Electronic Research Archive

ERA, 31(5): 2708–2732.
DOI: 10.3934/era.2023137
Received: 07 January 2023
Revised: 23 February 2023
Accepted: 01 March 2023
Published: 10 March 2023

http://www.aimspress.com/journal/ERA

Research article

An efficient S-box design scheme for image encryption based on the combination of a coset graph and a matrix transformer

Asima Razzaque[1,*], Abdul Razaq[2,*], Sheikh Muhammad Farooq[2], Ibtisam Masmali[3] and Muhammad Iftikhar Faraz[4]

[1] Department of Basic Sciences, Deanship of Preparatory Year, King Faisal University Al Ahsa, Hofuf, Saudi Arabia
[2] Department of Mathematics, Division of Science and Technology, University of Education, Lahore 54770, Pakistan
[3] Department of Mathematics, College of Science, Jazan University, Jazan 45142, Saudi Arabia
[4] College of Mechanical Engineering, King Faisal University Al-Ahsa Hofuf, Saudi Arabia

* **Correspondence:** Email: arazzaque@kfu.edu.sa, abdul.razaq@ue.edu.pk; Tel: +923175880494.

Abstract: Modern block ciphers deal with the development of security mechanisms to meet the security needs in several fields of application. The substitution box, which is an important constituent in block ciphers, necessarily has sufficient cryptographic robustness to counter different attacks. The basic problem with S-box design is that there is no evident pattern in its cryptographic properties. This study introduces a new mathematical algorithm for developing S-box based on the modular group coset graphs and a newly invented mathematical notion "matrix transformer". The proficiency of the proposed S-box is assessed through modern performance evaluation tools, and it has been observed that the constructed S-box has almost optimal features, indicating the effectiveness of the invented technique.

Keywords: coset graphs for the modular group; cryptography, block cipher; S-box; matrix transformer; security of the cryptosystem; image encryption

1. Introduction

Over the last few decades, the number of organizations and individuals working on the web has

increased remarkably. Because of the widespread availability of data and information in every field, which is accessible to everyone, serious issues such as unauthorized access to confidential information have cropped up. As a result of this massive quantity of work and traffic, the risks of valuable data theft have significantly increased, and preventing these situations is a challenging task. Various researchers in their respective fields have worked to secure data by employing various cryptographic, watermarking, and stenographic schemes. Cryptography is a technique that restricts access to original information to the sender and recipient only [1]. It contains algorithms to block potential unauthorized access. Cryptographic algorithms are mathematical tools that helps in protection of data. The cryptography has two main types, symmetric and asymmetric cryptography. A symmetric cryptography [2] involves the procedures requires sole key to encrypt and decrypt the related content, while the algorithm in asymmetric cryptography contains two different keys for the process of encryption and decryption [3]. The symmetric cipher is further classified into two types: stream cipher and block cipher. The stream cipher modifies the original information bit-by-bit or byte-by-byte while the block cipher does so in blocks involving several bits or bytes simultaneously [4]. Data Encryption Standard (DES), GOST, Advanced Encryption Standard (AES), BLOWFISH, etc., are the well-known block ciphers. The substitution box (S-box) is a pertinent non-linear ingredient in block cipher that plays a very decisive role in encrypting the plaintext [5]. An $n \times n$ S-box is a Boolean function $f: \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2^n$ which maps an input of n bits to an n bits output. It generates perplexity and responsible for the complex relationship between actual and encrypted contents [6]. Therefore, it is not an overstatement to state that the security level of a block cipher can be determined by analyzing the performance of S-box.

Considering the importance of the S-box in the security of cryptosystems, designing complex mathematical techniques to construct robust S-boxes has become a goal of cryptographers. The scientists working in this field are primarily interested in improving the performance of block ciphers. For this purpose, thousands of studies have been conducted and published in leading journals in recent years. A novel approach of S-box creation is introduced in [7]. The authors developed their proposed S-box using a chaotic system and fitness function. Javeed et al. [8] developed an effective framework for generating strong S-boxes relying on chaotic maps and symmetric groups. The authors designed an initial S-box with the help of chaotic dynamical system. Then the final proposed S-box is obtained by applying a permutation of S_{256}. In [9] a specific type of graphs based the concepts of group theory were employed to develop a new S-box. Multiple performance evaluation metrics validate the resilience of the suggested S-box.

In [10] Si et al. proposes a method to create a secure S-Box for symmetric cryptography using a 2D enhanced quadratic map, and an algorithm is designed to eliminate vulnerabilities. Experimental results confirm the method's effectiveness. Lambic [11] used usual multiplication and circular shift to generate an innovative discrete-space chaotic map which further employed in the construction of S-box having good security properties. Anees and Ahmed [12] designed a potent S-box by investigating the behavior of van der pol oscillator. Firstly, the author used a numerical technique to obtain the iterative solution of chaotic map. Then the ceiling function is employed to those solution to achieve the task. Liu et al. [13] proposes a strong S-Box construction method using a non-degenerate 3D improved quadratic map. The proposed algorithm satisfies six criteria and eliminates fixed points, reverse fixed points, and short cycles. Results show effectiveness in encrypting color images and verified security. A systematic scheme to evolve a S-box with high non-linearity value is given in [14]. The chaotic map iteration yields a 16×16 matrix on which the genetic technique is applied to obtain

the suggested S-box. We recommend to read [15–20] for further information on S-box generation methodologies. In [21], a secure image encryption method was introduced. It used a new framework to create chaotic signals with finite computer precision, and includes circular diffusion and local/global scrambling. In [22] the authors introduced a new encryption algorithm for color images using DNA dynamic encoding, self-adapting permutation, and a new 4D hyperchaotic system. Zhou et al. [23] proposes a secure color image cryptosystem using deep learning to train hyper-chaotic signals, which are then applied to increase the system's security. Liu et al. [24] developed a secure color image encryption algorithm using a conservative chaotic system without attractors. They employed techniques such as plane element rearrangement, dynamic selection row-column cross scrambling, and cross-plane diffusion to enhance the encryption's security and mixing. The study [25] proposed a 2D hyperchaotic map to generate S-boxes and combine them to create a secure image encryption algorithm that passed NIST and TestU01 tests and resists common attacks. In [26], a new n-dimensional conservative chaos was designed to address security issues with encryption algorithms based on dissipative chaos. A new image encryption system using true random numbers and chaotic systems has been proposed in [27]. The method is found to be more secure and resistant to classical attacks compared to existing models.

The study presents a novel method for constructing robust S-boxes for use in block ciphers. The following factors were considered during the creation of the S-box:

i. The generated S-box must be cryptographically robust and comply with the mandatory information security standards.
ii. The S-box must exhibit a sufficient level of confusion and complexity, while the method used to construct it remains simple and computationally efficient.
iii. The S-box should demonstrate good performance when evaluated using modern cryptographic performance assessment parameters.
iv. The S-box must meet the requirements for suitability in multimedia image encryption, as determined through a thorough evaluation of its cryptographic properties and performance under relevant metrics.

The following paragraph summarizes the main contributions and proposed scheme of this article.

By utilizing the action of the modular group on a Galois field of order 1024, $GF(2^{10}) = \{0, \kappa^1, \kappa^2, \kappa^4, \ldots, \kappa^{1023}\}$ a coset graph is constructed. The vertices of the coset graph are utilized in a specific manner to generate a random sequence of the elements in $GF(2^{10})^* = \{\kappa^1, \kappa^5, \kappa^9, \ldots, \kappa^{1021}\}$, which is presented in a 16×16 matrix. Then, a bijective mapping from the group $GF(2^{10})^*$ to $GF(2^8)$ yields an initial S-box that exhibits reasonable security. A new notion named "matrix transformer" which transforms a matrix into another matrix has been introduced. By applying a specific matrix transformer to the initial S-box, we obtain a proposed S-box with almost optimal features. Furthermore, a series of well-established analyses are carried out to establish the potential effectiveness of the proposed S-boxes for image encryption in the context of multimedia encryption.

The arrangement of the remaining content of this paper is as follows: The purpose of Section 2 is to discuss the newly developed matrix transformer and modular group-based coset graphs over finite fields. Using the concepts described in Section 2 as a foundation, we propose our S-box design scheme in Section 3. Assessing the algebraic robustness of the constructed S-box is the focus of Section 4. This section also includes a comparison with some recently developed S-boxes. Sections 5–7 are devoted to examining the suitability of constructed S-box for image protection. We reveal the concluding remark in Section 8.

2. Preliminaries

In this section, we will discuss some fundamental concepts that are required to comprehend the proposed S-box construction scheme.

2.1. Coset diagrams for modular group

The modular group $\mathcal{M}$ is an infinite non-cyclic group of linear transformations. It is generated by x and y such that $(s)x = \frac{-1}{s}$ and $(s)y = \frac{s-1}{s}$. The finite presentation of $\mathcal{M}$ is $\langle x, y : x^2 = y^3 = 1\rangle$. Let p be a prime number and $n \in \mathbb{N}$. Then $GF(p^n)$ denote a Galois field of order p^n, it is well known that $\mathcal{M}$ cannot act directly on $GF(p^n)$ as $(0)x = \frac{-1}{0} \notin GF(p^n)$, so the action of $\mathcal{M}$ is possible if ∞ is adjoined with $GF(p^n)$, that is $\mathcal{M}$ acts on $GF(p^n) \cup \{\infty\}$. The graphical interpretation of the action of $\mathcal{M}$ is described with the help of coset graphs [28–31]. As $(s)y^3 = s$, so y has cycles of length three which are represented by triangles whose vertices are elements of $GF(p^n) \cup \{\infty\}$ are permuted counter-clockwise by y. Moreover, since $(s)x^2 = s$, therefore an undirected line connecting a pair of vertices of the triangles is drawn to represent x. The heavy dots are used to denote fixed points of x and y, if they exist. For the better understanding of readers, here we describe the action of $\mathcal{M}$ on $GF(23) \cup \{\infty\}$ and draw the corresponding coset graph. We apply $(s)x = \frac{-1}{s}$ and $(s)y = \frac{s-1}{s}$ on each element of $GF(23) \cup \{\infty\}$ and obtain permutation representations of x and y. For example, $(1)x = \frac{-1}{1} \equiv 22$ and $(22)x = \frac{-1}{22} \equiv 1$ mean a cycle $(1,22)$ of x. Moreover, $(2)y = \frac{1}{2} \equiv 12$, $(12)y = \frac{11}{12} \equiv 22$ and $(22)y = \frac{21}{22} \equiv 2$ give rise to a cycle $(2,12,22)$ of y. In a similar way, all other cycles of x and y can be computed and we have the following permutation representations of x and y.

$$x: (0,\infty)(22,1)(11,2)(15,3)(17,4)(9,5)(19,6)(13,7)(20,8)(16,10)(21,12)(18,14);$$
$$y: (1,0,\infty)(2,12,22)(11,3,16)(15,4,18)(17,5,10)(9,6,20)(19,7,14)(13,8,21).$$

The permutation representation of y consists of 8 cycles. Consequently, the resulting coset graph has eight triangles. The graphical version of the cycle $(1,0,\infty)$ in y is a triangle with the vertices $1,0$ and ∞ permuted counter-clockwise by y. In a similar way, we can draw and label all triangles. The permutation representation of x contains 12 transpositions which correspond to12 undirected lines joining all 24 vertices of 8 triangles. For instance, $(1, 22)$ means the vertices 1 and 22 are connected through an undirected line. Similarly, the remaining vertices can be joined with each other through x and the following coset graph is emerged (See Figure 1).

In the next subsection, we have introduced a new notion namely matrix transformer to generate a strong S-box from an initial S-box.

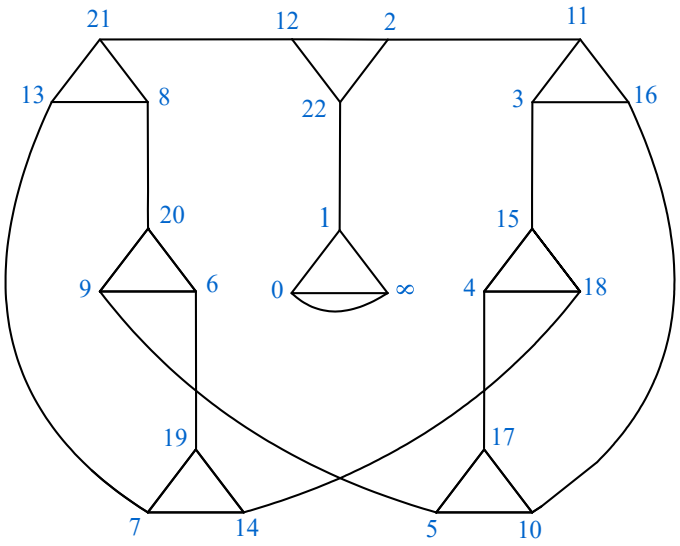

Figure 1. Coset graph of $\mathcal{M}$ on $F_{23} \cup \{\infty\}$.

2.2. Matrix transformer

Suppose M is a square matrix of order n. Let us define the position of the elements of M as follows;

$$k^{\text{th}} \text{ element} = m^{th} \text{ element of } \left\lceil \frac{k}{n} \right\rceil^{th} \text{ row}$$

where $m = \begin{cases} n & if\ n\ divides\ m \\ k\ mod(n) & otherwise \end{cases}$, and $\left\lceil \frac{k}{n} \right\rceil$ means ceiling of $\left\lceil \frac{k}{n} \right\rceil$.

For example, in a 3×3 matrix, we have 1st element means 1st element of 1st row, 2nd element means 2nd element of 1st row, 3rd element means 3rd element of 1st row, 4th element means 1st element of 2nd row and so on.

Definition 2.1. A square matrix A of order n with entries from $\{1,2,3,\ldots,n^2\}$ is called matrix transformer of square matrix M of order n if the action of A on M evolves a new matrix M' of order n in the following way; $t \in \{1,2,3,\ldots,n^2\}$ is the i^{th} element of the matrix transformer $A \Leftrightarrow t^{\text{th}}$ element of M' is equal to i^{th} element of M.

Example 2.1. Consider $M = \begin{pmatrix} f & d & g \\ c & a & i \\ e & h & b \end{pmatrix}$ and $A = \begin{pmatrix} 3 & 9 & 7 \\ 8 & 6 & 2 \\ 4 & 1 & 5 \end{pmatrix}$. Then the action of of A on M generates $M' = \begin{pmatrix} h & i & f \\ e & b & a \\ g & c & d \end{pmatrix}$.

3. S-box generation

In this section, we propose our S-box construction method based on the concepts describe in the previous section.

3.1. Coset graphs used in the proposed scheme

The proposed S-box generation scheme involves coset graph of the modular group $\mathcal{M}$ on $GF(2^{10}) \cup \{\infty\}$. So, in the 1st phase, we have to construct the Galois field $GF(2^{10})$. It is well-known that a primitive irreducible polynomial of degree 10 over $\mathbb{Z}_2$ is required to compute all the elements of $GF(2^{10})$ [32]. For that purpose, we choose $p(\kappa) = \kappa^{10} + \kappa^7 + 1$ and obtain $GF(2^{10}) = \{0, \kappa^1, \kappa^2, \kappa^3, \dots, \kappa^{1023} = 1\}$. In Table 1, we present some of the elements of $GF(2^{10})$ along with their binary and decimal form.

To draw the coset graph of $\mathcal{M}$ on $GF(2^{10}) \cup \infty$, we firstly apply the generators $(s)x = \frac{-1}{s}$ and $(s)y = \frac{s-1}{s}$ of $\mathcal{M}$ on all elements of $GF(2^{10}) \cup \infty$ to get permutation representations of x and y. For instance, $(\kappa^1)x = \frac{-1}{\kappa^1} = \frac{1}{\kappa^1} = \frac{\kappa^{1023}}{\kappa^1} = \kappa^{1022}$ and $(\kappa^{1022})x = \frac{-1}{\kappa^{1022}} = \frac{1}{\kappa^{1022}} = \frac{\kappa^{1023}}{\kappa^{1022}} = \kappa^1$ yield a cycle (κ^1, κ^{126}) of x. Moreover, $(\kappa^1)y = \frac{\kappa^1 - 1}{\kappa^1} = \frac{\kappa^{947}}{\kappa^1} = \kappa^{946}$, $(\kappa^{946})y = \frac{\kappa^{946}-1}{\kappa^{946}} = \frac{\kappa^{1022}}{\kappa^{946}} = \kappa^{76}$ and $(\kappa^{76})y = \frac{\kappa^{76}-1}{\kappa^{76}} = \frac{\kappa^{77}}{\kappa^{76}} = \kappa^1$, generate a $(\kappa^1, \kappa^{946}, \kappa^{76})$ of y.

Similarly, the remaining cycles of x and y can be found and some of them are presented below;

x: $(0, \infty)(1)(\kappa^1, \kappa^{1022})(\kappa^2, \kappa^{1021})(\kappa^3, \kappa^{1020})(\kappa^4, \kappa^{1019})(\kappa^5, \kappa^{1018})(\kappa^6, \kappa^{1017})(\kappa^7, \kappa^{1016})(\kappa^8, \kappa^{1015})$
$(\kappa^9, \kappa^{1014}) \dots (\kappa^{507}, \kappa^{516})(\kappa^{508}, \kappa^{515})(\kappa^{509}, \kappa^{514})(\kappa^{510}, \kappa^{513})(\kappa^{511}, \kappa^{512})$;

y: $(\kappa^1, \kappa^{946}, \kappa^{76})(\kappa^2, \kappa^{869}, \kappa^{152})(\kappa^3, \kappa^{1013}, \kappa^7)(\kappa^4, \kappa^{715}, \kappa^{304})(\kappa^5, \kappa^{510}, \kappa^{508})(\kappa^6, \kappa^{1003}, \kappa^{14})$
$(\kappa^8, \kappa^{407}, \kappa^{608}) \dots (\kappa^{650}, \kappa^{713}, \kappa^{683})(\kappa^{652}, \kappa^{656}, \kappa^{738})(\kappa^{654}, \kappa^{695}, \kappa^{697})(0, \infty, 1)(\kappa^{341})(\kappa^{682})$.

Both permutations of x and y produced a disconnected coset graph which contains 172 number of patches. It is important to note that out of these 172 patches, 170 are of the same type, denoted by $\eta_1, \eta_2, \eta_3, \dots, \eta_{170}$. The other two patches are denoted by η_{171} and η_{172}. We denote this coset graph by D and $D = \eta_1 \cup \eta_2 \cup \eta_3 \cup \dots \cup \eta_{170} \cup \eta_{171} \cup \eta_{172}$ The Figures 2–4 represent η_1, η_{171} and η_{172} respectively.

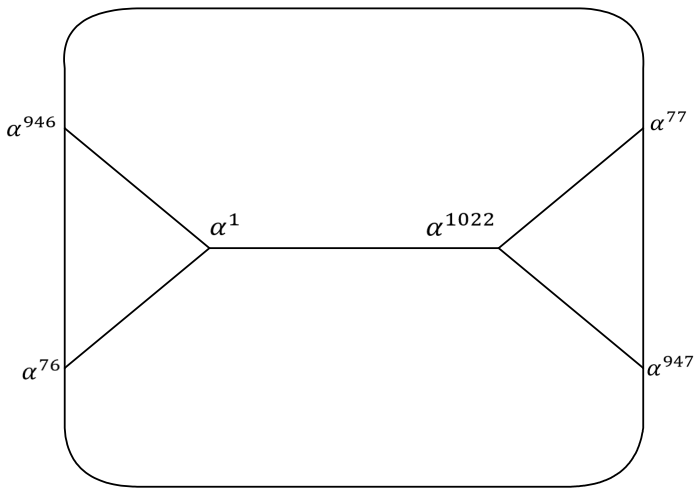

Figure 2. A copy of the patches η_1 of constructed graph.

Table 1. Structure of $GF\ (2^{10})$.

Binary form	Decimal	$GF(2^{10})$	Binary form	Decimal	$GF(2^{10})$	Binary form	Decimal	$GF(2^{10})$	Binary form	Decimal	$GF(2^{10})$
0000000000	0	0	0000000001	1	1	0000000010	2	κ^1	0000000100	4	κ^2
0000001000	8	κ^3	0000010000	16	κ^4	0000100000	32	κ^5	0001000000	64	κ^6
0010000000	128	κ^7	0100000000	256	κ^8	1000000000	512	κ^9	0010000001	129	κ^{10}
0100000010	258	κ^{11}	1000000100	516	κ^{12}	0010001001	137	κ^{13}	0100010010	274	κ^{14}
1000100100	548	κ^{15}	0011001001	201	κ^{16}	0110010010	402	κ^{17}	1100100100	804	κ^{18}
1011001001	713	κ^{19}	0100010011	275	κ^{20}	1000100110	550	κ^{21}	0011001101	205	κ^{22}
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…
1010111011	699	κ^{311}	0111110111	503	κ^{312}	1111101110	1006	κ^{313}	1101011101	861	κ^{314}
1000111011	571	κ^{315}	0011110111	247	κ^{316}	0111101110	494	κ^{317}	1111011100	988	κ^{318}
1100111001	825	κ^{319}	1011110011	755	κ^{320}	0101100111	359	κ^{321}	1011001110	718	κ^{322}
0100011101	285	κ^{323}	1000111010	570	κ^{324}	0011110101	245	κ^{325}	0111101010	490	κ^{326}
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…
0100110000	304	κ^{1007}	1001100000	608	κ^{1008}	0001000001	65	κ^{1009}	0010000010	130	κ^{1010}
0100000100	260	κ^{1011}	1000001000	520	κ^{1012}	0010010001	145	κ^{1013}	0100100010	290	κ^{1014}
1001000100	580	κ^{1015}	0000001001	9	κ^{1016}	0000010010	18	κ^{1017}	0000100100	36	κ^{1018}
0001001000	72	κ^{1019}	0010010000	144	κ^{1020}	0100100000	288	κ^{1021}	1001000000	576	κ^{1022}

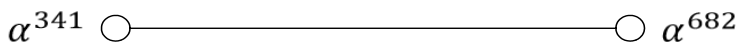

Figure 3. The patch η_{171} of constructed graph.

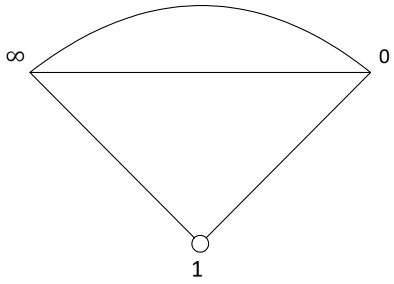

Figure 4. The patch η_{172} of constructed graph.

3.2. The proposed scheme

Step I: We first construct a square matrix of order 16 using vertices of coset graph in a specific way.

Consider a patch η_1 containing κ^1 as vertex from the coset graph D. The application of $xyxy^{-1}x$ on κ^1 carries us to κ^{77} by following the route $\kappa^1 \xrightarrow{x} \kappa^{1022} \xrightarrow{y} \kappa^{947} \xrightarrow{x} \kappa^{76} \xrightarrow{y^{-1}} \kappa^{946} \xrightarrow{x} \kappa^{77}$ (see Figure 2). So, in this way, we generate a sequence $\kappa^1, \kappa^{1022}, \kappa^{947}, \kappa^{76}, \kappa^{946}, \kappa^{77}$ of vertices. Consider a sub-sequence $\{\kappa^i : i \equiv 1\ mod\ (4)\} = \kappa^1, \kappa^{77}\}$ of this sequence and place κ^1 and κ^{77} at 1st and 2nd position of the first row respectively. Thereafter, we find the vertex from $D - \{\eta_1\}$ having the smallest power of κ, that is, κ^2. Let us denote the copy from $D - \{\eta_1\}$ containing κ^2 by η_2. *Note that if* κ^2 *would been exhausted in* η_1*, then* η_2 *is a copy from* $D - \{\Gamma_1\}$ *containing* κ^3. Generate a sequence of the vertices of the type $\kappa^i : i \equiv 1\ mod\ (4)$, present in η_2, in a similar way as done in the case of η_1. Write this sequence at the 1st row after κ^{77} by maintaining the order of sequence. After that, we chose a copy from $d - \{\eta_1, \eta_2\}$ possessing a vertex κ^m, where m is the least positive integer. In a similar way, continue to select the copies η_i and write vertices of the type κ^i such that $i \equiv 1\ mod\ (4)$ in the matrix until all copies η_i are used. So, a square matrix of 256 distinct entries from $GF(2^{10})^* = \{\kappa^1, \kappa^5, \kappa^9, \dots, \kappa^{1021}\}$ is generated (see Table 2).

We can generate 3 more tables simply by replacing the type of vertices in step I, from $\kappa^i : i \equiv 1\ mod\ (4)$ to $\kappa^i : i \equiv 0\ mod\ (4)$, $\kappa^i : i \equiv 2\ mod\ (4)$ and $\kappa^i : i \equiv 3\ mod\ (4)$.

Step II: The outcome of Step I yields a 16×16 matrix of distinct element from $GF(2^{10})^* = \{\kappa^1, \kappa^5, \kappa^9, \dots, \kappa^{1021}\}$. To bring all the element in the range of 0 to 255, we define a mapping $f : GF(2^{10})^* \longrightarrow GF(2^8)$ by $f(\kappa^n) = \beta^{\frac{n-1}{4}}$. Note the Galois $GF(2^8)$ is generated by primitive irreducible polynomial $\beta^8 + \beta^6 + \beta^5 + \beta^3 + 1$. Table 3 shows some of the elements of $GF(2^8)$ and their binary and decimal form.

In this manner, we have designed our initial S-box (See Table 4). We have examined its cryptographic strength via some well-known performance evaluation criteria and found that it provides

adequate security for transmitting sensitive information. To increase its security even further, let us proceed to step III.

Step III: Since an S-box is a square matrix of order 16. Therefore, the newly defined notion "matrix transformer" (see Section 2.2) can be used on initial S-box to enhance the security level. For this purpose, we tried several matrix transformers on our initial S-box by using MATLAB program and found that the matrix transformer displayed in Table 5 is the most suitable. The application of this matrix transformer on our initial S-box gives rise an S-box (See Table 6) with very high NL value 111. We call it our proposed S-box. An algorithm illustrating the process of using matrix transformers on the initial S-box is presented in Figure 5, while a flowchart can be found in Figure 6 to facilitate comprehension.

```
1. Start
2. Read Initial S-box IS
3. Construct matrix transformer M
4. Loop:
   4.1 Apply M on IS to evolve a new S-box NS
   4.2 Calculate NL of NS
   4.3 If NL < 110, go to step 3
   4.4 Else, display NS and M, and exit the loop
5. Stop
```

Figure 5. Algorithm describing step III.

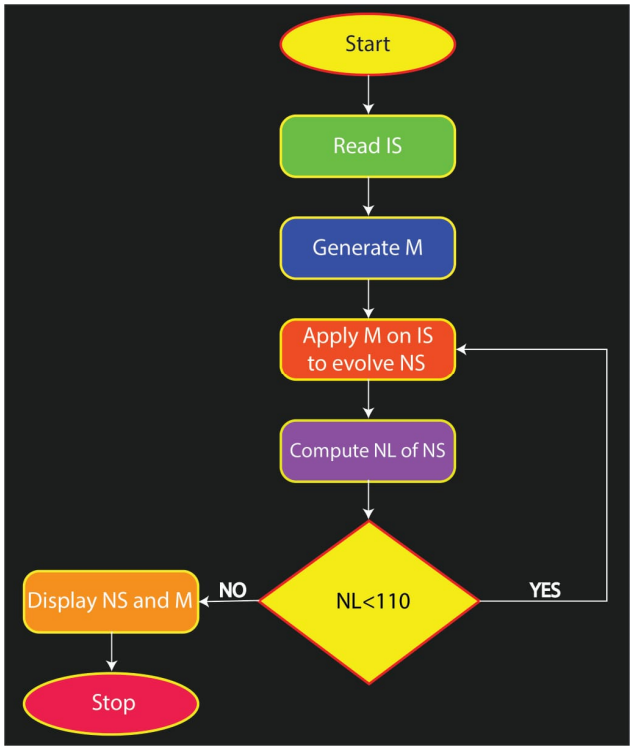

Figure 6. Flow chart of Step III.

Table 2. Outcome of Step I.

κ^{1}	κ^{77}	κ^{1021}	κ^{869}	κ^{1013}	κ^{5}	κ^{513}	κ^{1017}	κ^{1009}	κ^{9}	κ^{189}	κ^{13}	κ^{301}	κ^{709}	κ^{353}	κ^{193}
κ^{209}	κ^{17}	κ^{729}	κ^{1005}	κ^{393}	κ^{21}	κ^{305}	κ^{1001}	κ^{645}	κ^{937}	κ^{25}	κ^{385}	κ^{997}	κ^{421}	κ^{817}	κ^{29}
κ^{537}	κ^{457}	κ^{993}	κ^{317}	κ^{265}	κ^{637}	κ^{605}	κ^{33}	κ^{989}	κ^{401}	κ^{909}	κ^{149}	κ^{237}	κ^{273}	κ^{37}	κ^{161}
κ^{985}	κ^{473}	κ^{545}	κ^{41}	κ^{849}	κ^{981}	κ^{413}	κ^{45}	κ^{977}	κ^{897}	κ^{673}	κ^{397}	κ^{49}	κ^{225}	κ^{749}	κ^{973}
κ^{253}	κ^{109}	κ^{965}	κ^{181}	κ^{233}	κ^{53}	κ^{481}	κ^{969}	κ^{665}	κ^{213}	κ^{865}	κ^{57}	κ^{437}	κ^{529}	κ^{345}	κ^{737}
κ^{449}	κ^{389}	κ^{61}	κ^{917}	κ^{961}	κ^{493}	κ^{65}	κ^{621}	κ^{957}	κ^{297}	κ^{945}	κ^{145}	κ^{153}	κ^{221}	κ^{69}	κ^{953}
κ^{725}	κ^{261}	κ^{549}	κ^{477}	κ^{73}	κ^{949}	κ^{701}	κ^{405}	κ^{81}	κ^{177}	κ^{765}	κ^{941}	κ^{593}	κ^{785}	κ^{321}	κ^{113}
κ^{197}	κ^{85}	κ^{349}	κ^{589}	κ^{489}	κ^{577}	κ^{89}	κ^{893}	κ^{933}	κ^{761}	κ^{93}	κ^{657}	κ^{929}	κ^{229}	κ^{721}	κ^{97}
κ^{925}	κ^{573}	κ^{165}	κ^{417}	κ^{517}	κ^{101}	κ^{789}	κ^{133}	κ^{921}	κ^{805}	κ^{601}	κ^{525}	κ^{661}	κ^{557}	κ^{105}	κ^{837}
κ^{269}	κ^{913}	κ^{597}	κ^{169}	κ^{705}	κ^{117}	κ^{461}	κ^{445}	κ^{905}	κ^{333}	κ^{553}	κ^{125}	κ^{245}	κ^{121}	κ^{357}	κ^{901}
κ^{689}	κ^{257}	κ^{521}	κ^{649}	κ^{129}	κ^{561}	κ^{429}	κ^{889}	κ^{733}	κ^{329}	κ^{829}	κ^{717}	κ^{581}	κ^{137}	κ^{885}	κ^{873}
κ^{141}	κ^{881}	κ^{501}	κ^{541}	κ^{877}	κ^{777}	κ^{853}	κ^{325}	κ^{157}	κ^{361}	κ^{505}	κ^{569}	κ^{613}	κ^{861}	κ^{669}	κ^{857}
κ^{381}	κ^{797}	κ^{629}	κ^{173}	κ^{313}	κ^{845}	κ^{585}	κ^{841}	κ^{425}	κ^{465}	κ^{741}	κ^{185}	κ^{377}	κ^{565}	κ^{833}	κ^{609}
κ^{825}	κ^{693}	κ^{201}	κ^{745}	κ^{821}	κ^{757}	κ^{205}	κ^{813}	κ^{441}	κ^{249}	κ^{809}	κ^{485}	κ^{409}	κ^{625}	κ^{217}	κ^{337}
κ^{469}	κ^{801}	κ^{685}	κ^{793}	κ^{617}	κ^{773}	κ^{533}	κ^{241}	κ^{681}	κ^{781}	κ^{309}	κ^{497}	κ^{293}	κ^{769}	κ^{509}	κ^{433}
κ^{633}	κ^{653}	κ^{753}	κ^{365}	κ^{277}	κ^{281}	κ^{453}	κ^{289}	κ^{285}	κ^{677}	κ^{641}	κ^{713}	κ^{373}	κ^{697}	κ^{369}	κ^{381}

Table 3. Structure of $GF\ (2^8)$.

Binary form	Decimal	GF (2^8)	Binary form	Decimal	GF (2^8)	Binary form	Decimal	GF (2^8)	Binary form	Decimal	GF (2^8)
00000000	*0*	0	00000001	*1*	1	00000010	*2*	β^1	00000100	4	β^2
00001000	*8*	β^3	00010000	*16*	β^4	00100000	*32*	β^5	01000000	64	β^6
10000000	*128*	β^7	01101001	*105*	β^8	11010010	*210*	β^9	11001101	205	β^{10}
11110011	*243*	β^{11}	10001111	*143*	β^{12}	01110111	*119*	β^{13}	11101110	238	β^{14}
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…
10101100	*172*	β^{163}	00110001	*49*	β^{164}	01100010	*98*	β^{165}	11000100	196	β^{166}
11100001	*225*	β^{167}	10101011	*171*	β^{168}	00111111	*63*	β^{169}	01111110	126	β^{170}
11111100	*252*	β^{171}	10010001	*145*	β^{172}	01001011	*75*	β^{173}	10010110	150	β^{174}
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…	…	…
11010111	*215*	β^{243}	11000111	*199*	β^{244}	11100111	*231*	β^{245}	10100111	167	β^{246}
00100111	*39*	β^{247}	01001110	*78*	β^{248}	10011100	*156*	β^{249}	01010001	81	β^{250}
10100010	*162*	β^{251}	00101101	*45*	β^{252}	01011010	*90*	β^{253}	10110100	180	β^{254}

Table 4. Initial S-box.

24	41	1	180	2	140	113	52	32	4	190	42	125	102	90	60
8	128	205	45	253	16	250	86	162	109	17	115	244	81	217	64
238	48	101	57	156	59	148	78	35	105	122	98	100	39	210	182
104	167	50	239	46	231	38	13	243	221	213	97	72	132	199	143
248	164	83	215	119	55	214	223	219	181	177	200	3	135	224	235
111	216	6	54	80	99	108	241	12	73	30	94	27	76	149	185
96	232	87	129	192	195	67	116	240	166	233	188	254	23	69	58
7	187	133	51	203	63	212	29	68	31	153	186	62	74	93	79
124	157	28	173	154	141	77	14	92	146	171	91	229	137	144	85
5	155	193	10	82	36	20	168	174	230	18	121	21	40	71	249
227	130	196	9	252	61	176	134	201	160	178	43	88	117	107	44
22	208	11	150	33	19	66	236	114	246	112	202	118	152	34	194
138	251	197	169	237	26	145	158	56	179	95	15	255	161	159	106
234	120	220	198	110	222	147	183	142	218	123	191	228	131	139	151
245	165	89	163	209	189	206	65	47	225	175	103	53	247	207	75
211	136	226	25	170	242	70	184	126	84	172	49	37	127	204	0

Table 5. Matrix Transformer.

102	62	108	235	184	163	44	240	53	89	70	150	160	155	220	164
191	172	135	79	174	109	12	201	144	251	133	186	134	71	228	147
96	14	50	114	65	32	106	120	255	218	94	177	136	233	115	219
226	250	211	176	68	230	6	199	156	61	9	165	26	196	139	41
1	22	209	125	215	180	63	113	193	192	241	43	17	127	20	67
169	208	256	198	33	28	243	54	234	45	247	101	73	202	252	248
246	154	207	78	19	3	232	236	224	131	59	31	171	39	238	34
40	24	142	72	83	217	103	82	187	52	210	23	7	205	124	123
64	110	170	153	57	112	253	189	56	229	188	60	86	42	36	121
30	140	76	168	122	141	97	152	146	137	27	16	162	195	145	25
221	105	111	69	81	13	194	15	107	48	249	119	8	74	254	35
117	128	173	2	18	242	90	84	167	116	143	132	11	26	99	46
138	88	190	77	104	231	200	204	151	197	178	158	183	213	87	222
55	58	92	161	37	95	100	166	157	85	148	245	91	179	181	4
75	214	38	98	212	149	5	130	244	175	21	203	51	227	182	66
185	225	47	10	129	206	118	49	80	223	216	237	239	126	93	159

Table 6. Proposed S-box.

248	150	195	151	206	38	62	88	213	25	118	250	61	48	134	121
3	33	192	224	175	164	186	187	249	152	18	99	72	5	188	59
80	58	44	144	110	89	23	7	143	137	200	113	73	194	226	160
184	101	53	31	32	241	234	92	154	120	233	91	221	41	214	124
156	75	235	46	9	190	81	51	27	117	245	193	169	129	45	126
252	29	203	236	218	229	159	251	4	66	228	220	204	122	222	238
20	163	34	147	94	24	212	237	130	148	201	1	16	157	196	141
223	57	210	246	22	70	43	78	85	82	79	93	215	127	135	208
170	65	166	202	17	244	205	100	230	138	199	155	36	133	112	162
71	174	64	123	189	42	56	168	173	232	102	243	142	15	0	125
198	21	140	60	97	183	114	10	111	28	254	128	11	253	225	239
98	95	131	55	139	207	255	2	211	115	68	171	14	197	8	181
219	176	40	132	179	54	13	145	86	76	103	158	74	242	87	216
83	153	50	209	161	165	119	172	63	105	182	90	227	106	84	240
136	104	247	217	146	231	26	67	39	12	180	116	49	69	37	52
177	19	108	47	191	96	30	185	178	167	109	149	77	107	35	6

4. Performance evaluation

This section contains performance evaluation of the suggested S-box through different state of the art metrics such as the nonlinearity test, differential uniformity, bit independence criterion, strict avalanche criterion and linear approximation probability. We see that the outcome scores of our S-box obtained via these analyses are nearly equals to the ideal ones, demonstrating the effectiveness and capability of the proposed scheme. The analyses applied on our S-box are detailed below.

4.1. Nonlinearity (NL)

Nonlinearity is a key factor to determine the robustness of a substitution box. If an S-box maps input to output linearly, its resistance is very low [33]. A powerful S-box nonlinearly maps input to output. Any S-box with a higher nonlinearity value guarantees more security against cryptanalytic attacks. In the case of Boolean function of the form $\theta : F_2^n \longrightarrow F_2$, The nonlinearity is calculated as

$$N_\theta = 2^{n-1} - \frac{1}{2}\left[\left(_h \in GF(2)^{n^{\max}} \quad \right)|S_\theta(h)| \right. \tag{4.1}$$

Note that, $S_\theta(h) = \sum_{g \in GF(2)^n}(-1)^{\theta(g) \oplus g.h}$ represents the Walsh spectrum of $\theta(g)$. Table 7 indicates the nonlinearity values of all Boolean functions of the proposed S-box. The average Nonlinearity of our S-box is 110.75.

Table 7. Nonlinearities of all Boolean mappings involved in the suggested S-box.

Boolean mapping	θ_0	θ_1	θ_2	θ_3	θ_4	θ_5	θ_6	θ_7	Mean
NL score	110	112	110	112	110	110	110	112	110

4.2. Strict Avalanche Criteria (SAC)

SAC is another effective tool to judge the security of an S-box. It was proposed by Webster and Tavares [34]. To meet this requirement, the input bit of any cryptosystem must change along with a 50% change in the output bits. The SAC performance of the S-box is determined by the dependency matrix. The perfect SAC score for the best cryptographic confusion is 0.5. Table 8 shows the dependency matrix of SAC values obtain by proposed S-box. The mean SAC value of proposed S-box is 0.5051, which differs slightly from the optimal value. Therefore, the suggested S-box fulfills the SAC criterion.

Table 8. SAC values of constructed S-box.

0.4844	0.5469	0.4688	0.5625	0.5312	0.5312	0.5156	0.4844
0.4531	0.4844	0.5469	0.5	0.5	0.4844	0.4844	0.5625
0.5312	0.4688	0.5312	0.5312	0.4375	0.4688	0.5156	0.5
0.4375	0.5	0.5469	0.5	0.5469	0.5312	0.4844	0.5156
0.4531	0.5625	0.5625	0.4688	0.4688	0.5156	0.4375	0.5312
0.5781	0.4844	0.5312	0.5469	0.5156	0.5	0.5156	0.5
0.5	0.4531	0.4531	0.4219	0.5156	0.5469	0.5312	0.4844
0.5	0.4844	0.5312	0.5312	0.5	0.5312	0.4375	0.5469

4.3. Bit independence criterion (BIC)

This test [34] is satisfied if the output bits operate independently, i.e., do not depend on each other. More specifically, no statistical dependencies or patterns should be present in the bits of the output vectors. It is intended to boost output bit autonomy for greater security. An S-box is said to be meet the BIC criterion if it satisfies SAC and possess nonlinearity score for all Boolean mappings. The Tables 9 and 10 depict the dependency matrices for BIC-nonlinearity and BIC-SAC respectively. The results show that the proposed S-box conforms to the required BIC standards.

Table 9. BIC outcomes for nonlinearity related to newly constructed S-box.

-	110	110	112	112	110	112	110
110	-	108	110	112	112	108	110
110	108	-	110	112	110	110	112
112	110	110	-	110	110	110	112
112	112	112	110	-	110	110	110
110	112	110	110	110	-	112	110
112	108	110	110	110	112	-	112
110	110	112	112	110	110	112	-

Table 10. BIC outcomes for SAC related to newly constructed S-box.

-	0.4805	0.5098	0.4941	0.4902	0.498	0.5215	0.4824
0.4805	-	0.5195	0.5176	0.4922	0.4922	0.4766	0.4902
0.5098	0.5195	-	0.5	0.4902	0.5137	0.4922	0.498
0.4941	0.5176	0.5	-	0.4961	0.5117	0.5273	0.4902
0.4902	0.4922	0.4902	0.4961	-	0.4922	0.5293	0.5195
0.498	0.4922	0.5137	0.5117	0.4922	-	0.4707	0.4863
0.5215	0.4766	0.4922	0.5273	0.5293	0.4707	-	0.4883
0.4824	0.4902	0.498	0.4902	0.5195	0.4863	0.4883	-

4.4. Linear Probability

Modern block ciphers are designed to create as much complexity among the bits as possible to protect the privacy of the information and to offer protection against various decryption techniques employed by the cryptanalysts. It is accomplished by S-box. The lower the value of LP, the better the capability of S-box to withstand linear attacks. The LP value of an S-box can be calculated by using the following equation [35];

$$LP = (_{\Gamma \mathrm{w}}, \Gamma w' \neq 0^{max} \left| \frac{\#\{w \in K : w.\Gamma \mathrm{w} = \mathrm{S}(w).\Gamma w'\}}{2^n} - \frac{1}{2} \right| \tag{4.2}$$

where $K = \{0,1,\ldots,2^n\}$ and $\Gamma \mathrm{w}$ and $\Gamma w'$ are the input mask and output mask respectively. The designed S-box has an LP score of 0.0781.

4.5. Differential uniformity (DU)

Table 11. DU scores of newly constructed S-box.

4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	2	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	6
4	4	4	4	4	6	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	6	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	6	4	4	6	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	6	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	6	4	6	4	4	4	4	4	4	4	4
6	4	4	4	4	4	4	4	6	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	-

The resistance of S-box to differential cryptanalysis is investigated by DU [35]. To determine DU, a input differential $\Delta\sigma_i$ is uniquely linked to an output differential $\Delta\rho_i$, for all i. For a given S-box, its value can be calculated by using the following equation:

$$DU = (_{\Delta\sigma_i} \neq 0, \Delta\rho_i^{max}\{\sigma_i \in \Gamma: S(\sigma_i) \oplus S(\sigma_i + \Delta\sigma_i) = \Delta\rho_i\} \tag{4.3}$$

It is necessary to develop an S-box with smaller DU values in order to withstand differential cryptanalysis attacks. The maximum DU score of the proposed S-box is 6 (See Table 11), indicating its ability to counter differential attacks.

According to the performance study and comparative analysis, our S-box has better cryptographic properties than many recently designed S-boxes based on optimization, chaos and algebraic techniques. The comparison present in Table 12 demonstrates the suggested technique of designing S-boxes outperforms many of the available approaches. Here are our findings:

1. The S-box must have a high nonlinear value to resist linear attacks. According to Table 12, the average nonlinearity of our S-box is almost equal to AES, outperforming all other S-boxes show in Table 12. Therefore, there is considerable confusion, which makes the proposed method resistant to all the existing linear cryptanalysis.
2. The prime goal of every S-box designer is to achieve a SAC score close to the optimal value (0.50). From Table 12 demonstrates that the suggested S-box satisfies the requirements of strict avalanche criterion.
3. The reading of BIC-NL and BIC-SAC obtained from the prosed S-box are very encouraging are better than those of most of the S-boxes in Table 12
4. A potent S-box has a smaller DU value. As seen in Table 12, the DU score of the suggested S-box is less than the S-boxes developed in [37–44].
5. A smaller LP score makes an S-box more resistant to linear cryptanalysis. The LP score of our S-box is 0.0781, which is slightly higher than AES but lower than the LP values of all S-boxes in Table 12.

Table 12. Comparison of the various analyses between different S-boxes.

S-box	Nonlinearity			SAC	BIC-SAC	BIC-NL	DU	LP
	Min	Max	Average					
Suggested S-box	110	112	110.75	0.5051	0.4989	110.55	6	0.0781
AES [36]	112	112	112	0.5058	0.5046	112	4	0.0625
Reference [37]	106	108	106.25	0.5112	0.4975	103.93	12	0.1484
Reference [38]	106	110	106.5	0.5010	0.4987	103.93	10	0.125
Reference [39]	106	108	107	0.4949	0.5019	102.29	12	0.141
Reference [40]	106	110	108.5	0.4995	0.5011	103.85	10	0.109
Reference [41]	108	110	109.75	0.5042	0.4987	110.6	6	0.0859
Reference [42]	102	110	106.5	0.4943	0.5019	103.35	12	0.1468
Reference [43]	104	108	105.5	0.5065	0.5031	103.57	10	0.1328
Reference [44]	104	110	107	0.4993	0.5050	103.29	10	0.1328

5. Majority logic criterion

The evaluating the suitability of an S-box to be employed in an encryption process using the majority logic criteria (MLC) is a useful approach [45]. Randomness in the encoded picture is assessed using these five analyses energy, entropy, homogeneity, contrast and correlation.

Homogeneity and energy are utilized to identify the features of the encoded picture. The correlation test assesses the resemblance level between the host and encrypted picture. The lower correlation value implies more distortion caused by encryption. Through contrast, the decrease of brightness of the plaintext image is assessed. The greater the contrast value, the more efficient the encryption procedure. The process of encryption distorts the plaintext, and statistical parameters characterize the resiliency of S-box. The S-box that is formed is utilized to encrypt digital photos. To conduct MLC four 256×256 JPEG photos of Cameraman, Pepper, Lena and Baboon are selected. Two steps of substitution using our S-box are performed in the encrypting process. Encryption is accomplished through two steps of S-box substitution. During the 1st phase, the substitution is performed in a forward direction (from the start pixel to the end pixel) and subsequently in an opposite way. All simulations were conducted using the MATLAB programming. The original and encrypted photos are shown in Figure 7. The distorted pictures differ significantly from their corresponding undistorted versions. The level of visual distortion is quite large, since the graphics lack a pattern that promotes security breaches from the host picture. Table 13 shows the findings of all MLC testing performed. Table 14 presents the calculated correlation coefficients for pictures.

The results suggest that the created substitution box is suitable for encryption purposes and are good enough to be used in the systems designed to ensure the reliability and security of sensitive data.

Figure 7. Plain and distorted images using proposed S-box.

Table 13. Results of MLC for our S-box.

Image	Correlation	Entropy	Energy	Homogeneity	Contrast
Cameraman Host	0.9227	7.0097	0.1805	0.8952	0.5871
Cameraman-Enc	0.0394	7.9972	0.0149	0.3999	10.0509
Pepper Host	0.9312	7.5326	0.1096	0.8880	0.3849
Pepper-Enc	0.0021	7.9972	0.0156	0.3902	10.4802
Baboon Host	0.7983	7.2649	0.0943	0.7820	0.6326
Baboon-Enc	0.0071	7.9975	0.0156	0.3945	10.3994
Lena Host	0.9024	7.4439	0.1127	0.8622	0.4482
Lena-Enc	−0.0379	7.9976	0.0157	0.3822	10.8896

Table 14. Horizontal and vertical correlation matrices for S-box.

Image		Cameraman	Pepper	Baboon	Lena
Vertical	Plain Image	0.9745	0.9137	0.9090	0.9321
	Distorted Image	0.0310	−0.0392	−0.0128	−0.0117
Horizontal	Plain Image	0.9610	0.9204	0.8727	0.883
	Distorted Image	−0.0026	−0.0015	0.0039	−0.0021

6. Measurement of encrypted image quality

The experimental assessments of the proposed image encryption technique are discussed in this section. The 256×256 pixel grayscale photos of Cameraman, Pepper and Baboon are picked for the experiment. Table 15 contains a variety of image quality measurements that have been suggested for use with two rounds of encryption using S-boxes. These methods have been thoroughly discussed. The findings indicate that the recommended S-box is robust enough to survive various attacks.

6.1. Mean Square Error (MSE)

During encryption *MSE* analysis assesses the unpredictability of the encrypted picture [46]. This technique computes the squared difference between the original and distorted picture. It can be computed as follows:

$$MSE = \frac{1}{U \times V} \sum_{y_2=1}^{U} \sum_{y_1=1}^{V} \left(O(y_1, y_2) - E(y_1, y_2) \right)^2 \tag{6.1}$$

where U and V represent the dimensions of original $O(y_1, y_2)$ and distorted $E(y_1, y_2)$ pictures respectively. For effective encryption methods, the *MSE* rating must be as high as conceivable [46].

6.2. The Peak Signal-to-Noise Ratio (PSNR)

The *PSNR* test [38] is an ideal criterion for assessing the quality of picture encryption techniques. It estimates how well the original picture matches the ciphertext. *PSNR* value is calculated using the following formula;

$$PSNR = 10log_{10}\frac{V^2}{\sqrt{MSE}} \tag{6.2}$$

where V is the amount of variance that was at its highest in the original picture data. It is necessary to have a higher value of *PSNR* in order to get a superior encoded picture [47].

6.3. Average & Maximum Difference (AD & MD)

To determine the average and maximum dissimilarities between the unencrypted O and encrypted E pictures, researchers used the *AD* and *MD* test [47]. *AD* and *MD* values are determined using the following formulas;

$$AD = \frac{\sum_{y_2=1}^{R}\sum_{y_1=1}^{S}[O(y_1,y_2)-E(y_1,y_2)]}{R\times S} \tag{6.3}$$

$$MD = \max|O(y_1,y_2) - E(y_1,y_2)| \tag{6.4}$$

6.4. Mutual Information (MI)

MI measures how much information can be retrieved about the original picture from a distorted version of it. Let us denote the joint probability function of O and E by $\rho(y_1,y_2)$, then the value of *MI* can be determined by using the formula below;

$$MI = \sum_{y_1\in O}\sum_{y_2\in E}\rho(y_1,y_2)log_2\frac{\rho(y_1,y_2)}{\rho(y_1)\rho(y_2)} \tag{6.5}$$

The MI value must always be kept to a minimum in a decent encryption system [48].

6.5. Universal Quality Index (UQI)

As stated in reference [49], the *UQI* method partitions the evaluation of image distortion into three components: luminance, structural comparisons and contrast. The *UQI* metric for a pair of images O and E can be expressed as follows;

$$UQ(O,E) = \frac{4\rho_O\rho_E\rho_{OE}}{(\rho_0^2-\rho_E^2)(\varphi_0^2-\varphi_E^2)} \tag{6.6}$$

where ρ_o, ρ_E represent the mean values of the original and distorted images, respectively, and φ_o, φ_E represent the standard deviation of the original and distorted images, respectively.

6.6. Structural Similarity (SSIM)

SSIM is an enhanced version of the *UQI* designed to assess the similarity between two images. In particular, *SSIM* evaluates the fidelity of one of the images by assuming that the other image is free from errors. The computation of the *SSIM* score involves analyzing a pair of windows (R,S) of the image using the following formula:

$$SSIM(R,S) = \frac{(\nu_R \nu_S + a_1)(2\varphi_R \varphi_S + a_2)}{(\nu_R^2 + \nu_R^2 + a_1)(\varphi_R^2 + \varphi_R^2 + a_2)} \tag{6.7}$$

where φ_R and φ_S are the variances of R and S and ν_R and ν_S are the average scores of R and S respectively. The range of the *SSIM* score lies between -1 to 1, where a score of 1 indicates that the images are identical. A score close to 0 indicates a strong encryption scheme [48].

6.7. Normalized Cross Correlation (NCC)

As stated in citation [49], the correlation function provides a means of measuring the proximity of two digital images. The *NCC* method is a well-established technique for assessing the similarity between two images. Its calculation is based on the following formula:

$$NCC = \sum_{y_2=1}^{U} \sum_{y_1=1}^{V} \left(\frac{O(y_1,y_2) \times E(y_1,y_2)}{\sum_{y_2=1}^{U} \sum_{y_1=1}^{V} |O(y_1,y_2)|^2} \right) \tag{6.8}$$

6.8. Normalized Absolute Error (NAE)

NAE [49] can be used to assess the efficiency of an image encryption process by comparing the pixel values of the original image with those of the encrypted (ciphered) image. To calculate the *NAE* between the plain and ciphered image, the formula is:

$$NAE = \frac{\sum_{y_2=1}^{U} \sum_{y_1=1}^{V} |O(y_1,y_2) - E(y_1,y_2)|}{\sum_{y_2=1}^{U} \sum_{y_1=1}^{V} |O(y_1,y_2)|} \tag{6.9}$$

6.9. Root Mean Square Error (RMSE)

The assessment of an image encryption algorithm's effectiveness can be facilitated by utilizing *RMSE* as a performance metric. The calculation of *RMSE* involves determining the square root of the average of all the squared errors [49]. Its frequent use and flexibility make it a versatile and valuable error metric for numerical forecasting. The mathematical expression for RMSE is indicated below;

$$RMSE = \sqrt{\frac{\sum_{y_2=1}^{U} \sum_{y_1=1}^{V} |O(y_1,y_2) - E(y_1,y_2)|^2}{U \times V}} \tag{6.10}$$

6.10. Structural Content (SC)

SC is a correlation-based measure that quantifies the similarity between two images. The following mathematical equation is used to compute its score;

$$SC = \frac{\sum_{y_2=1}^{U} \sum_{y_1=1}^{V} |O(y_1,y_2)|^2}{\sum_{y_2=1}^{U} \sum_{y_1=1}^{V} |E(y_1,y_2)|^2} \tag{6.11}$$

Table 15. Outcomes of various image quality measures.

Test	Cameraman-Enc	Pepper-Enc	Baboon-Enc	Lena-Enc
MSE	9212.16	8656.41	7854.44	8414.71
MSE [6]	9079.09	8190.01	8011.23	8239.51
MSE [15]	9189.41	8612.09	7599.03	7930.39
MSE [17]	9187.38	8423.61	7865.21	8274.13
PSNR	8.4723	8.8563	9.8912	8.9912
PSNR [6]	8.1129	8.9710	8.5539	9.1902
PSNR [15]	8.2897	8.7091	8.1331	8.9500
PSNR [17]	8.2891	8.3353	8.9361	8.0032
SSIM1	0.0009	0.0012	0.0010	0.0011
SSIM1 [6]	0.0013	0.0008	0.0011	0.0012
SSIM1 [15]	0.0010	0.0012	0.0008	0.0014
SSIM1 [17]	0.0009	0.0015	0.0012	0.0013
NCC	0.8633	0.8710	0.9121	0.8803
NCC [6]	0.8537	0.8675	0.8912	0.9016
NCC [15]	0.8733	0.8712	0.8543	0.8461
NCC [17]	0.8640	0.87134	0.9001	0.8692
AD	−7.4523	−4.9812	−2.3419	−5.3881
AD [6]	−3,4511	−5.6634	−1.4529	−2.3319
AD [15]	−6,7819	−3.8873	−2.8827	−4.1198
AD [17]	−3.4429	−4.9821	−2.3872	−7.6594
SC	0.8496	0.8345	0.8456	0.8247
SC [6]	0.8455	0.8451	0.8401	0.8342
SC [15]	0.8341	0.8489	0.8465	0.8231
SC [17]	0.8436	0.8111	0.8265	0.8490
MD	240	238	212	234
MD [6]	211	231	233	241
MD [15]	223	227	227	228
MD [17]	234	238	221	219
NAE	0.6358	0.6273	0.6147	0.6384
NAE [6]	0.6455	0.5932	0.5813	0.6459
NAE [15]	0.6040	0.6193	0.6388	0.6026
NAE [17]	0.6219	0.6243	0.6012	0.5856
RMSE	94.6682	91.7245	84.9561	87.9349
RMSE [6]	90.6638	92.3402	88.3476	86.7938
RMSE [15]	93,4428	89.7690	91.2398	87.3947
RMSE [17]	90.4582	85.1109	84.8934	88.1831
UQI	0.0218	0.0332	0.0314	0.0338
UQI [6]	0.0127	0.0412	0.0279	0.0178
UQI [15]	0.0347	0.0456	0.0127	0.0391
UQI [17]	0.0234	0.0401	0.0298	0.0281
MI	−1.0292	−1.0187	−1.0184	−1.0281
MI [6]	−1.0195	−1.0490	−1.0328	−1.0402
MI [15]	−1.0371	−1.0197	−1.0294	−1.0406
MI [17]	−1.341	−1.0198	−1.0384	−1.0327

7. Differential analysis of image protection

A robust cryptosystem is extremely sensitive to modifications in one bit of the plaintext. Through UACI, NPCR and BACI testing, the sensitivity of the system is assessed.

UACI indicates the unified mean intensity change between original and encrypted image while NPCR calculates the number of pixels change rate of the encrypted image if a single pixel is altered in the original image. In BACI analysis, the image difference $\Delta = abs(E_1 - E_2)$ is partitioned into blocks of pixels and arranged in a 2 × 2 matrix. This involves dividing the image into smaller, non-overlapping regions, or "blocks", to facilitate the comparison of pixel values before and after the intervention.

The following formulae are used to compute the values of UACI, NPCR and BACI:

$$UACI = \frac{1}{JK}\sum_{j,k}\frac{E_1(j,k)-E_2(j,k)}{255} \times 100\% \tag{7.1}$$

$$NPCR = \frac{\sum_{jk} D(j,k)}{JK} \times 100\% \tag{7.2}$$

$$BACI = \frac{1}{(J-1)(K-1)}\sum_{i=1}^{(J-1)(K-1)}\frac{Z_i}{255} \times 100\% \tag{7.3}$$

where $E_1(j,k)$ and $E_2(j,k)$ denote the grayscale values of pixels obtained (j,k)th position and $D(j,k) = \begin{cases} 0 & if\ E_1(j,k) \text{ and } E_2(j,k)\ are\ equal \\ 1 & otherwise \end{cases}$ and $Z_i = \frac{1}{6}(|a_1 - a_2| + |a_1 - a_3| + |a_1 - a_4| + |a_2 - a_3| + |a_2 - a_4| + |a_3 - a_4|)$ and $\Delta_i = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$.

Table 16 depicts the findings of the differential analysis for NPCR, UACI, and BACI, confirming the excellent performance of encryption effect provided by the designed S-box.

Table 16. NPCR, UACI and BACI outcomes.

Image	NPCR	UACI	BACI
Cameraman	99.63%	33.12%	24.60%
Pepper	99.81%	33.21%	26.38%
Baboon	99.76%	32.86%	24.25%
Lena	99.79%	33.16%	23.09%

8. Conclusions

Summing up, the present work has discussed and examined the development of modular group coset graphs over a finite field of order 1024 and a matrix transformer for application in S-box construction. An initial S-box is formed through coset graphs and after that the application of a matrix transformer on it enhances its working efficiency significantly, resulting in a robust S-box. Comparison of proposed method with other state-of-the-art S-box construction algorithms shows that the proposed mechanism outperforms other algorithms in terms of mean nonlinear score, LP, SAC, BIC and DU scores. In addition, the performance of the designed S-box when applied to encrypt certain plaintext graphics has been determined to be extraordinary using a variety of assessment tools.

As our experience with applying matrix transformer to coset graph S-box to improve its resilience has been promising, we plan to research novel ways for designing S-boxes combining matrix transformers and chaotic systems. Moreover, we intend to evaluate the application of S-box to cloud encryption.

Acknowledgments

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. 3011).

Conflict of interest

The authors declare there is no conflict of interest.

References

1. H. Delfs, H. Knebl, H. Knebl, *Introduction to Cryptography*, Heidelberg, Springer, 2002. https://doi.org/10.1007/978-3-662-47974-2
2. S. Kumar, T. Wollinger, Fundamentals of symmetric cryptography, in *Embedded Security Cars*, Springer, (2006), 125–143. https://doi.org/10.1007/3-540-28428-1_8
3. A. D. Gordon, A. Jeffrey, Types and effects for asymmetric cryptographic protocols, *J. Comput. Secur.*, **12** (2004), 435–483. https://doi.org/10.3233/JCS-2004-123-406
4. L. R. Knudsen, M. J. B. Robshaw, *The Block Cipher Companion*, Springer Science & Business Media, 2011. https://doi.org/10.1007/978-3-642-17342-4
5. P. Nastou, Y. Stamatiou, Enhancing the security of block ciphers with the aid of parallel substitution box construction, in *Proceedings 22nd International Conference on Distributed Computing Systems Workshops*, IEEE, (2002), 29–34.
6. A. Razaq, S. Akhter, A. Yousaf, U. Shuaib, M. Ahmad, A group theoretic construction of highly nonlinear substitution box and its applications in image encryption, *Multimedia Tools Appl.*, **81** (2022), 4163–4184. https://doi.org/10.1007/s11042-021-11635-z
7. H. Zhu, X. Tong, Z. Wang, J. Ma, A novel method of dynamic S-box design based on combined chaotic map and fitness function, *Multimedia Tools Appl.*, **79** (2020), 12329–12347. https://doi.org/10.1007/s11042-019-08478-0
8. A. Javeed, T. Shah, A. Ullah, Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group, *Wireless Pers. Commun.*, **112** (2020), 467–480. https://doi.org/10.1007/s11277-020-07052-4
9. A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah, A. Waheed, A novel construction of substitution box involving coset diagram and a bijective map, *Secur. Commun. Netw.*, **2017** (2017), 1–16. https://doi.org/10.1155/2017/5101934
10. Y. Si, H. Liu, Y. Chen, Constructing keyed strong S-box using an enhanced quadratic map, *Int. J. Bifurcation Chaos*, **31** (2021), 2150146. https://doi.org/10.1142/S0218127421501467
11. D. Lambić, A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design, *Nonlinear Dyn.*, **100** (2020), 699–711. https://doi.org/10.1007/s11071-020-05503-y

12. A. Anees, Z. Ahmed, A technique for designing substitution box based on van der pol oscillator. *Wireless Pers. Commun.*, **82** (2015), 1497–1503. https://doi.org/10.1007/s11277-015-2295-4
13. H. Liu, J. Liu, C. Ma, Constructing dynamic strong S-box using 3D chaotic map and application to image encryption, *Multimedia Tools Appl.*, (2022), 1–16. https://doi.org/10.1007/s11042-022-12069-x
14. Y. Wang, K. W. Wong, C. Li, Y. Li, A novel method to design S-box based on chaotic map and genetic algorithm, *Phys. Lett. A*, **376** (2012), 827–833. https://doi.org/10.1016/j.physleta.2012.01.009
15. Z. M. Z. Muhammad, F. Özkaynak, An image encryption algorithm based on chaotic selection of robust cryptographic primitives, *IEEE Access*, **8** (2022), 56581–56589. https://doi.org/10.1109/ACCESS.2020.2982827
16. F. Artuğer, F. Özkaynak, A novel method for performance improvement of chaos-based substitution boxes, *Symmetry*, **12** (2020), 571. https://doi.org/10.3390/sym12040571
17. Y. Q. Zhang, J. L. Hao, X. Y. Wang, An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map, *IEEE Access*, **8** (2020), 54175–54188. https://doi.org/10.1109/ACCESS.2020.2979827
18. B. B. Cassal-Quiroga, E. Campos-Cantón, Generation of dynamical S-boxes for block ciphers via extended logistic map, *Math. Probl. Eng.*, **2020** (2020), 1–12. https://doi.org/10.1155/2020/2702653
19. M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar, A. Razaq, Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes, *IEEE Access*, **8** (2020), 39781–39792. https://doi.org/10.1109/ACCESS.2020.2975880
20. B. Abd-El-Atty, M. Amin, A. Abd-El-Latif, H. Ugail, I. Mehmood, An efficient cryptosystem based on the logistic-chebyshev map, in *13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*, IEEE, (2019), 1–6, https://doi.org/10.1109/SKIMA47702.2019.8982535.
21. S. Zhou, X. Wang, Y. Zhang, Novel image encryption scheme based on chaotic signals with finite-precision error, *Inf. Sci.*, **621** (2023), 782–798. https://doi.org/10.1016/j.ins.2022.11.104
22. X. Liu, X. Tong, Z. Wang, M. Zhang, A novel hyperchaotic encryption algorithm for color image utilizing DNA dynamic encoding and self-adapting permutation, *Multimedia Tools Appl.*, **81** (2022), 21779–21810. https://doi.org/10.1007/s11042-022-12472-4
23. S. Zhou, Z. Zhao, X. Wang, Novel chaotic colour image cryptosystem with deep learning, *Chaos, Solitons Fractals*, **161** (2022), 112380. https://doi.org/10.1016/j.chaos.2022.112380
24. X. Liu, X. Tong, Z. Wang, M. Zhang, Construction of controlled multi-scroll conservative chaotic system and its application in color image encryption, *Nonlinear Dyn.*, **2** (2022), 1897–1934. https://doi.org/10.1007/s11071-022-07702-1
25. S. Zhou, Y. Qiu, X. Wang, Y. Zhang, Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box, *Nonlinear Dyn.*, **2023** (2023), 1–19. https://doi.org/10.1007/s11071-023-08312-1
26. X. Liu, X. Tong, Z. Wang, M. Zhang, A new n-dimensional conservative chaos based on Generalized Hamiltonian System and its' applications in image encryption, *Chaos, Solitons Fractals*, **154** (2022), 111693. https://doi.org/10.1016/j.chaos.2021.111693

27. S. Zhou, X. Wang, Y. Zhang, B. Ge, M. Wang, S. Gao, A novel image encryption cryptosystem based on true random numbers and chaotic systems, *Multimedia Syst.*, **28** (2022), 95–112. https://doi.org/10.1007/s00530-021-00803-8
28. M. Aamir, M. A. Yousaf, A. Razaq, Number of distinct homomorphic images in coset diagrams, *J. Math.*, **2021** (2021), 1–29, https://doi.org/10.1155/2021/6669459
29. R. C. Lyndon, P. E. Schupp, R. C. Lyndon, P. E. Schupp, *Combinatorial Group Theory*, Springer, Berlin, **188** (1977). https://doi.org/10.1007/978-3-642-61896-3
30. A. Razaq, Q. Mushtaq, A Yousaf, The number of circuits of length 4 in PSL (2,$\mathbb{Z}$)-space, *Commun. Algebra*, **46** (2018), 5136–5145. https://doi.org/10.1080/00927872.2018.1461880
31. A. Torstensson, Coset diagrams in the study of finitely presented groups with an application to quotients of the modular group, *J. Commut. Algebra*, **2** (2010), 501–514. https://doi.org/10.1216/JCA-2010-2-4-501
32. J. R. Bastida, *Field Extensions and Galois Theory*, Cambridge University Press, **22** (1984).
33. J. Pieprzyk, G. Finkelstein, Towards effective nonlinear cryptosystem design, *IEE J. Comput. Digital Tech.*, **135** (1988), 325–335. https://doi.org/10.1049/ip-e.1988.0044
34. A. F. Webster, S. E. Tavares, On the design of S-boxes, in *Advances in Cryptology—CRYPTO'85 Proceedings*, **218** (1985), 523–534.
35. M. Matsui, Linear cryptanalysis method for DES cipher, in *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, Berlin, Heidelberg, (1985), 386–397. https://doi.org/10.1007/3-540-48285-7
36. J. Daemen, V. Rijmen, The advanced encryption standard, in *The Design of Rijndael*, Springer, Berlin, Heidelberg, (2002), 1–8. https://doi.org/10.1007/978-3-662-04722-4_1
37. U. Hayat, N. A. Azam, H. R. Gallegos-Ruiz, S. Naz, L. Batool, A truly dynamic substitution box generator for block ciphers based on elliptic curves over finite rings, *Arabian J. Sci. Eng.*, **46** (2021), 8887–8899. https://doi.org/10.1007/s13369-021-05666-9
38. S. Ibrahim, A. M. Abbas, Efficient key-dependent dynamic S-boxes based on permutated elliptic curves, *Inf. Sci.*, **558** (2021), 246–264. https://doi.org/10.1016/j.ins.2021.01.014
39. B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, A. Alzamil, Implementing a symmetric lightweight cryptosystem in highly constrained IoT devices by using a chaotic S-box, *Symmetry*, **13** (2021), 129. https://doi.org/10.3390/sym13010129
40. H. S. Alhadawi, M. A. Majid, D. Lambić, M. Ahmad, A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm, *Multimedia Tools Appl.*, **80** (2021), 7333–7350. https://doi.org/10.1007/s11042-020-10048-8
41. M. Long, L. Wang, S-box design based on discrete chaotic map and improved artificial bee colony algorithm, *IEEE Access*, **9** (2021), 86144–86154. https://doi.org/10.1109/ACCESS.2021.3069965
42. R. Soto, B. Crawford, F. González, R. Olivares, Human behaviour based optimization supported with self-organizing maps for solving the S-box design problem, *IEEE Access,* **9** (2021), 84605–84618. https://doi.org/ 10.1109/ACCESS.2021.3087139
43. W. Yan, Q. Ding, A novel S-box dynamic design based on nonlinear-transform of 1D chaotic maps, *Electronics*, **10** (2021), 1313. https://doi.org/10.3390/electronics10111313
44. P. Zhou, J. Du, K. Zhou, S. Wei, 2D mixed pseudo-random coupling PS map lattice and its application in S-box generation, *Nonlinear Dyn.*, **103** (2021), 1151–1166. https://doi.org/10.1007/s11071-020-06098-0

45. I. Hussain, T. Shah, M. A. Gondal, H. Mahmood, Generalized majority logic criterion to analyze the statistical strength of S-boxes, *Z. Naturforsch. A*, **67** (2012), 282–288. https://doi.org/10.5560/zna.2012-0022
46. A. M. Eskicioglu, P. S. Fisher, Image quality measures and their performance, *IEEE Trans. Commun.*, **43** (1995), 2959–2965, https://doi.org/10.1109/26.477498
47. Q. Huynh-Thu, M. Ghanbari, Scope of validity of PSNR in image/video quality assessment, *IET Electron. Lett.*, **44** (2008), 800–801. https://doi.org/10.1049/el:20080522
48. X. J. Wu, H. B. Kan, J. Kurths, A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps, *Appl. Soft Comput.*, **37** (2015), 24–39. https://doi.org/10.1016/j.asoc.2015.08.008
49. Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, Image quality assessment: from error visibility to structural similarity, *IEEE Trans. Image Process.*, **13** (2004), 600–612. https://doi.org/10.1109/TIP.2003.819861

AIMS Press