IEEE Access

Received 19 May 2022, accepted 5 June 2022, date of publication 17 June 2022, date of current version 27 June 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3183990

Efficient Image Encryption Based on New Substitution Box Using DNA Coding and Bent Function

HEND ALI MOHAMMED ALI BASHA[1], ASHRAF SHAWKY SELIEM MOHRA[1], TAMER OMAR MOHAMED DIAB[1], AND WAGEDA IBRAHIM EL SOBKY[2,3]

[1]Electrical Engineering Department, Benha Faculty of Engineering, Benha University, Banha 13511, Egypt
[2]Basic Engineering Sciences Department, Benha Faculty of Engineering, Benha University, Banha 13511, Egypt
[3]Basic Engineering Sciences Department, Canadian International College (CIC), New Cairo 11865, Egypt

Corresponding authors: Hend Ali Mohammed Ali Basha (hend.ali@bhit.bu.edu.eg) and Wageda Ibrahim El Sobky (wageda.alsobky@bhit.bu.edu.eg)

ABSTRACT This study contributes to creating an unbreakable S-Box based on a strong bent function expanded by DNA sequences and investigates and analyzes the strength of the proposed S-Box against major standard criteria and benchmarks, such as interpolation attacks, algebraic attacks, avalanche effect, nonlinearity, and period. The outcome of the tests shows that the proposed S-box has good security, as well as it is passed all the randomness tests. On an average, the results after the tests applied have been come with SAC = 0.50122, NL = 112, BIC =103.40625, and an iterative period with a maximum value of 256. The complexity of the proposed S-Box increased with an algebraic expression of 255 terms, which implies an algebraic attack resistance of 2^{160}. Based on the proposed S-Box, a candidate image-enciphering scheme is suggested to prove the strength of the S-Box. The analysis of the experiments that applied two modes of images, grey and RGB images, supports the scheme's robustness against different differential and statical attacks using standard criteria such as correlation coefficient analysis, information entropy, histogram analysis, unified average change intensity, number of pixels change rate and many others. This enforces its capability for use in modern-day cryptosystems that are utilized in multimedia data exchange.

INDEX TERMS S-Box, DNA, algebraic attack, affine transformation, image encryption.

I. INTRODUCTION

A. BACKGROUND

Modern-day information technologies are in acute need to be protected against different security threats. With the significant development of these technologies, complex security issues have always been present. The information privacy/data must be protected by keeping it secret, which can be achieved by converting it into an unreadable form [1]. Cryptography is a well-known science that is responsible for fulfilling this process. It aims to protect this data from exploitation, alteration, or being missed and make sure that the intended receiver can comprehend the message [2].

For the pre-mentioned purpose, different symmetric and asymmetric ciphers have been designed. The symmetric ciphers which are used in a large domain fall into two primary categories: stream ciphers and block ciphers. In the former, the plaintext is encrypted in a bit-by-bit way, but in the latter, the plaintext block with a fixed size of a number of bits is encrypted simultaneously [3]

For any cryptographic algorithm, it is important to have the confusion property in the ciphertext, which is related between ciphertext and plain text. One of the known techniques used to provide this is the Substitution Box (S-Box) [2]. The S-Box, known as the nonlinear transformation, is of the utmost importance in all different types of symmetric encryption algorithms [4]. There is a candid link between security and confusion as the confusion level in ciphertext indicates its robustness [5].

The National Institute of Standards and Technology (NIST) has admitted several criteria to judge the strength of S-Box, such as the strict avalanche criterion, non-linearity, and bit independence criterion [6]. Most of

The associate editor coordinating the review of this manuscript and approving it for publication was Jun Wang.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

the properties depend on linear components that are composed of n-parameters called boolean functions, which have several methods to be calculated, like Univariate Polynomial Form (UPF), Minterms, and Algebraic Normal Form (ANF) [7].

As the S-box design criteria are vulnerable to the different newly invented attacks, the most important challenge that has been concentrated on by the researchers is exploring new techniques to get better performance. This has prompted researchers to use the concept of DNA computing. DNA cryptography, the arising direction of information security, is considered a promising technology for unbreakable algorithms. It is a branch of biology with great potential for storing data based on DNA biology. It contains information about living organisms. DNA is an abbreviation for (Deoxyribose Nucleic Acid) which is a genetic substance of an organism that plays a role in passing genetic traits from the parents to offspring [8]. Organisms possess their own DNA information. DNA is a polymer composed of several units of monomers called nucleotides. Each nucleotide is made up of three components: phosphate group, deoxyribose sugar, and nitrogen bases [9], [10].

B. DEOXYRIBO-NUCLEIC ACID (DNA)

DNA is considered the genetic pattern of living creatures. All cosmetic cells contain a complete set of DNA that is unique to every creature. Small units, called monomers, are combined together to form a DNA polymer. These units are deoxyribose nucleotides. Nitrogen bases, one of the nucleotides' basic components, are Adenine (A), Cytosine (C), Guanine (G) and Thymine (T) [3]. Binary numbers 00, 01, 10 and 11 are used to encode the binary data using four bases (A, C, G, and T). According to this coding, we can replace every eight binary bits with only four characters in DNA coding. Therefore, we must deeply study DNA components/properties in order to be able to analyze its computations. [3]

DNA is the cell's memory as it is responsible for retaining all the information that's formed based on the coding of the four characters. Watson Crick proposed a complementary DNA structure. This structure is essentially used for DNA calculations to obtain the base pairs. T and A complement each other, and G and C also complement each other. Each base combines with one sugar molecule and another phosphate molecule. The arrangement of these bases creates the uniqueness of the DNA, which determines the manner of the creature.

The eight conventional rules are shown in **Table 1**.

The addition and subtraction rules for DNA nucleotides are listed in **Table 2** and **Table 3**, respectively.

In this research, these rules are used while expanding the S-box process.

The remainder of this paper is structured as follows: Section II explains the steps followed to get the proposed S-Box and the analysis of its performance using NIST tests is illustrated in Section III. Section IV presents the proposed scheme based on the proposed S-Box to protect multimedia data, and its subsections that illustrate the analysis against various known types of attacks.

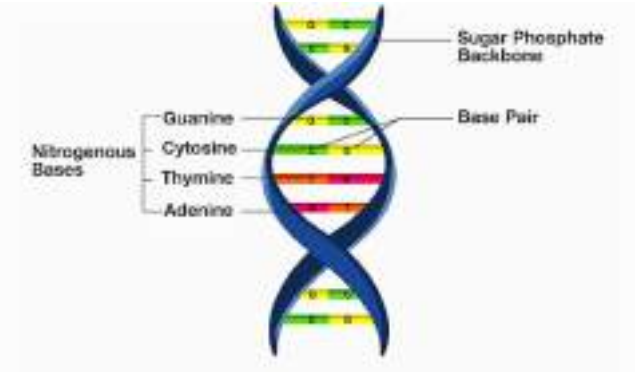


FIGURE 1. DNA structure.

TABLE 1. DNA eight rules.

	$Code_1$	$Code_2$	$Code_3$	$Code_4$	$Code_5$	$Code_6$	$Code_7$	$Code_8$
00	A	A	C	C	G	G	T	T
01	C	G	A	T	A	T	C	G
10	G	C	T	A	T	A	G	C
11	T	T	G	G	C	C	A	A

TABLE 2. 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 3. Substraction 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

II. PROPOSED NEW S-BOX

In this section, a new highly non-linear S-Box is generated depending on high non-linear bent functions. The S-Box is a one-to-one function that substitutes a byte with its corresponding one. It is an invertible function that can be obtained using a few transformations.

1. An affine transformation is applied, which is defined by:

$$Y = \mathrm{T}\left(\boldsymbol{a}X^2 + \boldsymbol{b}X + \boldsymbol{C}\right)$$

$$= \begin{bmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & a_7 & a_6 & a_5 \\ a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & a_7 & a_6 \\ a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & a_7 \\ a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 \\ a_0 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_7 & a_6 & a_5 & a_4 & a_3 \\ a_3 & a_2 & a_1 & a_0 & a_7 & a_6 & a_5 & a_4 \end{bmatrix} \times \begin{bmatrix} X_7 \\ X_6 \\ X_5 \\ X_4 \\ X_3 \\ X_2 \\ X_1 \\ X_0 \end{bmatrix}^2 + \begin{bmatrix} b_4 & b_3 & b_2 & b_1 & b_0 & b_7 & b_6 & b_5 \\ b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & b_7 & b_6 \\ b_6 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & b_7 \\ b_7 & b_6 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 \\ b_0 & b_7 & b_6 & b_5 & b_4 & b_3 & b_2 & b_1 \\ b_1 & b_0 & b_7 & b_6 & b_5 & b_4 & b_3 & b_2 \\ b_2 & b_1 & b_0 & b_7 & b_6 & b_5 & b_4 & b_3 \\ b_3 & b_2 & b_1 & b_0 & b_7 & b_6 & b_5 & b_4 \end{bmatrix} \times \begin{bmatrix} X_7 \\ X_6 \\ X_5 \\ X_4 \\ X_3 \\ X_2 \\ X_1 \\ X_0 \end{bmatrix} + \begin{bmatrix} C_7 \\ C_6 \\ C_5 \\ C_4 \\ C_3 \\ C_2 \\ C_1 \\ C_0 \end{bmatrix}$$

$$a = 0 \times 76H, \quad b = 0 \times 6D, \; C = 0XDA \tag{1}$$

2. The multiplicative inverse of the result computed Y : $Y = Y^{-1} inGF\left(2^8\right)$, that's defined as follow:

$$Y = Y^{-1} = \begin{cases} Y^{254} & Y \neq 0 \\ 0 & Y = 0 \end{cases} \tag{2}$$

3. Apply affine transformation in 1 for the second time:

$$Y = T(\boldsymbol{a}Y^2 + \boldsymbol{b}Y + \boldsymbol{C})$$

$$= \begin{bmatrix} a_4 & a_3 & a_2 & a_1 & a_0 & a_7 & a_6 & a_5 \\ a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & a_7 & a_6 \\ a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & a_7 \\ a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 \\ a_0 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_7 & a_6 & a_5 & a_4 & a_3 \\ a_3 & a_2 & a_1 & a_0 & a_7 & a_6 & a_5 & a_4 \end{bmatrix} \times \begin{bmatrix} Y_7 \\ Y_6 \\ Y_5 \\ Y_4 \\ Y_3 \\ Y_2 \\ Y_1 \\ Y_0 \end{bmatrix}^2 + \begin{bmatrix} b_4 & b_3 & b_2 & b_1 & b_0 & b_7 & b_6 & b_5 \\ b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & b_7 & b_6 \\ b_6 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 & b_7 \\ b_7 & b_6 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 \\ b_0 & b_7 & b_6 & b_5 & b_4 & b_3 & b_2 & b_1 \\ b_1 & b_0 & b_7 & b_6 & b_5 & b_4 & b_3 & b_2 \\ b_2 & b_1 & b_0 & b_7 & b_6 & b_5 & b_4 & b_3 \\ b_3 & b_2 & b_1 & b_0 & b_7 & b_6 & b_5 & b_4 \end{bmatrix} \times \begin{bmatrix} Y_7 \\ Y_6 \\ Y_5 \\ Y_4 \\ Y_3 \\ Y_2 \\ Y_1 \\ Y_0 \end{bmatrix} + \begin{bmatrix} C_7 \\ C_6 \\ C_5 \\ C_4 \\ C_3 \\ C_2 \\ C_1 \\ C_0 \end{bmatrix}$$

$$a = 0 \times 76, \quad b = 0 \times 6D, \; C = 0XDA \tag{3}$$

The generated S-box is presented in ***Table 4***.

4. Now, the values are converted into a binary form, and its length must be a multiple of 8. Otherwise, zeros are added to the left to adjust the number.
5. The next step is to replace each double bit with one DNA code, i.e., in code 8, 00 is substituted with T, 01 with G, 10 by C, and 11 by A.
5. Using the eight aforementioned codes, we can get the following different eight-S-boxes written in the tables of **VI. Appendix** from **Table 25-Table 32**.

Input	*Read a, b, c, and IP*
Output	S-Box of size (8 × 8).

For $i = 0 : 255$
  Apply affine to number i
  Substitute affine of i in Equ.1:
  $Y = T\left(aX^2 + bX + C\right) mod\ IP$
  $Y \leftarrow Y^{-1} mod\ IP$
  Repeat step 3 to get new Y value using the same values of a, b, c.
  S-Box[i] =Y
End For
Return S-Box

In this step, the DNA addition operation is used based on the additional rules in **Table 2**. The addition

TABLE 4. The proposed S-box (HEX).

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2B	56	0A	6C	A7	F0	19	AE	24	E8	49	A0	CC	7E	27	D9
1	F3	31	95	EF	30	F8	3B	14	F9	40	BE	42	39	4D	FB	FD
2	18	B3	CB	68	29	AA	60	21	78	0F	17	BA	DC	00	D2	BC
3	35	C1	FF	BB	67	66	3E	AF	05	7A	01	5A	96	47	50	3A
4	20	4C	80	2F	B0	E0	D7	79	2E	7F	7D	06	73	C3	97	5D
5	10	34	EE	DA	8C	08	B2	9C	CA	55	F7	A2	B6	70	C2	1C
6	B4	09	B9	9E	62	A9	9A	9F	EA	A8	3D	1B	71	44	D4	0B
7	E9	C0	46	C6	04	4A	61	75	FE	41	52	6A	6B	1E	4F	AC
8	65	2A	B1	11	B5	38	A4	A3	43	28	99	93	CE	72	DD	FC
9	3C	D8	76	E1	16	E6	23	12	6D	85	8E	26	54	BF	36	ED
A	92	1A	E3	0D	98	57	32	94	DF	D0	EB	E2	22	88	3F	84
B	63	7B	1D	8D	86	DE	2D	AB	C7	4E	83	91	F5	6E	07	33
C	74	D3	5C	8F	CF	D1	E5	C9	0E	F1	9D	1F	8B	15	53	5E
D	51	5F	87	BD	4B	A6	F6	77	A5	37	25	59	89	2C	0C	6F
E	02	13	E4	D6	F4	C8	7C	A1	45	82	D5	8A	CD	E7	FA	F2
F	9B	58	5B	81	64	C5	B8	EC	69	90	03	B7	AD	C4	48	DB

TABLE 5. Coefficients of algebraic expression of the proposed S-box (Hex).

$E_{(XY)}$	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
F	00	88	3E	FD	9D	4B	2E	93	59	E0	D8	0C	D5	AD	D4	8E
E	1A	84	4A	F9	62	6A	89	E4	7E	11	FC	35	C2	3B	F2	6D
D	FC	5B	D8	14	12	BC	D5	F9	7C	7D	FE	8D	F4	58	8E	59
C	82	5E	0F	69	50	5D	AE	4A	02	F3	56	46	68	96	5D	D8
B	B2	45	07	61	BB	9F	9B	AE	E7	07	36	8E	1F	FE	39	B5
A	DD	AF	2F	59	E2	D2	A2	72	B1	15	9D	E1	EF	FB	EF	F5
9	3B	55	54	66	F7	7B	61	98	3C	74	B0	79	6C	F6	C6	D6
8	13	18	B2	F2	E8	3F	6A	92	73	3B	D7	C2	26	06	48	96
7	80	A4	9D	B7	B0	F7	94	6A	8F	3B	5F	65	59	30	CB	57
6	8A	C2	D6	D8	8E	D5	1F	A5	0C	E5	F4	39	D5	CF	0D	E5
5	5D	A6	78	61	2A	85	C5	63	AF	21	C6	C3	49	49	89	F6
4	8C	53	DF	A5	B0	40	14	81	1B	46	D9	38	B9	1D	F8	39
3	17	D6	EB	73	FF	02	ED	55	6B	C3	D6	D5	90	36	60	CB
2	A6	F4	D5	F1	5B	A6	0E	4A	25	4F	26	C7	63	1F	64	80
1	3D	7C	41	68	20	CE	F7	90	4B	1D	E5	93	A0	93	5E	B7
0	57	6D	83	90	3D	56	57	BE	32	D6	36	6F	3F	97	A9	2B

operation is implemented between every two characters in DNA sequence 1 and DNA sequence 2 resulting from the previous step. In this step, the DNA sequence size is reduced to analysis the S-Box.

III. THE PROPOSED S-BOX PERFORMANCE ANALYSIS

The analysis of the S-box is proceeded by using some well-known tests such as NL, SAC and BIC. These tests are dynamic properties that address the relationship between plaintext and ciphertext changes. The ANF method, which is used to get the Boolean function, is represented as a polynomial in n-variables, the input binary bits, with terms of their input bits and then these terms are bitwise summed. Each of the aforementioned tests is performed based on the Boolen function and will be illustrated in brief as in the following.

A. THE ALGEBRAIC EXPRESSION

The security of the standard AES S-Box is questionable owing to its such low complexity. To eliminate the weakness of these simple algebraic expressions which its reason

TABLE 6. Standard AES S-Box iterative period.

P (MN)	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	59	81	59	59	87	59	59	59	87	81	87	27	81	81	81	59
1	81	81	81	81	27	87	81	81	87	59	81	87	87	87	81	57
2	59	59	87	27	59	59	27	81	87	59	87	27	87	27	59	87
3	87	59	27	59	87	87	59	87	59	81	81	87	81	81	87	59
4	81	81	87	81	87	27	87	81	59	87	87	81	59	81	87	81
5	87	87	59	87	59	87	27	81	59	87	87	81	87	59	59	81
6	87	27	81	59	81	81	59	87	27	87	59	59	87	81	27	59
7	87	87	81	02	81	59	59	59	81	87	81	59	81	81	81	59
8	81	81	81	81	81	87	87	81	87	87	81	81	81	59	59	02
9	87	81	81	87	87	87	87	87	87	87	87	27	87	59	27	27
A	81	27	81	87	87	59	59	87	59	59	81	81	81	87	87	87
B	87	27	87	81	59	59	87	59	87	27	87	81	81	81	87	87
C	87	81	59	59	87	59	59	59	27	81	81	87	81	81	81	81
D	87	87	59	59	59	59	87	81	27	87	81	27	87	81	87	27
E	81	81	87	81	87	87	59	87	27	81	81	81	81	87	87	27
F	81	27	87	81	87	59	87	27	81	87	27	59	87	59	81	81

TABLE 7. SAC of the proposed S-Box.

SAC	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
1	128	136	132	128	128	124	128	120
2	128	120	124	128	140	128	136	136
4	128	136	128	132	136	132	120	116
8	132	128	136	136	124	132	136	132
16	120	124	128	132	128	112	116	116
32	124	124	124	128	128	132	116	128
64	124	132	136	128	132	132	140	128
128	136	116	132	120	136	132	132	128

TABLE 8. BIC of the proposed S-Box.

BIC	β_1	β_2	β_3	β_4	β_5	β_6	β_7	β_8
1	-	128	128	128	128	128	128	128
2	126	-	136	132	142	100	136	116
4	128	122	-	124	122	126	120	130
8	118	122	126	-	132	120	116	120
16	120	140	124	122	-	118	44	90
32	124	128	128	104	118	-	72	64
64	124	128	130	108	134	82	-	80
128	134	130	132	96	166	88	80	-

was illustrated in [11], the proposed S-box was improved by applying multiple steps of transformation not only one. In the proposed S-box, by using the irreducible polynomial $P(x) = x^9 + x^4 + x^3 + x + 1$, the affine transformation matrices and affine constants, we notice that the complexity of the algebraic expression is increased from 9 to 255 terms, which has the same ability to resist differential cryptanalysis.

TABLE 9. Non-linearity of boolean functions.

B_{f_i}	f_1	f_2	f_3	f_3	f_4	f_5	f_6	f_7
NL (B_{f_i})	112	112	112	112	112	112	112	112

The workload of grade 255 is considered to be very large. The simplest and most common method is to replace the 256 S-Box values in **Table 5** with the Lagrange interpolation formula:

$$A_k(x) = \frac{(x-x_0)\ldots(x-x_{k-1})(x-x_{k+1})\ldots(x-x_n)}{(x_k-x_0)\ldots(x_k-x_{k-1})(x_k-x_{k+1})\ldots(x_k-x_n)}, \quad k = 0, 1\ldots, n-1 = 255 \tag{4}$$

and substitute the middle-value is in the equation.

$$S_{x_i} = \sum_{j=0}^{m-1} y_k F_k(x_j) = y_i, \quad i = 0, 1\ldots, n-1 = 255 \tag{5}$$

All coefficients of the algebraic expression of the improved S-box can be resolved.

The relationship that links between the coefficients of the proposed AES S-box algebraic expression and Data E shown in **Table 5** is defined as follows:

$$S_x = \sum_{x,y}^{15} E_{16x+y} x^{16x+y} \tag{6}$$

TABLE 10. Comparison of proposed S-Box and other S-Boxes; SAC, BIC, NL.

NIST Tests / S-Box	SAC			BIC	NL		
	Max	Avg	Min		Max	Avg	Min
Proposed S-Box	**0.53125**	**0.50122**	**0.4375**	**103.40625**	**112**	**112**	**112**
Ref. [5]	0.5625	0.4956	0.4531	112	112	112	112
Ref. [23]	0.625	0.507	0.421	106	108	105.5	100
Ref. [24]	0.5938	0.5049	0.4219	103.71	106	103.25	100
Ref. [25]	0.5938	0.4971	0.4063	103.86	108	108	108
Ref. [26]	0.5781	0.5017	0.3906	106.07	110	106.5	104
Ref. [27]	0.5625	0.4978	0.4375	103.86	116	112	114
Ref. [28]	0.5781	0.5010	0.4219	104.07	108	106.5	106
Ref. [29]	0.6094	0.5037	0.4062	102.6	108	105.25	102
Ref. [30]	0.5938	0.5029	0.4219	103.93	110	106.25	104
Ref. [31]	0.5938	0.5046	0.4375	106.79	110	106	108
Ref. [32]	0.5625	0.5017	0.4375	112	112	112	112
Ref. [33]	0.5781	0.4990	0.4063	104.29	110	106	108
Ref. [34]	0.6094	0.5037	0.3594	103.93	106	102.5	96
Ref. [35]	0.5625	0.5049	0.4531	112	116	114	112
Ref. [36]	0.594	0.507	0.406	103.9	108	106.8	104
Ref. [37]	0.5625	0.5065	0.4219	106.43	112	110.5	108
Ref. [38]	0.5625	0.506	0.4375	104.2	112	110	115

The algebraic complexity of the proposed S-Box has multiple terms up to 255. This reinforces the security and complexity.

B. THE ALGEBRAIC CRITERION OF THE BOOLEAN FUNCTION

A good S-box meets a number of criteria, as its non-linear properties determine the performance of the entire block cipher [12], [13]. Therefore, the S-box is considered the core of the entire block cipher. It is worth checking whether the improved algorithm can meet the required performance or not [14].

Different cryptanalysis methods guarantee the resistance of a single S-box cipher with good cryptographic characteristics; therefore, any shortcomings in the S-box can impair cipher security. The S-Box is an 8×8 logic functions that functions interact and influence each other. Although these have certain properties simultaneously, S-box reasoning does not have the same properties. Therefore, it is necessary to analyze the algebraic properties of the S-box function.

1) THE ALGEBRAIC ATTACKS RESISTANCE

This quantity reflects the resistance of the proposed S-Box against various algebraic attacks.

Theorem 1 [15], [16]:

Given l equations of k terms in $GF(2^8)$, the algebraic attacks resistance (AAR) is denoted by Γ and is defined as follows:

$$\Gamma = \left(\frac{k-l}{n}\right)^{\left\lceil \frac{k-l}{n} \right\rceil} \tag{7}$$

It was claimed in [17] that Γ should be greater than 2^{32} to avoid the shortcomings of the S-box. For the proposed S-box, $l = 255$, $k = 510$ terms, and $n = 8$, we obtain $\mathbf{\Gamma = 2^{160}}$ for the proposed S-Box, which explains how much the strength of S-Box is against algebraic attacks.

2) ITERATIVE PERIOD OF S-BOX

The iterative period the of S-Box can be defined as follows:

Theorem 2 [18], [19]:

Assume that the S-box bent function is denoted by B (n). $B(n)$ fulfills the periodicity if $B^m(n) = n$ such that m is any positive.

For every $n \in GF(2^8)$, let the equation $B^m(n) = n$, the iterative period is deduced for the standard AES S-box to have the results shown in **Table 6**. Note that the iterative periods obtained were 2, 27, 59, 81 and 87. These periods fulfill 2+27+59+81+87 =256, so no intersection occurs among

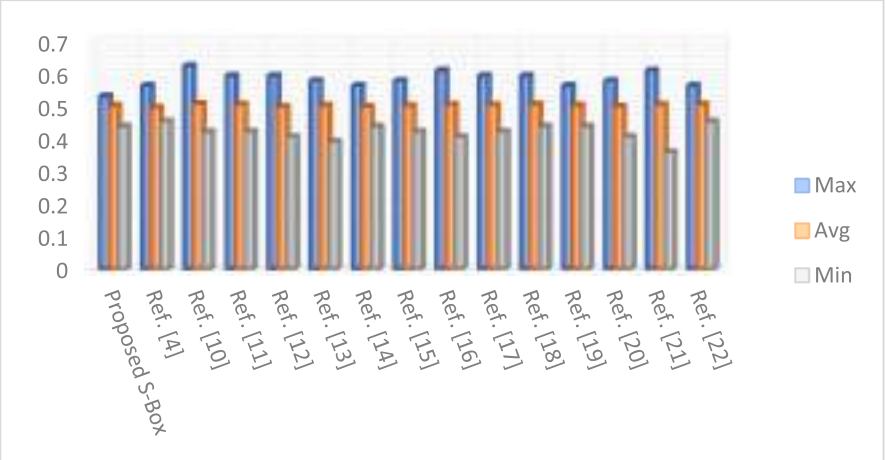


FIGURE 2. Strict avalanche criterion of the proposed S-Box and other S-Boxes.

FIGURE 3. Average bit independent criterion of the proposed S-Box and other S-Boxes.

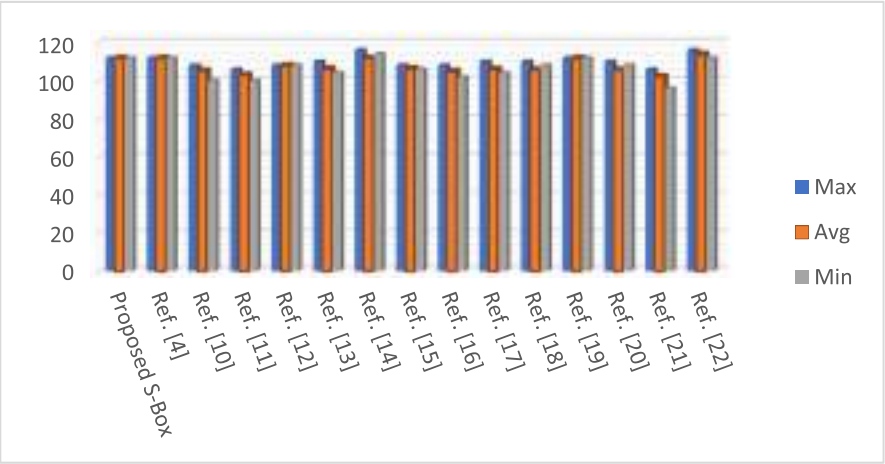


FIGURE 4. Average of non-linearity of the proposed S-Box and other S-Boxes.

the period orbits. It is obvious that the standard S-box has short periods and inadequate distribution, which can result in some hiatus.

For the proposed one, the iterative period is increased to its maximum value until it reaches 255 for any positive number of $GF(2^8)$.

TABLE 11. The Correlation coefficients of the Gray plain-images and their corresponding enciphered ones.

Im-	Baboon		Lenna		Digital Electronics		MonaLiza		Egyptian civilization		Raccoon Face		Peppers	
Siz	256 × 256		256 × 256		600 × 450		900 × 1285		259 × 194		1024 × 768		225 × 225	
	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher
Horizontal	0.857846796	-0.007812258	0.945715621	0.001832771	0.911060766	-0.058094371	0.982511304	-0.056833696	0.730244007	-0.006368061	0.972062612	-0.010542755	0.944093523	-0.008424801
Vertical	0.808607899	-0.038548223	0.970877783	0.000930025	0.904015592	0.014900031	0.977825937	0.005486942	0.801432972	0.012145997	0.961289417	0.006365637	0.953582849	-0.004822204
Diagonal	0.764855077	-0.002078437	0.919291692	-0.001189499	0.854284946	-0.0285122	0.965693383	0.005279706	0.640879394	-0.009761958	0.942186748	0.000658096	0.910008601	0.00576905

TABLE 12. The Correlation coefficients of the RGB plain-images and their corresponding enciphered ones.

	Image	Baboon		Lenna		Digital Electronics		MonaLiza		Egyptian civilization		Raccoon Face		Peppers	
	Size	256 × 256		256 × 256		600 × 450		900 × 1285		259 × 194		1024 × 768		225 × 225	
		Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher
Horizontal	Red	0.91316	0.0466	0.951328	0.078871	0.743567	-0.11251	0.987688	-0.068	0.74671	0.016527	0.97491	-0.05173	0.942187	0.030879
	Green	0.8873	0.04187	0.939624	0.023948	0.899011	-0.07257	0.979396	-0.04917	0.736277	0.001119	0.975053	-0.01444	0.96667	0.000453
	Blue	0.9093	0.04131	0.904271	0.038807	0.922228	-0.05708	0.930638	-0.0605	0.672011	0.025348	0.98142	-0.03308	0.915503	0.109496
Vertical	Red	0.88846	0.02528	0.971148	-0.00738	0.748312	-0.02269	0.983761	0.002468	0.82267	0.031842	0.963181	0.050081	0.94413	0.031071
	Green	0.86338	0.01994	0.969613	-0.00365	0.897515	0.009905	0.972425	-0.00469	0.82598	0.006339	0.963289	-0.02039	0.967374	0.001235
	Blue	0.88138	0.00966	0.946	-0.00329	0.920564	-0.02841	0.914459	0.015062	0.768843	0.02336	0.972222	0.015992	0.925141	0.000289
Diago-nal	Red	0.85334	0.01022	0.929575	-0.00985	0.649234	-0.01759	0.974899	0.011713	0.656662	-0.01058	0.945303	0.018158	0.891525	0.018151
	Green	0.8126	0.01812	0.914955	0.00239	0.838772	0.023939	0.95792	0.002046	0.652131	0.003172	0.945524	0.006551	0.935919	0.935919
	Blue	0.83585	0.03672	0.876547	-0.02433	0.873721	0.015262	0.863135	-0.01486	0.561599	0.006702	0.959037	0.042122	0.846083	0.044014

3) STRICT AVALANCHE CRITERION

The SAC concept was introduced by Webster and Traverse that reflects the variance in the output bits when one input bit is changed. Approximately half of the output bits change when only one input bit is complemented.

Theorem 3 [20]:

Suppose that $F(x) = (f_1(x), \ldots, f_m(x))$ from $GF(2)^m$to $GF(2)^m$ is a Boolean function of multiple outputs, $\forall\sigma = (\sigma_m, \sigma_{m-1}, \ldots \sigma_1) \epsilon GF(2)^m$, $w(\sigma) = 1$, if $w(f_l(x+a) + f_l(x)) = 2^{n-1}$, $(1 \le l \le m)$, then $F(x)$ fulfills the Strict Avalanche Criterion (SAC).

Theorem 4 [20]:

Suppose $F(x) = (f_1(x), \ldots, f_m(x))$ from $GF(2)^m$ to $GF(2)^m$ is a Boolean function of multiple outputs. the distance to SAC is denoted by DSAC(F) and it is defined as follows:

$$\mathrm{DSAC}(\mathrm{F}) = \sum_{l=1}^{n} \sum_{\substack{\sigma \in GF(2)^m \\ w(\sigma)=1}} \left| w\left(f_l(x+\sigma) + f_l(x) - 2^{m-1}\right)\right| \tag{8}$$

When $\boldsymbol{DSAC} = \boldsymbol{0}$, this implies that $\boldsymbol{F(x)}$ fulfills the SAC. The existing S-Boxes do not satisfy SAC.

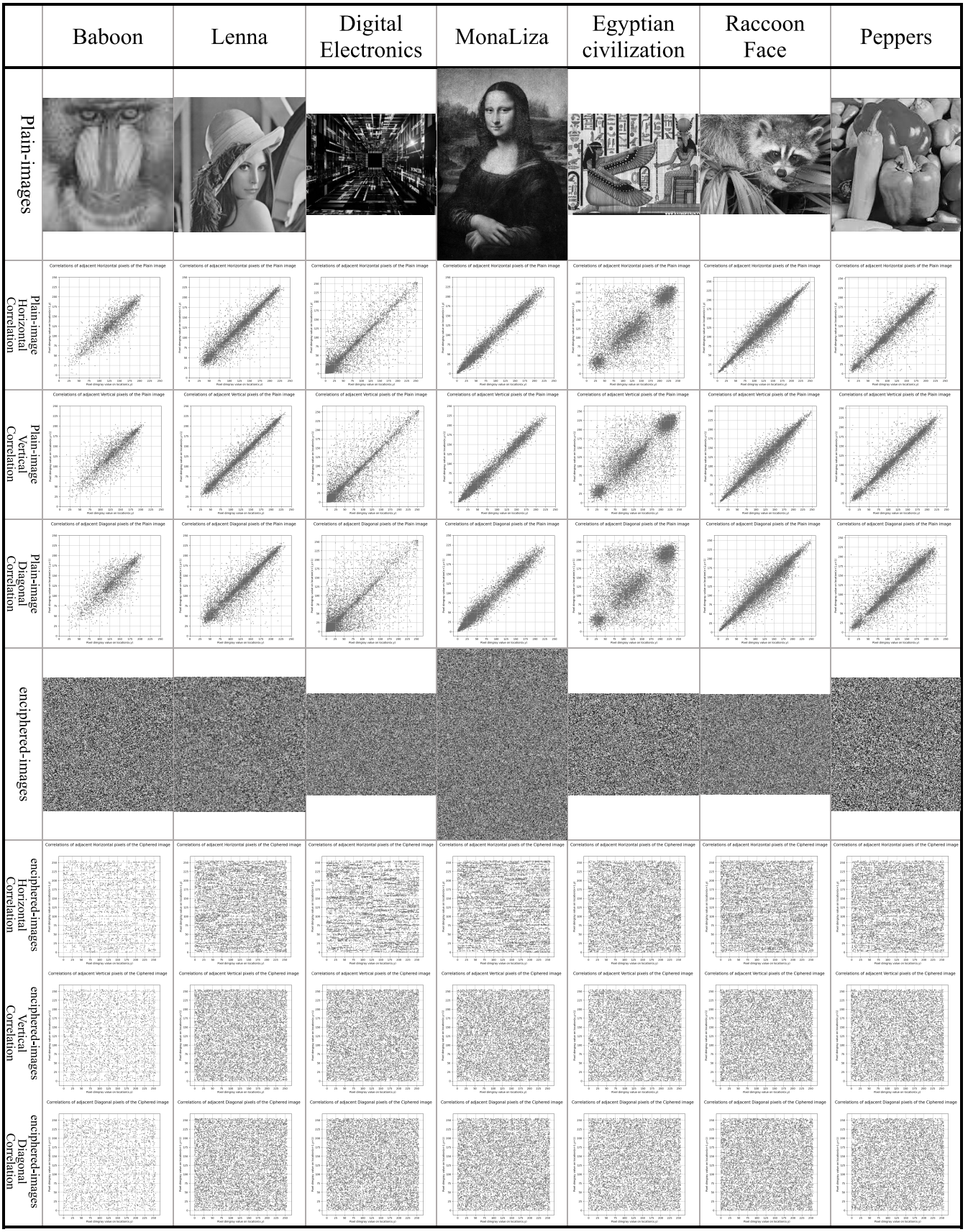


FIGURE 5. The Correlation of the Gray plain-images and their corresponding enciphered ones.

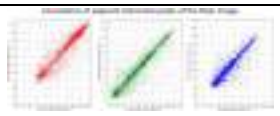
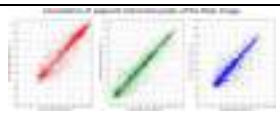
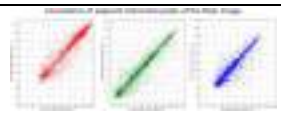
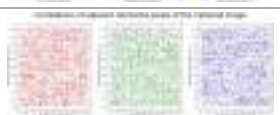
Image	Size	Image type	Correlation		
			Horizontal	Horizontal	Horizontal
Baboon	256 × 256	Plain-image			
		Enciphered-image			
Lenna	256 × 256	Plain-image			
		Enciphered-image			
Digital Electronics	600 × 450	Plain-image			
		Enciphered-image			
MonaLiza	900 × 1285	Plain-image			
		Enciphered-image			
Egyptian civilization	259 × 194	Plain-image			
		Enciphered-image			
Raccoon Face	1024 × 768	Plain-image			
		Enciphered-image			
Peppers	225 × 225	Plain-image			
		Enciphered-image			

FIGURE 6. The Correlation of the RGB plain-images and their corresponding enciphered ones.

TABLE 13. Information entropies of the Gray plain-images and their corresponding enciphered ones.

Image	Size	Entropy	
		Plain-image	Enciphered-image
Baboon	256 × 256	7.237393	7.997023
Lenna	256 × 256	7.452783	7.997807
Digital Electronics	600 × 450	6.634116	7.999379
MonaLiza	900 × 1285	7.264233	7.999845
Egyptian civilization	259 × 194	6.634116	7.999379
Raccoon Face	1024 × 768	7.731369	7.999778
Peppers	225 × 225	7.608369	7.996123

The SAC of the proposed S-box function $F(x) = (f_1(x), f_2(x), \ldots, f_8(x))$is illustrated **Table 7**, and then its DSAC is obtained to have

$$\text{DSAC (proposed S-Box)} = 316$$

According to previous results, however, the SAC is not satisfied, but the rate of changing in the output bits is acceptable as it has bounds near $0.5{*}2^m = 128$ bit.

4) BIT INDEPENDENCE CRITERION

The BIC parameter was introduced by Webster and Traverses. It is used as a standard to check the level of security of the S-Boxes against different attacks [4], [21], [22].

Theorem 5 [18]:

Suppose $F(x) = (f_1(x), \ldots, f_m(x))$ from $GF(2)^m$ to $GF(2)^m$ is a Boolean function of multiple outputs, The BIC computation is made by getting m×m - dimensional matrix $BIC(F) = b_{lk}$ such that l, k, then b_{lk} is defined to be:

$$BIC(F) = \sum_{l=1}^{n} \sum_{\substack{\sigma \in GF(2)^m \\ w(\sigma)=1}} \left| w(f_l(x) + f_k(x) - 2^{m-1}) \right| \tag{9}$$

5) NON-LINEARITY

Nonlinearity (NL) is one of the most important criteria in the cryptosystem, which was introduced for the first time in the 1980s by Meier and Staffelbach and later in the early 1990s by Nyberg. As it is known, the S-Box is the non-linear part of the cryptographic algorithm that gives it the ability to withstand differential and linear cryptanalysis. A higher nonlinearity value is an indication of its resistance against differential and linear attacks. Mathematically, nonlinearity is calculated using Walsh's spectrum [3].

Theorem 6 [18]:

Suppose $F(x) = (f_1(x), \ldots, f_m(x))$ from $GF(2)^m$ to $GF(2)^m$ is a Boolean function of multiple outputs, the nonlinearity that is calculated for *m-bit* Boolean functions as $NL(f_i)$ is expressed as follow:

$$NL(f_i) = 2^{m-1} - \frac{1}{2}\left(\left|W_{f_i}(u)\right|\right) \tag{10}$$

where $u \in f_2^m$.

$$W_f(u) = \sum_{t \in \{0,1\}^m} (-1)^{f(t) \oplus t.u} \tag{11}$$

$$NL(f) = \min_{\substack{0 \neq v \in GF(2)^m \\ l(x) \in L_m[X]}} d(v.F(x), l(x)) \tag{12}$$

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

$NL(f)$ is a measure of the resistance of the S-Box against linear attacks. The ideal Non-Linear function $NL(f)$ should be $NL(f) = 2^{m-1} - 2^{\frac{m}{2}-1} = 120$. We get *NL(f)=112* for the proposed S-box, it's very close to the ideal $NL(f)$.

TABLE 14. Information entropies of RGB plain-images and their corresponding enciphered images.

Image	Size	The Plain-Image				The Enciphered-Image			
		Red	Green	Blue	Image	Red	Green	Blue	Image
Baboon	256 × 256	7.6637	7.36	7.6921	7.6904	7.99751	7.99759	7.99735	7.99927
Lenna	256 × 256	7.26883	7.59763	6.9716	7.75077	7.997345	7.997697	7.997328	7.999184
Digital Electronics	600 × 450	7.75635	7.81551	7.61261	7.94258	7.996204	7.996102	7.996611	7.998784
MonaLiza	900 × 1285	7.5572	7.24613	6.38616	7.25257	7.999844	7.999845	7.999827	7.999946
Egyptian civilization	259 × 194	7.75635	7.81551	7.61261	7.94258	7.996204	7.996102	7.996611	7.998784
Raccoon Face	1024 × 768	7.73397	7.76838	7.80269	7.79204	7.999763	7.999776	7.999796	7.999934
Peppers	225 × 225	7.4462	7.70062	7.2262	7.79589	7.995604	7.995446	7.996344	7.9988

IV. PROPOSED IMAGE SECURE SCHEME USING S-BOX

In this section, the proposed encryption scheme based on the prementioned S-Box, presented in **Table 3**, is illustrated. It is used to encrypt images in two modes: gray scale and RGB images. We employed our S-box to execute the permutation-substitution operations based purely on the S-box.

The proposed encryption scheme based on the generated S-Box is illustrated below.

Input	The Plain-image P of size $3 \times \alpha \times \beta$ in RGB mode
Output	The Enciphered image
Proposed Scheme	1 Read the generated S-Box (S) mentioned above in **Table 4** as LUT. 2 Split the RGB image into three $\alpha \times \beta$ components. 3 For each frame in P 4 Temp = Key of component (K_r, K_g, K_b) 5 For $i = 0 : \alpha - 1$ 6 For $j = 0 : \beta - 1$ 7 $Pixel(i,j) = S\,(Pixel(i,j) \oplus Temp)$ 8 $Temp = Pixel(i,j)$ 9 End For 10 End For 11 End For 12 Combine three components again to get the enciphered-image C

A. STATICAL ATTACK ANALYSIS

1) CORRELATION COEFFICIENT ANALYSIS

A pixel is the base unit of any image. Each pixel can be represented by a value depending on its resolution. The pixel resolution is the number of bits used to define its value; so, the pixel resolution here is 8.

As the correlation is the mirror of the image meaningful, whenever the correlation is high, it is an indication of understanding/ having a meaningful visual image. It expresses the relationship between any neighboring pixels, even they are horizontal, vertical or diagonal [39]. For meaningful images, it's said that the neighboring pixels are almost the same. On the other hand, it is desirable to have poor/ low correlation for enciphered images and that's our target [40].

Any coefficient can be computed using the following expression.

$$\mathrm{Co} = \frac{\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}\left(P_{ij}-\overline{P}\right)\left(C_{ij}-\overline{C}\right)}{\sqrt{\left(\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}\left(P_{ij}-\overline{P}\right)^2\right)\left(\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}\left(C_{ij}-\overline{C}\right)^2\right)}} \tag{13}$$

TABLE 15. UACI and NPCR of the enciphered Gray images.

Image	*Size*	*UACI (%)*	*NPCR (%)*
Baboon	256 × 256	33.5923438	100
Lenna	256 × 256	33.6641857670802	100
Digital Electronics	600 × 450	33.6585693536673	100
MonaLiza	900 × 1285	33.5772084467163	100
Egyptian civilization	259 × 194	33.6880118444703	100
Raccoon Face	1024 × 768	33.5990491879531	100
Peppers	225 × 225	33.4490709271362	100

where α and β represent the width and height of the image, respectively. C_{ij} and P_{ij} are the pixel positions in the cipher-image and their corresponding in the plain-image with i^{th} column and j^{th} row, respectively. $\overline{P}$ and $\overline{C}$ are the mean values of P and C.

2) INFORMATION ENTROPY

The information entropy was reported by Shannon in 1948. It is considered a basic concept/ feature in statics [41]. This is a way to measure the randomness nature in the information of the encrypted/ciphered image. The pixel resolution is the ideal value of this criterion, so, in our case, the optimal entropy value is 8 [42]. This can be mathematically calculated as follows:

$$H(m) = \sum_{j=0}^{L} P(x_j) \cdot \log_2\left(P(x_j)\right) \tag{14}$$

$$L = 2^m - 1 \tag{15}$$

where $P(x_j)$ is the occurrence repetition of each possible color level/ pixel value, L expresses the countable color level for each frame/color, m represents the pixel resolution.

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

3) HISTOGRAM ANALYSIS

The histogram shows the distribution of the color levels using the pixel values throughout/within the image plane. It reflects the resistance of an image, especially enciphered ones, against statical attacks [43].

The histograms of both the plain images and their corresponding enciphered ones are shows below. It is clear that the histogram for the enciphered images in all frames is flattened, implying that the equality of the pixel values is repeated.

Table 7 and **Table 8** illustrate the histogram for images in Gray and RGB modes, respectively.

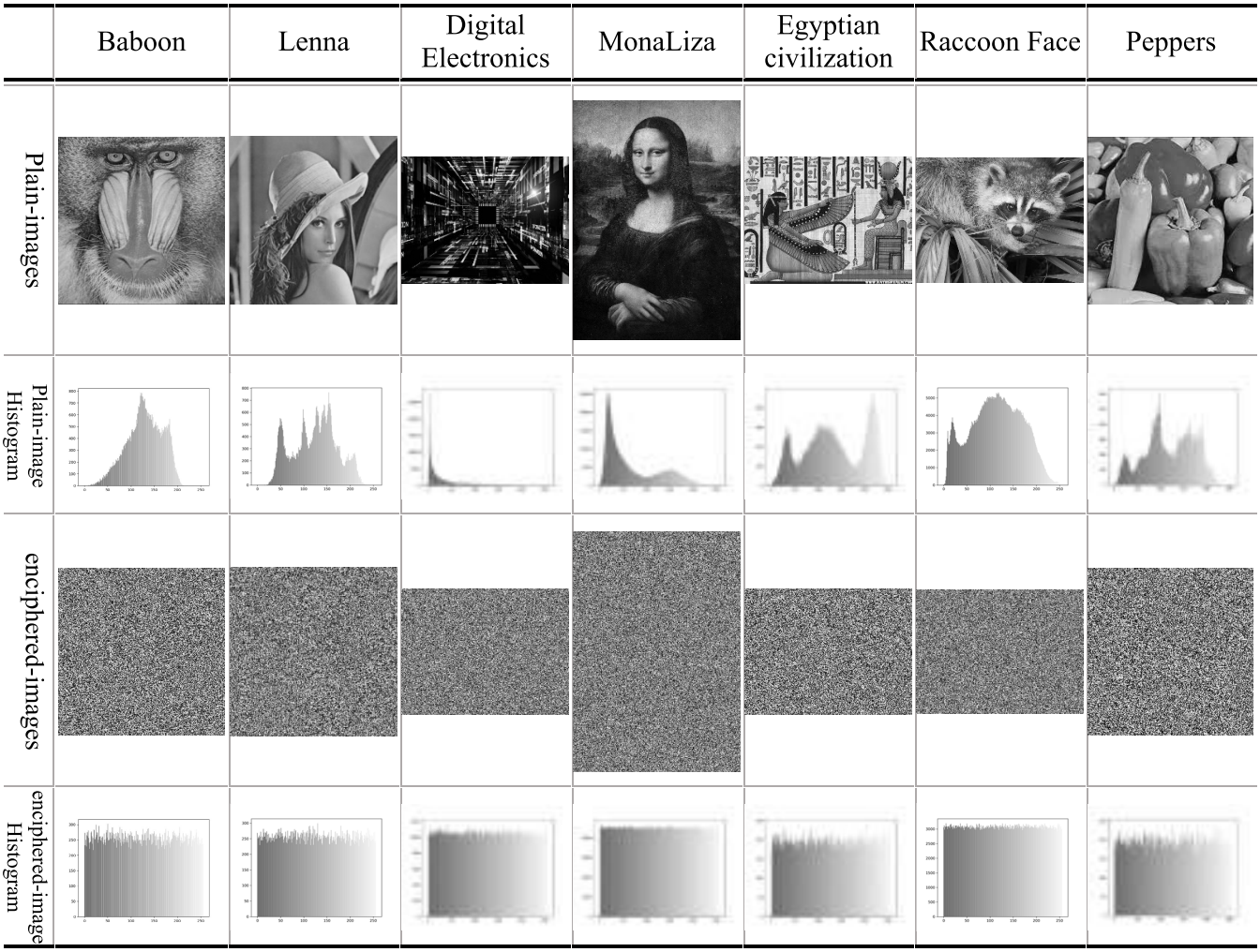


FIGURE 7. Gray-mode Plain-images and enciphered- images using proposed enciphering scheme based on proposed S-Box with their corresponding histograms.

TABLE 16. UACI and NPCR of the enciphered RGB images.

Image	Size	UACI (%)				NPCR (%)			
		Red	Green	Blue	Image	Red	Green	Blue	Image
Baboon	256 × 256	33.506	33.5933	33.6152	33.5715	100	100	100	100
Lenna	256 × 256	33.6313	33.4737	33.652	33.5857	100	100	100	100
Digital Electronics	600 × 450	33.5711	33.592	33.5858	33.583	100	100	100	100
MonaLiza	900 × 1285	33.6396	33.5786	33.5984	33.6056	100	100	100	100
Egyptian civilization	259 × 194	33.5801	33.5916	33.5634	33.5783	100	100	100	100
Raccoon Face	1024 × 768	33.6108	33.6151	33.5609	33.5956	100	100	100	100
Peppers	225 × 225	33.4769	33.6529	33.4767	33.5355	100	100	100	100

B. DIFFERENTIAL ATTACKS

One of the attackers' known behaviors to discover the enciphering scheme is to make changes in the plain message and have their corresponding ciphered message. Therefore, the target was achieved after analyzing the data pairs [38]. Therefore, it is important to guarantee that this method is not applicable. This can be achieved when the scheme depends on tiny data exist in the image, so we can be sure that the system

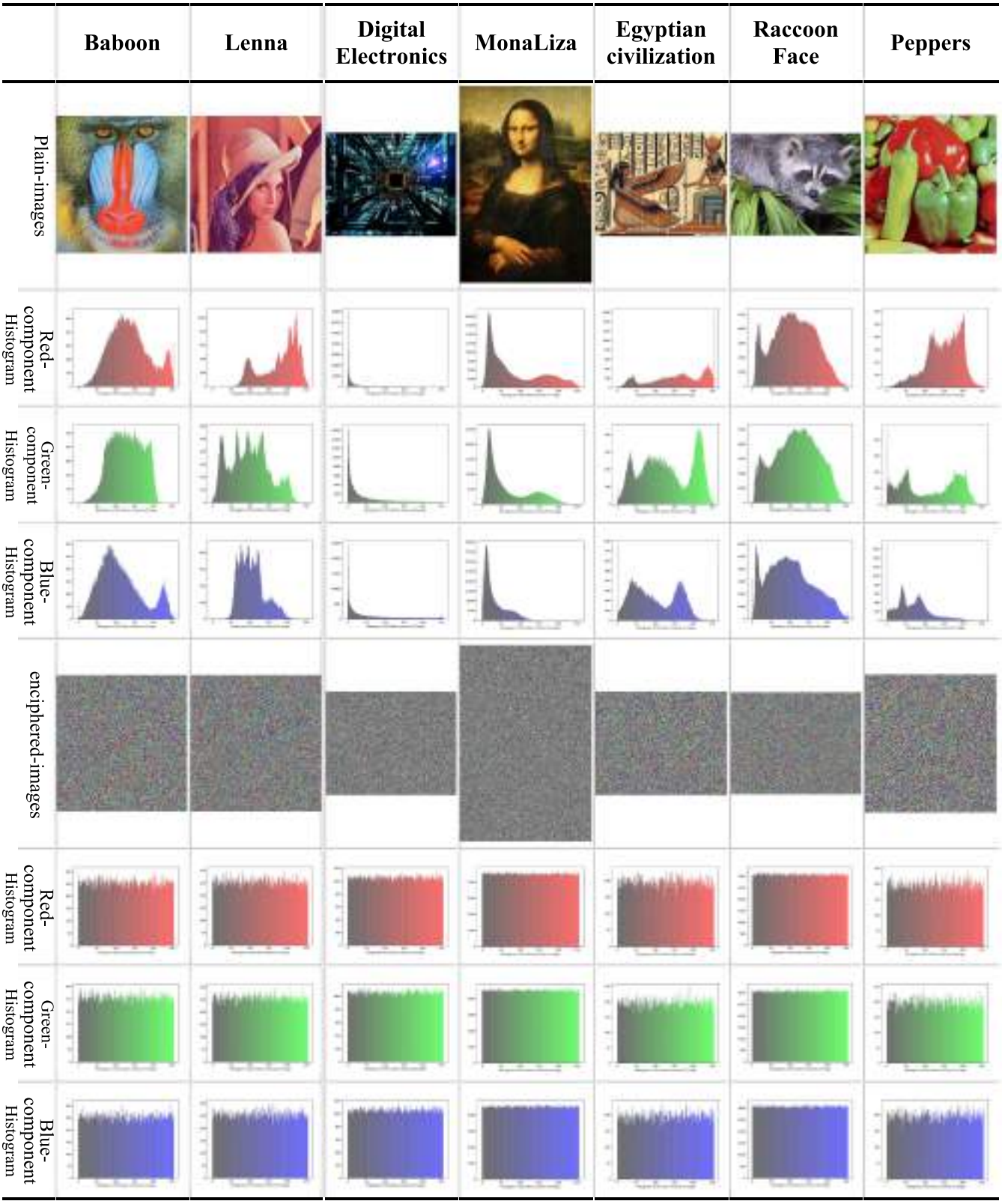


FIGURE 8. RGB mode Plain-images and enciphered- images using the the proposed enciphering scheme based on proposed S-Box with their corresponding histograms.

TABLE 17. MSE and PSNR of the enciphered Gray images.

Image	Size	MSE	PSNR (DB)
Baboon	256 × 256	6952.402603	9.709454474
Lenna	256 × 256	7719.914917	9.25467847
Digital Electronics	600 × 450	15636.35502	6.189448384
MonaLiza	900 × 1285	12263.8952	7.244519301
Egyptian civilization	259 × 194	9932.9797	8.16000813
Raccoon Face	1024 × 768	8679.359673	8.74592675
Peppers	225 × 225	8331.407802	8.923619682

is against differential attacks. In order to decide whether our scheme has this feature - dependence on tiny data- or not, a number of tests are taken places.

These techniques check the scheme behavior against a one-bit difference in plain-images.

1) UACI AND NPCR

One of the highly recommended tests is the Unified Average Change Intensity (UACI) and the Number of Pixel Change Rate (NPCR). UACI aims to calculate the average difference in intensity between two ciphered images [38]. The higher the value, the better the scheme. The expected theoretical value of the UACI is 33.4635%. This is mathematically computed as follows:

$$\mathrm{UACI}_{\mathrm{R,G,B}} = \frac{1}{\alpha\beta}\left[\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}\frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \tag{16}$$

where $C_1(i,j)$ and $C_2(i,j)$ are the enciphered images and their corresponding plain-images are the same but with a bit change in one of them.

The NPCR is denoted to the percentage of different pixels between two encrypted images [44]. The higher the value is, the better the scheme. The expected theoretical value is 99.6094%. This is mathematically computed as follow:

$$NPCR_{R,G,B} = \frac{1}{\alpha\beta}\left[\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}D(i,j)\right] \tag{17}$$

$$D(i,j) = \begin{cases} 1 & if\ C_1(i,j) \neq C_2(i,j) \\ 0 & if\ C_1(i,j) = C_2(i,j) \end{cases} \tag{18}$$

C. DATA LOSS

During data transmission in a noisy medium, data corruption is a natural behavior that occurs in the cipher-image. It's essential to an have an enciphered-image that's not the same as the plain image.

1) MSE AND PSNR

Mean Square Error (MSE) is a check between the plain-image and cipher-image to determine the encryption level [40], As the larger the value of MSE is, the higher distortion/ error between plain images and its enciphered one. MSE is defined as:

$$\mathrm{MSE}_{\mathrm{R,G,B}} = \frac{1}{\alpha\beta}\left[\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}\left(C_{ij} - P_{ij}\right)^2\right] \tag{19}$$

Peak Signal to Noise Ratio (PSNR) is a robustness measure of the encipher scheme in noise medium.

$$\mathrm{PSNR} = 20\log\left(\frac{P_{MAX}}{\sqrt{MSE}}\right) \tag{20}$$

where P_{max} is the expected maximum value of the pixel.

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

TABLE 18. MSE and PSNR of the enciphered RGB images.

Image	Size	MSE				PSNR (DB)
		Red	Green	Blue	Image	
Baboon	256 × 256	8350.8315	7256.772	9026.853	8211.4854	8.9865864
Lenna	256 × 256	10610.337	8994.436	7060.3545	8888.3758	8.6425795
Digital Electronics	600 × 450	18198.505	15452.83	15067.245	16239.527	6.0250699
MonaLiza	900 × 1285	12223.742	12452.09	15244.142	13306.658	6.8901137
Egyptian civilization	259 × 194	11407.935	10165.76	9813.6446	10462.447	7.9344708
Raccoon Face	1024 × 768	8780.56	8733.278	9679.735	9064.5245	8.5573533
Peppers	225 × 225	8001.4341	10906.41	10878.131	9928.6595	8.1618974

TABLE 19. MAE of the enciphered Gray images.

Image	Size	MAE
Baboon	256 × 256	69.8742218
Lenna	256 × 256	72.80337524
Digital Electronics	600 × 450	103.763963
MonaLiza	900 × 1285	90.5466649
Egyptian civilization	259 × 194	81.3916332
Raccoon Face	1024 × 768	76.5500895
Peppers	225 × 225	75.10885926

2) MEAN ABSOLUTE ERROR

Average difference in color intensity between the cipher-image and the plain-image. Whenever the higher that value is, this is an indication for the high security of the proposed scheme. MAE is defined as follows:

$$MAE_{R,G,B} = \frac{1}{\alpha\beta}\left[\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta}|C(i,j) - P(i,j)|\right] \tag{21}$$

D. OCCLUSION ATTACK

During the digital transmission process of data through public channels, the data are exposed to be missed. The stolen password of the image is applied by a data-loss attack in which the attackers seek to remove parts of the data [45]. So, various data loss sizes were made to test the level of recovery of the enciphered images. A Raccoon face image was selected as the plain image, and the results after applying the attack are shown in **Figure 9**.

E. SPEED ANALYSIS

With the current development in data transfer, it is become so important to concentrate on finding enciphering schemes that are able to generate the encrypted data in low computational time, which benefits the real-time applications.

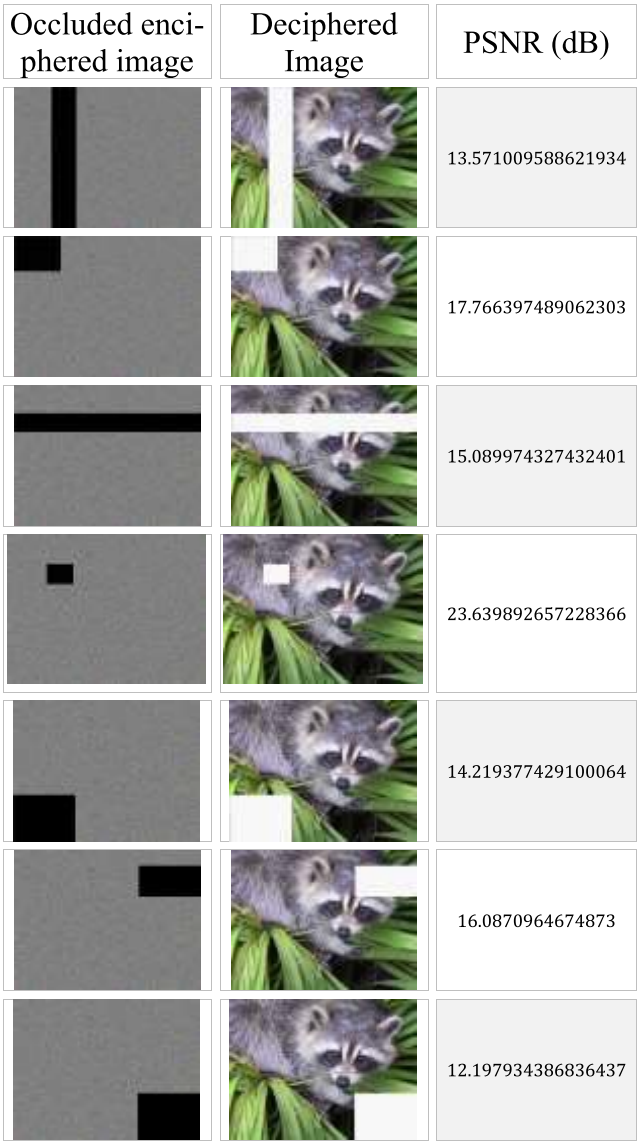


FIGURE 9. Experimental results of occlusion attacks.

In this study, the proposed algorithm with their analytical criteria were implemented using python programming language on ***Windows 10 OS with Intel (R) Core ^{TM}i5-CPU @***

TABLE 20. MAE of the enciphered RGB image.

Image	Size	MAE			
		Red	Green	Blue	Image
Baboon	256 × 256	75.20597839	71.07707214	77.90866089	74.73057048
Lenna	256 × 256	83.98094177	77.76554871	70.18855286	77.31168111
Digital Electronics	600 × 450	113.7074815	103.022563	101.5674815	106.0991753
MonaLiza	900 × 1285	90.41904453	91.32516732	102.2511492	94.66512033
Egyptian civilization	259 × 194	87.312602	82.45945946	81.01219998	83.59475381
Raccoon Face	1024 × 768	76.96766663	76.80047735	80.46578852	78.0779775
Peppers	225 × 225	73.87369877	85.30968889	85.18577778	81.45638848

TABLE 21. Speed analysis for the gray images.

Image	Size	Total Bytes	Encryption time (Sec)	Throughput (MBps)	Cycles per Byte
Baboon	256 × 256	196608	0.03124213	2.09768013	762.747368
Lenna	256 × 256	196608	0.03114724	2.10407075	760.430703
Digital Electronics	600 × 450	810000	0.12496519	2.16060167	740.534465
MonaLiza	900 × 1285	3469500	0.51550484	2.24343191	713.19303
Egyptian civilization	259 × 194	150738	0.01562119	3.21652929	497.430571
Raccoon Face	1024 × 768	2359296	0.34366989	2.28833546	699.198184
Peppers	225 × 225	151875	0.01562023	3.24098907	493.676456

TABLE 22. Speed analysis for the RGB images.

Image	Size	Total Bytes	Encryption time (Sec)	Throughput (MBps)	Cycles per Byte
Baboon	256 × 256	196608	0.121083021	1.623745411	985.3761488
Lenna	256 × 256	196608	0.124969482	1.573248094	1017.004251
Digital Electronics	600 × 450	810000	0.515621185	1.570920713	1018.510983
MonaLiza	900 × 1285	3469500	2.405650616	1.442229382	1109.393568
Egyptian civilization	259 × 194	150738	0.094664574	1.592338022	1004.811779
Raccoon Face	1024 × 768	2359296	1.499654055	1.573226834	1017.017995
Peppers	225 × 225	151875	0.0970737551	1.553906343	1029.663086

1.60GHz speed and 8 GB RAM.

$$Throughput = \frac{image\ size\ in\ bytes}{encryption\ time}\ (Bytes/Sec) \tag{22}$$

$$Cycles\ per\ byte = \frac{processor\ speed\ [in\ Hertz]}{throughput\ rate}(Cycle/Byte) \tag{23}$$

V. CONCLUSION

A methodology to generate a robust S-Box based on a strong algebraic base was introduced in this study.

The quality of S-Box is augmented to the optimum level by the action of a powerful permutation of S_{256}. The features of the proposed S-boxes are compared against a number of recent S-boxes. It is found that our proposed S-box has excellent performance strength compared with almost all other parameters especially DSAC which has a great value, equals to 316, that not another S-Box has. In our upcoming research, we aim to use another bent function, as we have a large number of functions that's reaches 886 various ones, in order to minimize the DSAC value. Because no one has it until now has the optimal value of DSAC that is equal to zero. The proposed S-box is expanded by DNA sequence, and it's

TABLE 23. Comparison of proposed encryption scheme and other schemes for Gray images; entropy, correlation, UACI, NPCR, time, throughput.

Image	Baboon				Lena	
Used scheme	**Proposed scheme**	**Ref. [38]**	**Ref. [46]**		**Proposed scheme**	**Ref. [38]**
Information entropy	7.997023	7.9964	7.9969	7.9969	7.997807	7.9968
Correlation	Hor. **−0.007812** Ver. **−0.038548** Dig. **−0.002078**	0.00568	-0.00098	-0.00284	Hor. **0.00183277** Ver. **0.00093002** Dig. **−0.0011894**	0.01014
UACI	33.5923438	99.684	33.56	33.34	33.664185	33.61
NPCR	100	33.43	99.62	99.54	100	99.693
System description	• Windows 10 OS • Intel(R) Core (TM) i5- CPU @ 1.60GHz speed • 8GB RAM	• Windows 8 OS • Intel corei7 @ 2.2GHz speed • 4GB RAM	• Windows 8 OS • CPU Core i7 2.2GHz • 4GB RAM		• Windows 10 OS • Intel (R) Core (TM) i5- CPU @ 1.60GHz speed • 8GB RAM	• Windows 8 OS • Intel corei7 @ 2.2GHz speed • 4GB RAM
Enc Time	0.03124213	0.08632	0.2634		0. 03114724	0.08632
Throughput (Mbps)	16.78144106	5.9313	1.99		16.83256601	5.9313

TABLE 24. Comparison of proposed encryption scheme and other schemes for RGB images; entropy, correlation, UACI, NPCR, time, throughput.

Image		Lena		
Used scheme		**Proposed scheme**	**Ref. [39]**	**Ref. [47]**
Information entropy	*RED*	7.997345	7.9893	7.9974
	GREEN	7.997697	7.9896	7.9976
	BLUE	7.997328	7.9903	7.9974
	IMAGE	7.999184	-	-
Correlation	*H RED*	0.078871	-	0.0064
	H GREEN	0.023948	-	0.0009
	H BLUE	0.038807	-	0.0091
	V RED	-0.00738	-	0.0160
	V GREEN	-0.00365	-	0.0034
	V BLUE	-0.00329	-	−0.0045
	D RED	-0.00985	-	−0.0026
	D GREEN	0.00239	-	0.0125
	D BLUE	-0.02433	-	−0.0090
UACI	*RED*	33.6313225	33.4639	33.4666
	GREEN	33.4737321	33.5042	33.4241
	BLUE	33.65200267	33.4776	33.4212
	IMAGE	33.5856858	-	
NPCR	*RED*	100	99.6100	99.6094
	GREEN	100	99.6092	99.6124
	BLUE	100	99.6099	99.6307
System description		• *Windows 10 OS* • *Intel(R) Core (TM) i5-CPU @ 1.60GHz speed* • *8GB RAM*	• *Windows 8 OS* • *Intel (R) Core (TM) i5-4300U CPU @ 2.49 GHz* • *8GB RAM*	• *Windows 7 OS* • *Core i5-2430M @ 2.4GH CPU* • *4 GB RAM*
Enc Time		0.124969482		-
Throughput (Mbps)		12.58598475	3.348	-

TABLE 25. Proposed S-box using DNA's Rule 1.

	AA	AG	AC	AT	GA	GG	GC	GT	CA	CG	CC	CT	TA	TG	TC	TT
AA	ACCT	GGGC	AACC	GCTA	CCGT	TTAA	AGCG	CCTC	ACGA	TCCA	GACG	CCAA	TATA	GTTC	ACGT	TGCG
AG	TTAT	ATAG	CGGG	TCTT	ATAA	TTCA	ATCT	AGGA	TTCG	GAAA	CTTC	GAAC	ATCG	GATG	TTCT	TTTG
AC	AGCA	CTAT	TACT	GCCA	ACCG	CCCC	GCAA	ACAG	GTCA	AATT	AGGT	CTCC	TGTA	AAAA	TGAC	CTTA
AT	ATGG	TAAG	TTTT	CTCT	GCGT	GCGC	ATTC	CCTT	AAGG	GTCC	AAAG	GGCC	CGGC	GAGT	GGAA	ATCC
GA	ACAA	GATA	CAAA	ACTT	CTAA	TCAA	TGGT	GTCG	ACTC	GTTT	GTTG	AAGC	GTAT	TAAT	CGGT	GGTG
GG	AGAA	ATGA	TCTC	TGCC	CATA	AACA	CTAC	CGTA	TACC	GGGG	TTGT	CCAC	CTGC	GTAA	TAAC	AGTA
GC	CTGA	AACG	CTCG	CGTC	GCAC	CCCG	CGCC	CGTT	TCCC	CCCA	ATTG	AGCT	GTAG	GAGA	TGGA	AACT
GT	TCCG	TAAA	GAGC	TAGC	AAGA	GACC	GCAG	GTGG	TTTC	GAAG	GGAC	GCCC	GCCT	AGTC	GATT	CCTA
CA	GCGG	ACCC	CTAG	AGAG	CTGG	ATCA	CCGA	CCAT	GAAT	ACCA	CGCG	CGAT	TATC	GTAC	TGTG	TTTA
CC	ATTA	TGCA	GTGC	TCAG	AGGC	TCGC	ACAT	AGAC	GCTG	CAGG	CATC	ACGC	GGGA	CTTT	ATGC	TCTG
CG	CGAC	AGCC	TCAT	AATG	CGCA	GGGT	ATAC	CGGA	TGTT	TGAA	TCCT	TCAC	ACAC	CACA	ATTT	CAGA
CT	GCAT	GTCT	AGTG	CATG	CAGC	TGTC	ACTG	CCCT	TAGT	GATC	CAAT	CGAG	TTGG	GCTC	AAGT	ATAT
TA	GTGA	TGAT	GGTA	CATT	TATT	TGAG	TCGG	TACG	AATC	TTAG	CGTG	AGTT	CACT	AGGG	GGAT	GGTC
TG	GGAG	GGTT	CAGT	CTTG	GACT	CCGC	TTGC	GTGT	CCGG	ATGT	ACGG	GGCG	CACG	ACTA	AATA	GCTT
TC	AAAC	AGAT	TCGA	TGGC	TTGA	TACA	GTTA	CCAG	GAGG	CAAC	TGGG	CACC	TATG	TCGT	TTCC	TTAC
TT	CGCT	GGCA	GGCT	CAAG	GCGA	TAGG	CTCA	TCTA	GCCG	CGAA	AAAT	CTGT	CCTG	TAGA	GACA	TGCT

TABLE 26. Proposed S-box using DNA's Rule 2.

	AA	AC	AG	AT	CA	CC	CG	CT	GA	GC	GG	GT	TA	TC	TG	TT
AA	AGGT	CCCG	AAGG	CGTA	GGCT	TTAA	ACGC	GGTG	AGCA	TGGA	CAGC	GGAA	TATA	CTTG	AGCT	TCGC
AC	TTAT	ATAC	GCCC	TGTT	ATAA	TTGA	ATGT	ACCA	TTGC	CAAA	GTTG	CAAG	ATGC	CATC	TTGT	TTTC
AG	ACGA	GTAT	TAGT	CGGA	AGGC	GGGG	CGAA	AGAC	CTGA	AATT	ACCT	GTGG	TCTA	AAAA	TCAG	GTTA
AT	ATCC	TAAC	TTTT	GTGT	CGCT	CGCG	ATTG	GGTT	AACC	CTGG	AAAC	CCGG	GCCG	CACT	CCAA	ATGG
CA	AGAA	CATA	GAAA	AGTT	GTAA	TGAA	TCCT	CTGC	AGTG	CTTT	CTTC	AACG	CTAT	TAAT	GCCT	CCTC
CC	ACAA	ATCA	TGTG	TCGG	GATA	AAGA	GTAG	GCTA	TAGG	CCCC	TTCT	GGAG	GTCG	CTAA	TAAG	ACTA
CG	GTCA	AAGC	GTGC	GCTG	CGAG	GGGC	GCGG	GCTT	TGGG	GGGA	ATTC	ACGT	CTAC	CACA	TCCA	AAGT
CT	TGGC	TAAA	CACG	TACG	AACA	CAGG	CGAC	CTCC	TTTG	CAAC	CCAG	CGGG	CGGT	ACTG	CATT	GGTA
GA	CGCC	AGGG	GTAC	ACAC	GTCC	ATGA	GGCA	GGAT	CAAT	AGGA	GCGC	GCAT	TATG	CTAG	TCTC	TTTA
GC	ATTA	TCGA	CTCG	TGAC	ACCG	TGCG	AGAT	ACAG	CGTC	GACC	GATG	AGCG	CCCA	GTTT	ATCG	TGTC
GG	GCAG	ACGG	TGAT	AATC	GCGA	CCCT	ATAG	GCCA	TCTT	TCAA	TGGT	TGAG	AGAG	GAGA	ATTT	GACA
GT	CGAT	CTGT	ACTC	GATC	GACG	TCTG	AGTC	GGGT	TACT	CATG	GAAT	GCAC	TTCC	CGTG	AACT	ATAT
TA	CTCA	TCAT	CCTA	GATT	TATT	TCAC	TGCC	TAGC	AATG	TTAC	GCTC	ACTT	GAGT	ACCC	CCAT	CCTG
TC	CCAC	CCTT	GACT	GTTC	CAGT	GGCG	TTCG	CTCT	GGCC	ATCT	AGCC	CCGC	GAGC	AGTA	AATA	CGTT
TG	AAAG	ACAT	TGCA	TCCG	TTCA	TAGA	CTTA	GGAC	CACC	GAAG	TCCC	GAGG	TATC	TGCT	TTGG	TTAG
TT	GCGT	CCGA	CCGT	GAAC	CGCA	TACC	GTGA	TGTA	CGGC	GCAA	AAAT	GTCT	GGTC	TACA	CAGA	TCGT

planned to use RNA sequence in the future work in a trial to improve the proposed one. Based on the aforementioned S-Box, a proposed encryption scheme was used to encrypt some standard plain-images to evaluate their encryption performance. The results show that they are sufficiently suitable for use in secure multimedia applications as well as its low

TABLE 27. Proposed S-box using DNA's Rule 3.

	GG	GA	GT	GC	AG	AA	AT	AC	TG	TA	TT	TC	CG	CA	CT	CC
GG	GTTC	AAAT	GGTT	ATCG	TTAC	CCGG	GATA	TTCT	GTAG	CTTG	AGTA	TTGG	CGCG	ACCT	GTAC	CATA
GA	CCGC	GCGA	TAAA	CTCC	GCGG	CCTG	GCTC	GAAG	CCTA	AGGG	TCCT	AGGT	GCTA	AGCA	CCTC	CCCA
GT	GATG	TCGC	CGTC	ATTG	GTTA	TTTT	ATGG	GTGA	ACTG	GGCC	GAAC	TCTT	CACG	GGGG	CAGT	TCCG
GC	GCAA	CGGA	CCCC	TCTC	ATAC	ATAT	GCCT	TTCC	GGAA	ACTT	GGGA	AATT	TAAT	AGAC	AAGG	GCTT
AG	GTGG	AGCG	TGGG	GTCC	TCGG	CTGG	CAAC	ACTA	GTCT	ACCC	ACCA	GGAT	ACGC	CGGC	TAAC	AACA
AA	GAGG	GCAG	CTCT	CATT	TGCG	GGTG	TCGT	TACG	CGTT	AAAA	CCAC	TTGT	TCAT	ACGG	CGGT	GACG
AT	TCAG	GGTA	TCTA	TACT	ATGT	TTTA	TATT	TACC	CTTT	TTTG	GCCA	GATC	ACGA	AGAG	CAAG	GGTC
AC	CTTA	CGGG	AGAT	CGAT	GGAG	AGTT	ATGA	ACAA	CCCT	AGGA	AAGT	ATTT	ATTC	GACT	AGCC	TTCG
TG	ATAA	GTTT	TCGA	GAGA	TCAA	GCTG	TTAG	TTGC	AGGC	GTTG	TATA	TAGC	CGCT	ACGT	CACA	CCCG
TA	GCCG	CATG	ACAT	CTGA	GAAT	CTAT	GTGC	GAGT	ATCA	TGAA	TGCT	GTAT	AAAG	TCCC	GCAT	CTCA
TT	TAGT	GATT	CTGC	GGCA	TATG	AAAC	GCGT	TAAG	CACC	CAGG	CTTC	CTGT	GTGT	TGTG	GCCC	TGAG
TC	ATGC	ACTC	GACA	TGCA	TGAT	CACT	GTCA	TTTC	CGAC	AGCT	TGGC	TAGA	CCAA	ATCT	GGAC	GCGC
CG	ACAG	CAGC	AACG	TGCC	CGCC	CAGA	CTAA	CGTA	GGCT	CCGA	TACA	GACC	TGTC	GAAA	AAGC	AACT
CA	AAGA	AACC	TGAC	TCCA	AGTC	TTAT	CCAT	ACAC	TTAA	GCAC	GTAA	AATA	TGTA	GTCG	GGCG	ATCC
CT	GGGT	GAGC	CTAG	CAAT	CCAG	CGTG	ACCG	TTGA	AGAA	TGGT	CAAA	TGTT	CGCA	CTAC	CCTT	CCGT
CC	TATC	AATG	AATC	TGGA	ATAG	CGAA	TCTG	CTCG	ATTA	TAGG	GGGC	TCAC	TTCA	CGAG	AGTG	CATC

TABLE 28. Proposed S-box using DNA's Rule 4.

	CC	CA	CT	CG	AC	AA	AT	AG	TC	TA	TT	TG	GC	GA	GT	GG
CC	CTTG	AAAT	CCTT	ATGC	TTAG	GGCC	CATA	TTGT	CTAC	GTTC	ACTA	TTCC	GCGC	AGGT	CTAG	GATA
CA	GGCG	CGCA	TAAA	GTGG	CGCC	GGTC	CGTG	CAAC	GGTA	ACCC	TGGT	ACCT	CGTA	ACGA	GGTG	GGGA
CT	CATC	TGCG	GCTG	ATTC	CTTA	TTTT	ATCC	CTCA	AGTC	CCGG	CAAG	TGTT	GAGC	CCCC	GACT	TGGC
CG	CGAA	GCCA	GGGG	TGTG	ATAG	ATAT	CGGT	TTGG	CCAA	AGTT	CCCA	AATT	TAAT	ACAG	AACC	CGTT
AC	CTCC	ACGC	TCCC	CTGG	TGCC	GTCC	GAAG	AGTA	CTGT	AGGG	AGGA	CCAT	AGCG	GCCG	TAAG	AAGA
AA	CACC	CGAC	GTGT	GATT	TCGC	CCTC	TGCT	TAGC	GCTT	AAAA	GGAG	TTCT	TGAT	AGCC	GCCT	CAGC
AT	TGAC	CCTA	TGTA	TAGT	ATCT	TTTA	TATT	TAGG	GTTT	TTTC	CGGA	CATG	AGCA	ACAC	GAAC	CCTG
AG	GTTA	GCCC	ACAT	GCAT	CCAC	ACTT	ATCA	AGAA	GGGT	ACCA	AACT	ATTT	ATTG	CAGT	ACGG	TTGC
TC	ATAA	CTTT	TGCA	CACA	TGAA	CGTC	TTAC	TTCG	ACCG	CTTC	TATA	TACG	GCGT	AGCT	GAGA	GGGC
TA	CGGC	GATC	AGAT	GTCA	CAAT	GTAT	CTCG	CACT	ATGA	TCAA	TCGT	CTAT	AAAC	TGGG	CGAT	GTGA
TT	TACT	CATT	GTCG	CCGA	TATC	AAAG	CGCT	TAAC	GAGG	GACC	GTTG	GTCT	CTCT	TCTC	CGGG	TCAC
TG	ATCG	AGTG	CAGA	TCGA	TCAT	GAGT	CTGA	TTTG	GCAG	ACGT	TCCG	TACA	GGAA	ATGT	CCAG	CGCG
GC	AGAC	GACG	AAGC	TCGG	GCGG	GACA	GTAA	GCTA	CCGT	GGCA	TAGA	CAGG	TCTG	CAAA	AACG	AAGT
GA	AACA	AAGG	TCAG	TGGA	ACTG	TTAT	GGAT	AGAG	TTAA	CGAG	CTAA	AATA	TCTA	CTGC	CCGC	ATGG
GT	CCCT	CACG	GTAC	GAAT	GGAC	GCTC	AGGC	TTCA	ACAA	TCCT	GAAA	TCTT	GCGA	GTAG	GGTT	GGCT
GG	TATG	AATC	AATG	TCCA	ATAC	GCAA	TGTC	GTGC	ATTA	TACC	CCCG	TGAG	TTGA	GCAC	ACTC	GATG

TABLE 29. Proposed S-box using DNA's Rule 5.

	GG	GT	GA	GC	TG	TT	TA	TC	AG	AT	AA	AC	CG	CT	CA	CC
GG	GAAC	TTTA	GGAA	TACG	AATC	CCGG	GTAT	AACA	GATG	CAAG	TGAT	AAGG	CGCG	TCCA	GATC	CTAT
GT	CCGC	GCGT	ATTT	CACC	GCGG	CCAG	GCAC	GTTG	CCAT	TGGG	ACCA	TGGA	GCAT	TGCT	CCAC	CCCT
GA	GTAG	ACGC	CGAC	TAAG	GAAT	AAAA	TAGG	GAGT	TCAG	GGCC	GTTC	ACAA	CTCG	GGGG	CTGA	ACCG
GC	GCTT	CGGT	CCCC	ACAC	TATC	TATA	GCCA	AACC	GGTT	TCAA	GGGT	TTAA	ATTA	TGTC	TTGG	GCAA
TG	GAGG	TGCG	AGGG	GACC	ACGG	CAGG	CTTC	TCAT	GACA	TCCC	TCCT	GGTA	TCGC	CGGC	ATTC	TTCT
TT	GTGG	GCTG	CACA	CTAA	AGCG	GGAG	ACGA	ATCG	CGAA	TTTT	CCTC	AAGA	ACTA	TCGG	CGGA	GTCG
TA	ACTG	GGAT	ACAT	ATCA	TAGA	AAAT	ATAA	ATCC	CAAA	AAAG	GCCT	GTAC	TCGT	TGTG	CTTG	GGAC
TC	CAAT	CGGG	TGTA	CGTA	GGTG	TGAA	TAGT	TCTT	CCCA	TGGT	TTGA	TAAA	TAAC	GTCA	TGCC	AACG
AG	TATT	GAAA	ACGT	GTGT	ACTT	GCAG	AATG	AAGC	TGGC	GAAG	ATAT	ATGC	CGCA	TCGA	CTCT	CCCG
AT	GCCG	CTAG	TCTA	CAGT	GTTA	CATA	GAGC	GTGA	TACT	AGTT	AGCA	GATA	TTTG	ACCC	GCTA	CACT
AA	ATGA	GTAA	CAGC	GGCT	ATAG	TTTC	GCGA	ATTG	CTCC	CTGG	CAAC	CAGA	GAGA	AGAG	GCCC	AGTG
AC	TAGC	TCAC	GTCT	AGCT	AGTA	CTCA	GACT	AAAC	CGTC	TGCA	AGGC	ATGT	CCTT	TACA	GGTC	GCGC
CG	TCTG	CTGC	TTCG	AGCC	CGCC	CTGT	CATT	CGAT	GGCA	CCGT	ATCT	GTCC	AGAC	GTTT	TTGC	TTCA
CT	TTGT	TTCC	AGTC	ACCT	TGAC	AATA	CCTA	TCTC	AATT	GCTC	GATT	TTAT	AGAT	GACG	GGCG	TACC
CA	GGGA	GTGC	CATG	CTTA	CCTG	CGAG	TCCG	AAGT	TGTT	AGGA	CTTT	AGAA	CGCT	CATC	CCAA	CCGA
CC	ATAC	TTAG	TTAC	AGGT	TATG	CGTT	ACAG	CACG	TAAT	ATGG	GGGC	ACTC	AACT	CGTG	TGAG	CTAC

TABLE 30. Proposed S-box using DNA's Rule 6.

	CC	CT	CA	CG	TC	TT	TA	TG	AC	AT	AA	AG	GC	GT	GA	GG
CC	CAAG	TTTA	CCAA	TAGC	AATG	GGCC	CTAT	AAGA	CATC	GAAC	TCAT	AACC	GCGC	TGGA	CATG	GTAT
CT	GGCG	CGCT	ATTT	GAGG	CGCC	GGAC	CGAG	CTTC	GGAT	TCCC	AGGA	TCCA	CGAT	TCGT	GGAG	GGGT
CA	CTAC	AGCG	GCAG	TAAC	CAAT	AAAA	TACC	CACT	TGAC	CCGG	CTTG	AGAA	GTGC	CCCC	GTCA	AGGC
CG	CGTT	GCCT	GGGG	AGAG	TATG	TATA	CGGA	AAGG	CCTT	TGAA	CCCT	TTAA	ATTA	TCTG	TTCC	CGAA
TC	CACC	TCGC	ACCC	CAGG	AGCC	GACC	GTTG	TGAT	CAGA	TGGG	TGGT	CCTA	TGCG	GCCG	ATTG	TTGT
TT	CTCC	CGTC	GAGA	GTAA	ACGC	CCAC	AGCA	ATGC	GCAA	TTTT	GGTG	AACA	AGTA	TGCC	GCCA	CTGC
TA	AGTC	CCAT	AGAT	ATGA	TACA	AAAT	ATAA	ATGG	GAAA	AAAC	CGGT	CTAG	TGCT	TCTC	GTTC	CCAG
TG	GAAT	GCCC	TCTA	GCTA	CCTC	TCAA	TACT	TGTT	GGGA	TCCT	TTCA	TAAA	TAAG	CTGA	TCGG	AAGC
AC	TATT	CAAA	AGCT	CTCT	AGTT	CGAC	AATC	AACG	TCCG	CAAC	ATAT	ATCG	GCGA	TGCA	GTGT	GGGC
AT	CGGC	GTAC	TGTA	GACT	CTTA	GATA	CACG	CTCA	TAGT	ACTT	ACGA	CATA	TTTC	AGGG	CGTA	GAGT
AA	ATCA	CTAA	GACG	CCGT	ATAC	TTTG	CGCA	ATTC	GTGG	GTCC	GAAG	GACA	CACA	ACAC	CGGG	ACTC
AG	TACG	TGAG	CTGT	ACGT	ACTA	GTGA	CAGT	AAAG	GCTG	TCGA	ACCG	ATCT	GGTT	TAGA	CCTG	CGCG
GC	TGTC	GTCG	TTGC	ACGG	GCGG	GTCT	GATT	GCAT	CCGA	GGCT	ATGT	CTGG	ACAG	CTTT	TTCG	TTGA
GT	TTCT	TTGG	ACTG	AGGT	TCAG	AATA	GGTA	TGTG	AATT	CGTG	CATT	TTAT	ACAT	CAGC	CCGC	TAGG
GA	CCCA	CTCG	GATC	GTTA	GGTC	GCAC	TGGC	AACT	TCTT	ACCA	GTTT	ACAA	GCGT	GATG	GGAA	GGCA
GG	ATAG	TTAC	TTAG	ACCT	TATC	GCTT	AGAC	GAGC	TAAT	ATCC	CCCG	AGTG	AAGT	GCTC	TCAC	GTAG

computational time. Its performance is a good response to use it in a live stream secure application like military field that requires high security such as unmanned Aerial vehicles.

VI. APPENDIX

A. THE PROPOSED S-BOX BASED ON DNA CODING

See Tables 25–32.

TABLE 31. Proposed S-box using DNA's Rule 7.

	TT	TC	TG	TA	CT	CC	CG	CA	GT	GC	GG	GA	AT	AC	AG	AA
TT	TGGA	CCCG	TTGG	CGAT	GGCA	AATT	TCGC	GGAG	TGCT	AGGT	CTGC	GGTT	ATAT	CAAG	TGCA	ACGC
TC	AATA	TATC	GCCC	AGAA	TATT	AAGT	TAGA	TCCT	AAGC	CTTT	GAAG	CTTG	TAGC	CTAC	AAGA	AAAC
TG	TCGT	GATA	ATGA	CGGT	TGGC	GGGG	CGTT	TGTC	CAGT	TTAA	TCCA	GAGG	ACAT	TTTT	ACTG	GAAT
TA	TACC	ATTC	AAAA	GAGA	CGCA	CGCG	TAAG	GGAA	TTCC	CAGG	TTTC	CCGG	GCCG	CTCA	CCTT	TAGG
CT	TGTT	CTAT	GTTT	TGAA	GATT	AGTT	ACCA	CAGC	TGAG	CAAA	CAAC	TTCG	CATA	ATTA	GCCA	CCAC
CC	TCTT	TACT	AGAG	ACGG	GTAT	TTGT	GATG	GCAT	ATGG	CCCC	AACA	GGTG	GACG	CATT	ATTG	TCAT
CG	GACT	TTGC	GAGC	GCAG	CGTG	GGGC	GCGG	GCAA	AGGG	GGGT	TAAC	TCGA	CATC	CTCT	ACCT	TTGA
CA	AGGC	ATTT	CTCG	ATCG	TTCT	CTGG	CGTC	CACC	AAAG	CTTC	CCTG	CGGG	CGGA	TCAG	CTAA	GGAT
GT	CGCC	TGGG	GATC	TCTC	GACC	TAGT	GGCT	GGTA	CTTA	TGGT	GCGC	GCTA	ATAG	CATG	ACAC	AAAT
GC	TAAT	ACGT	CACG	AGTC	TCCG	AGCG	TGTA	TCTG	CGAC	GTCC	GTAG	TGCG	CCCT	GAAA	TACG	AGAC
GG	GCTG	TCGG	AGTA	TTAC	GCGT	CCCA	TATG	GCCT	ACAA	ACTT	AGGA	AGTG	TGTG	GTGT	TAAA	GTCT
GA	CGTA	CAGA	TCAC	GTAC	GTCG	ACAG	TGAC	GGGA	ATCA	CTAG	GTTA	GCTC	AACC	CGAG	TTCA	TATA
AT	CACT	ACTA	CCAT	GTAA	ATAA	ACTC	AGCC	ATGC	TTAG	AATC	GCAC	TCAA	GTGA	TCCC	CCTA	CCAG
AC	CCTC	CCAA	GTCA	GAAC	CTGA	GGCG	AACG	CACA	GGCC	TACA	TGCC	CCGC	GTGC	TGAT	TTAT	CGAA
AG	TTTG	TCTA	AGCT	ACCG	AACT	ATGT	CAAT	GGTC	CTCC	GTTG	ACCC	GTGG	ATAC	AGCA	AAGG	AATG
AA	GCGA	CCGT	CCGA	GTTC	CGCT	ATCC	GAGT	AGAT	CGGC	GCTT	TTTA	GACA	GGAC	ATCT	CTGT	ACGA

TABLE 32. Proposed S-box using DNA's Rule 8.

	TT	TG	TC	TA	GT	GG	GC	GA	CT	CG	CC	CA	AT	AG	AC	AA
TT	TCCA	GGGC	TTCC	GCAT	CCGA	AATT	TGCG	CCAC	TCGT	ACCT	GTCG	CCTT	ATAT	GAAC	TCGA	AGCG
TG	AATA	TATG	CGGG	ACAA	TATT	AACT	TACA	TGGT	AACG	GTTT	CAAC	GTTC	TACG	GTAG	AACA	AAAG
TC	TGCT	CATA	ATCA	GCCT	TCCG	CCCC	GCTT	TCTG	GACT	TTAA	TGGA	CACC	AGAT	TTTT	AGTC	CAAT
TA	TAGG	ATTG	AAAA	CACA	GCGA	GCGC	TAAC	CCAA	TTGG	GACC	TTTG	GGCC	CGGC	GTGA	GGTT	TACC
GT	TCTT	GTAT	CTTT	TCAA	CATT	ACTT	AGGA	GACG	TCAC	GAAA	GAAG	TTGC	GATA	ATTA	CGGA	GGAG
GG	TGTT	TAGT	ACAC	AGCC	CTAT	TTCT	CATC	CGAT	ATCC	GGGG	AAGA	CCTC	CAGC	GATT	ATTC	TGAT
GC	CAGT	TTCG	CACG	CGAC	GCTC	CCCG	CGCC	CGAA	ACCC	CCCT	TAAG	TGCA	GATG	GTGT	AGGT	TTCA
GA	ACCG	ATTT	GTGC	ATGC	TTGT	GTCC	GCTG	GAGG	AAAC	GTTG	GGTC	GCCC	GCCA	TGAC	GTAA	CCAT
CT	GCGG	TCCC	CATG	TGTG	CAGG	TACT	CCGT	CCTA	GTTA	TCCT	CGCG	CGTA	ATAC	GATC	AGAG	AAAT
CG	TAAT	AGCT	GAGC	ACTG	TGGC	ACGC	TCTA	TGTC	GCAG	CTGG	CTAC	TCGC	GGGT	CAAA	TAGC	ACAG
CC	CGTC	TGCC	ACTA	TTAG	CGCT	GGGA	TATC	CGGT	AGAA	AGTT	ACCA	ACTC	TCTC	CTCT	TAAA	CTGT
CA	GCTA	GACA	TGAG	CTAG	CTGC	AGAC	TCAG	CCCA	ATGA	GTAC	CTTA	CGTG	AAGG	GCAC	TTGA	TATA
AT	GAGT	AGTA	GGAT	CTAA	ATAA	AGTG	ACGG	ATCG	TTAC	AATG	CGAG	TGAA	CTCA	TGGG	GGTA	GGAC
AG	GGTG	GGAA	CTGA	CAAG	GTCA	CCGC	AAGC	GAGA	CCGG	TAGA	TCGG	GGCG	CTCG	TCAT	TTAT	GCAA
AC	TTTC	TGTA	ACGT	AGGC	AAGT	ATCT	GAAT	CCTG	GTGG	CTTC	AGGG	CTCC	ATAG	ACGA	AACC	AATC
AA	CGCA	GGCT	GGCA	CTTG	GCGT	ATGG	CACT	ACAT	GCCG	CGTT	TTTA	CAGA	CCAG	ATGT	GTCT	AGCA

ACKNOWLEDGMENT

The authors would like to express their gratitude to Prof. Dr. Alaa Kadhim Farhan for his valuable comments that helped enhance the presentation of this work.

REFERENCES

[1] 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," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 2, pp. 523–542, 2020.

[2] A. Kumar and S. Tejani, "S-BOX architecture," in *Communications in Computer and Information Science*. Singapore: Springer, 2019, pp. 17–27.

[3] 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," *Int. J. Innov. Comput., Inf. Control*, vol. 16, no. 1, pp. 331–348, 2020.

[4] A. H. Zahid, M. J. Arshad, and M. Ahmed, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Inf. Theory, Probab. Statist.*, vol. 21, no. 3, p. 13, 2019.

[5] M. S. Mahmood Malik, M. A. Ali, M. A. Khan, M. Ehatisham-Ul-Haq, S. N. M. Shah, M. Rehman, and W. Ahmad, "Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices," *IEEE Access*, vol. 8, pp. 35682–35695, 2020.

[6] M. Mansour, W. Elsobky, A. Hasan, and W. Anis, "Appraisal of multiple AES modes behavior using traditional and enhanced substitution boxes," *Int. J. Recent Technol. Eng. (IJRTE)*, vol. 8, no. 5, pp. 530–539, Jan. 2020.

[7] J. M. Cheung, "The designa of S-boxes," Ph.D. dissertation, San Diego State Univ., San Diego, CA, USA, 2010.

[8] F. A. Kadhim, G. H. A. Majeed, and R. S. Ali, "Proposal new s-box depending on DNA computing and mathematical operations," in *Proc. Al-Sadeq Int. Conf. Multidisciplinary IT Commun. Sci. Appl. (AIC-MITCSA)*, May 2016, pp. 1–6.

[9] A. H. Al-Wattar, R. Mahmod, Z. A. Zukarnain, and N. I. Udzir, "A new DNA-based S-box," *Int. J. Eng. Technol.*, vol. 15, no. 4, pp. 1–9, 2015.

[10] A. Majumdar, A. Biswas, A. Majumder, S. K. Sood, and K. L. Baishnab, "A novel DNA-inspired encryption strategy for concealing cloud storage," *Frontiers Comput. Sci.*, vol. 15, no. 3, Jun. 2021, Art. no. 153807.

[11] L. Jinomeiq, W. Baoduui, and W. Xinmei, "One AES S-box to increase complexity and its cryptanalysis," *J. Syst. Eng. Electron.*, vol. 18, no. 2, pp. 427–433, Jun. 2007.

[12] A. A. Abdel-Hafez, R. Elbarkouky, and W. Hafez, "Comparative study of algebraic attacks," *Int. Adv. Res. J. Sci., Eng. Technol.*, vol. 3, no. 5, pp. 85–90, May 2016.

[13] K. Mohamed, M. N. Mohammed Pauzi, F. H. Hj Mohd Ali, S. Ariffin, and N. H. Nik Zulkipli, "Study of S-box properties in block cipher," in *Proc. Int. Conf. Comput., Commun., Control Technol. (I4CT)*, Sep. 2014, pp. 362–366.

[14] A. A. Abdel-Hafez, R. Elbarkouky, and W. Hafez, "Algebraic cryptanalysis of AES using Gröbner basis," *Int. Adv. Res. J. Sci., Eng. Technol.*, vol. 3, no. 12, pp. 183–189, 2016.

[15] W. Alsobky, H. Saeed, and A. N. Elwakeil, "Different types of attacks on block ciphers," *Int. J. Recent Technol. Eng. (IJRTE)*, vol. 9, no. 3, pp. 28–31, Sep. 2020.

[16] E. W. Afify, R. Abo Alez, A. T. Khalil, and W. I. Alsobky, "Performance analysis of advanced encryption standard (AES) S-boxes," *Int. J. Recent Technol. Eng.*, vol. 9, no. 1, pp. 2214–2218, 2020.

[17] J. H. Cheon and D. H. Lee, "Resistance of S-boxes against algebraic attacks," in *Proc. Int. Workshop Fast Software Encryption* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2004, pp. 83–93.

[18] J. Cui, L. Huang, H. Zhong, C. Chang, and W. Yang, "An improved AES S-box and its performance analysis," *Int. J. Innov. Comput., Inf. Control*, vol. 7, no. 5, pp. 2291–2302, 2011.

[19] E. W. Afify, R. Abo Alez, A. T. Khalil, and W. I. Alsobky, "Algebraic construction of powerful substitution box," *Int. J. Recent Technol. Eng. (IJRTE)*, vol. 8, no. 6, pp. 405–409, Mar. 2020.

[20] 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," *J. Commun.*, vol. 15, no. 12, pp. 905–912, 2020.

[21] M. Chakraborty, S. RoyChatterjee, and K. Sur, "Study on S-box properties of convolution coder," in *Proc. Int. Ethical Hacking Conf.*, vol. 1065. Singapore: Springer, 2019, pp. 119–128.

[22] N. A. Azam, U. Hayat, and M. Ayub, "A substitution box generator, its analysis, and applications in image encryption," *Signal Process.*, vol. 187, Oct. 2021, Art. no. 108144.

[23] 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 Comput. Appl.*, vol. 22, no. 6, pp. 1085–1093, 2013.

[24] F. Özkaynak and A. B. Özer, "A method for designing strong S-boxes based on chaotic Lorenz system," *Phys. Lett. A*, vol. 374, no. 36, pp. 3373–3738, 2010.
[25] R. Guesmi, M. A. Ben Farah, A. Kachouri, and M. Samet, "A novel design of chaos based S-boxes using genetic algorithm techniques," in *Proc. IEEE/ACS 11th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2014, pp. 678–684.
[26] G. Ivanov, N. Nikolov, and S. Nikova, "Cryptographically strong S-boxes generated by modified immune algorithm," in *Proc. Int. Conf. Cryptogr. Inf. Secur. Balkans*. Cham, Switzerland: Springer, 2016, pp. 31–42.
[27] 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.
[28] D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlinear Dyn.*, vol. 100, no. 1, pp. 699–711, 2020.
[29] F. Özkaynak, "On the effect of chaotic system in performance characteristics of chaos based s-box designs," *Phys. A, Stat. Mech. Appl.*, vol. 550, Jul. 2020, Art. no. 124072.
[30] 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.
[31] M. Rodinko, R. Oliynykov, and Y. Gorbenko, "Optimization of the high nonlinear S-boxes generation method," *Tatra Mountains Math. Publications*, vol. 70, no. 1, pp. 70–93, 2017.
[32] A. Razaq, H. Alolaiyan, M. Ahmad, M. A. Yousaf, U. Shuaib, W. Aslam, and M. Alawida, "A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups," *IEEE Access*, vol. 8, pp. 75473–75490, 2020.
[33] S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou, G. Muhammad, M. S. Hossain, and A. M. Abbas, "Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps," *IEEE Access*, vol. 8, pp. 160433–160449, 2020.
[34] A. A. Abd El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, pp. 92–102, Aug. 2019.
[35] 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.
[36] A. Zahid and M. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, Mar. 2019.
[37] A. Alhudhaif, M. Ahmad, A. Alkhayyat, N. Tsafack, A. K. Farhan, and R. Ahmed, "Block cipher nonlinear confusion components based on new 5-D hyperchaotic system," *IEEE Access*, vol. 9, pp. 87686–87696, 2021.
[38] A. H. Zahid, L. Tawalbeh, M. Ahmad, A. Alkhayyat, M. T. Hassan, A. Manzoor, and A. K. Farhan, "Efficient dynamic S-box generation using linear trigonometric transformation for security applications," *IEEE Access*, vol. 9, pp. 98460–98475, 2021.
[39] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput.*, vol. 37, pp. 24–39, Dec. 2015.
[40] M. Khan and H. M. Waseem, "A novel image encryption scheme based on quantum dynamical spinning and rotations," *PLoS ONE*, vol. 13, no. 11, Nov. 2018, Art. no. e0206460.
[41] 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 Dyn.*, vol. 81, no. 3, pp. 1151–1166, 2015.
[42] Y. Zhang, X. Li, and W. Hou, "A fast image encryption scheme based on AES," in *Proc. 2nd Int. Conf. Image, Vis. Comput. (ICIVC)*, Jun. 2017, pp. 624–628.
[43] 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, p. 1393, Aug. 2020.
[44] 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," *J. Real-Time Image Process.*, vol. 17, no. 6, pp. 2139–2151, Dec. 2020.
[45] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," *IEEE Access*, vol. 9, pp. 61334–61345, 2021.
[46] M. Ahmad, I. A. Khaja, A. Baz, H. Alhakami, and W. Alhakami, "Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications," *IEEE Access*, vol. 8, pp. 116132–116147, 2020.
[47] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "A color image encryption technique using block scrambling and chaos," *Multimedia Tools Appl.*, vol. 81, pp. 505–525, Sep. 2021.

HEND ALI MOHAMMED ALI BASHA was born in Egypt, in 1995. She received the B.Sc. degree in communication and computer engineering from the Benha Faculty of Engineering, Benha University, Egypt, in 2018.

She is currently a Demonstrator at the Benha Faculty of Engineering, Benha University.

ASHRAF SHAWKY SELIEM MOHRA was born in Egypt, in 1963. He received the B.Sc. degree in electronics and communications from the Shoubra Faculty of Engineering, in 1986, and the M.Sc. and Ph.D. degrees in electronics and communications from Ain Shams University, Cairo, Egypt, in 1994 and 2000, respectively. He is currently a Professor of electrical engineering at the Benha Faculty of Engineering, Benha University, Egypt. His current research interests include microstrip antennas, filters, couplers, hybrid junctions, computer-aided design of planar and uniplanar of MIC's and MMIC's, non-destructive techniques, metamaterials, and defected ground struct.

TAMER OMAR MOHAMED DIAB was born in Egypt, in 1971. He received the B.Sc. degree (Hons.) in communications and computer engineering from the Benha Higher Institute of Technology (BHIT), in 1994, the M.Sc. degree in computer engineering from Cairo University, Egypt, in 2000, and the Ph.D. degree in computer engineering from Vladimir State University, Russia, in 2005. He is currently a Lecturer of computer engineering at the Benha Faculty of Engineering, Benha University, Egypt. His current research interests include image processing, neural networks, and fuzzy logic.

WAGEDA IBRAHIM EL SOBKY was born in Egypt, in 1982. She received the B.Sc. degree in communications and computer engineering from the Benha Faculty of Engineering, Benha University, Cairo, Egypt, in 2003, the B.Sc. degree in science from the Benha Faculty of Science, Benha University, in 2008, the M.Sc. degree in applied mathematics from Benha University, in 2012, and the Ph.D. degree in cryptography from Ain Shams University, Cairo, in 2017. She is currently a Doctor in basic engineering sciences at the Benha Faculty of Engineering, Benha University, and the Higher Canadian Institute for Engineering, Egypt, in October. Her current research interests include data security and cryptography.