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

HEND ALI MOHAMMED ALI BASHA, ASHRAF SHAWKY SELIEM MOHRA, TAMER OMAR MOHAMED DIAB, AND WAGEDA IBRAHIM EL SOBKY

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 average, the results after the tests applied have been come with\( \text{SAC} = 0.50122, \text{NL} = 112, \text{BIC} = 103.40625, \) 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 statistical 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.

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 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.

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:

\[ Y = T \left( aX^2 + bX + C \right) \]
\[
S-box \begin{bmatrix}
a_4 & a_3 & a_2 & a_1 & a_0 & a_7 & a_6 & a_5 \\
a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & a_7 & a_6 \\
a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & a_7 \\
a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 \\
a_0 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 \\
a_1 & a_0 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 \\
a_2 & a_1 & a_0 & a_7 & a_6 & a_5 & a_4 & a_3 \\
a_3 & a_2 & a_1 & a_0 & a_7 & a_6 & a_5 & a_4 \\
\end{bmatrix}
\]

\[
X^2 = \begin{bmatrix}
X_7 & X_6 & X_5 & X_4 & X_3 & X_2 & X_1 & X_0 \\
Y & Y & Y & Y & Y & Y & Y & Y \\
Y & Y & Y & Y & Y & Y & Y & Y \\
Y & Y & Y & Y & Y & Y & Y & Y \\
Y & Y & Y & Y & Y & Y & Y & Y \\
Y & Y & Y & Y & Y & Y & Y & Y \\
Y & Y & Y & Y & Y & Y & Y & Y \\
Y & Y & Y & Y & Y & Y & Y & Y \\
\end{bmatrix}
\]

\[
= \begin{bmatrix}
y_7 & y_6 & y_5 & y_4 & y_3 & y_2 & y_1 & y_0 \\
C_7 & C_6 & C_5 & C_4 & C_3 & C_2 & C_1 & C_0 \\
\end{bmatrix}
\]

\[
a = 0 \times 76H, \quad b = 0 \times 6D, \quad C = 0XDA
\]  

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

\[
Y = Y^{-1} = \begin{cases} 
y^{254} & Y \neq 0 \\
0 & Y = 0 
\end{cases}
\]

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

\[
Y = T(aY^2 + bY + C)
\]

\[
= \begin{bmatrix}
a_4 & a_3 & a_2 & a_1 & a_0 & a_7 & a_6 & a_5 \\
a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & a_7 & a_6 \\
a_4 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & a_7 \\
a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & a_7 \\
a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 \\
a_0 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 \\
a_1 & a_0 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 \\
a_2 & a_1 & a_0 & a_7 & a_6 & a_5 & a_4 & a_3 \\
a_3 & a_2 & a_1 & a_0 & a_7 & a_6 & a_5 & a_4 \\
\end{bmatrix}
\]

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, 10 by C, and 11 by A.

6. 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.

In this step, the DNA addition operation is used based on the additional rules in Table 2. The addition...
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 Boolean 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 4.** The proposed S-box (HEX).

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

| SBox | f1  | f2  | f3  | f4  | f5  | f6  | f7  |
|------|-----|-----|-----|-----|-----|-----|-----|
| 1    | 128 | 136 | 132 | 128 | 128 | 128 | 128 |
| 2    | 128 | 120 | 128 | 140 | 128 | 136 | 136 |
| 3    | 128 | 136 | 132 | 136 | 132 | 120 | 116 |
| 4    | 132 | 128 | 136 | 132 | 136 | 132 | 120 |
| 5    | 120 | 124 | 128 | 132 | 128 | 112 | 116 |
| 6    | 124 | 124 | 124 | 128 | 132 | 112 | 116 |
| 7    | 124 | 132 | 136 | 128 | 132 | 132 | 140 |
| 8    | 136 | 116 | 132 | 120 | 136 | 132 | 128 |

TABLE 8. BIC of the proposed S-Box.

| BBox | β1 | β2 | β3 | β4 | β5 | β6 | β7 |
|------|----|----|----|----|----|----|----|
| 1    | -  | 128| 128| 128| 128| 128| 128|
| 2    | -  | 126| 136| 132| 142| 100| 136|
| 4    | 128| 128| -  | 124| 122| 126| 120|
| 8    | 118| 128| 126| -  | 132| 120| 116|
| 16   | 120| 140| 124| 122| -  | 118| 44 |
| 32   | 124| 128| 128| 104| 118| 72 | 64 |
| 64   | 124| 128| 130| 108| 134| 82 | -  |
| 128  | 134| 130| 132| 96 | 166| 88 | 80 |

TABLE 9. Non-linearity of boolean functions.

| $B_{f_i}$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ |
|-----------|-------|-------|-------|-------|-------|-------|-------|
| $\text{NL} (B_{f_i})$ | 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:

$$A_k(x) = \frac{(x-x_0) \cdots (x-x_{k-1}) (x-x_{k+1}) \cdots (x-x_n)}{(x_k-x_0) \cdots (x_k-x_{k-1}) (x_k-x_{k+1}) \cdots (x_k-x_n)},$$

$$k = 0, 1, \ldots, n-1 = 255$$

(4)

and substitute the middle-value is in the equation.

$$S_{x_i} = \sum_{j=0}^{m-1} y_k F_k(x_j) = y_i,$$

$$i = 0, 1, \ldots, n - 1 = 255$$

(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:

$$S_{x_i} = \sum_{x,y}^{15} E_{16x+y} x^{16x+y}$$

(6)

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 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 |
| 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 |
| 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.

\[ \Gamma = \left( k - l \right)^{\frac{\log_2 n}{m}} \]

(7)

Theorem 1 [15], [16]:
Given \( l \) equations of \( k \) terms in \( GF(2^8) \), the algebraic attacks resistance (AAR) is denoted by \( \Gamma \) and is defined as follows:

It was claimed in [17] that \( \Gamma \) 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 \( \Gamma = 2^{160} \) 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
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 $GF(2^8)$. 
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, the distance to SAC is denoted by $DSAC(F)$ and it is defined as follows:

$$DSAC(F) = \sum_{\sigma = \sum_{l=1}^{m} \sigma_l = 1}^{2^m} \left| w \left( f_i(x+\sigma) + f_i(x) - 2^{m-1} \right) \right|$$

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

---

**TABLE 11.** The Correlation coefficients of the Gray 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   |        |       |                    |          |           |              |         |
| Cipher         |        |       |                    |          |           |              |         |

|     | 0.857846 | 0.0078122 | 0.945715 | 0.001832 | 0.911060 | 0.058094 | 0.982511 | 0.056833 | 0.730244 | 0.006368 | 0.972062 | 0.010542 | 0.944093 | 0.008424 |
|     | 796      | 52     | 371       | 771      | 376       | 304      | 369       | 601      | 755      | 801      | 201      | 849      | 204      | 801      |

**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   |        |       |                    |          |           |              |         |
| Cipher         |        |       |                    |          |           |              |         |

|     | 0.91316 | 0.0466 | 0.951328 | 0.078877 | 0.743567 | 0.11251 | 0.987688 | 0.0680 | 0.74761 | 0.016527 | 0.97491 | -0.05733 | 0.942187 | 0.030879 |
|     | 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 |
|     | 0.9093 | 0.04131 | 0.909271 | 0.038807 | 0.922228 | -0.05708 | 0.930638 | -0.0605 | 0.672011 | 0.023548 | 0.98142 | -0.03308 | 0.915503 | 0.109496 |
|     | 0.88846 | 0.02528 | 0.971148 | -0.00738 | 0.748312 | -0.02269 | 0.988761 | 0.002468 | 0.82267 | 0.031384 | 0.963181 | 0.050081 | 0.94413 | 0.031071 |
|     | 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 | 0.01235 |
|     | 0.88138 | 0.00696 | 0.946 | -0.00329 | 0.920564 | -0.02841 | 0.941459 | 0.015062 | 0.768843 | 0.02336 | 0.972222 | 0.015992 | 0.925141 | 0.000289 |
|     | 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 |
|     | 0.8126 | 0.01812 | 0.914955 | 0.00239 | 0.838772 | 0.023939 | 0.95792 | 0.002466 | 0.562131 | 0.003172 | 0.945524 | 0.006551 | 0.939519 | 0.039319 |
|     | 0.83585 | 0.03672 | 0.876547 | -0.02433 | 0.873721 | 0.015262 | 0.863135 | -0.00486 | 0.561599 | 0.006702 | 0.959037 | 0.042122 | 0.846083 | 0.044014 |
FIGURE 5. The Correlation of the Gray plain-images and their corresponding enciphered ones.
| Image          | Size      | Image type      | Correlation                      |
|---------------|-----------|-----------------|----------------------------------|
| Baboon        | 256 x 256 | Plain-image     | ![Graphs](image1.png)            |
|               |           | Enciphered-image| ![Graphs](image2.png)            |
| Lenna         | 256 x 256 | Plain-image     | ![Graphs](image3.png)            |
|               |           | Enciphered-image| ![Graphs](image4.png)            |
| Digital        | 600 x 450 | Plain-image     | ![Graphs](image5.png)            |
| Electrons     |           | Enciphered-image| ![Graphs](image6.png)            |
| MonaLisa      | 960 x 1285| Plain-image     | ![Graphs](image7.png)            |
|               |           | Enciphered-image| ![Graphs](image8.png)            |
| Egyptian       | 259 x 194 | Plain-image     | ![Graphs](image9.png)            |
| Civilization  |           | Enciphered-image| ![Graphs](image10.png)           |
| Raccoon Face  | 1024 x 768| Plain-image     | ![Graphs](image11.png)           |
|               |           | Enciphered-image| ![Graphs](image12.png)           |
| Peppers       | 225 x 225 | Plain-image     | ![Graphs](image13.png)           |
|               |           | Enciphered-image| ![Graphs](image14.png)           |

**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 x 256 | 7.237393      | 7.997023         |
| Lenna        | 256 x 256 | 7.452783      | 7.997807         |
| Digital      | 600 x 450 | 6.634116      | 7.999379         |
| Electronics  |          |               |                  |
| MonaLiza     | 900 x 1285| 7.264233      | 7.999845         |
| Egyptian     | 259 x 194 | 6.634116      | 7.999379         |
| civilization |          |               |                  |
| Raccoon      | 1024 x 768| 7.731369      | 7.999778         |
| Face         |          |               |                  |
| Peppers      | 225 x 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 $m \times m$ - dimensional matrix $BIC(F) = b_{lk}$ such that $l, k$, then $b_{lk}$ is defined to be:

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

(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 $NL(f_l)$ is expressed as follow:

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

(10)

where $u \in f_2^m$.

$$W_{f_l}(u) = \sum_{t \in \{0,1\}^m} \left( -1 \right)^{t \cdot u}$$

(11)

$$NL(f) = \min_{0 \neq v \in GF(2)^m} d(v, F(x), l(x))$$

(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 $NL(f) = 2^m - 2^{\frac{m}{2}} - 1 = 120$. 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 x 256  | 7.6637 | 7.36  | 7.6921 | 7.6904 | 7.99751 | 7.99759 | 7.99735 | 7.99927 |
| Lenna       | 256 x 256  | 7.26883 | 7.59763 | 6.9716 | 7.75077 | 7.997345 | 7.997697 | 7.997328 | 7.999184 |
| Digital      | 600 x 450  | 7.75635 | 7.81551 | 7.61261 | 7.94258 | 7.996204 | 7.996102 | 7.996611 | 7.998784 |
| Electronics  |            |      |       |       |       |      |       |       |       |
| MonaLiza     | 900 x 1285 | 7.5572 | 7.24613 | 6.38616 | 7.25257 | 7.999844 | 7.999845 | 7.999827 | 7.999946 |
| Egyptian     | 259 x 194  | 7.75635 | 7.81551 | 7.61261 | 7.94258 | 7.996204 | 7.996102 | 7.996611 | 7.998784 |
| civilization |            |      |       |       |       |      |       |       |       |
| Raccoon      | 1024 x 768 | 7.73397 | 7.76838 | 7.80269 | 7.79204 | 7.999763 | 7.999776 | 7.999796 | 7.999934 |
| Face         |            |      |       |       |       |      |       |       |       |
| Peppers      | 225 x 225  | 7.4462 | 7.70062 | 7.2262 | 7.79589 | 7.995604 | 7.995446 | 7.996344 | 7.99888 |
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.

\[
Co = \frac{\sum_{i=1}^{\alpha} \sum_{j=1}^{\beta} (P_{ij} - \bar{P}) (C_{ij} - \bar{C})}{\sqrt{\left(\sum_{i=1}^{\alpha} \sum_{j=1}^{\beta} (P_{ij} - \bar{P})^2\right) \left(\sum_{i=1}^{\alpha} \sum_{j=1}^{\beta} (C_{ij} - \bar{C})^2\right)}}
\]

(13)

where $\alpha$ and $\beta$ 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. $\bar{P}$ and $\bar{C}$ 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:

\[
H(m) = \sum_{j=0}^{L} P(x_j) \cdot \log_2 (P(x_j))
\]

(14)

\[
L = 2^m - 1
\]

(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 shown 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.

| Image      | Size   | UACI (%) | NPCR (%) |
|------------|--------|----------|----------|
| Baboon     | 256 x 256 | 33.5923438 | 100      |
| Lenna      | 256 x 256 | 33.6641857670802 | 100      |
| Digital Electronics | 600 x 450 | 33.6585693536673 | 100      |
| MonaLiza   | 900 x 1285 | 33.5772084467163 | 100      |
| Egyptian civilization | 259 x 194 | 33.6880118444703 | 100      |
| Raccoon Face | 1024 x 768 | 33.5990491879531 | 100      |
| Peppers    | 225 x 225 | 33.449079271362 | 100      |

Table 15. UACI and NPCR of the enciphered Gray images.
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...
| Baboon | Lenna | Digital Electronics | MonaLiza | Egyptian civilization | Raccoon Face | Peppers |
|--------|-------|---------------------|---------|-----------------------|-------------|---------|
| ![Plain-images](image1.jpg) | ![Plain-images](image2.jpg) | ![Plain-images](image3.jpg) | ![Plain-images](image4.jpg) | ![Plain-images](image5.jpg) | ![Plain-images](image6.jpg) | ![Plain-images](image7.jpg) |
| ![Red-component Histogram](image8.jpg) | ![Red-component Histogram](image9.jpg) | ![Red-component Histogram](image10.jpg) | ![Red-component Histogram](image11.jpg) | ![Red-component Histogram](image12.jpg) | ![Red-component Histogram](image13.jpg) | ![Red-component Histogram](image14.jpg) |
| ![Green-component Histogram](image15.jpg) | ![Green-component Histogram](image16.jpg) | ![Green-component Histogram](image17.jpg) | ![Green-component Histogram](image18.jpg) | ![Green-component Histogram](image19.jpg) | ![Green-component Histogram](image20.jpg) | ![Green-component Histogram](image21.jpg) |
| ![Blue-component Histogram](image22.jpg) | ![Blue-component Histogram](image23.jpg) | ![Blue-component Histogram](image24.jpg) | ![Blue-component Histogram](image25.jpg) | ![Blue-component Histogram](image26.jpg) | ![Blue-component Histogram](image27.jpg) | ![Blue-component Histogram](image28.jpg) |
| ![Enciphered-images](image29.jpg) | ![Enciphered-images](image30.jpg) | ![Enciphered-images](image31.jpg) | ![Enciphered-images](image32.jpg) | ![Enciphered-images](image33.jpg) | ![Enciphered-images](image34.jpg) | ![Enciphered-images](image35.jpg) |
| ![Red-component Histogram](image36.jpg) | ![Red-component Histogram](image37.jpg) | ![Red-component Histogram](image38.jpg) | ![Red-component Histogram](image39.jpg) | ![Red-component Histogram](image40.jpg) | ![Red-component Histogram](image41.jpg) | ![Red-component Histogram](image42.jpg) |
| ![Green-component Histogram](image43.jpg) | ![Green-component Histogram](image44.jpg) | ![Green-component Histogram](image45.jpg) | ![Green-component Histogram](image46.jpg) | ![Green-component Histogram](image47.jpg) | ![Green-component Histogram](image48.jpg) | ![Green-component Histogram](image49.jpg) |
| ![Blue-component Histogram](image50.jpg) | ![Blue-component Histogram](image51.jpg) | ![Blue-component Histogram](image52.jpg) | ![Blue-component Histogram](image53.jpg) | ![Blue-component Histogram](image54.jpg) | ![Blue-component Histogram](image55.jpg) | ![Blue-component Histogram](image56.jpg) |

**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 | 6.189443843 |
| 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:

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

(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:

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

(17)

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

(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:

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

(19)

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

\[
PSNR = 20 \log \left( \frac{P_{\text{MAX}}}{\sqrt{MSE}} \right)
\]  

(20)

where \( P_{\text{MAX}} \) 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    | Red    | Green   | Blue    | Image    | PSNR (DB) |
|---------------|---------|--------|---------|---------|----------|-----------|
| Baboon        | 256 × 256 | 8350.8315 | 7256.772 | 9026.853 | 8211.4845 | 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 | 6.890137 |
| 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:

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

(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.

### TABLE 20. MAE of the enciphered RGB image.

| Image              | Size   | Red | Green | Blue | Image         |
|--------------------|--------|-----|-------|------|---------------|
| Baboon             | 256 × 256 | 75.20597839 | 71.07707214 | 77.90866089 | 74.73057048 |
| Lenna              | 256 × 256 | 83.98904177 | 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 | 78.07797775 |
| Peppers            | 225 × 225 | 73.87369877 | 85.30968889 | 85.18577778 | 81.45638848 |

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 @

![Figure 9. Experimental results of occlusion attacks.](image-url)
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            | 2.09976013        | 762.747368      |
| Lena     | 256 × 256 | 196608     | 0.03114724            | 2.10407075        | 760.430703      |
| Digital  | 600 × 450 | 810000     | 0.1249519             | 2.16060167        | 740.534465      |
| Electri- | 900 × 1285 | 3469500   | 0.51550484            | 2.24334319        | 713.19303       |
| cs       | Egyptian | 259 × 194  | 150738                | 0.01562119        | 3.21652929      |
| civiliza- | MonaLiz- | 1024 × 768 | 2359296              | 0.34366989        | 699.198104      |
| tion     | a        | Peppers    | 225 × 225             | 151875            | 0.01506203      |

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

Cycles per byte = \( \frac{\text{processor speed \ [in Hertz]}}{\text{throughput rate}} \) (Cycle/Byte) \quad (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 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       | 985.3761485     |
| Lena     | 256 × 256 | 196608     | 0.124969482           | 1.573248904       | 1017.004251     |
| Digital  | 600 × 450 | 810000     | 0.515621185           | 1.570920713       | 1018.510983     |
| Electro- | 900 × 1285 | 3469500   | 2.405650616           | 1.44229382       | 1109.393568     |
| cs       | Egyptian | 259 × 194  | 150738                | 0.094664574       | 1.592338022     |
| civiliza- | MonaLiz- | 1024 × 768 | 2359296              | 1.499654055       | 1.573226834     |
| tion     | a        | Peppers    | 225 × 225             | 151875            | 0.097073551     |

VOLUME 10, 2022

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

| Image    | Proposed scheme | Ref. [38] | Ref. [46] | Ref. [38] |
|----------|-----------------|-----------|-----------|-----------|
| Information entropy | 7.997023 | 7.9964 | 7.9969 | 7.9969 | 7.997807 | 7.9968 |
| Correlation | Hor. = 0.007812 | 0.00568 | -0.00098 | -0.00284 | Hor. = 0.00183277 | 0.01014 |
| Ver. = 0.003548 | 0.000278 | 0.00568 | -0.00098 | -0.00284 | Ver. = 0.0023002 | 0.001185 |
| Dig. = 0.002078 | 0.00568 | 0.000278 | 0.00568 | -0.00098 | Dig. = 0.000278 | 0.001185 |
| UACI | 33.59234353 | 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 | Windows 8 OS | Windows 8 OS | Windows 10 OS |
| & Intel(R) Core(TM) i5-CPU @ 1.6GHz speed & CPU @ 2.2GHz speed & 6GB RAM & 6GB RAM | 6GB RAM & 6GB RAM & 6GB RAM | 6GB RAM & 6GB RAM & 6GB RAM | 6GB RAM & 6GB RAM & 6GB RAM |
| Enc Time | 0.03124213 | 0.08632 | 0.2634 | 0.03124724 | 0.08632 |
| Throughput (Mbps) | 16.78144106 | 5.9313 | 1.99 | 16.83256601 | 5.9313 |
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

| Image 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 | - | 0.0664 |
| | H GREEN 0.023948 | - | 0.0099 |
| | 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 33.7747682 | 33.5042 | 33.4241 |
| | BLUE 33.65520267 | 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) i5-10600 @ 3.10 GHz speed * 8 GB RAM |
| Throughput (Mbps) | 0.124964982 | - | - |

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

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

| TABLE 26. Proposed S-box using DNA’s Rule 2. |
TABLE 27. Proposed S-box using DNA's Rule 3.

| GG | GA | TT | GC | AG | AA | AT | AC | TG | TA | TT | TC | CG | CA | CC |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| GCTT | AACG | GGTT | TTCG | GTAC | GGGG | CATG | AGTA | TTCT | CTAT | GGAT | TAGG | CGCC | GACT | ATCG |

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

| CC | CA | AT | GC | AC | AA | AT | AG | TC | TA | AA | TG | GC | GA | CT |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| CTTG | AATG | CCGT | TTAG | GGGG | CAGG | CATA | TGCT | CAGT | CAGT | AGGT | ATCG | CAGG | CAGG | CTGG |

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

| CC | CA | AT | GC | AC | AA | AT | AG | TC | TA | AA | TG | GC | GA | CT |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| CTTT | AATG | CCGT | TTAG | GGGG | CAGG | CATA | TGCT | CAGT | CAGT | AGGT | ATCG | CAGG | CAGG | CTGG |

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

| CC | CA | AT | GC | AC | AA | AT | AG | TC | TA | AA | TG | GC | GA | CT |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| CTTG | AATG | CCGT | TTAG | GGGG | CAGG | CATA | TGCT | CAGT | CAGT | AGGT | ATCG | CAGG | CAGG | CTGG |

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.
ACKNOWLEDGMENT

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

REFERENCES

[1] R. Y. Sasse, N. M. G. Al-Saidi, and A. K. Farhan, “A new NTRU cryptosystem performance through highly secured NTRU-analog systems through an innovative 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,” in Proc. Int. Workshop Fast Software Encryption (FSE). Berlin, Germany: Springer, 2004, pp. 83–93.

[4] A. A. Abdel-Hafez, R. Elbarkouky, and W. Hafez, “Algebraic cryptanalysis of AES using Gröbner basis,” Int. J. Innov. Comput., Inf. Control, vol. 9, no. 1, pp. 2214–2218, 2020.

[5] E. W. Afify, R. Abo Alez, and A. N. Elwakeil, “Different types of attacks on block ciphers,” in Int. J. Recent Technol. Eng. (IJRTE), vol. 8, no. 5, pp. 530–539, Jan. 2020.

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

[7] J. H. Cheon and D. H. Lee, “Resistance of S-boxes against algebraic attacks,” in Proc. Int. Workshop Fast Software Encryption (FSE). Berlin, Germany: Springer, 2004, pp. 83–93.

[8] J. Cui, L. Huang, H. Zhong, 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. 328–331.

[9] 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.

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

[11] L. Jinomeiq, W. Baoduui, and W. Xinmei, “One AES S-box to increase its efficiency and its cryptanalysis,” J. Syst. Eng. Electron., vol. 18, no. 2, pp. 277–283, 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. Mohammad 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, “Algebraic cryptanalysis of AES using Gröbner basis,” Int. J. Innov. Comput., Inf. Control, 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] M. S. Mahmood Malik, M. A. Ali, M. A. Khan, M. Ehatisham-Ul-Haq, S. M. Shah, M. Rehman, and W. Ahmad, “Generation of highly non-linear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices,” IEEE Access, vol. 8, pp. 35682–35695, 2020.

[18] M. Mansour, W. Elsobky, and A. Anis, “Appraisal of multiple linear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices,” Int. J. Recent Technol. Eng. (IJRTE), vol. 8, no. 5, pp. 530–539, Jun. 2020.

[19] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, “A projective general complex coding for concealing cloud storage,” Frontiers Comput. Sci., vol. 15, no. 3, Jun. 2021, Art. no. 153807.

[20] J. Cui, L. Huang, and H. Zhong, “Algebraic cryptanalysis of AES using Gröbner basis,” Int. J. Innov. Comput., Inf. Control, vol. 7, no. 12, pp. 183–189, 2011.

[21] J. Cui, L. Huang, and H. Zhong, “Algebraic cryptanalysis of AES using Gröbner basis,” Int. J. Recent Technol. Eng. (IJRTE), vol. 8, no. 6, pp. 405–409, Mar. 2020.

[22] W. I. E. Sobky, A. R. Mahmoud, and A. S. Mohra, “Enhancing Hierocrypt-3 performance by modifying its S-box and modes of operations,” J. Commun., vol. 15, no. 12, pp. 905–912, 2020.

[23] M. Chakraborty, S. RoyChatterjee, and K. Sur, “Study on S-box properties in block cipher,” in Proc. Int. Workshop Fast Software Encryption (FSE). Berlin, Germany: Springer, 2004, pp. 83–93.
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 unipolar of MIC’s and MMIC’s, non-destructive techniques, metamaterials, and defeated 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.

HEND ALI MOHAMMED ALI BASHA was born in Egypt, in 1995. He 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.