
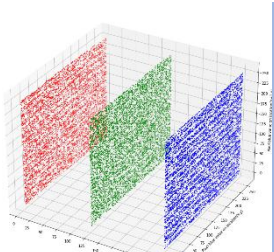
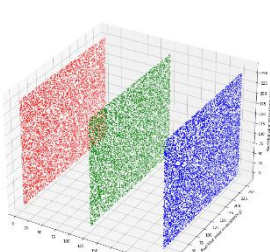
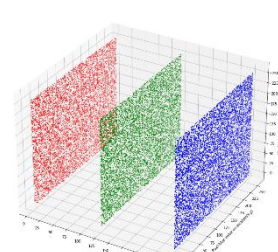
<b>Swirling</b>	728 × 455	Plain-image			
		Enciphered-image			
<b>Tower</b>	648 × 1080	Plain-image			
		Enciphered-image			
<b>Peppers</b>	225 × 225	Plain-image			
		Enciphered-image			

Figure 3. The Correlation of the RGB plain-images and their corresponding enciphered ones

### 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:

$$IE(m) = \sum_{i=0}^{L-1} p(m_i) \log \frac{1}{p(m_i)} \quad (13)$$

$$L = 2^m - 1 \quad (14)$$

Where  $\log \frac{1}{p(m_i)}$  is the information content associated with the pixel intensity value  $m_i$ . Thus, the average amount of the intensity values information in the image is provided by the information entropy as shown in the equation (13). The value of entropy is tested for both plain and ciphered images in Table 18.

Table 13. Information entropies of the RGB plain-images and their corresponding enciphered ones.

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

From the previous results, it's 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 statically attacks [41]. Plain images and their related ciphered had there's histogram shown below. A secure image encryption has uniform distribution of pixel intensity between [0,255]. The histogram for images in RGB mode is shown in the following Figure 4.

	<b>BFOE</b>	<b>Baboon</b>	<b>Racoon Face</b>	<b>Lena</b>	<b>Swirling</b>	<b>Tower</b>	<b>Peppers</b>
--	-------------	---------------	--------------------	-------------	-----------------	--------------	----------------

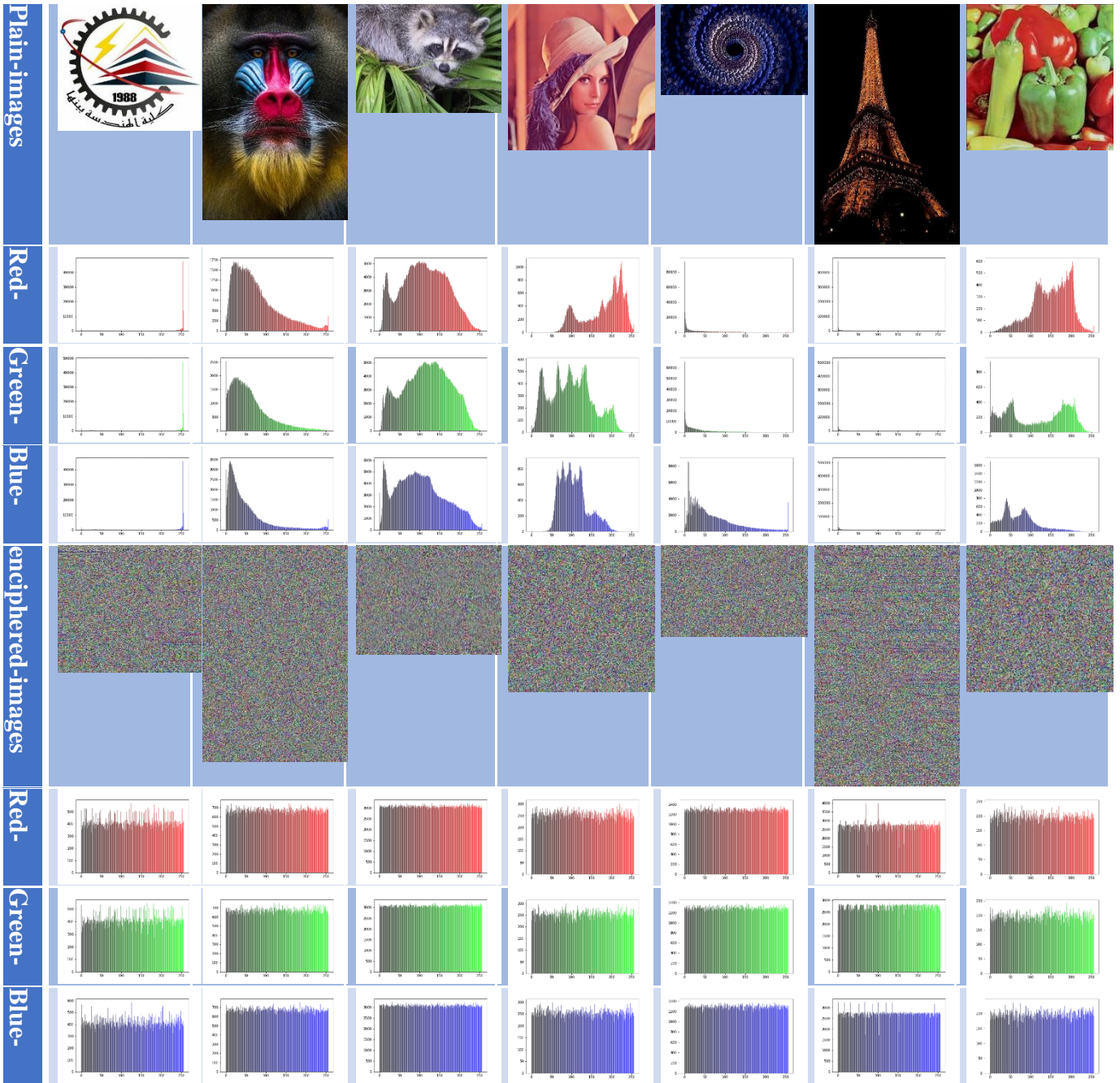


Figure 4. RGB mode Plain-images and enciphered- images using proposed enciphering scheme based on proposed S-Box with their corresponding histograms.

## 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 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 isn't applicable. This will be accomplished when the scheme is dependent on minor data 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 used to estimate the average difference in intensity between two ciphered images [42]. The expected theoretical value of UACI is 33.4635%. The UACI is defined as follows:

$$UACI_{R,G,B} = \frac{1}{\alpha * \beta} \left[ \sum_{i=1}^{\alpha} \sum_{j=1}^{\beta} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \quad (15)$$

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 change.

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 from the followings and see all parameter of differential analysis in Table 19:

$$NPCR_{R,G,B} = \frac{1}{\alpha * \beta} \left[ \sum_{i=1}^{\alpha} \sum_{j=1}^{\beta} D(i,j) \right] \quad (16)$$

$$D(i,j) = \begin{cases} 1 & \text{if } C_1(i,j) \neq C_2(i,j) \\ 0 & \text{if } C_1(i,j) = C_2(i,j) \end{cases} \quad (17)$$

Table 14. Theoretical Acceptance interval for the parameter of differential analysis

Paramete r	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, , 33.64	[33.2255, ,33.70	[33.1594, ,33.76
	512 × 512	[33.3730, , 33.55	[33.3445, ,33.58	[33.3115, ,33.61
	1024 × 1024	[33.4183, , 33.50	[33.4040, ,33.52	[33.3875, ,33.53

The calculated value of both testes are written in Table 15.

Table 15. UACI and NPCR of the enciphered RGB images.

Image	Size	The Plain-Image			The Enciphered-Image				
		Red	Green	Blue	Image	Red	Green	Blue	Image
BFOE	350 × 306	33.84149 7	33.72179 6	33.52713 43	33.69681	100	100	100	100
Baboon	339 × 509	33.54442 4	33.61304 8	33.51064 7	33.55604	100	100	100	100
Raccon Face	1024 × 768	33.61809 8	33.58906 17	33.59921 6	33.60212 5	100	100	100	100
Lena	256 × 256	33.45452 4	33.52711 4	33.65166 76	33.54443 5	100	100	100	100



<b>Swirling</b>	728 × 455	33.59114 5	33.61056 85	33.59815 17	33.59995 5	100	100	100	100
<b>Tower</b>	648 × 1080	33.65405 7	33.53762 76	33.61559 11	33.60242 5	100	100	100	100
<b>Peppers</b>	225 × 225	33.33334 1	33.49583 54	33.67094 84	33.50004 2	100	100	100	100

## 7.2 Data loss

Data loss occurs when all elements that store 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.

$$MSE_{R,G,B} = \frac{1}{\alpha * \beta} \left[ \sum_{i=1}^{\alpha} \sum_{j=1}^{\beta} (C_{ij} - P_{ij})^2 \right] \quad (18)$$

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:

$$PSNR = 20 * \log \left( \frac{P_{MAX}}{\sqrt{MSE}} \right) \quad (19)$$

Where  $P_{MAX}$  is the pixel expected maximum value.

The MSE and PSNR for seven enciphered images are found in Table 16.

Table 16. MSE and PSNR of the enciphered RGB images

Image	Size	The Plain-Image				PSNR (DB)
		Red	Green	Blue	Image	
<b>BFOE</b>	350 × 306	18747.811363	18325.3397	18478.7679178	18517.306327	5.4550254980815
<b>Baboon</b>	339 × 509	11282.5009418	12295.63284 5	14148.5229410 4	12575.55224253	7.135532951228
<b>Raccon Face</b>	1024 × 768	8780.6692822	8737.578709 9	9693.97708637	9070.74169283	8.554375611358
<b>Lena</b>	256 × 256	10722.7294464	9053.083938 6	7081.42718505 8	8952.413523356	8.6114022627033
<b>Swirling</b>	728 × 455	17373.1678239 4	16541.38630 3	12225.0284869 2	15379.86087128	6.2612795408327
<b>Tower</b>	648 × 1080	19474.1586991 3	20223.67608 3	20464.6098965 4	20054.14822626	5.108761402491
<b>Peppers</b>	225 × 225	8121.16821728 4	10953.25165 43	10978.6010469 1	10017.67363951	8.1231348193428

It's 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 ciphered image according to the following equation. And, the MAE of the enciphered RGB images is in Table 17.

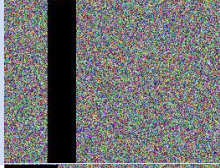
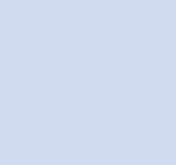
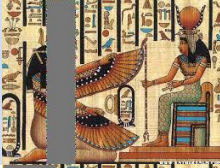
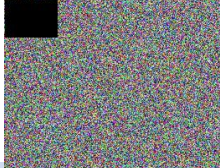
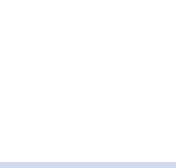


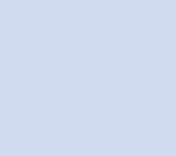
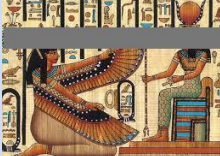
$$MAE_{R,G,B} = \frac{1}{\tau * \mu} \left[ \sum_{i=1}^{\tau} \sum_{j=1}^{\mu} |C(i,j) - P(i,j)| \right] \quad (20)$$

Table 17. MAE of the enciphered RGB images

Image	Size	The Plain-Image			
		Blue	Red	Blue	Image
BFOE	350 × 306	114.8353688 1421	115.9508029 8787	114.8353688 1421	115.0370214 7527
Baboon	339 × 509	97.97266895 0047	86.71625200 6647	97.97266895 0047	91.81182181 8859
Racoon Face	1024 × 768	80.54194132 487	76.95348739 6242	80.54194132 487	78.08836407 1317
Lena	256 × 256	70.33291625 9766	84.70878601 0742	70.33291625 9766	77.65564982 0964
Swirling	728 × 455	90.48034657 6541	110.5126494 3851	90.48034657 6541	102.7664523 2061
Tower	648 × 1080	122.5859310 6999	118.7602223 3658	122.5859310 6999	121.0081370 9805
Peppers	225 × 225	85.54208395 0626	74.44375308 6428	85.54208395 0626	81.82165596 7087

### 7.2.3 OCCLUSION ATTACK

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

Occluded image	enciphered	Deciphered Image	PSNR (dB)
			20.181278742840657
			22.44917666069743
			19.295214680802502

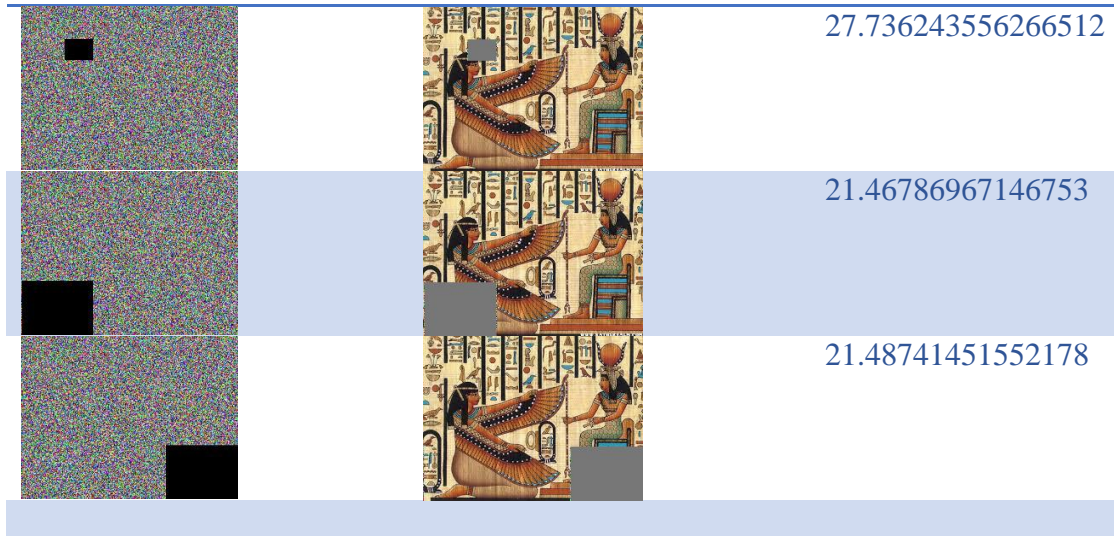


Figure 5. Experimental results of occlusion attacks

## 8. CONCLUSION

The presented work consists of three light weights 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-bit only.
2. Provide DSAC ideal value equals to zero.
3. Provide a maximum period equals 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

## Acknowledgment

We would like to express our deep and sincere gratitude to our post student Hend Ali for her cooperation to finish this paper in this good form.

## Appendix A

Table 18. The ANF for 1st Proposed S-Box

### F1 Equation

$$X_1 + X_2 + X_3 + X_4 + X_1X_2 + X_1X_3 + X_2X_4 + X_3X_4 + X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4$$

### F2 Equation

$$X_1 + X_3 + X_4 + X_1X_2 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 + X_1X_3X_4$$

### F3 Equation

$$1 + X_1 + X_2 + X_3 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 + X_1X_2X_3$$

### F4 Equation

$$1 + X_1 + X_2 + X_4 + X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_3X_4 + X_1X_2X_4$$

Table 19. 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 20. 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 21. 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 22. 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 23. 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 24. 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 25. 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 26. 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

## Appendix B

Table 27. The ANF for 2nd Proposed S-Box

### F1 Equation

$$X_1 + X_2 + X_3 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 + X_1X_2X_3$$

### F2 Equation

$$X_1 + X_2 + X_4 + X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_3X_4 + X_1X_2X_4$$

### F3 Equation

$$X_1 + X_2 + X_3 + X_4 + X_1X_2 + X_1X_3 + X_2X_4 + X_3X_4 + X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4$$

### F4 Equation

$$1 + X_1 + X_3 + X_4 + X_1X_2 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 + X_1X_3X_4$$

Table 28. 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 29. 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 30. 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 31. 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 32. 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 33. 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 34. 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 35. 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

**Appendix C**

Table 36. The ANF for 3rd Proposed S-Box

**F1 Equation**

$$X_1 + X_2 + X_3 + X_4 + X_1X_2 + X_1X_3 + X_2X_4 + X_3X_4 + X_1X_2X_3 + X_1X_2X_4 + X_1X_3X_4 + X_2X_3X_4$$

**F2 Equation**

$$1 + X_1 + X_3 + X_4 + X_1X_2 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 + X_1X_3X_4$$

**F3 Equation**

$$1 + X_1 + X_2 + X_3 + X_1X_3 + X_1X_4 + X_2X_3 + X_2X_4 + X_3X_4 + X_1X_2X_3$$

**F4 Equation**

$$X_1 + X_2 + X_4 + X_1X_2 + X_1X_3 + X_1X_4 + X_2X_3 + X_3X_4 + X_1X_2X_4$$

Table 37. 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 38. 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 39. 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 40. 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 41. 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 42. 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 43. 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 44. 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

## References

1. Yassein, H.R.; Al-Saidi, N.M.G.; Farhan, A.K. A New NTRU Cryptosystem Outperforms Three Highly Secured NTRU-Analog Systems through an Innovational Algebraic Structure. *J. Discrete Math. Sci. Cryptogr.* 2020, 25, 523–542, doi:10.1080/09720529.2020.1741218.
2. Jinomeiq, L.; Baoduui, W.; Xinmei, W. One AES S-Box to Increase Complexity and Its Cryptanalysis. *J. Syst. Eng. Electron.* 2007, 18, 427–433, doi:10.1016/s1004-4132(07)60108-x.
3. Malik, M.S.M.; Ali, M.A.; Khan, M.A.; Ehatisham-Ul-Haq, M.; Shah, S.N.M.; Rehman, M.; Ahmad, W. Generation of Highly Nonlinear and Dynamic AES Substitution-Boxes (S-Boxes) Using Chaos-Based Rotational Matrices. *IEEE Access* 2020, 8, 35682–35695, doi:10.1109/ACCESS.2020.2973679.
4. Cheung, J.M. *The Design of S-Boxes*; 2010;
5. Mansour, M.; Elsobky, W.; Hasan, A.; Anis, W. Appraisal of Multiple AES Modes Behavior Using Traditional and Enhanced Substitution Boxes. *Int. J. Recent Technol. Eng.* 2020, 8, 530–539, doi:10.35940/ijrte.E6541.018520.
6. Kumar, A.; Tejani, S. S-BOX Architecture. *Commun. Comput. Inf. Sci.* 17–27, doi:10.1007/978-981-13-3804-5\_2.
7. Basha, H.A.M.A.; Mohra, A.S.S.; Diab, T.O.M.; EL Sobky, W.I. Efficient Image Encryption Based on New Substitution Box Using DNA Coding and Bent Function. 2022, 10, 66409–66429, doi:10.1109/ACCESS.2022.3183990.
8. Al-Wattar, A.H.; Mahmood, R.; Zukarnain, Z.A.; Udzir, N.I. A New DNA-Based S-Box. *Int. J. Eng. Technol. IJET* 2015, 15, 1–9.
9. Majumdar, A.; Biswas, A.; Majumder, A.; Sood, S.K.; Baishnab, K.L. A Novel DNA-Inspired Encryption Strategy for Concealing Cloud Storage. *Front. Comput. Sci.* 2020, 15, 153807, doi:10.1007/s11704-019-9015-2.
10. Alsobky, W.I.; Saeed, H.; Elwakeil, A.N. Different Types of Attacks on Block Ciphers. *Int. J. Recent Technol. Eng. IJRTE* 2020, 9, 28–31, doi:10.35940/ijrte.c4214.099320.
11. Afify, E.W.; Abo Alez, R.; Khalil, A.T.; Alsobky, W.I. Performance Analysis of Advanced Encryption Standard (AES) S-Boxes. *Int. J. Recent Technol. Eng.* 2020, 9, 2214–2218, doi:10.35940/ijrte.f9712.059120.
12. El-Meligy, N.E.; Diab, T.O.; Mohra, A.S.S.; Hassan, A.Y.; Sobky, W.I.E. A Novel Dynamic Mathematical Model Applied in Hash Function Based on DNA Algorithm and Chaotic Maps. *Mathematics* 2022, 10, 1333, doi:10.3390/math10081333.

13. Farhan, A.K.; Ali, Rasha Subhi; Abdul-Majeed, G.H. Proposal New S-Box Depending on DNA Computing and Mathematical Operations.; 2016.
14. Farhan, A.K.; Ali, R.S.; Yassein, H.R.; Al-Saidi, N.M.G.; Abdul-Majeed, G.H. A New Approach to Generate Multi S-Boxes Based on RNA Computing. *Int. J. Innov. Comput. Inf. Control* 2020, 16, 331–348, doi:10.24507/ijicic.16.01.331.
15. Mohamed, K.; Pauzi, M.N.M.; Ali, F.H.H.M.; Ariffin, S.; Zulkipli, N.H.N. Study of S-Box Properties in Block Cipher.; 2014.
16. Abdel-Hafez, Ahmed A; Elbarkouky, Reda; Hafez, Wageda Comparative Study of Algebraic Attacks. 2016, 3, 85–90, doi:10.17148/iarjset.2016.3519.
17. Cui, J.; Huang, L.; Zhong, H.; Chang, C.; Yang, W. An Improved AES S-Box and Its Performance Analysis. *Int. J. Innov. Comput. Inf. Control* 2011, 7, 2291–2302.
18. Afify, E.W.; Abo Alez, R.; Khalil, A.T.; Alsobky, W.I. Algebraic Construction of Powerful Substitution Box. *Int. J. Recent Technol. Eng.* 2020, 8, 405–409, doi:10.35940/ijrte.D8279.038620.
19. Sobky, W.I.E.; Mahmoud, A.R.; Mohra, A.S.; El-Garf, T. Enhancing Hierocrypt-3 Performance by Modifying Its S-Box and Modes of Operations. *J. Commun.* 2020, 905–912, doi:10.12720/jcm.15.12.905-912.
20. Zahid, A.H.; Arshad, M.J.; Ahmad, M. A Novel Construction of Efficient Substitution-Boxes Using Cubic Fractional Transformation. *Entropy* 2019, 21, 245, doi:10.3390/e21030245.
21. RoyChatterjee, S.; Sur, K.; Chakraborty, M. Study on S-Box Properties of Convolution Coder. In *Proceedings of the Proceedings of International Ethical Hacking Conference 2019*; Chakraborty, M., Chakrabarti, S., Balas, V.E., Eds.; Springer: Singapore, 2020; pp. 119–128.
22. Azam, N.A.; Hayat, U.; Ayub, M. A Substitution Box Generator, Its Analysis, and Applications in Image Encryption. *Signal Process.* 2021, 187, 108144, doi:10.1016/j.sigpro.2021.108144.
23. Hussain, I.; Shah, T.; Mahmood, H.; Gondal, M.A. A Projective General Linear Group Based Algorithm for the Construction of Substitution Box for Block Ciphers. *Neural Comput. Appl.* 2013, 22, 1085–1093, doi:10.1007/s00521-012-0870-0.
24. Özkaynak, F.; Özer, A.B. A Method for Designing Strong S-Boxes Based on Chaotic Lorenz System. *Phys. Lett. A* 2010, 374, 3733–3738, doi:10.1016/j.physleta.2010.07.019.
25. Guesmi, R.; Ben Farah, M.A.; Kachouri, A.; Samet, M. 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)*; November 2014; pp. 678–684.
26. Ivanov, G.; Nikolov, N.; Nikova, S. Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm. In *Proceedings of the Cryptography and Information Security in the Balkans*; Pasalic, E., Knudsen, L.R., Eds.; Springer International Publishing: Cham, 2016; pp. 31–42.
27. 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, doi:10.1109/ACCESS.2020.3001868.
28. Lambić, 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, doi:10.1007/s11071-020-05503-y.
29. Özkaynak, F. On the Effect of Chaotic System in Performance Characteristics of Chaos Based S-Box Designs. *Phys. Stat. Mech. Its Appl.* 2020, 550, 124072, doi:10.1016/j.physa.2019.124072.
30. Lu, Q.; Zhu, C.; Deng, X. An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box. *IEEE Access* 2020, 8, 25664–25678, doi:10.1109/ACCESS.2020.2970806.
31. Rodinko, M.; Oliynykov, R.; Gorbenko, Y. Optimization of the High Nonlinear S-Boxes Generation Method. *Tatra Mt. Math. Publ.* 2017, 70, 93–105, doi:10.1515/tmmp-2017-0020.

32. Razaq, A.; Alolaiyan, H.; Ahmad, M.; Yousaf, M.A.; Shuaib, U.; Aslam, W.; Alawida, M. A Novel Method for Generation of Strong Substitution-Boxes Based on Coset Graphs and Symmetric Groups. *IEEE Access* 2020, 8, 75473–75490, doi:10.1109/ACCESS.2020.2989676.
33. Ibrahim, S.; Alhumyani, H.; Masud, M.; Alshamrani, S.S.; Cheikhrouhou, 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, doi:10.1109/ACCESS.2020.3020746.
34. Abd EL-Latif, A.A.; Abd-El-Atty, B.; Venegas-Andraca, S.E. A Novel Image Steganography Technique Based on Quantum Substitution Boxes. *Opt. Laser Technol.* 2019, 116, 92–102, doi:10.1016/j.optlastec.2019.03.005.
35. Jamal, S.S.; Anees, A.; Ahmad, M.; Khan, M.F.; Hussain, I. Construction of Cryptographic S-Boxes Based on Mobius Transformation and Chaotic Tent-Sine System. *IEEE Access* 2019, 7, 173273–173285, doi:10.1109/ACCESS.2019.2956385.
36. Zahid, A.H.; Arshad, M.J. An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping. *Symmetry* 2019, 11, 437, doi:10.3390/sym11030437.
37. Khan, M.; Waseem, H.M. A Novel Image Encryption Scheme Based on Quantum Dynamical Spinning and Rotations. *PLOS ONE* 2018, 13, e0206460, doi:10.1371/journal.pone.0206460.
38. 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, doi:10.1016/j.asoc.2015.08.008.
39. Chen, J.; Zhu, Z.; Fu, C.; Zhang, L.; Zhang, Y. An Efficient Image Encryption Scheme Using Lookup Table-Based Confusion and Diffusion. *Nonlinear Dyn.* 2015, 81, 1151–1166, doi:10.1007/s11071-015-2057-6.
40. Zhang, Y.; Li, X.; Hou, W. A Fast Image Encryption Scheme Based on AES.; 2017.
41. Kang, Y.; Huang, L.; He, Y.; Xiong, X.; Cai, S.; Zhang, H. On a Symmetric Image Encryption Algorithm Based on the Peculiarity of Plaintext DNA Coding. *Symmetry* 12, 1393, doi:10.3390/sym12091393.
42. Hussain, Z.A.; Tawalbeh, L.; Ahmad, M.; Alkhayyat, A.; Hassan, M.T.; Manzoor, A.; Farhan, A.K. Efficient Dynamic S-Box Generation Using Linear Trigonometric Transformation for Security Applications. *IEEE Access* 2021, 9, 98460–98475, doi:10.1109/access.2021.3095618.
43. Shah, A.; Parah, S.A.; Rashid, M.; Elhoseny, M. Efficient Image Encryption Scheme Based on Generalized Logistic Map for Real Time Image Processing. *J. Real-Time Image Process.* 2020, 17, 2139–2151, doi:10.1007/s11554-020-01008-4.
44. Qian, X.; Yang, Q.; Li, Q.; Liu, Q.; Wu, Y.; Wang, W. A Novel Color Image Encryption Algorithm Based on Three-Dimensionalchaotic Maps and Reconstruction techniques. *IEEE Access* 2021, 9, 61334–61345, doi:10.1109/ACCESS.2021.3073514.
45. 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," in *IEEE Access*, vol. 10, pp. 66409- 66429, 2022, doi: 10.1109/ACCESS.2022.3183990.
46. El-Meligy, N. E., Diab, T. O., Mohra, A. S., Hassan, A. Y., & El-Sobky, W. I. (2022). A Novel Dynamic Mathematical Model Applied in Hash Function Based on DNA Algorithm and Chaotic Maps. *Mathematics*, 10(8), 1333