IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 6, 2021, accepted November 10, 2021, date of publication November 24, 2021,
date of current version December 2, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3128177

Construction of S-Boxes Using Different Maps Over Elliptic Curves for Image Encryption

MUHAMMAD RAMZAN[1], **TARIQ SHAH**[1], **MOHAMMAD MAZYAD HAZZAZI**[2], **AMER ALJAEDI**[3], **AND ADEL R. ALHARBI**[3]

[1]Department of Mathematics, Quaid-I-Azam University, Islamabad 45320, Pakistan
[2]Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia
[3]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia

Corresponding author: Muhammad Ramzan (mramzan@math.qau.edu.pk)

This work was supported by the Deanship of Scientific Research at King Khalid University through Research Groups Program under Grant R. G. P. 2/150/42.

ABSTRACT In this article, we present an encryption technique that can encrypt any digital data. The proposed scheme basically depends on a substitution-permutation network. Two separate bijective maps are used in the proposed algorithm. Firstly, the substitution boxes are used to perform the substitution process. This technique uses elliptic curves (ECs) to create several substitution boxes with good cryptographic properties. The generated substitution boxes are utilized to replace the arrange data that produces the most uncertainty in the plain image data. Further, we used the permutation process to generate strong randomness in the proposed technique. For the evaluation of the stability of the proposed algorithm; nonlinearity, linear approximation probability, bit independence criterion, strict avalanche criterion and differential approximation probability were performed on the substitution boxes. Differential attacks (Number of Changing Pixel Rate (NPCR), Uniform Average Change Intensity (UACI)) and statistical tests (Entropy, Correlation) were performed on the encrypted images to check their resistance against different attacks. The execution and image analysis reveals that the proposed scheme attains good encryption results while requiring minimal computing ability and has efficient potential in real-time image encryption applications.

INDEX TERMS Elliptic curves, substitution box, image encryption, security analysis.

I. INTRODUCTION

The protection of information communicated through any channel or network is a challenging problem because of the appearance of evil and doubtful users whose purpose is just to disturb the verbal exchange. Their aim is to recognize the conditions of the information transfer by authentic users. The most important history of secure direction is lying below the extent of cryptography, steganography, and watermarking. The purpose of security techniques like cryptography, steganography, and watermarking is the secure data to transmission. To ensure the secure transformation of data, fast improvement has occurred within the area of digital database generation and multimedia facts. This progress aims to protect the conditional data from any unauthenticated users. A particular dependable procedure for this intention is an image as a base, the use of general-primarily establish cryptosystems. Images themselves are extremely essential, sending someone in ordinary or uncommon pastimes concerning the private, conventional, navy group, clinical records, and so forth. To make certain the safety of comfortable image channeling, diverse techniques have been built consisting of chaotic and strategy primarily based systems ([1]–[10]).

A. RELATED WORK

Elliptic curve-based algorithms are generally used to yield extra safety to the data. We'll focus our attention on EC-based cryptography (ECC), which employs innovative solutions proposed by several analysts. Miller [11] and Koblitz [12] were the first to suggest using the EC as a public key cryptosystem in 1985. A unique type of cryptosystem is one that is based on various mathematical systems. S-box is solely responsible for uncertainty and scattering in load facts in a variety of cryptographic algorithms. ECs are also utilized to create secure cryptographic systems. Other than the Diffie-Hellmans protocol, Miller created a cryptographic

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

system based entirely on ECs in [11] that is 20 percent faster.

Koblitz *et al.* [13] are used to create yet another fast and stable cryptographic system is entirely based on the concept of a disjoined arithmetic debate over elliptic curves. Except for RSA, Khan and Asghar [14] found that elliptic curve cryptography (ECC) had better certainty than RSA. The goal of this paper is to present a novel and well-organized method for constructing cryptographically secure substitution boxes (S-boxes) and securing secret images with ECs beyond prime field (PF). The x and y-coordinates of point of (ECs) are used in two bijective mappings in the new created s-box technique. The proposed image cryptosystem, on the other hand, is based on a method that generates an effective S-box.

After the first stage, steganography employing the least significant bit technique was used. Traditional cryptographic methodologies, on the other hand, were not fully utilized; instead, some basic ideas and techniques were applied to the encryption of images as a building block of ciphering methodology ([6], [32]–[36], [40], [41]). The substitute boxes also help to secure the image. It is the principle a part of the same old cryptographic algorithms like DES (facts encryption preferred) and AES (superior encryption fashionable) etc. [42].

The S-box is the only nonlinear component of block ciphers. The link between plain and ciphertext data is muddied by S-boxes. This mysterious interaction is described as "confusion." There are numerous techniques for creating non-linear components that raise the cryptosystem's uncertainty. Many scholars have used mappings on the elements of the Galois field (GF), such as the chaotic mapping, to improve the strength of S-boxes throughout the last few decades [6]. The key stream generation process, three-round scrambling process, and one-round diffusion process are the three processes that make up the encryption system by employing Josephus Traversing and mixed chaotic map [32]. Three stages of significant operations are carried out during the encryption process in [33]: DNA coded selected hyperchaotic sequence based pixel shuffling, DNA coded pixel diffusion, and DNA coded pixel shuffling. A new multi-dimensional multiple image encryption method has been developed [34]. The encryption operation does a one-round shuffling and diffusion of blocks and pixels (if any). Bitplanes decomposition and the parallel GA algorithm are used to create a new image encryption solution. GA performs permutation and substitution steps, which are the most important parts of this approach [35]. Khalid *et al.* [36] divide the image's pixels into LSB and MSB, then transform the MSB to LSB. The S-box was used to create uncertainty in the original image. The researchers used two or more methods in the majority of their studies, step-by-step approaches for improving image privacy. The author explored the consequences of the ECC-based encryption technique and compared it to other asymmetric key cryptographic protocols such as RSA and others. The authors proved the ECC scheme's security flaws. The majority of the schemes have a tiny key-space and take a long time to execute. The development of EC points is typically a time-consuming technique that has an impact on the overall computing time; as a result, there is a desire for the approach to generate EC points relatively quickly.

B. MOTIVATION

Because of the widespread use of ECC-based image encryption techniques, the inspiration for our research article is presented below.

i. By using ECC we get not only diffusion in cryptosystem, but it also helps us to create confusion for a strong cryptosystem.
ii. Furthermore, the traditional transformation of EC points into (x,y) affects the algorithmic complexity, necessitating a constructive and productive process for conversion.
iii. The creation of EC points is mostly a time taking technique that affects the entire computing time, hence the approach must generate EC points relatively quickly.

C. OUR CONTRIBUTION

The goal of this work is to demonstrate a new and productive method for constructing cryptographically well-built S-boxes with high Non-linearity, as well as the security of independent images depends on ECs above PF. The newly proposed S-box approach employs the x and y component of points in a finite EC, as well as the modulo 256 operation. The suggested s-box production scheme depends on the generality of two separate maps, along with the suggested image cryptographic technique is based on S-boxes produce by newly discovered methods.

The rest of the paper is laid out as follows: Preliminaries are included in Section 2. Section 3 provides an overview of existent S-box generating schemes. Section 4 presents a new method for the production of S-boxes across EC while section 5 contains their analysis and comparison. The proposed S-box algorithm is used to create a new image encryption system in Section 6. In addition, Section 7 carries a full examination and observation of the proposed image secure system. Finally, Sections 8 and 9 discusses the conclusion and future directions respectively.

II. PRELIMINARIES

Let F_p be the PF with p elements, and let p be a prime. The non-singular $EC(a, b, p)$ across the field F_p is describe as follows $a, b \in W$ where $a, b \leq p$.

$$E(a, b, p) = \left[\left\{(x, y) \in F_p^2 \mid (y^2 = x^3 + ax + b)\right\} \cup \{\infty\}\right] \tag{1}$$

if the ECs discriminant $(4a^3 + 27b^2)(mod p)$ is not zero. The parameters of the $E(a, b, p)$ are denoted by a,b and p. Unless otherwise stated, an EC over a PF is referred to as simply an elliptic curve, and the no. of entries in set B(finite) is indicated by $\#B$, and its ith entry is represented by i.

The no. of elements $\#E(a, b, p)$ on an EC is extremely valued. In general, determining the correct $\#E(a, b, p)$ is a difficult project. However, Hasse's Theorem [15] may be used to determine a border on $\#E(a, b, p)$ as follows:

$$p + 1 - 2\sqrt{p} \leq \#E(a, b, p) \leq p + 1 + 2\sqrt{p}$$

The injective function $rho(x, y) \mapsto (x^p, y^p)(modp)$ through $E(a, b, p)$ to ρ is termed as Frobenius function.

A. ELLIPTIC CURVE POINTS ADDITION

We can define Elliptic curve addition over the extraordinary subject like R and addition modulo P.

Addition over R [15]

An EC over the field R is representing by $\mathbf{E}(\mathbf{R})$ and describe by

$$y^2 = x^3 + Ax + B$$

having two points

$$p_1(x_1, y_1), \quad p_2(x_2, y_2),$$

on **E**

$$E : y^2 = x^3 + Ax + B.$$

Define a new point p_3 as follows

$$p_1 + p_2 = p_3.$$

An expression below will show that this is not the same as adding coordinates of the points. We assume that the first point $p_1 \neq p_2$ and that neither point is ∞. Its slope is

$$m' = \frac{y_2 - y_1}{x_2 - x_1}.$$

Suppose we have two points $R_1, R_2 \in E(R)$ with $R_1 = (x_1, y_1)$ and $R_2 = (x_2, y_2)$, we want to add these two points for this we discuss some cases.

case 1

$$R_1 + R_2 = \begin{cases} R_1, & if \quad R_2 = \infty, \\ R_2, & if \quad R_1 = \infty, \end{cases} \tag{2}$$

case 2

$$R_1 + R_2 = \begin{cases} \infty, & if\ x_1 = x_2\ and\ y_1 \neq y_2, \\ \infty, & if\ x_1 = x_2\ and\ y_1, y_2 = 0. \end{cases} \tag{3}$$

if case 1 and case 2 do not meet each other then we discuss case 3 for the addition of two points.

case 3

$$R_1 + R_2 = R_3 = (x_3, y_3,)$$

where

$$x_3 = m^2 - x_1 - x_2,$$
$$y_3 = m(x_1 - x_3) - y_1,$$

where m is

$$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & if \quad R_1 \neq R_2, \\ \dfrac{3x^2 - A}{2y}, & if \quad R_1 = R_2, \end{cases} \tag{4}$$

III. QUICK OVERVIEW OF S-BOX CONSTRUCTION APPROACHES

The Rijndael block cipher [16] has been adopted as the Advanced Encryption Standard by the National Institute of Standards and Technology (NIST) (AES). One of the most used cryptosystems is AES. Because of AES's importance, several cryptographers have looked into the cryptographic features of the S-box. In [17], authors find an analytical description of the AES S-box. Also, authors discovered that the AES may be described by a quadratic equation system. Rosenthal investigates the non-linear aspect of AES in [19] by looking at its polynomial representation. Because the AES S-box has few non-zero terms in its linear polynomial, it is concluded that it has low algebraic complexity, and so AES may be vulnerable against algebraic attacks. The EC function is used in the image encryption technique [19]. The approach in [19] alters the dimension of the original image by using the constant k, which is the ECs starting reservations and control parameter. The security assessments show that the encryption strategy based on the chaotic elliptic map is advantageous and resistant to well-known attacks. The article [20] presents an image encryption system for ECC based on a fast-mapping scheme with matrix method. The researchers exploited various attributes of the matrix and EC in the proposed work to transform alphanumeric character values to elliptic curve coordinates (x,y) using a non-singular matrix. A novel scheme in [43] based on modified Pascal's triangle and elliptic curve. A new transformation and suggested a novel method to construct efficient S-Boxes using cubic fractional transformation are define in [44]. Authors [45] suggested an effective image encryption method based on three dimensional chaotic dynamical systems and confusion components. The confusion and diffusion were added by utilizing Rabinovich-Fabrikant chaotic system and nonlinear component based on discrete two-dimensional S8 S-boxes. In article [46], using a new nonlinear mapping (cubic polynomial mapping), the authors suggested an innovative and simple method to design efficient S-Boxes. Some others techniques for S-box construction and image encryption schemes are discuss in ([47]–[51]). Many of the methods have small key-space and high level execution times.

IV. THE PROPOSED APPROACH FOR GENERATING S-BOXES

In this section, we'll present a quickly and easily method to generate a large number of different, unrelated objects and comfy injective $m \times n$ s-boxes primarily based on the x,y coordinates of an EC for the encryption of distinctly correlated data. The proposed method take inputs integers a,b,p s.t $a, b \leq p - 1$, where p is taken so large that we get our required result with the best statistical analysis.

A. THE ALGORITHM

The five main steps of the proposed S-box generating method are listed below.

TABLE 1. The S-box $S_{u(909,230,1723)}$ generated by the proposed algorithm.

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

Step 1: Choose any $a, b \in W$ as well as a prime number p such that $a, b \leq p - 1$.

Step 2: The p-value is chosen to ensure that the EC $E(a, b, p)$ contains minimum 256 different elements. Because an s-box on the $GF(2^8)$ contains 256 different entries, this restriction is required necessary.

Step 3: In the third step, take the EC defined in eq. (1) to generate the points on it:

$$E : y^2 = x^3 + ax + b \quad (mod\, p)$$

Step 4: In this step, we take a EC point (x,y) and apply bijective transformations and get two different output values about each point on the EC $E(a, b, p)$ except the point having x coordinate is zero. Bijective mappings [21] are defined as follows:

$$E^{u(x,y)}_{(a,b,p)} = \left\{x, y|u = \frac{2(y+1)}{x^2}; (x, y) \in E(a, b, p)\right\} \quad (5)$$

$$E^{v(x,y)}_{(a,b,p)} = \left\{x, y|v = \frac{4(y+1)}{x^3}; (x, y) \in E(a, b, p)\right\} \quad (6)$$

Step 5: Finally, the first 256 different numbers in each of the above two relations that are defined in eqs. (5) and (6) of the multi-sets $\left(E^{u(x,y)}_{(a,b,p)}, E^{v(x,y)}_{(a,b,p)}\right)$ are selected to form an S-boxes $S_{u(a,b,p)}$ and $S_{v(a,b,p)}$. If the element in (5) and (6) does not have 256 distinct numbers following it, the proposed approach will not find an S-box.

The newly created S-box is bijective, as seen in step 5. The proposed approach is used to generate S-boxes on various ECs. Table 1 shows the S-boxes $S_{u(a,b,p)}$, $S_{v(a,b,p)}$ produce by the new suggested approach in 16 × 16 standard form.

Construction of S-Boxes Using Elliptic Curve Over Prime Field

```
Input: Bijective mappings and EC with $a, b \leq p-1$, where p is prime
Output: S-box1, S-box2
$W1 = \{\}, W2 = \{\}$
$A =$ the point $(a, b, p)$;
$x = A(3 : length(A), 1)$;
$y = A(3 : length(A), 2)$;
for $i = 1 : length(x)$; do
    for $i = 1 : length(y)$ do
        $u = \frac{2*(y+1)}{x^2}$
        $v = \frac{4*(y+1)}{x^3}$
        $w1(i, :) = s1$;
        $w2(i, :) = s2$;
    end for
end for
```

V. S-BOX ANALYSIS AND COMPARISON

We analyze the experimental findings of randomly generated S-boxes using the suggested methodology in this section. The S-boxes formed by the proposed technique is particularly efficient for secure communication, as can be seen. Randomly generated distinct S-boxes, various standard security analysis tests are adapted on $S_{u(909,230,1723)}$,$S_{v(431,1148,1723)}$,$S_{v(431,1159,1723)}$ by the suggested scheme. One can examine the S-boxes formed by the proposed technique are extremely efficient for secure communication. In addition, the experimental outturn are analyze to several of the previously published s-boxes [[22], [23], [36]–[41]]

TABLE 2. The S-box $S_{v(431,1148,1723)}$ generated by the proposed algorithm.

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

A. NON-LINEARITY (NL)

It is a cryptosystem's most important feature. The nonlinearity of an excellent cryptographic system is primarily higher. It assesses a system's ability to withstand linear cryptanalysis. The ability of an S-box to cause confusion is measured using the idea of non-linearity [24]. NL $\tau(S)$ of S is describe in eq. (7) as the distance between S and the affine functions over $GF(2^8)$ for a specified S-box $S : GF(2^8) \rightarrow GF(2^8)$.

$$\tau(S)=min(\alpha,\beta,\gamma)\left\{\lambda \in GF(2^n)|\alpha.S(\lambda) \neq \beta.\lambda \oplus \gamma\right\} \tag{7}$$

where $\alpha \in GF(2^8), \beta \in GF(2), \gamma \in GF(2^8) \setminus \{0\}$ and "·"represent the dot product over $GF(2)$.

An S-box can achieve a maximum value of non-linearity of 120. If $\tau(S)$ is maximum, the consequence of further cryptographic analysis on S might not be in the desired range [24]. As a result, S-boxes with the best NL and valuable additional security execution tests are most important. Using the proposed methodology and some other existing s-box, we calculated the NL of the freshly constructed S-boxes. Table 4 shows the experimental findings of the NL test. The proposed S-boxes maximum (110,110,110), minimum (104,102,106), and average (107.25, 107.25,107) NL values respectively. It's clear that the newly built S-boxes have when compared to the elliptic curve-based S-boxes in [36]–[41], there is more nonlinearity. The freshly designed S-boxes have a lot of resistance against linear attacks.

B. LINEAR APPROXIMATION PROBABILITY (LP)

This test was developed by Mitsuru *et al.* [25] to determine the probability of obtaining an LP about the S-box. The density of bits of the original and ciphered text determines the LP of an S-box. The mathematical form of LP define in eq. (8) is given below

$$LP(S) = \frac{1}{2^n}\left\{max_{(\phi,\varphi)}[M(\phi,\varphi)]\right\} \tag{8}$$

where

$$M(\phi,\varphi) = \left[\#\left\{\mu \in GF(2^8)|\phi.\mu = \varphi.S(\mu)\right\} - 2^{n-1}\right] \tag{9}$$

where $\phi \in GF(2^8)$, $\varphi \in GF(2^8) \setminus \{0\}$ and "·"represents the dot product over $GF(2)$.

S-boxes with a low LP score is cryptographically strong. Table 5 lists examples of the freshly proposed s-boxes and their accompanying LP values, demonstrating that the proposed scheme's S-boxes are acceptable for secured transmission against LP attacks.

C. STRICT AVALANCHE CRITERION (SAC)

Matsui *et al.* [26] proposed this criterion based on a mix of the avalanche outcomes and integrity. When one input bit is inverted, the test determines the probability of a shift of cipher bit. An 8 × 8 dependence matrix is used to calculate the SAC (eq.10) of an S-box matrix

$$M = [m(j,k)]_{j=1,k=1}^{8,8}$$

where

$$\begin{aligned} m(j,k) = \Bigg\{&\frac{1}{2^n}\left[\alpha\left(S_j(s+h_k)+S_j(s)\right)\right] \\ &|h_j \in GF(2^8).\alpha(h_k) = 1 \\ &and \quad 1 \leq j,k \leq 8\Bigg\} \end{aligned} \tag{10}$$

where $\alpha(h_k)$ is the number of non-zero bits in h_k.

TABLE 3. The S-box $S_{v(431,1159,1723)}$ generated by the proposed algorithm.

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

TABLE 4. Proposed S-box nonlinearity.

S-Boxes	Proposed	Max. Non-linearity	Min. Non-linearity	Avg. Non-linearity
1	$S_{v(431,1148,1723)}$	110	104	107.25
2	$S_{v(431,1159,1723)}$	110	102	107.25
3	$S_{u(909,230,1723)}$	110	106	107

TABLE 5. The proposed S-boxes were compared to standard S-boxes in terms of their experimental findings.

S-Boxes	Non-linearity	SAC	BIC	LP	DP
$S_{v(431,1159,1723)}$	107.25	0.502441	0.500419	0.125	0.0390625
$S_{v(431,1148,1723)}$	107.25	0.49682	0.49909	0.132813	0.046875
$S_{u(909,230,1723)}$	107	0.499756	0.504255	0.171875	0.0390625
Ref. [14]	103.25	0.5151	0.4864	0.15625	0.171875
Ref. [7]	106.25	0.5037	0.5065	0.1016	0.0391
Ref. [41]	107	0.499023	0.50635	0.125000	0.0390620
Ref. [8]	107	0.4973	0.5052	0.1172	0.0391
Ref. [37]	106	0.51565	0.49805	0.0469	0.0391
Ref. [38]	107	0.5014	0.5016	0.1484	0.0390625
Ref. [39]	105.5	0.5000	0.4970	0.125	0.03125
Ref. [40]	106.7	0.5034	0.5015	0.132813	0.0390625

If all of the self-reliance matrix entries are close to 0.5, the SAC is satisfied. In addition, we ran the SAC test on a variety of different planned and current S-boxes, with the results shown in Table 5. The proposed S-boxes have an average SAC maximum and minimum of 0.5914 and 0.4111, respectively. As a result, the S-boxes created using the suggested method pass the SAC test. Furthermore, the SAC results of freshly designed S-boxes are equivalent to the SAC results of S-boxes that are already listed.

D. BIT INDEPENDENCE CRITERION (BIC)

The BIC test was proposed by author in [26] to evaluate how distinct a pair of outcome bits is when one input bit is complemented. In BIC, one bit is commended, and the influence on the output bits is measured using the CC (correlation coefficient). An S-box is regarded to pass the BIC test if its BIC value is close to 0.5. The BIC is based on the recommended and some already surviving S-boxes. Table 5 lists the BIC minimum and maximum for proposed S-boxes and already exist various S-boxes. The proposed S-boxes'

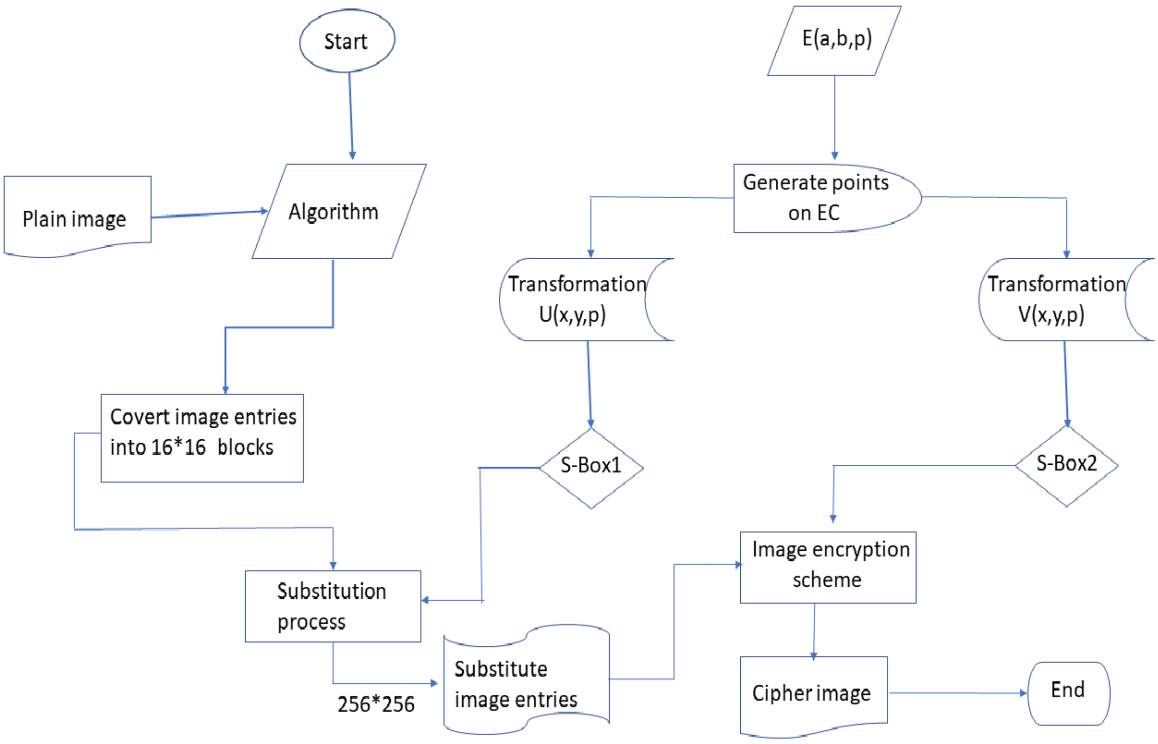


FIGURE 1. Flow chart for image encryption scheme.

average BIC values 0.500419,0.49909, and 0.504225 which are very close to 0.5. Table 3 shows the S-boxes. The results of the BIC test ensure that the suggested S-boxes are resistant to common attacks.

E. DIFFERENTIAL APPROXIMATION PROBABILITY (DP)

In [27] authors used this DP test to find out the probability effect of a specific input bit change on the difference of the consequent output bits. The DP(defined in eq. (11)) of an S-box S is calculated using the following mathematical formula

$$DP(S) = \max_{\partial s, \partial t} \left[\# \left\{ s \in GF(2^8) | S(s + \partial s) - S(s) = \partial t \right\} \right], \tag{11}$$

where $\partial s, \partial t \in GF(2^8)$.

If it has a low DP, an S-box can effectively resist differential attacks. Table 5 lists the DP of the proposed and already existing S-boxes employed in this article. Some of the suggested S-boxes have a DP value of 0.0390, which is lower than the S-boxes in [7], [8]. When compared to some of the current S-boxes, this means that the S-boxes constructed by the suggested approach may withstand differential attacks more successfully.

VI. PROPOSED IMAGE ENCRYPTION SCHEME

Without loss of generality, we assume that the plain-image is a 256×256 gray-scale image with a dimension of $T = N1 \times N2$ and that the plain-image is an integer matrix with N1 rows and N2 columns, with values ranging from [0-255]. Convert the gray-scale image pixels into $n \times n$ squares matrices each of which contains 256 elements, and proposed s-boxes also contain 256 different elements range from [0-255]. In the first phase, we use the obtained s-box to Substitute the image's scrambled component (the procedure is the same as AES substitution). In the next phase, we take another obtained s-box (which is not used in the first phase) as a key k and perform an addition operation with $n \times n$ squares matrix of scrambled image (obtained in the first phase) under mod 256.

A. ENCRYPTION ALGORITHM

In this subsection, we discussed the process of image encryption in detail.

i. First we take a gray-scale image of size $N1 \times N2$, and that the chosen image is an integer matrix with N1 rows and N2 columns. The plain image is shown in fig. 2a.

ii. We convert this image into 16×16 squares matrices and each of these single matrices contains 256 elements rang in [0-255].

iii. The substitution step is an important part of any cryptographic algorithm since it improves the scheme's security strength against the chosen plain-text attacks. The suggested S-box methodology (described in section 5) is used in the proposed approach to generate high-quality S-boxes with strong cryptographic properties. Now we choose one of the above proposed

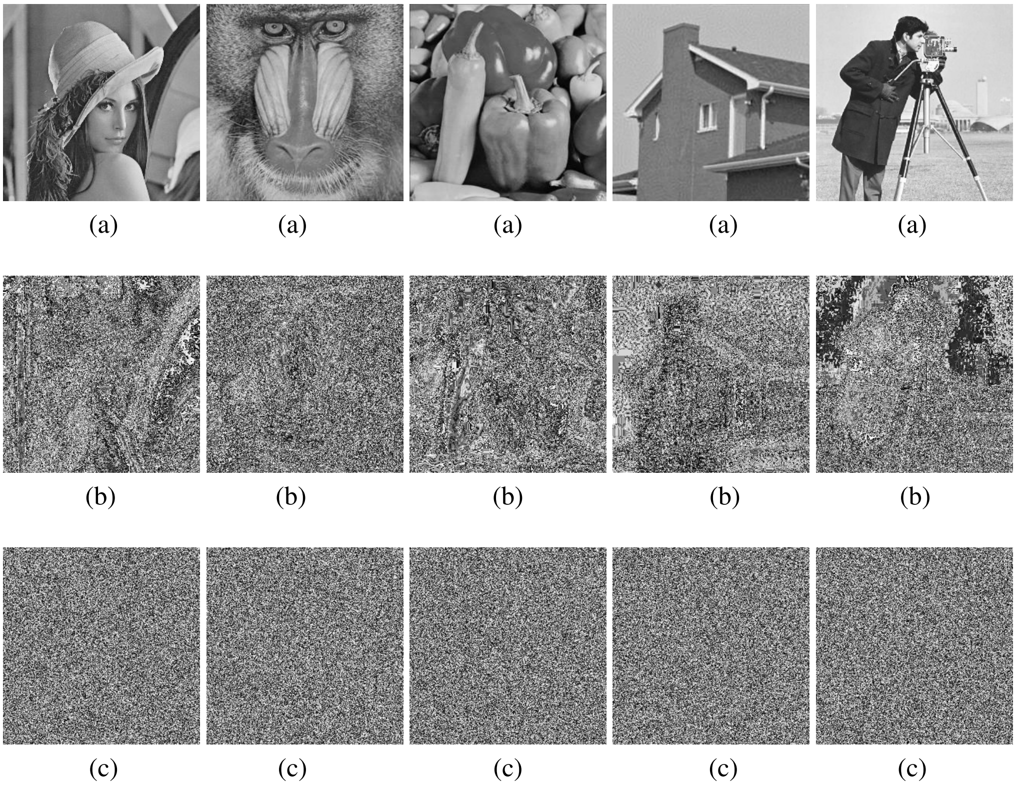


FIGURE 2. (a) plain image of lena, baboon, peppers, house and cameraman; where (b),(c) are substitution and cipher image's respectively.

s-box(we choose $S_u(a, b, p)$) for substitution. Here the substitution process consists of three parts Permutation, Entries exchange and Scrambling. Permutation generates by a sequence $\{z_n\}$ for pixels ranging from 1 to $N_1 \times N2$. Then, using the following equation, convert each member of the sequence into the 0-255 range.

$$z'_n = mod(z_n, 256)$$

Now we substitute the obtained permuted pixels of image to enhance the nonlinearity of the proposed scheme. The scrambled image(Is) after substitution is shown in Fig. 2b.

iv. S-box generally contain a 16 × 16 matrix with 256 different elements rang in [0-255]. Now we take another proposed s-box that is not used in the substitution process and repeat this s-box matrix 16 × 16 times so that we get matrix M_s of size 256 × 256 by repeating the entries of the proposed s-box.

v. Now we have two matrix of size 256 × $256(I_s, M_s)$. Let $x \in I_s$ as an input entry and corresponding $k \in M_s$ is a secret key for the proposed scheme. Now we compute this mathematical expression to get cipher image entries as follows

$$y = (x + k)(modp) \tag{12}$$

where we take $p = 256$ to restrict the range of entries between 0 and 255.

vi. In the last step, we get cipher image entries illustrated in figure 2(c).

The suggested encryption scheme is used to encrypt images of various sizes, including dimension, intensity levels, and encryption parameter range. Figure 2 displays some of the encrypted images.

B. DECRYPTION ALGORITHM

In this subsection, we discussed the process of image decryption in detail. First, we take cipher image that's obtained from the encryption process which is defined in the previous subsection. The cipher image is shown in fig 2c. Then we convert this cipher image into 16 × 16 squares matrices and substitute the inverse s-box used in the encryption substitution process. To produce inv($S_u(a, b, p)$) of ($S_u(a, b, p)$) the parameters a,b,p and of the S-box generating method must be sent to the receiver as keys. If the channel is assumed to be noiseless, applying inv($S_u(a, b, p)$) to I_c yields $I_{s^{-1}}$. Now in the next step, we take proposed s-box($S_v(a, b, p)$) and by repeating entries of this s-box we get matrix M_s of size 256 × 256. In the last step, we take one by one entry from $I_{s^{-1}}$ and corresponding entries from M_s as a key. Now compute this mathematical expression to get plain image entries as follows

$$y = (x - k)(modp) \tag{13}$$

where we take $p = 256$ to restrict the range of entries between 0 and 255.

```
Image Encryption Algorithm
    Input: Gray scale plane image
    Output: Gray scale cipher image
    I=imread('xyz.jpg');
    R=double(I);
    Substitution process using S-box1
    S=substitution(R,S-box1)
    convert 'S' into 16*16 matrices,
    M=matrices(S,16,16)
    T=M + S-box2 (mod 256)
    C=uint8(T)
    Get cipher image 'C'
```

VII. IMAGE ANALYSIS

A cryptosystem's security is evaluated to see if it can withstand malicious attacks. It should be able to withstand all types of known attacks to be considered good encryption. For this, we employ a variety of ways to counter different forms of attacks. We address the security examination of suggested image encryption in this section, including statistical analysis, histogram analysis, entropy, key-space analysis, and so on, to show that the suggested scheme prevents from the prevalent attacks. After passing through the proposed encryption technique, the simulations are run using various input images of Lena, baboon, deblur, house, and cameraman. Figures 2(a) show the Lena, baboon, deblur, house, and cameraman in their plain form, while Figures 2(b), show their encrypted versions with substitution, and Figures 2(c), show their cipher image's respectively. The results of encryption are visually strong, as can be seen from the encrypted image.

A. KEY ANALYSIS

The key area plays an important role in the encryption and decryption process's security. Cryptoanalysts frequently utilize key attacks to compromise the security of a cryptosystem. As a result, having a high key strength is essential for a robust security system.

1) KEY SPACING ANALYSIS

When the key size of the set of rules is large, it is difficult to use a brute force attack to obtain any information about the encryption or decryption method. If a cryptosystem's key spacing is greater than 2^{128}, it usually attracts key space analysis. We employed a 512-bit in our proposed method, which means that the keyspace analysis of our suggested method is considerably greater than 2^{128}. We employed seven keys a, b, p, a', b', p', k, and each one is 512-bits, which means that our proposed algorithm's key spacing analysis is significantly bigger than 2^{128}. As a result, our suggested scheme has enough key size to withstand any attack from exclusive attackers.

2) KEY SENSITIVITY ANALYSIS

The keys should be highly sensitive in a secure cryptosystem. This means that a small change in the keys produces a vastly different cipher-image of the same plain-image. The proposed cryptosystem makes advantage of EC-generated dynamic S-boxes. The parameters of the ECs employed in the proposed cryptosystem are dependent on the plain images, as shown in Equations (5), (6), (12), and (13). Furthermore, because ECs are extremely sensitive to their parameters, the dynamic S- boxes generated by the suggested approaches are also extremely sensitive to the keys. In the end, this means that the suggested encryption scheme passes the key sensitivity analysis.

B. DIFFERENTIAL ATTACK

An encryption method is stable in opposition to differential attacks if it can create successfully distinct encrypted images from two marginally different simple images. Various techniques are applied to assess the robustness of an encryption scheme to a differential attack. The NPCR (Number of pixel change rate) analysis counts how many pixels alternate when one byte of the plain picture is modified. When modifying original data, a precise cryptosystem's NPCR value is near 100. The UACI represents the average difference in strength between the simple gray-scale image and the cipher image. The cryptosystem's strength to differential attacks better as UACI analysis better. The NPCR and UACI analyses are represented in eqs. (14,15) as

$$NPCR = \frac{\sum_{\gamma_1,\gamma_2} M(\gamma_1,\gamma_2)}{X \times Y} \times 100\% \tag{14}$$

$$UACI = \left[\sum_{\gamma_1,\gamma_2} \left\{ \frac{|N_1(\gamma_1,\gamma_2) - N_2(\gamma_1,\gamma_2)|}{255} \right\} \times 100\% \right] \times \frac{1}{X \times Y} \tag{15}$$

$$M = \begin{cases} 1, & if\ N_1(\gamma_1,\gamma_2) = N_2(\gamma_1,\gamma_2) \\ 0, & if\ N_1(\gamma_1,\gamma_2) \neq N_2(\gamma_1,\gamma_2) \end{cases} \tag{16}$$

The original image and one-pixel alteration picture are represented by $N_1(\gamma_1, \gamma_2)$ and $N_2(\gamma_1, \gamma_2)$. The proposed and already exist cryptosystems were analyzed using NPCR and UACI, as shown in Table 6. Table 6 shows that the suggested approach performs well and is resistant to differential attacks.

C. STATISTICAL CRYPTANALYSIS

The entropy test and correlation test are used to evaluate the security of an image encryption technique against statistical attacks. Each of these tests, as well as the outcomes of our proposed methodology for these tests, are discussed below.

1) ENTROPY TEST

The entropy of a data collection is a measure of its randomness. Let$p_x(\eta)$ signify the probability of occurrence of the symbol $\eta \in \varphi$ in x for a data collection x over symbols φ.

TABLE 6. NPCR and UACI analysis and comparison of proposed encryption scheme over different images with some of already existing cryptosystem.

Scheme	Images	Images size	NPCR %	UACI %
Proposed				
	lena	256 × 256	99.61	33.65
	baboon	....	99.61	33.42
	peppers	....	99.63	33.68
	house	....	99.60	33.49
	cameraman	....	99.67	33.66
Ref. [33]				
	lena	256 × 256	99.61	33.47
Ref. [34]				
	lena	256 × 256	99.61	33.47
Ref. [9]				
	lena	256 × 256	99.60	33.47
Ref. [6]				
	lena	256 × 256	98.91	32.78
Ref. [32]				
	lena	256 × 256	99.59	33.45
	cameraman	....	99.55	33.44
Ref. [35]				
	lena	256 × 256	99.58	33.08
	peppers	....	99.71	32.19
	cameraman	....	99.60	33.15
	baboon	....	99.59	31.56
Ref. [36]				
	lena	256 × 256	99.66	33.71
	peppers	....	99.61	33.71
	baboon	....	99.65	33.70

The entropy of x is thus defined as H(x) in eq (17)

$$H(x) = \sum_{\eta \in \varphi} p_x(\eta) log_2 p_x(\eta) \tag{17}$$

The chance of the pixel x occurring is represented by p(x).

All of the ciphertexts in the database images had their entropy calculated. All gray image's absolute entropy is in the range[7.9974,7.9976,7.9969,7.9976,7.9971], which is extremely close to the ideal value of 8. As a result of the entropy measurements, it is clear that the cipher images have a high degree of randomness in their pixel values. Its encryption strength is resistant to typical attacks, in addition to the high entropy.

Table 7 shows the entropy findings of the proposed system as well as some of the existing schemes. The outcomes of the new scheme are almost equivalent to 8, which is significantly better than the results of the present scheme, as shown in table 7. As a result, the system can well withstand statistical analysis.

2) CORRELATION TEST

Plain-pixels images are highly correlated with each other, allowing them to form a meaningful shape. To create a secure cryptosystem cipher images must have the extremely least correlation between the pixels in such a way the cryptanalyst cannot extract any details. The encryption scheme's major goal is to distort the pixels so that there is the least amount of connection between neighboring pixels in the image's horizontal, diagonal, and vertical axes. An image encryption approach is resilient and well-being enough for security reasons if the ciphered image's correlation coefficient is around zero. The correlation coefficient of two adjacent pixels m and n is represented by the equation below.

$$R_{mn} = \frac{cov(m,n)}{\sqrt{D_m.D_n}} \tag{18}$$

$$cov(m,n) = \left\{ \frac{1}{X \times Y} \sum_{j=1}^{X \times Y} \left[\left(m_j - E(m) \right) \left(n_j - E(n) \right) \right] \right\} \tag{19}$$

$$E(x) = \frac{1}{X \times Y} \sum_{j=1}^{255} x_j \tag{20}$$

TABLE 7. Entropy analysis and comparison of proposed encryption scheme over different images with some of already existing cryptosystem.

Scheme	Images	Images size	entropy of plain images	entropy of encrypted images
Proposed				
	lena	256 × 256	7.4750	7.9974
	baboon	....	7.2004	7.9976
	peppers	....	7.5834	7.9969
	house	....	6.6323	7.9976
	cameraman	....	6.9083	7.9971
Ref. [6]				
	lena	256 × 256	....	7.9046
Ref. [9]				
	lena	256 × 256	......	7.9971
Ref. [36]				
	lena	256 × 256	6.4498	7.9975
	baboon	....	6.6962	7.9972
	peppers	....	6.6959	7.9971
Ref. [33]				
	lena	256 × 256	7.4750	7.9974
	cameraman	....	7.0097	7.9972
Ref. [34]				
	lena	256 × 256	....	7.9974
Ref. [35]				
	lena	256 × 256	....	7.9968
	cameraman	....	....	7.9904
	peppers	....	....	7.9961
	baboon	....	....	7.9971
Ref. [32]				
	lena	256 × 256	7.5755	7.9971
	cameraman	....	7.0701	7.9971
	peppers	....	7.5819	7.9968

Table 8 displays the experimental findings of the correlation test of different plain and cipher images along each channel. It is easy to see in this study that the correlation between two neighboring pixels of original images in the vertical, horizontal, and diagonal directions is nearly equal to 1. While the suggested scheme's correlation coefficient results in all directions of two neighboring pixels in encrypted images are approximately 0. Furthermore, in correspondence to some already current related literature, the correlation coefficient results suggest that the suggested encryption system is substantially more efficient and immune to statistical attacks (Figs.3,4 and 5).

3) HISTOGRAM TEST

If the histogram of the cipher image is consistently distributed, a cryptosystem can effectively resist statistical attacks. We ran this test on a number of images, and the results of a few of them are given in Fig. 6. The histogram of images after encryption using the suggested technique is uniformly distributed, as shown in Fig. 6, and thus the proposed security system satisfies the histogram requirement.

D. MEAN SQUARE ERROR (MSE) AND PEAK SIGNAL-TO -NOISE RATIO (PSNR)

Image compression quality is measured using the mean-square error (MSE) and peak signal-to-noise ratio (PSNR). The MSE is a measure of the peak error, whereas the PSNR is a measure of the cumulative squared error between the compressed and original image. The error is proportional to the MSE value. High MSE values indicate a significant difference between plain and encrypted photos, and low MSE values indicate a little difference between decrypted and plain images. PSNR, on the other hand, calculates an image's degree of accuracy. The lower the PSNR number, the greater the disparity between the plain and encrypted image. Furthermore, between the plain and decrypted images, the PSNR value is infinite. The following equations $(21 - 24)$ are defined for MSE and PSNR.

$$MSE_{PE} = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(p_{ij} - e_{ij}) \tag{21}$$

$$MSE_{PD} = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}(p_{ij} - d_{ij}) \tag{22}$$

$$PSNR_{PE} = 20log_{10}\frac{max(P)}{\sqrt{MSE_{PE}}} \tag{23}$$

$$PSNR_{PD} = 20log_{10}\frac{max(P)}{\sqrt{MSE_{PD}}} \tag{24}$$

where P is the plain image, E is the encrypted image, and D is the decrypted image and M, N and max(P) represent the image's height, width, and maximum feasible value, respectively. Table 9 presents the MSE and PSNR results, which

TABLE 8. **Correlation coefficient results of proposed encryption scheme over different images and comparison with some of already existing cryptosystem.**

Test Images	Images size	Horizontal correlation	Vertical correlation	Diagonal correlation
Proposed				
lena	256 × 256	0.9221	0.9476	0.8877
encrypted lena	....	-0.0012	-0.0014	0.0016
baboon	....	0.9113	0.8745	0.8482
encrypted baboon	....	0.0010	0.0010	-0.0013
peppers	....	0.9732	0.9757	0.9589
encrypted peppers	....	-0.0013	-0.0016	-0.0013
house	....	0.9808	0.9765	0.9584
encrypted house	....	-0.0014	-0.0017	0.0010
cameraman	....	0.9247	0.9623	0.9159
encrypted cameraman	....	-0.0010	0.0012	0.0012
Ref [33]				
lena	256 × 256	0.9379	0.9482	0.8802
encrypted lena	....	-0.0008	-0.0019	0.0016
Ref [34]				
baboon	....	....	....	......
encrypted baboon	256 × 256	0.0024	-0.0038	0.0019
Ref [6]				
lena	....	....	....	....
encrypted lena	256 × 256	0.0164	0.0324	-0.0098
Ref [35]				
lena	....	....	....	....
encrypted lena	256 × 256	-0.00058	0.0048	-0.0243
Ref [36]				
lena	....	....	....	....
encrypted lena	256 × 256	-0.0090	-0.0079	-0.0032
Ref [32]				
lena	256 × 256	0.9721	0.9739	0.9705
encrypted lena	....	-0.0029	-0.0017	0.0004
cameraman	....	0.9634	0.9732	0.9449
encrypted cameraman	....	0.0047	-0.0066	0.0031
peppers	....	0.9674	0.9710	0.9332
encrypted peppers	....	0.0021	0.0084	0.0007

reveal that there is a significant difference between plain and encrypted images for the proposed technique, but no difference between plain and decrypted images.

E. CHI-SQUARE TEST

The histogram analysis is used to visualize the pixels distribution of digital images. This gives image pixels a visual representation. The chi-square test can be used to interpret the uniformity of the pixels distribution numerically. It is calculated using the following formula:

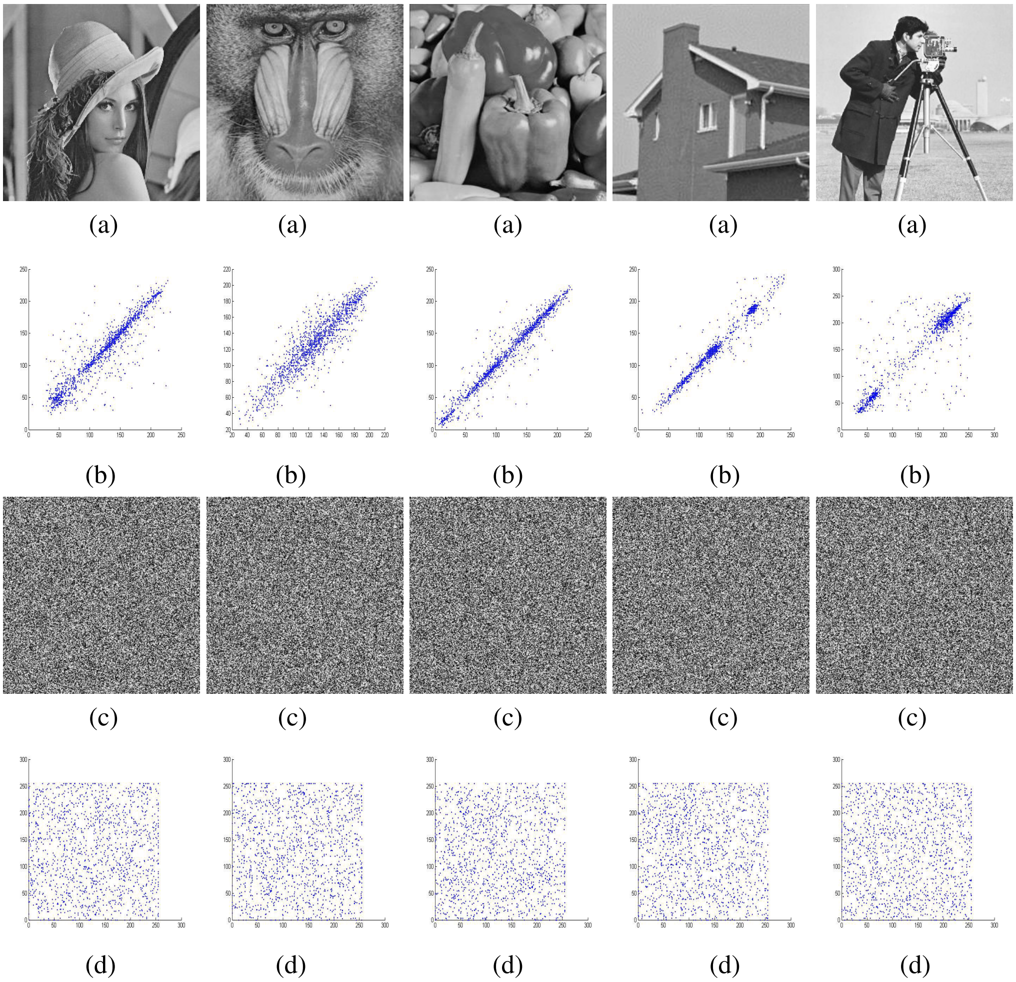
$$X^2 = \sum_{i=1}^{m} \frac{(ob(f_i) - ex(f_0))}{ex(f_0)} \tag{25}$$

$$ex(f_0) = \frac{(M \times N)}{256} \tag{26}$$

where $ob(f_i)$ represents the observed frequency i$(i = 0 to 255)$ and $ex(f_0)$ represents the estimated frequency. The chi-square test results for cipher images are shown in Table 10. According to the chi-square distribution table, $X^2_{255,0.01} = 311.570$ and $X^2_{255,0.05} = 294.1572$ indicate that the chi-square test hypothesis is accepted and a significant level for both values is 1% and 5% respectively. As a result of this, we can say that distribution of pixels is uniform.

F. COMPUTATIONAL COMPLEXITY

The number of bit operations necessary to complete the algorithm is the computational complexity of the scheme. The computational complexity of the suggested technique was explored in this section. The approach converts the images elements into the elliptic curve's points. As long as the image data is within a specified range, the technique maps each element of the image in constant time. As a result, the preprocessing will take $O(M \times N)$ bit operations to complete. In the same way, the substitution module was run in linear time. Because all of the algorithm's modules run in linear time, the suggested scheme's overall computational complexity is $O(M \times N)$ or linear time, where $M \times N$ is the plain image's dimension. The following is a comparison of the suggested encryption scheme's computational time complexities with those of other techniques [36]. All grayscale photos' sizes


(a) (a) (a) (a) (a)

(b) (b) (b) (b) (b)

(c) (c) (c) (c) (c)

(d) (d) (d) (d) (d)

FIGURE 3. **(a) plain image of lena, baboon, peppers, house and cameraman; where (b) Horizontal correlation of above plain images;(c) cipher images and (d) Horizontal correlation of above cipher images respectively.**

TABLE 9. **MSE, PSNR and comparison of proposed scheme over different images with already existing scheme.**

Images	MSE_{PE}	MSE_{PD}	$PSNR_{PE}$	$PSNR_{PD}$
Lena	7835.4	0	9.1902	∞
Baboon	6901.7	0	9.7412	∞
Pepper	8359.7	0	8.9089	∞
House	7720.3	0	9.2545	∞
Cameraman	11891.1	0	7.3786	∞
Ref. [6]				
Lena	40.2640	0	9.1244	∞
Ref. [36]				
Lena	7952.7	0	9.1812	∞
Baboon	7781.7	0	9.1572	∞
Pepper	7796.5	0	9.2681	∞
Cameraman	9504.7	0	8.2978	∞

are let M_1 and N_1. For a single round operation, the computational time complexity of generating the cross-coupled chaotic sequence is $O(M_x)$, where M_x is the maximum value of M_1 and N_1. The time complexity is $O(M_1 \times N_1)$ for the row-column permutation stage. The computational complexity of the diffusion operation of row column is $8(M_1 + N_1)$ resulting in an overall total computational time complexity of the encryption algorithm [36] of $O(M_x + 9(M_1 + N_1))$ which is nearly equivalent to the suggested algorithm.

VIII. COMPARISON AND DEBATE WITH OTHER ENCRYPTION METHODS

Comparison of our suggested encryption method to other current cryptosystems based on different mathematical

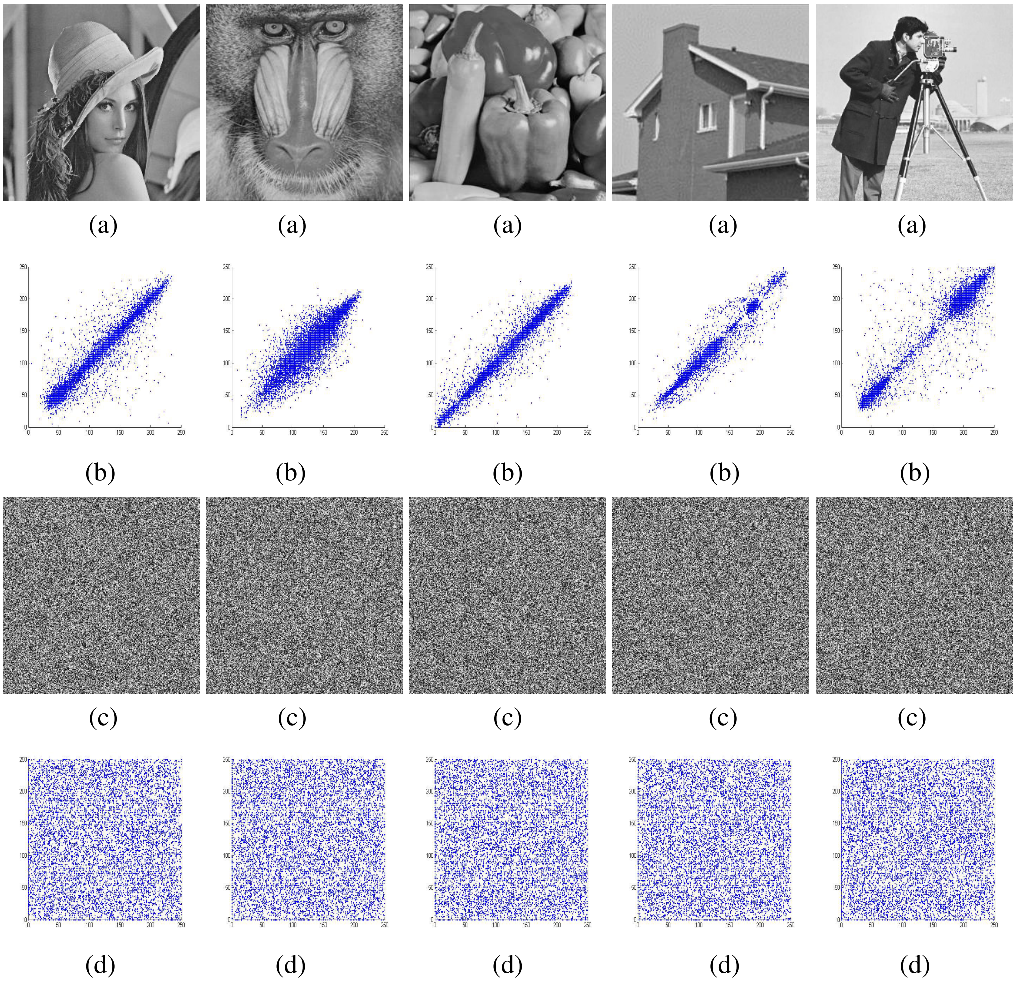


FIGURE 4. (a) plain image of lena, baboon, peppers, house and cameraman; where (b) Vertical correlation of above plain images;(c) cipher images and (d) Vertical correlation of above cipher images respectively.

TABLE 10. Result of Chi-square test.

Images				
Lena	Baboon	Pepper	House	Cameraman
X^2 Test				
234.1567	235.4812	236.1089	235.1402	236.0178
Result				
Success	Success	Success	Success	Success

structures. Structures like chaotic and dynamic-based image encryption [6] is presented in this subsection. First, apply the confusion step on each pixel and transforms each pixel value into a diffusion step. Apply burgers map on the image of size 256 × 256 to generate a sequence. Now apply this map to permute all rows and columns but this cipher image has not enough resistance against security analysis. The Logistic chaotic map is used to create a diffusion mechanism to improve resilience to the above-mentioned attacks. To generate dynamic s-boxes logistic map is iterated. Now divide a permuted image into 16 × 16 blocks and substitute each block via dynamic s-box. Finally, these substituted blocks are combined into one matrix to get cipher images. While in our proposed image encryption scheme we first obtained dynamic s-boxes through two different maps mentioned in subsection (5.1). We have a gray-scale image of size 256 × 256 convert this image into 16 × 16 blocks and apply any one of the above-proposed s-box that's generated with two different techniques to perform the substitution on each block of the image. Now pick another proposed s-box

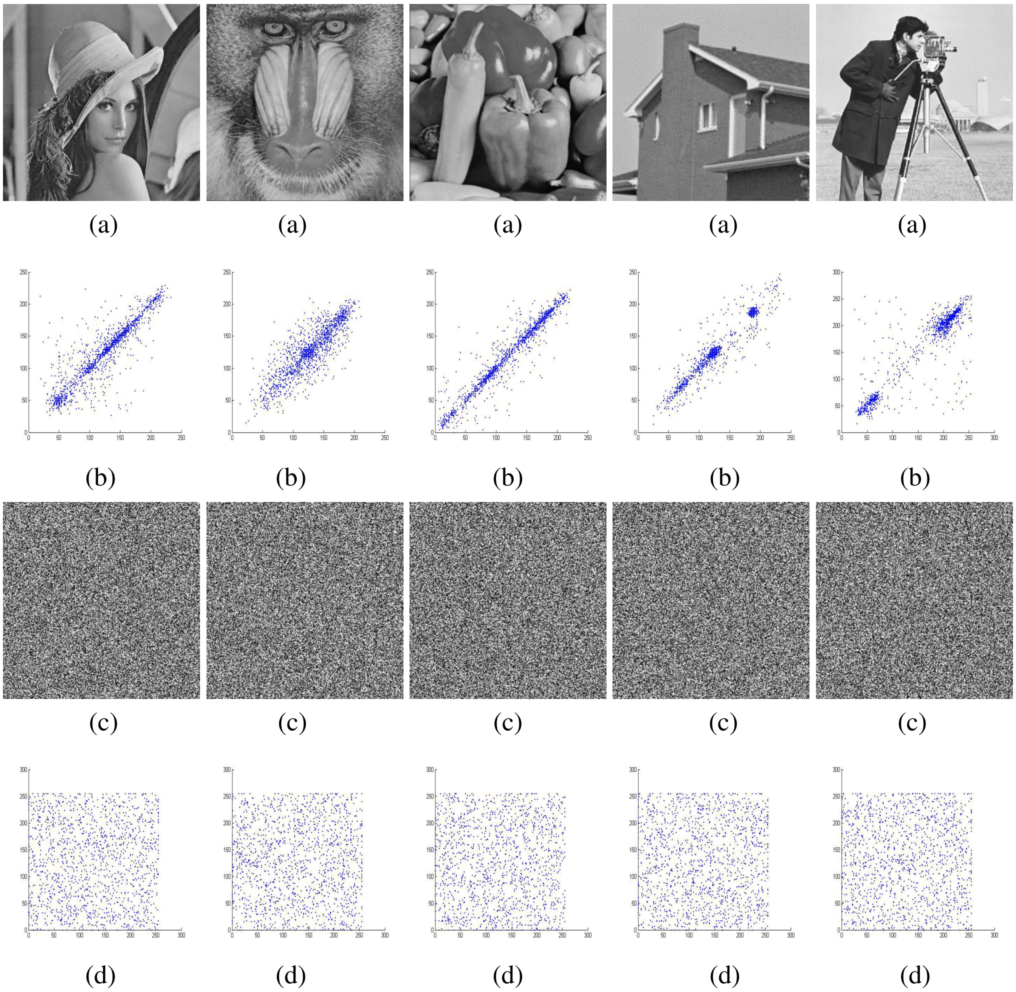
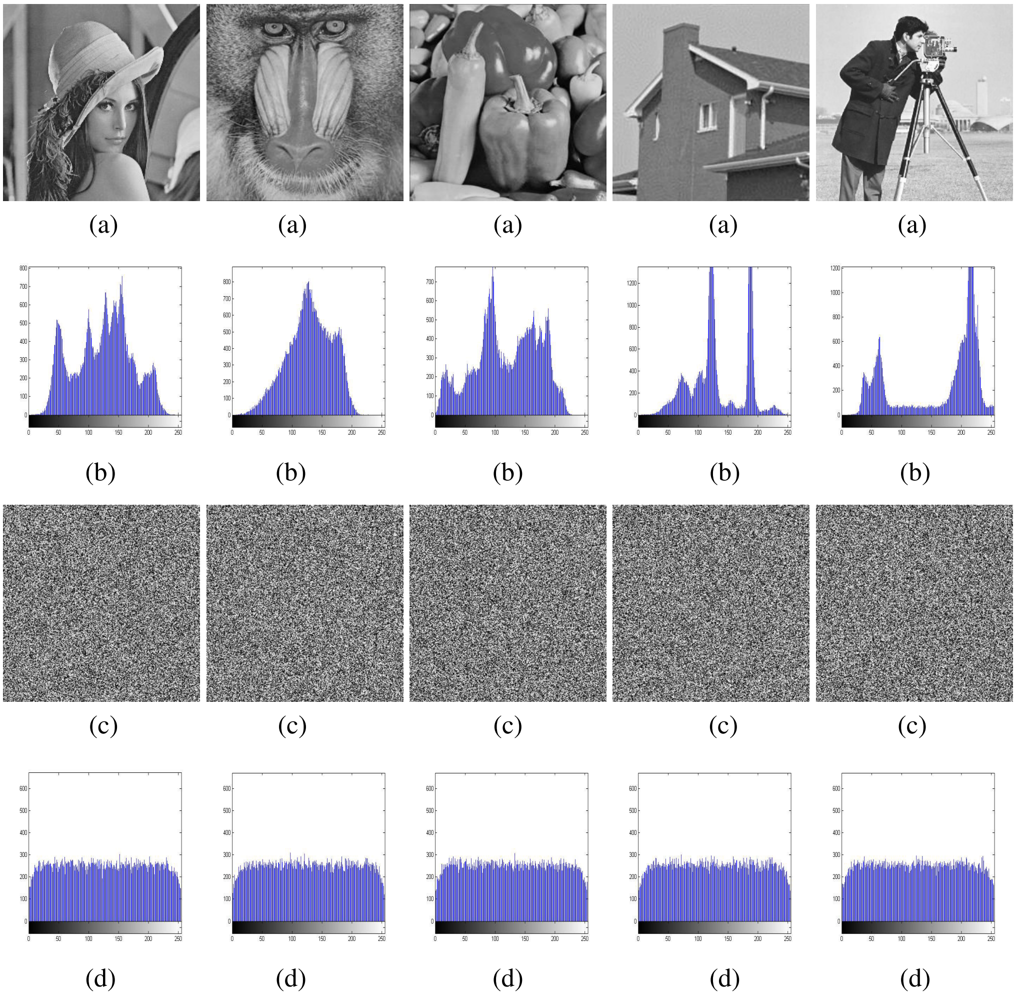


FIGURE 5. (a) plain image of lena, baboon, peppers, house and cameraman; where (b) Diagonal correlation of above plain images;(c) cipher images and (d) Diagonal correlation of above cipher images respectively.

as a key and execute a mathematical operation which is defined in eq. (12) in the proposed image technique to get cipher image entries. For practical applications, the speed of encryption systems is an important consideration. Our proposed technique takes less execution time than the technique defined in [6]. Image encryption schemes based on chaos [1], [2], [4], [9] and [14] which are extremely sophisticated and memory intensive. Similarly, the methodology in [6], [36] and [41] are based on numerous S-boxes and a random no. of increments of different S-boxes, which increases the computational time, but the suggested approach has less computing timing complexity than the current methodology in [[6], [36], [41]].

The majority of researchers have attempted to combine improved methodologies in order to eliminate the flaws in past work. In this paper, we investigate and compare the proposed cryptosystem to several previous studies, such as ECCs ([6], [9], [32]–[36]) Entropy, correlation, NPCR, UACI, PSNR, MSE and other evaluation metrics are used to make the comparison. The well-known encryption algorithms are used to assess all of these criteria on the digitized lena,baboon,house images. Tables [7,8,6,9] show the results of the above-mentioned tests' analysis. The tables [6,7,8,9] clearly show that the suggested system outperforms the specified encryption approaches in terms of security. Similarly, the examination of each channel's correlation coefficient scores in all three directions outperforms the other correlation coefficient scores of various current encryption methods in the table [36]. This demonstrates that the suggested image encryption technique is capable of breaking the correlation between neighboring pixels in the original image in a variety of ways. As a result, the suggested technique is very resistant to standard statistical attacks. Furthermore, in comparison to the most current existing cryptosystems available in ([6], [32]–[36]), the proposed encryption scheme is preferable for security application reasons because it is endowed with a strong dynamic S-box in terms of non-linearity. Finally, the studies show that the suggested method's diffusion property is surprisingly much superior than methods reported



(a) (a) (a) (a) (a)

(b) (b) (b) (b) (b)

(c) (c) (c) (c) (c)

(d) (d) (d) (d) (d)

FIGURE 6. (a) plain image of lena, baboon, peppers, house and cameraman; where (b) Histogram of above plain images;(c) cipher images and (d) Histogram of above cipher images respectively.

TABLE 11. Time execution values.

	Proposed sheme	Proposed sheme	Ref. [36]	Ref. [36]
Prime	4093	16381	4093	16381
A	9	1	9	1
B	7	17	7	17
Preprocessing time	0.107	2.3987	0.110	2.4567
Postprocessing time	0.000001	0.000002	0.000002	0.000002

in [[6], [32]–[36]] in terms of entropy and NPCR security analysis. The proposed encryption algorithm was compared to other recent encryption algorithms are discussed below.

i. The proposed algorithm's entropy information is approximately equivalent to 8, indicating that the proposed cryptosystem increases the randomness of pixel values. When compared to other cryptosystems ([6], [9], [32]–[36]) have less randomness given in table 6.

ii. The value of the correlation analysis can be determined by considering the correlation analysis. The coefficients of correlation are almost 0, indicating that the suggested cryptosystem outperforms when compared to ([32]– [36]) Other cryptographic algorithms which is discuss in table 7.

iii. Table 5 shows that the findings of the proposed cryptosystem's differential attack analysis (NPCR and UACI) are superior to those of other good existing algorithms ([6], [9], [32]–[36]).

iv. Our method X^2 test analysis result in table 10 is lower and higher than the chi-square value of [36], indicating that the suggested work has a high gray scale uniformity.

v. Table 11 shows the time complexity of Our proposed scheme are comparatively less than the recent existing encryption method in [36]. This prove our scheme need minimum time for execution.

vi. Table 9 shows that plain and cipher images have high MSE and low PSNR when compared to other recently developed encryption techniques in ([6], [36]), which ensure that the decryption process is completed without information loss.

IX. CONCLUSION

To secure the layout of the digital image, this work provides an asymmetric key cryptosystem primarily based on an EC. We constructed S-box using elliptic curves in the first section of this article. In comparison to the known ECC S-boxes, the newly discovered S-boxes offer improved statistical and algebraic properties. For the newly constructed S-boxes, we put both x and y-coordinates in two different maps and followed by modulo 256 operation. In the newly constructed image cryptosystem, the plain gray-scale image divides into 16×16 blocks and each block contains a 16×16 matrix. While using one of the S-box (substitution-box), which has a high nonlinearity value and meets the extreme avalanche conditions, the message image confirmed higher randomness and immunity against different attacks. The other one dynamic S-box provides a key role and creates more confusion in the substituted image by using the proposed image algorithm. Different analyses are used to examine the scheme's security strength, and the results show that the suggested scheme is secure enough to withstand entropy, brute force, and differential attacks. In comparison to other existing image encryption systems, the suggested technique has proved to be resistant to malicious attacks and to have a low time complexity.

Finding a way to encrypt a color image using only one cycle of the suggested scheme except increasing processing complexity will be interesting future work.

REFERENCES

[1] A. Belazi, A. A. A. El-Latif, A.-V. Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," *Opt. Lasers Eng.*, vol. 88, pp. 37–50, Jan. 2017.

[2] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons Fractals*, vol. 38, no. 1, pp. 213–220, Oct. 2008.

[3] S. Pallavi Indrakanti and P. S. Avadhani, "Permutation based image encryption technique," *Int. J. Comput. Appl.*, vol. 28, no. 8, pp. 45–47, Aug. 2011.

[4] G. Jakimoski and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 2, pp. 163–169, Feb. 2001.

[5] L. Li, B. Abd-El-Atty, S. Elseuofi, B. A. El-Rahiem, and A. A. A. El-Latif, "Quaternion and multiple chaotic systems based pseudo-random number generator," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–5.

[6] A. U. Rehman, J. S. Khan, J. Ahmad, and S. O. Hwang, "A new image encryption scheme based on dynamic S-boxes and chaotic maps," *3D Res.*, vol. 7, no. 1, p. 7, Mar. 2016.

[7] A. A. A. El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, pp. 92–102, Aug. 2019.

[8] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, pp. 118–131, Mar. 2020.

[9] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Inf. Sci.*, vol. 547, pp. 1154–1169, Feb. 2021.

[10] G. Ye and X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neurocomputing*, vol. 251, pp. 45–53, Aug. 2017.

[11] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, Berlin, Germany: Springer, Aug. 1985, pp. 417–426.

[12] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[13] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Des., Codes Cryptogr.*, vol. 19, nos. 2–3, pp. 173–193, Mar. 2000.

[14] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and s8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. 2018.

[15] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*. Boca Raton, FL, USA: CRC Press, 2008.

[16] J. Daemen and V. Rijmen, "The Rijndael block cipher: AES proposal," in *Proc. 1st Candidate Conf. (AeS1)*, Mar. 1999, pp. 343–348.

[17] S. Murphy and M. J. Robshaw, "Essential algebraic structure within the AES," in *Proc. Annu. Int. Cryptol. Conf.*, Berlin, Germany: Springer, Aug. 2002, pp. 1–16.

[18] J. Rosenthal, "A polynomial description of the Rijndael advanced encryption standard," *J. Algebra Appl.*, vol. 2, no. 2, pp. 223–236, Jun. 2003.

[19] S. Behnia, A. Akhavan, A. Akhshani, and A. Samsudin, "Image encryption based on the Jacobian elliptic maps," *J. Syst. Softw.*, vol. 86, no. 9, pp. 2429–2438, Sep. 2013.

[20] F. Amounas and E. El Kinani, "Fast mapping method based on matrix approach for elliptic curve cryptography," *Int. J. Inf. Netw. Secur.*, vol. 1, no. 2, pp. 54–59, 2012.

[21] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*. Boca Raton, FL, USA: CRC Press, 2008.

[22] M. Khan and T. Shah, "A novel image encryption technique based on Hénon chaotic map and S_8 symmetric group," *Neural Comput. Appl.*, vol. 25, nos. 7–8, pp. 1717–1722, Dec. 2014.

[23] I. Hussain, T. Shah, M. Gondal, W. Khan, and H. Mahmood, "A group theoretic approach to construct cryptographically strong substitution boxes," *Neural Comput. Appl.*, vol. 23, no. 1, pp. 97–104, 2013.

[24] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Proc. Workshop Theory Appl. Cryptograph. Techn.*, Berlin, Germany: Springer, Apr. 1989, pp. 549–562.

[25] M. Khan, T. Shah, and S. Batool, "Construction of S-box based on chaotic Boolean functions and its application in image encryption," *Neural Comput. Appl.*, vol. 27, no. 3, pp. 677–685, 2016.

[26] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Workshop Theory Appl. Cryptograph. Techn.*, Berlin, Germany: Springer, May 1993, pp. 386–397.

[27] A. F. Weister and S. E. Tavares, "On the design of S-boxes," in *Proc. Adv. Cryptol.-(CRYPTO)*, 1986, pp. 523–534.

[28] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, 1991.

[29] C. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, "Image encryption process based on chaotic synchronization phenomena," *Signal Process.*, vol. 93, no. 5, pp. 1328–1340, May 2013.

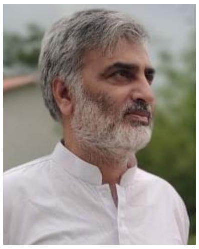
[30] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *J. Syst. Softw.*, vol. 85, no. 2, pp. 290–299, 2012.

[31] X. Wang, C. Liu, and D. Xu, "Image encryption scheme using chaos and simulated annealing algorithm," *Nonlinear Dyn.*, vol. 84, no. 3, pp. 1417–1429, 2016.

[32] X. Wang, X. Zhu, and Y. Zhang, "An image encryption algorithm based on Josephus traversing and mixed chaotic map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018.

[33] K. A. K. Patro, B. Acharya, and V. Nath, "Secure, lossless, and noise-resistive image encryption using chaos, hyper-chaos, and DNA sequence operation," *IETE Tech. Rev.*, vol. 37, no. 3, pp. 223–245, 2019.
[34] K. A. K. Patro and B. Acharya, "A novel multi-dimensional multiple image encryption technique," *Multimedia Tools Appl.*, vol. 79, nos. 19–20, pp. 12959–12994, May 2020.
[35] S. Mozaffari, "Parallel image encryption with bitplane decomposition and genetic algorithm," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 25799–25819, Oct. 2018.
[36] I. Khalid, S. S. Jamal, T. Shah, D. Shah, and M. M. Hazzazi, "A novel scheme of image encryption based on elliptic curves isomorphism and substitution boxes," *IEEE Access*, vol. 9, pp. 77798–77810, 2021.
[37] Y. Wang, L. Yang, M. Li, and S. Song, "A method for designing S-box based on chaotic neural network," in *Proc. 6th Int. Conf. Natural Comput.*, Aug. 2010, pp. 1033–1037.
[38] M. Ahmad, D. Bhatia, and Y. Hassan, "A novel ant colony optimization based scheme for substitution box design," *Proc. Comput. Sci.*, vol. 57, pp. 572–580, Jan. 2015.
[39] A. Belazi and A. A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Optik*, vol. 130, pp. 1438–1444, Feb. 2017.
[40] D. Lambić, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2407–2413, Mar. 2017.
[41] M. I. Haider, A. Ali, D. Shah, and T. Shah, "Block cipher's nonlinear component design by elliptic curves: An image encryption application," *Multimedia Tools Appl.*, vol. 80, no. 3, pp. 4693–4718, Jan. 2021.
[42] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2009.
[43] N. Siddiqui, A. Naseer, and M. Ehatisham-ul-Haq, "A novel scheme of substitution-box design based on modified Pascal's triangle and elliptic curve," *Wireless Pers. Commun.*, vol. 116, no. 4, pp. 3015–3030, Feb. 2021.
[44] A. Zahid, M. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Entropy*, vol. 21, no. 3, p. 245, Mar. 2019.
[45] A. Alghafis, N. Munir, and M. Khan, "An encryption scheme based on chaotic Rabinovich–Fabrikant system and s_8 confusion component," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 7967–7985, Feb. 2021.
[46] A. Zahid and M. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, Mar. 2019.
[47] A. H. Zahid, H. Rashid, M. M. U. Shaban, S. Ahmad, E. Ahmed, M. T. Amjad, M. A. T. Baig, M. J. Arshad, M. N. Tariq, M. W. Tariq, M. A. Zafar, and A. Basit, "Dynamic S-box design using a novel square polynomial transformation and permutation," *IEEE Access*, vol. 9, pp. 82390–82401, 2021.
[48] L. C. Nizam Chew and E. S. Ismail, "S-box construction based on linear fractional transformation and permutation function," *Symmetry*, vol. 12, no. 5, p. 826, May 2020.
[49] A. H. Zahid, A. M. Iliyasu, M. Ahmad, M. M. U. Shaban, M. J. Arshad, H. S. Alhadawi, and A. A. A. El-Latif, "A novel construction of dynamic S-box with high nonlinearity using heuristic evolution," *IEEE Access*, vol. 9, pp. 67797–67812, 2021.
[50] A. H. Zahid, L. Tawalbeh, M. Ahmad, A. Alkhayyat, M. T. Hassan, A. Manzoor, and A. K. Farhan, "Efficient dynamic S-box generation using linear trigonometric transformation for security applications," *IEEE Access*, vol. 9, pp. 98460–98475, 2021.
[51] A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," *IEEE Access*, vol. 8, pp. 150326–150340, 2020.

MUHAMMAD RAMZAN is currently pursuing the Ph.D. degree with the Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan. He has been working an elliptic curve cryptography, since 2018.



TARIQ SHAH received the Ph.D. degree in mathematics from the University of Bucharest, Romania, in 2000. He is currently a Professor with the Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan. His research interests include commutative algebra, non-associative algebra, and error-correcting codes and cryptography.

MOHAMMAD MAZYAD HAZZAZI received the Ph.D. degree in mathematics from the University of Sussex, Brighton, U.K. He is currently working as an Assistant Professor with the Department of Mathematics, King Khalid University, Abha, Saudi Arabia. His research interests include coding theory, cryptography, finite geometry, algebraic geometry, and group theory.

AMER ALJAEDI received the B.Sc. degree from King Saud University, Saudi Arabia, in 2007, the M.Sc. degree in information systems security from the Concordia University of Edmonton, Canada, in 2011, and the Ph.D. degree in security engineering from the Computer Science Department, Colorado University, Colorado Springs, USA, in 2018. He is currently an Assistant Professor with the College of Computing and Information Technology, University of Tabuk. Before that, he was a Senior Research Member with the Cybersecurity Laboratory, Colorado University. His research interests include software-defined networking, network traffic control and monitoring, cloud computing, and cybersecurity. He received multiple research awards from UCCS and SACM for his outstanding research papers.

ADEL R. ALHARBI received the Bachelor of Science degree in computer science from Qassim University, Saudi Arabia, in 2008, and the two Master of Science degrees in security engineering and computer engineering and the Doctor of Philosophy degree in computer engineering from Southern Methodist University, Texas, Dallas, USA, in 2013, 2015, and 2017, respectively. He has been a Faculty Staff Member at the College of Computing and Information Technology, University of Tabuk, Saudi Arabia, since 2009. He acquired several academic certificates and published many scientific papers. His research interests include mobile and smart device applications, biometric, security, networking, and machine learning techniques.