IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 23 December 2023, accepted 5 January 2024, date of publication 15 January 2024, date of current version 23 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3354170

RESEARCH ARTICLE

An Innovative Feasible Approach for Multi-Media Security Using Both Chaotic and Elliptic Curve Structures

TANVEER QAYYUM[1], TARIQ SHAH[1], ALI YAHYA HUMMDI[2], AMER ALJAEDI[3], AND ZAID BASSFAR[4]

[1]Department of Mathematics, Quaid-i-Azam University, Islamabad 45320, Pakistan
[2]Department of Mathematics, College of Science, King Khalid University, Abha 61421, Saudi Arabia
[3]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
[4]Department of Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia

Corresponding author: Tanveer Qayyum (tanveerqayyum@math.qau.edu.pk)

This work was supported by the Deanship of Scientific Research at King Khalid University through Large Group Research Project under Grant RGP2/552/44.

ABSTRACT Researchers concentrate on data security using cryptography, using different approaches to protect confidential data, such as digital images holding private information. They use cryptography techniques, frequently using elliptic curves and chaotic structures for secure transmission. This paper introduces a novel technique for constructing S-boxes and their application in color image encryption. The utilization of discrete chaotic maps and elliptic curves results in low computational complexity, which is crucial for high-speed communication systems. The generation of S-boxes is based on elliptic curves over prime fields and discrete chaotic maps. The color image encryption scheme involves permutation, substitution, and bit-wise XOR operations of key with the color image's corresponding substituted channels. The resistance of the newly constructed s-boxes against common attacks, such as linear, differential, and algebraic attacks, is analyzed by evaluating their non-linearity, linear approximation probability, differential approximation probability, bit avalanche criterion, and bit independence criterion. The encrypted images have strong resistance against statistical and differential attacks. Experimental results demonstrate that the newly constructed scheme can efficiently generate numerous distinct, uncorrelated, and secure S-boxes, outperforming some well-known existing techniques. The non-linearity of the proposed s-box is 107.5 and the entropy of the ciphered image of Baboon is 7.9989. The security analysis indicates that the color-encrypted image offers fast and higher protection against attacks, making it suitable for real-time applications with high security requirements.

INDEX TERMS Elliptic curve, finite prime field, image encryption, logistic map, prey-predator map, S-box.

I. INTRODUCTION

In recent decades, data security has garnered significant attention from researchers. The attainment of data security is made possible through the use of cryptography. Cryptographers have put forth various methods for safeguarding private data. The primary objective of cryptographic techniques is to conceal confidential data from adversaries who seek to alter the original message or collect confidential information for their own purposes. Digital images also contain sensitive data, including military, medical, and government secrets. To bolster security, a combination of cryptography, steganography, and watermarking techniques is employed. Multiple cryptographic techniques, founded on elliptic curves and chaotic structures, are harnessed to ensure the secure transmission of digital images [1], [2], [3], [4], [5], [6], [7], [8], [9].

The associate editor coordinating the review of this manuscript and approving it for publication was S. K. Hafizul Islam.

A. RELATED WORK

In 1949, Shannon demonstrated that if a cryptosystem can generate a specific amount of data confusion and diffusion,

it is considered secure [4]. Substitution boxes (S-boxes) stand as the primary nonlinear elements responsible for inducing confusion and diffusion in many cryptographic systems. The quality of an S-box is gauged by its resilience against linear, algebraic, and differential crypt-analysis [1], [3], [8], [14]. Parameters like non-linearity (NL), linear approximation probability (LP), differential approximation probability (DP), bit independence criterion (BIC), and strict avalanche criteria (SAC) collectively measure an S-box's resistance against well-known attacks. The Advanced Encryption Standard (AES), initially introduced by Rijndael, gained acceptance from the National Institute of Standards and Technology (NIST) and has maintained its status as the most popular and secure cryptosystem for the past two decades. The S-box, a pivotal nonlinear element in AES security, adds complexity to the encryption process. AES employs a static S-box. The extensive use of the AES encryption algorithm has prompted cryptographers to delve into the mathematical and implementation aspects of the S-box. A straightforward mathematical representation of an AES S-box is provided in [16] and [23]. In 2003, Rosenthal [57], delved deeper into the nonlinear aspects of AES by examining its polynomial representation. The research revealed that the AES S-box, within its permutation polynomial, comprises only a few non-zero terms. Further studies by Hussain et al. [13] and Azam [58] highlighted that using a single S-box for both encryption and decryption in a cryptosystem reduces security, particularly for highly correlated data. Dynamic S-boxes have demonstrated an ability to enhance the security of cryptosystems when compared to static S-boxes (Kazlauskas [59]; Mohan and Manjula [60]; Jeyanthi and Katiyar [61]; Gnanasekar and Maram [62]). Rahnama et al. [63] provided evidence that static S-boxes exhibit lower resistance against data analysis attacks. In subkey attacks, where the inverse of an S-box is known, subkeys are derived using an inverse subbyte. Dynamic S-boxes, with their added complexity, offer better protection against data analysis attacks than static S-boxes (Kazlauskas [59]; Mohan and Manjula [60]; Jeyanthi and Katiyar [61]; Gnanasekar and Maram [62]; Agarwal et al. [64]). Dynamic S-boxes find frequent application in various image encryption algorithms, providing heightened security. For security reasons, many cryptographers have crafted S-boxes using diverse mathematical techniques, including differential equations and algebraic methods. Numerous robust cryptosystems have been developed using elliptic curves (EC). In 1986, Miller, V., was the first to incorporate EC into cryptography. A novel EC-based cryptosystem is presented in [17], surpassing the existing Diffie-Hellman protocol in speed. Neal, K. [65] introduced an elliptic cryptosystem over a finite field. Neal, K., Alfred, M., and Scott, V. (2009) proposed leveraging discrete logarithmic problems to create a swift and highly secure cryptosystem. A comparison of elliptic curve cryptography (ECC) with RSA is outlined in [18], showcasing ECC's superiority in terms of key size and security over RSA. The advantages and applications of ECC are detailed in [24]. EC structures also play a vital role in generating pseudorandom numbers, a crucial component in many cryptosystems, as discussed in the literature [19], [20], [21], [22]. The chaotic-based image encryption algorithm depends upon constraints; in [48], these limitations are overcome by constructing a two-dimensional enhanced logistic modular map (2D-ELMM) and then developing a chaotic image encryption method (CIES-DVEM) that relies on vector-level operations and 2D-ELMM. In [49], an excellent block permutation and chaos-based color image compression-encryption technique is introduced. An encrypted image is produced using a series of cryptographic operations, including permutation, dynamic DNA-level diffusion, DNA encoding, chaotic sequence generation, and circular shifting depending on these sequences and hash values is discussed in [50]. In today's digital landscape, vast amounts of classified data are transmitted across the internet and various social media platforms. Ensuring the security of these communication channels is of paramount importance. Digital images frequently contain confidential data, with millions transmitted daily via both secure and insecure channels. Encrypting this sensitive data guarantees that adversaries cannot decipher the original content. The three primary methods for securing image data involve permutation (pixel scrambling), substitution (pixel replacement), or a combination of both, collectively referred to as the SPN (substitution and permutation) network.

B. MOTIVATION

The primary motivation, knowledge gaps and novelty of this script are described as follows:

(1) Elliptic curves are widely used in data protection. Chaos-based cryptosystems are also employed to construct substitution boxes and encrypt images. The motivation behind our work is rooted in the utilization of elliptic curve structures to derive a set of points residing on the curve. These points are subsequently employed for purposes of confusion and diffusion within the proposed cryptosystem. Using chaotic structures, we can map these points onto elliptic curves to create substitution boxes.

(2) Furthermore, the conventional transformation of elliptic curve points into (x, y) coordinates has an impact on algorithmic complexity, necessitating a constructive and efficient conversion process.

C. OUR CONTRIBUTION

The main contribution of this article are summarized as follows:

(1) There are numerous cryptosystems based on algebraic, elliptic, and chaotic structures for encrypting digital images. Image encryption grounded in chaotic structures offers enhanced security due to its high sensitivity, control parameters, pseudo-random number generation, data mixing, and other factors, all contributing to

data protection [44], [45], [46]. However, a drawback of chaotic-based cryptosystems is their vulnerability to statistical attacks, as noted by Li et al. in [47]. Conversely, elliptic curve and chaotic structure-based cryptosystems exhibit high resistance to differential statistical attacks.

(2) In our proposed work, we introduce a hybrid structure for image encryption that is both effective and robust against cryptographic attacks, leveraging elliptic curves and chaotic structures. In this study, we present a novel technique for generating S-boxes using elliptic curves over prime fields and chaotic mappings. The ordered pairs of EC's x and y coordinates are employed in the proposed S-box technique under the modulo operation of 256. After constructing the S-boxes, we introduce a fresh approach to encrypting color images, aiming to achieve the highest level of security.

D. ORGANIZATION OF THE PAPER

The article's remaining sections are organized as follows: Preliminaries are included in Section II. We go into great depth on the suggested algorithm for creating S-boxes in Section III. The security evaluations of the proposed S-boxes are discussed in Section IV. The newly suggested image encryption algorithm is discussed in Section V. The security analysis of encrypted images, including key space, entropy, information entropy, histogram analysis, correlation analysis, peak-to-noise analysis, occlusion attacks, and the computational complexity of the proposed algorithm, is discussed in Section VI. In Section VII, we give a comprehensive comparison and discussion of the proposed algorithm with some of the best-known existing algorithms. Furthermore, Section VIII focuses on concluding remarks and some recommendations for future research directions.

II. PRELIMINARIES

A. ELLIPTIC CURVE OVER FINITE PRIME FIELD

Let E be an EC over the finite prime field F_p, where p is the prime number and has p elements. There is a finite prime field, F_p, for each value of p. An elliptic curve E over a prime field F_p is given by:

$$E(F_p) = \begin{pmatrix} \{(x, y) \in F_p^2 | (y^2 = x^3 + ax + b, mod\ p) \\ a, b, x, y \in F_p\} \bigcup \{\infty\} \end{pmatrix} \tag{2.1}$$

with $\triangle = 4a^3 + 27b^2 \neq 0 \bmod p$, is the discriminant of the elliptic curve and is the point at infinity. Let $Q_1 = (x_1, y_1)$ and $Q_2 = (x_2, y_2)$ be two points lies on EC $E(F_p)$ such that $Q_1 \neq Q_2$. The addition of Q_1 and Q_2 is the point Q_3 lies on the same EC $E(F_p)$ i.e, $Q_1 \oplus Q_2 = Q_3$. where the coordinates of point $Q_3 = (x_3, y_3)$ can be calculated as:

$$x_3 = (m^2 - x_1 - x_2)\, mod(p), \tag{2.2}$$

$$y_3 = m(x_1 - x_3) - y_1\, mod(p) \tag{2.3}$$

and

$$m = \frac{y_2 - y_1}{x_2 - x_1}\, mod(p). \tag{2.4}$$

Let $Q = (x, y)$ be a point on $E(F_p)$, then double of Q is $2Q = Q \oplus Q = (x', y')$ is given by

$$x' = m^2 - 2x\ mod(p), y' = m(x - x') - y\ mod(p) \tag{2.5}$$

where

$$m = \frac{3x^2 + a}{2y}\, mod(p) \tag{2.6}$$

and

$$Q \oplus \{\infty\} = Q. \tag{2.7}$$

The formula $\#(E(F_p))$ indicates how many points are total on the EC over F_p. In [13], the order of $\#(E(F_p))$, for any elliptic curve E over F_p we have by a theorem of Hasse's

$$|\#E(F_p) - p - 1| \leq 2\sqrt{p}. \tag{2.8}$$

B. PREY-PREDATOR MAP

The interaction between a prey species (x) and a predator species (y) was described by a set of differential equations created by Lotka in 1920. These equations, which Volterra discovered in 1926, are referred to as the Lotka-Volterra equations. The equations are alternatively shown as a discrete map, which is

$$(x, y) \longrightarrow \big[\big((1 + r) - ay\big)x, (-c + bx)y\big] \tag{2.9}$$

A constant $(1 + r)$ resulting from the species itself less a term proportionate to the number of predators is how the map's first component reflects the growth rate of prey. The number of prey minus a term c that is brought on by the predator species itself also has an inverse relationship with the growth rate of the predator. Every constant is taken to be positive. Maynard Smith first unveiled the two-parameter family prey-predator map in 1996.

$$(x, y) \longrightarrow [((1 + r) - rx - ay)x, axy] \tag{2.10}$$

where $r > 0$, $a > 0$. This chaotic map creates diffusion and confusion. We can use this map for security purposes because it offers better security as compared with other chaotic structures.

C. LOGISTIC MAP

We'll talk about one-parameter chaotic maps that have been used in studies of population dynamics. The chaotic maps feature characteristics of diffusion and confusion. The logistic map, a non-linear polynomial dynamic map of degree 2, one such map, which is provided by:

$$n \longrightarrow \chi_r n(1 - n), \tag{2.11}$$

where $r > 0, n > 0$.

III. PROPOSED S-BOX CONSTRUCTION SCHEME

In this section, we discuss the construction of an S-box based on elliptic curves combined with chaotic maps. In [1], S-boxes are constructed over elliptic curves by finding their points. In [27], S-boxes are designed based on chaotic structures. However, we demonstrate a innovative approach for constructing S-boxes using chaotic maps and the Weierstrass normal form of an elliptic curve over a finite prime field. The proposed technique is able to produce up to $p-1$, the number of cryptographically strong S-boxes and among them, we choose the S-boxes with reasonable non-linearity. Let us consider a non-singular elliptic curve $E_p(a,b)$ over F_p.

$$E_p(a,b) \; : \; y^2 = x^3 + ax + b \; mod \; (p), \tag{3.1}$$

where the domain parameters belong to F_p, the array of points lying on the EC can be determined using the ordered pair (x, y). Several methods exist for creating an s-box based on the points of an elliptic curve. Additionally, discrete chaotic maps are employed to construct S-boxes through teaching-based optimization and permutation composition [1], [27], [28]. We propose a new, simple, and efficient technique based on EC points and the use of chaotic maps for permuting the EC points. When selecting a prime number p on the elliptic curve, we have at most $p-1$ points. Consider a chaotic map, such as a prey-predator model, expressed as $(x,y) \longrightarrow [((1+r)-rx-ay)x, axy]$, where $r > 0$ and $a > 0$. The parameter a in the prey-predator model is the same as in the elliptic curve, and the parameter r is a non-negative integer. To permute the points of the elliptic curve into another set of points, choose the value of r. For each value of r, a new set of points is obtained. Utilize an inner product space for the new set of points to yield a series of numbers belonging to F_p, and then apply the discrete logistic model $n \longrightarrow \chi_r n(1-n)$, where the parameter r has the same value as chosen in the prey-predator map. The entire proposed method comprises six steps, outlined below:

(1) Consider an EC over the finite prime field F_p. Choosing two distinct integers from the field F_p, where p is a large prime number. The value of the prime number p is selected in such a way that the EC has at least 256 distinct points that lies on it.

(2) The EC $E_p(a,b)$ is depicted by the following equation:

$$E_p(a,b) \; : \; y^2 = x^3 + ax + b \; mod \; (p). \tag{3.2}$$

(3) The set of all x,y coordinates of $E_p(a,b)$ is represented by $E^p_{x,y}(a,b)$.

(4) Using the x,y-coordinates of $E_p(a,b)$ in the prey-predator map. We obtained a new set of ordered pairs say (k,l).

$$(x,y) \longrightarrow [((1+r)-rx-ay)x, axy] = (k,l). \tag{3.3}$$

(5) Find the inner product of ordered pairs obtained from the prey-predator map and applying the modulus function p on the resultant points.

$$< k,l >= k.l = n \tag{3.4}$$

(6) Using the new set of points n in the logistic map, apply modulo 256 on the resultant points to get $E^{p,256}_{r,n}(a,b)$. Due to this modulo operation, the set of points is restricted to the range $0-255$.

$$n \longrightarrow \chi_r n(1-n) \tag{3.5}$$

(7) Finally, a S-box Ⓢ^a_b is generated by choosing 256 distinct integers of $E^{p,256}_{r,n}(a,b)$. By applying the suggested approach to various elliptic curves, numerous S-boxes are produced. For example, the S-box Ⓢ^{2520}_{13} obtained from the $E^{3571}_{97}(2520,13)$ is given in Table 1. The flowchart of the suggested method for building substitution boxes is depicted in FIGURE 1.

IV. S-BOXES SECURITY ANALYSIS

A. NON-LINEARITY (NL)

In [9], it is discussed how non-linearity (NL) works. For a certain S-box, Ⓢ

$$\text{Ⓢ} : GF(2^8) \longrightarrow GF(2^8),$$

The shortest distance between $\vartheta(\text{Ⓢ})$ of Ⓢ and the affine function over the Galois field is used to calculate NL.

$$\vartheta(\text{Ⓢ}) = min_{\sigma,\varsigma,\xi} \neq x \in GF(2^8) \mid \sigma.\text{Ⓢ}(x) \neq \varsigma.x \oplus \xi, \tag{4.1}$$

where $\sigma \in GF(2^8)$, $\varsigma \in GF(2)$, $\xi \in GF(2^8)\backslash 0$ and '.' denote dot product over GF(2).

A S-box's optimal non-linearity value is 120 over the GF(2^8). Better confusion in the data can be produced by an S-box with high NL. It is not necessary for an S-box to have an ideal NL to be capable of satisfying the other cryptographic tests. However, if a S-box satisfied the security tests with high NL is the topic of special interest. Here, we measured the NL of the S-box Ⓢ^{2917}_{97} generated from the suggested technique. The average value of NL of the S-box Ⓢ^{2917}_{97} is 107.50.

B. LINEAR APPROXIMATION PROBABILITY (LAP)

The idea of linear approximation probability is introduced in [10] for a S-box. The LAP of a given S-box is calculated by measuring the maximum value LAP(Ⓢ) of the similarity between input and output bits. Mathematically, the expression for LAP is given below:

$$W(\gamma,\delta) = \#\{x \in GF(2^8) \mid \gamma.x = \delta.\text{Ⓢ}(x)\} \tag{4.2}$$

$$LAP(\text{Ⓢ}) = \frac{1}{2^n}\{max_{\gamma,\delta}|W(\gamma,\delta)|\} \tag{4.3}$$

where $\gamma \in GF(2^8)$, $\delta \in GF(2^8)$ and '.' denotes the dot product over GF(2^8). The quality of an S-box depends on its resistance against approximation attacks. A S-box has a low LAP value. The S-box is highly resistant against approximation attacks. The maximum value of LAP of the proposed S-box Ⓢ^{2917}_{97} is 0.1484.

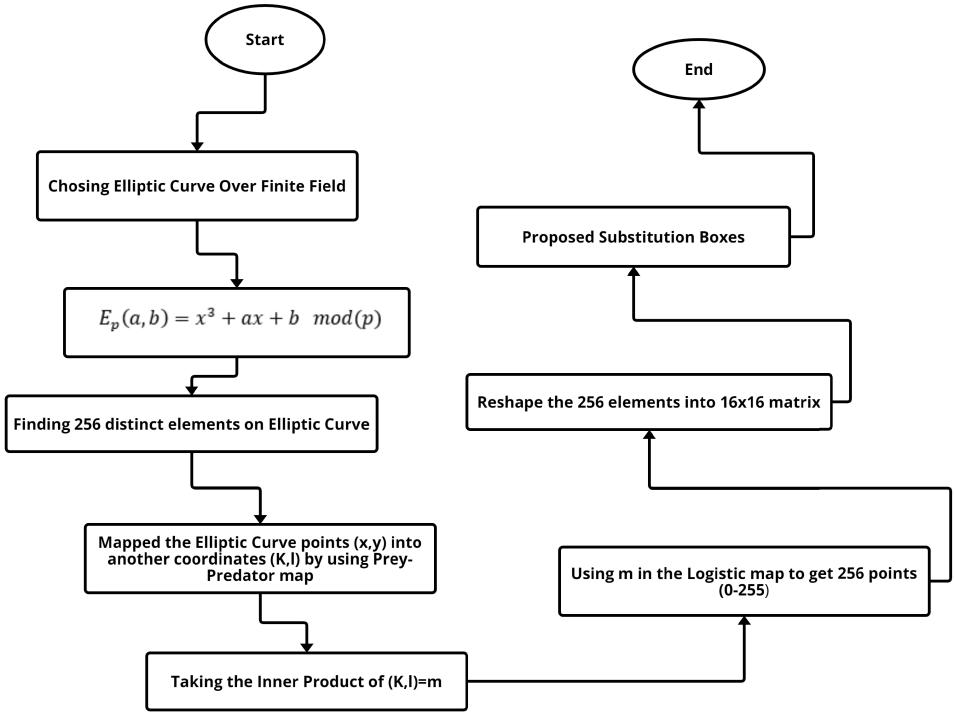


FIGURE 1. Graphical overview of the proposed method for S-box creation.

TABLE 1. S-box $Ⓢ_{13}^{2520}$ generated over the EC E_{97}^{3571} (2520, 13).

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

C. DIFFERENTIAL APPROXIMATION PROBABILITY (DAP)

The concept of differential approximation probability is introduced by Biham and Shamir in [12]. In this test, the likelihood of the impact of a specific input bit difference on the difference in the output bits was measured. DAP is represented mathematically for a S-box Ⓢ as:

$$N(\triangle x, \triangle y) = \#\{x \in GF(2^8) : Ⓢ(x \oplus \triangle x) = Ⓢ(x) \oplus \triangle y\} \tag{4.4}$$

$$DAP(Ⓢ) = \frac{1}{2^8}\{max_{\triangle x, \triangle y}(|N(\triangle x, \triangle y)|)\}, \tag{4.5}$$

where $\triangle x, \triangle y \in GF(2^8)$ and "$\oplus$" denote the bit-wise addition over $GF(2^8)$. An S-box has great strength against differential attacks if it has a low value of DAP(Ⓢ). The DAP of $Ⓢ_{97}^{2917}$ is 0.03906.

D. STRICT AVALANCHE CRITERION (SAC)

In [34], the concept of the strict avalanche criterion (SAC) is introduced. The SAC test is used to find the strength of an S-box by measuring its diffusion-creation ability. The SAC of an S-box is a measurement of how a tiny change in the input can result in a large change in the output, and thus, an avalanche of changes in [11]. The SAC of a S-box Ⓢ is

TABLE 2. SAC of $Ⓢ_{97}^{2917}$.

0.546875	0.515625	0.515625	0.484375	0.531250	0.484375	0.500000	0.515625
0.437500	0.562500	0.437500	0.468750	0.484375	0.500000	0.531250	0.546875
0.515625	0.562500	0.500000	0.531250	0.546875	0.453125	0.593750	0.578125
0.453125	0.531250	0.484375	0.500000	0.546875	0.500000	0.531250	0.437500
0.484375	0.562500	0.531250	0.500000	0.421875	0.531250	0.468750	0.531250
0.437500	0.500000	0.468750	0.484375	0.531250	0.500000	0.546875	0.562500
0.484375	0.500000	0.515625	0.468750	0.500000	0.484375	0.468750	0.468750
0.500000	0.546875	0.437500	0.531250	0.500000	0.546875	0.500000	0.468750

represented by a square matrix of order 8 i.e $K(Ⓢ) = [n_{ij}]$ and calculated with the boolean function $Ⓢ_i$, where $1 \leq i \leq 8$ the entries of the 8×8 matrix are funded by Table 2:

$$n_{ij} = \frac{1}{2^8}\{\sum_{x \in GF(2^8)} v(Ⓢ_i(x \oplus \eta_j) \oplus_i (x))\}, \tag{4.6}$$

where $\eta_j \in GF(2^8)$ and the number of non-zero bits is denoted by $v(w)$ in vector w. The average value of SAC of the newly constructed S-box $Ⓢ_{97}^{2917}$ is 0.50.

E. BIT INDEPENDENCE CRITERION (BIC)

The quality of a S-box is measured by another important test known as the bit independence criterion (BIC). According to [11], this test evaluates the interdependence between a pair of output bits when an input bit is inverted. When a suggested S-box's BIC value is close to 0.5, it is deemed strong resistance. We run the BIC test on the newly constructed S-boxes and compare the results to those of known S-boxes. The GF(2^8) field displays the BIC values for the suggested S-boxes as a matrix along with a boolean function of dimension 8 given in Table 3. The average value of BIC-SAC of the newly constructed S-box $Ⓢ_{97}^{2917}$ is 0.50.

V. PROPOSED IMAGE ENCRYPTION SCHEME

In this section, we introduce a novel image encryption technique. Let's consider a basic color image with dimensions of $I_M \times_N \times 3$, where M and N represent the image's width and height, respectively. The three color components in this scheme correspond to the red channel (R), green channel (G), and blue channel (B), each with a size of $M \times N$. In the proposed method, we treat each of these three channels (R, G, and B) as individual grayscale images, encrypting them independently.The proposed image encryption scheme consists of the following steps, outlined below:

(1) Firstly, we consider an unaltered color image with dimensions of M rows and N columns, encompassing a total of $M \times N \times 3$ pixels. These three layers correspond to the color image's primary components: red, green, and blue, respectively. To encrypt the color image, we read the image and then separate the red channel, green channel, and blue channel. We work separately on these three channels for encryption. Here, we generate a sequence of pseudo-numbers using an elliptic curve. These random numbers are generated using the structure of an elliptic curve.

$$E_{a,b}^{p} : y^2 = x^3 + ax + b\,(mod\ p) \tag{5.1}$$

The random number sequence is based on the domain parameters of the EC. After choosing the values of parameters a and b, we select a prime number p. Using the form of x- and y-coordinates, we obtain points on the EC. In this scheme, we vary the values of y-coordinates by applying the modulus function until we get the required sequence. Firstly, we generate a sequence of 512 elements that are unique and random in order. This can be achieved by using the general structure of the elliptic curve, choosing the values of parameters a and b, giving p a very large value, and applying the modulus function of 256 in such a way that all the numbers lie within the range $[0, 255]$. Since the prime number is large, there are more than 256 points on the elliptic curve, and they are in a random order. All of this is done using the software Matlab, and by applying the Matlab command 'unique' with the option 'stable', we obtained a set of points in the range $[0, 255]$ in a random order. A set of random numbers in the range $[1, 256]$ can be obtained by adding 1 to the random sequence ranging from 0 to 255. After obtaining the random sequence, we apply the permutation to each of the color channels. The red, green, and blue channels become permuted red channels (P_R), permuted green channels (P_G), and permuted blue channels (P_B). The scrambled picture after the permutation is shown in FIGURE 3.

(2) The substitution component of image encryption is a crucial element in ensuring the confidentiality and security of digital images. This component involves the replacement of pixel values or color intensities with new values based on a predefined algorithm or key. By substituting pixel values, the original content of the image becomes scrambled and indecipherable to unauthorized parties. The substitution process can be achieved through various techniques such as permutation, bit manipulation, or lookup tables. The effectiveness of the substitution component lies in its capability to transform the image into a form that is resistant to attacks and unauthorized access, ensuring the privacy and integrity of sensitive visual information. The construction of S-boxes is already discussed in Section *III*. The technique already explained in Section *III* is used to

TABLE 3. BIC of $\circledS_{97}^{2917}$.

—-	0.503906	0.498047	0.501953	0.498047	0.494141	0.494141	0.511719
0.503906	—-	0.525391	0.482422	0.505859	0.500000	0.537109	0.500000
0.498047	0.525391	—-	0.486328	0.527344	0.517578	0.501953	0.494141
0.501953	0.482422	0.486328	—-	0.521484	0.468750	0.496094	0.490234
0.498047	0.505859	0.527344	0.521484	—-	0.496094	0.501953	0.503906
0.494141	0.500000	0.517578	0.468750	0.496094	—-	0.482422	0.498047
0.494141	0.537109	0.501953	0.496094	0.501953	0.482422	—-	0.466797
0.511719	0.500000	0.494141	0.490234	0.503906	0.498047	0.466797	—-

generate the substitution box (S-box) in the proposed system. The generated substitution boxes have good cryptographic properties. In this scheme, we used three S-boxes as a substitution component for permuted red, green, and blue channels, respectively (the procedure is the same as in AES). After substitution, the substituted red, green, and blue components can be represented as S_R, S_G and S_B. The substituted picture is shown in FIGURE 3.

(3) Pseudorandom number generators (PRNGs), true random number generators (TRNGs), and hybrid random number generators (PRNGs) are the three categories of random number generators. Pseudorandom number generators (PRNGs) are used in cryptography for a wide range of security applications, such as encryption and protocols. Random numbers play a crucial role in creating diffusion in image encryption algorithms. In order to make it harder for unauthorized parties to understand the original material, diffusion is a procedure that makes sure the encryption is distributed uniformly throughout the image. In this part, we create PRNs using the logistic map's chaotic representation. A mathematical function called the logistic map produces a series of integers that seem random. In several applications, including picture encryption, it is frequently employed as a chaotic system to produce pseudo-random integers. The following equation defines the logistic map:

$$M_n + 1 = rM_n(1 - M_n), \tag{5.2}$$

where M_n represents the current value in the sequence, $M_n + 1$ is the next value in the sequence, and r is a constant parameter that determines the behavior of the map. Using the logistic map, one can produce a string of random numbers; an initial value (M_0) is chosen within a specific range, and the equation is iteratively applied to generate subsequent values. These values can then be scaled or transformed to fit the desired range or precision. The logistic map reveals chaos for specific r values, leading to a sequence of numbers that appears random. The fact that these numbers are deterministic and reproducible if the initial value and parameter r are known, however, makes it clear that they are not genuinely random. In image encryption, the logistic map can be used as a source of randomness to determine the substitution values for pixel encryption. By applying the logistic map to the pixel values or their positions, the encryption algorithm can introduce randomness and diffusion, preventing unauthorized parties from deciphering the encrypted image. It is worth mentioning that while the logistic map can generate pseudo-random numbers, it may not provide the same level of randomness and security as cryptographic random number generators (CSPRNGs) specifically designed for encryption purposes. Therefore, it is important to carefully evaluate the security requirements of the image encryption system and consider using established cryptographic algorithms and random number generators for robust security. After the generation of random numbers, one can use these numbers as a key. This key was bit-mapped with the substituted channels separately, i.e., substituted red, green, and blue channels. After this, the encrypted red, green, and blue channels are received. We obtain the whole encrypted image of the test plain image by combining all these encrypted channels, as shown in FIGURE 3. The flowchart of the overall suggested image encryption scheme is shown in FIGURE 2.

VI. SECURITY ANALYSIS OF ENCRYPTED IMAGE

A. KEY SPACE ANALYSIS

In the context of image encryption and decryption schemes, the key plays a central role. Researchers employ key search attacks to deepen their understanding of encryption and decryption systems. When the key space is extensive, attempts to break the encryption through brute-force methods are likely to be ineffective. A cryptosystem is considered secure if it possesses a vast key space. A larger key space implies a stronger encryption method because it makes it computationally impossible for attackers to conduct exhaustive searches and successfully crack the encryption. A cryptosystem is deemed secure if the number of possible key combinations is greater than or equal to 2^{128}. In our proposed technique, we used elliptic curves and chaotic maps for the secret keys. In order to encrypt the image, we used three sets of keys. The first key, which generates random numbers used for permutation, uses three parameters (a_1, b_1, p_1) of at least 10 bits in length. Therefore, 2^{30} is the total precision. In the substitution step, we apply three s-boxes to the red, green, and blue channels of the plain image separately. These three S-boxes use nine parameters:

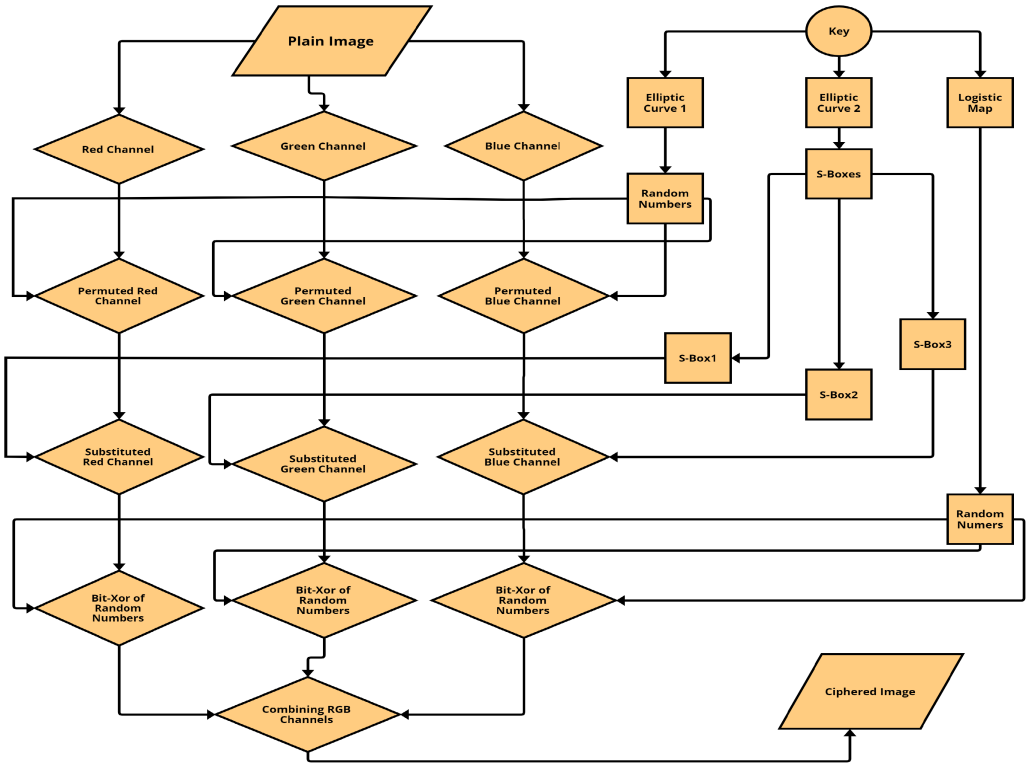


FIGURE 2. The proposed image encryption scheme's flowchart.

$(a_2, b_2, p_2, a_3, b_3, p_3, a_4, b_4, p_4)$, each of which consists of 10 bits. So, 2^{90} is the total precision outcomes in the substitution keys. The third key, which is used for bit-xor operation and is generated by the logistic map, uses two parameters (x_0, r). The key space of a one-dimensional logistics map is 2^{53}. The total key space for the encryption is $2^{30} \times 2^{90} \times 2^{53} = 2^{173}$, the number of possible combinations of the secret key exceeds 2^{128}, which is employed in the first, second, and third steps of the proposed scheme. Therefore, the suggested strategy incorporates a large key space to provide effective defense against brute-force attacks.

B. HISTOGRAM ANALYSIS

Histograms, which graphically display the distribution of pixel intensities within an image, are essential for both image encryption and decryption. A balanced histogram in the encrypted image is preferred in image encryption, as it signifies effective security. Data integrity is ensured during decryption by maintaining a consistent histogram between the encrypted and decrypted images. In encrypted images, a flat histogram indicates unpredictability and contributes to strong encryption. The reliability and security of image encryption and decryption procedures are further enhanced by using histogram analysis to evaluate the resilience of an encryption scheme against statistical attacks. The histogram analysis of the suggested encryption algorithm is depicted in FIGURE 4.

C. ENTROPY ANALYSIS

Entropy analysis is used to assess the degree of randomness in a ciphered image. For an encrypted image, the optimal entropy value should be 8. The entropy of an image is calculated using the mathematical formula provided below:

$$E(I) = -\sum_{\iota=0}^{q-1}\sum_{\jmath=0}^{q-1} p(\iota, \jmath) log_a p(\iota, \jmath). \tag{6.1}$$

Entropy $E(I)$ is determined using equation (2), where "a" denotes the log's base and the possibility of a pixel in a color image is shown by $p(\iota, \jmath)$. The ciphered image's entropy needs to be high to withstand attacks. According to our technique, the ciphered image's entropy is provided in Table 4. When compared to several other existing schemes, which we compared below, the ciphered images of the proposed technique have good entropy. As a result, the suggested encryption method offers a good defense against statistical attacks.

D. INFORMATION ENTROPY ANALYSIS

Information entropy quantifies the statistical uncertainty of the newly suggested scheme. It is calculated using the following mathematical expression:

$$J(n) = -\sum_{j=1}^{n} p(n_j) \log_2 p(n_j) \tag{6.2}$$

Here, 'n' stands for distinctive random variables, 'J(n)' represents information entropy, and '$p(n_j)$' denotes the

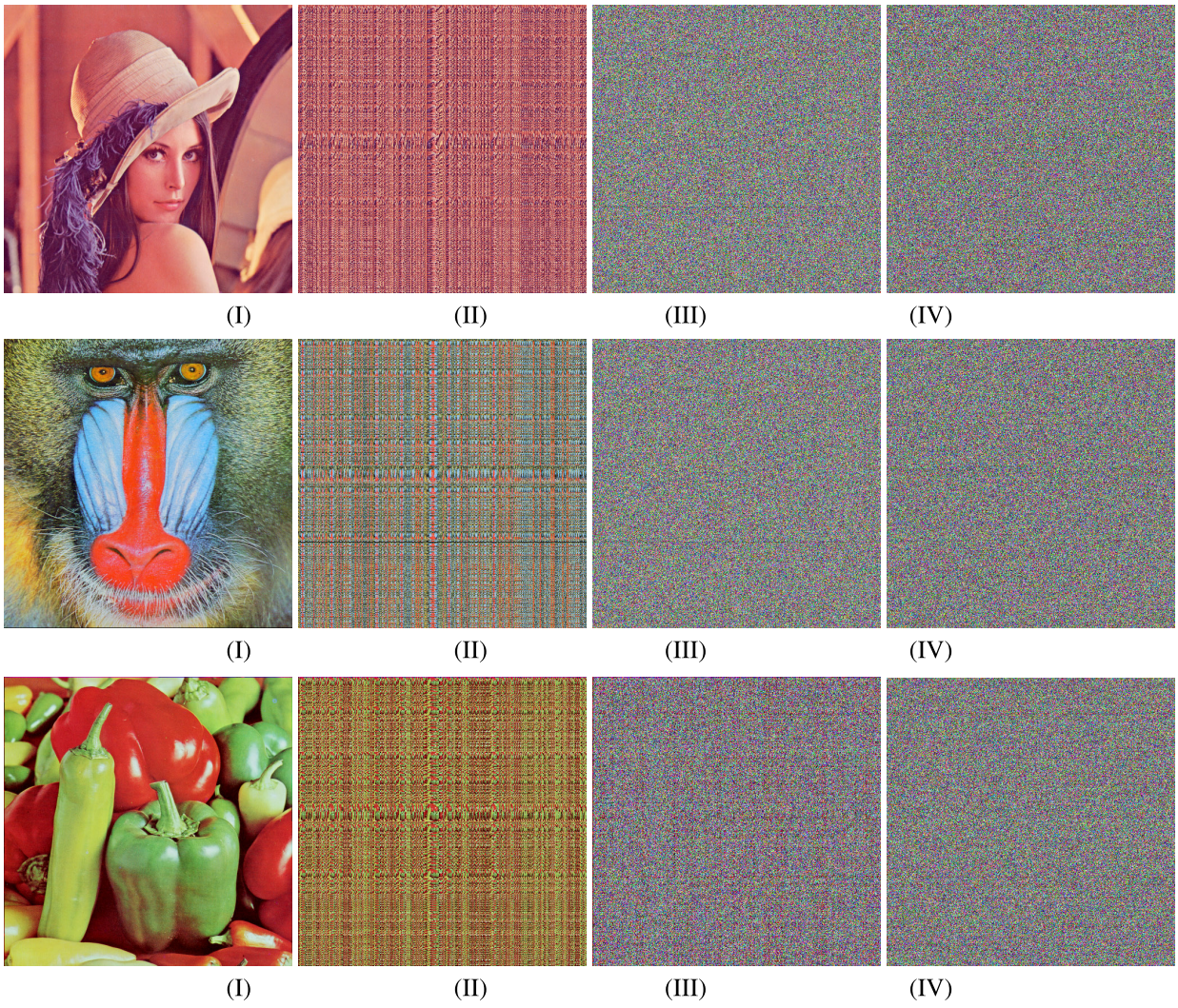


FIGURE 3. Unencrypted and encrypted images: (I) The unencrypted images of lena, baboon, and peppers;(II) The permuted images of lena, baboon, and pepper;(III) The substituted images of lena, baboon and pepper(IV) The encrypted images of lena, baboon and pepper.

TABLE 4. Entropy results.

Test Images	Images of size	Cipher Images
Lena	512×512	7.9985
Baboon	512×512	7.9989
Pepper	512×512	7.9971
Ref. [39] Lena	512×512	7.9927
Ref. [40] Lena	512×512	7.9952
Ref. [41] Lena	512×515	7.9978
Ref. [42] Lena	512×515	7.9971
Ref. [43] Lena	512×515	7.9974

probability of 'n_j'. The randomness in altered images is calculated through entropy. Entropy measures the strength of the encryption technique, revealing that the method may produce extremely unpredictable pixel patterns in encrypted images. The entropy of altered images should be 8. Table 5 lists the entropy analysis of the red, blue, and green components of the plain image and their corresponding encrypted image. The experimental results reveal that the entropy of the encrypted images is very close to the ideal value of 8, up to one hundred percent.

E. CORRELATION

Every image we see in our daily lives is made up of pixels. These pixels are related to one another in numerous directions, such as the horizontal, vertical, and diagonal directions. If there is little connection between the encrypted pixels in an image, it is said to be well encrypted. The 2000 pixel values of the image are randomly selected for correlation analysis, and FIGURES 5 & 6 demonstrate the relationship between these pixels in the horizontal, vertical, and diagonal directions. Here, we identify the comparison of the encrypted image's pixel values with those of the

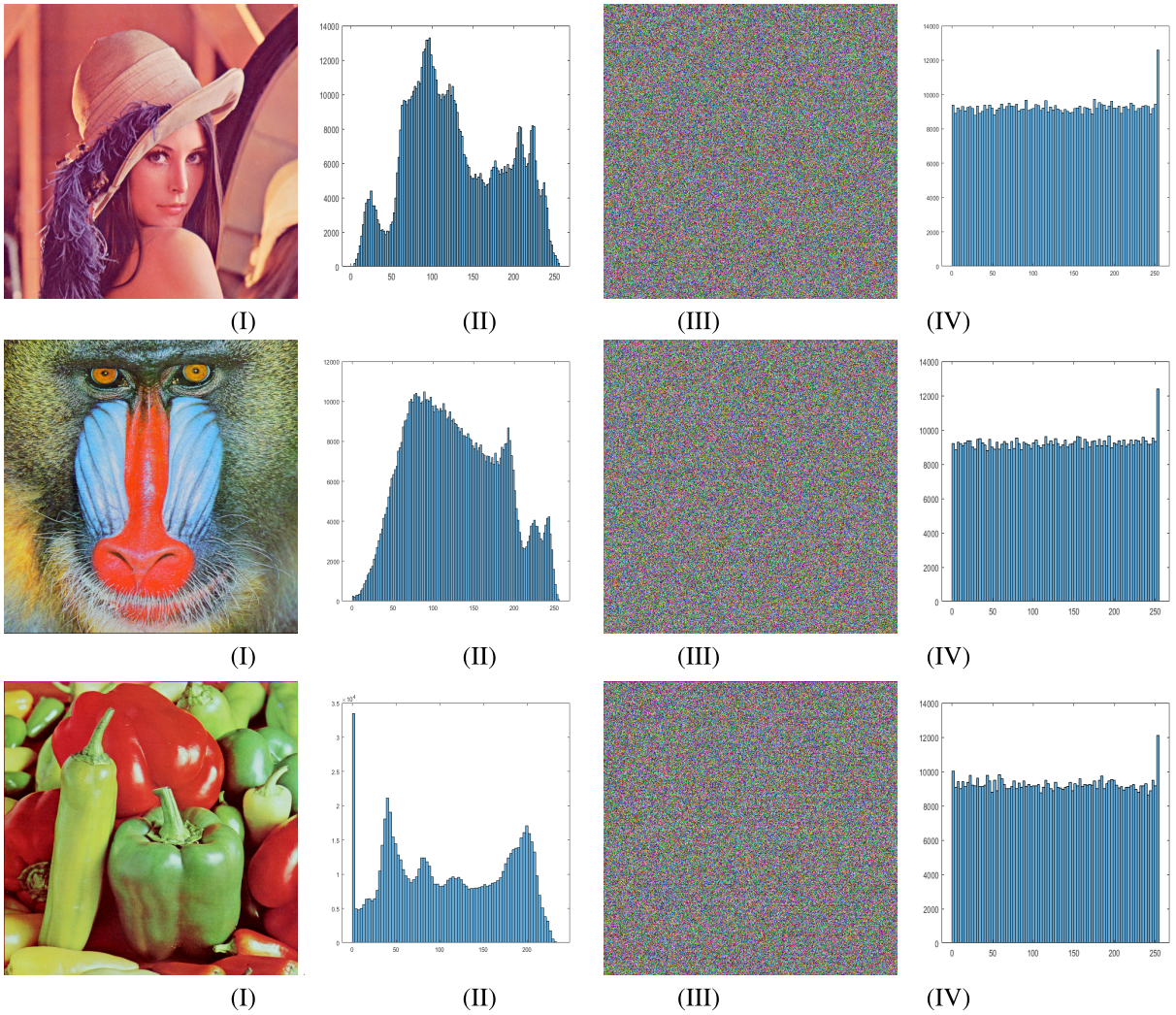


FIGURE 4. Histogram of the original RGB images and ciphered images: (I) The plain RGB images of lena, baboon and pepper; (II) The Histogram of the original images of lena, baboon and pepper; (III) The ciphered images of lena, baboon and pepper; (IV) The histogram of ciphered images of lena, baboon and pepper.

TABLE 5. Information entropy results.

Proposed Scheme	Images	Plain Image R	Plain Image G	Plain Image B	Ciphered Image R	Ciphered Image G	Ciphered Image B
	Lena(512×512)	7.2531	7.5940	6.9684	7.9970	7.9982	7.9964
	Baboon(512×512)	7.7067	7.4744	7.7522	7.9987	7.9981	7.9981
	Pepper(512×512)	7.3388	7.4963	7.0583	7.9965	7.9954	7.9949
	Lena(256×256)	7.3301	7.6231	7.1317	7.9986	7.9978	7.9981
	Baboon(256×256)	7.6942	7.4637	7.7443	7.9970	7.9971	7.9981
	Pepper(256×256)	7.3905	7.6023	7.1277	7.9975	7.9976	7.9973
Ref. [54]	Lena(256×256)	7.7317	7.7864	7.6481	7.9892	7.9902	7.9896
Ref. [55]	Lena(256×256)	7.2325	7.5683	6.9176	7.9967	7.9964	7.9943
Ref. [56]	Lena(256×256)	—-	—-	—-	7.9973	7.9973	7.9971

original image, compare them, and demonstrate how our cryptosystem causes confusion in the original image's pixel setting. An analysis of the encrypted photos' correlations is given in Table 6.

F. DIFFERENTIAL ATTACKS

The NPCR means that the number of pixels changes when a byte of the unencrypted image is changed. NPCR analysis calculated the pixel change rate. An image is well encrypted if the NPCR value of the ciphered image is approximately 100%, and the proposed cryptosystem has good resistance against known plain text attacks. The UACI measured the average intensity of dissimilarity between the original image and the ciphered image. If the value of UACI analysis rises, a cryptosystem will be well protected against differential attacks. If the value of UACI analysis rises, the proposed cryptosystem's resistance to differential attacks will be good. A mathematical illustration of the NPCR and UACI analyses

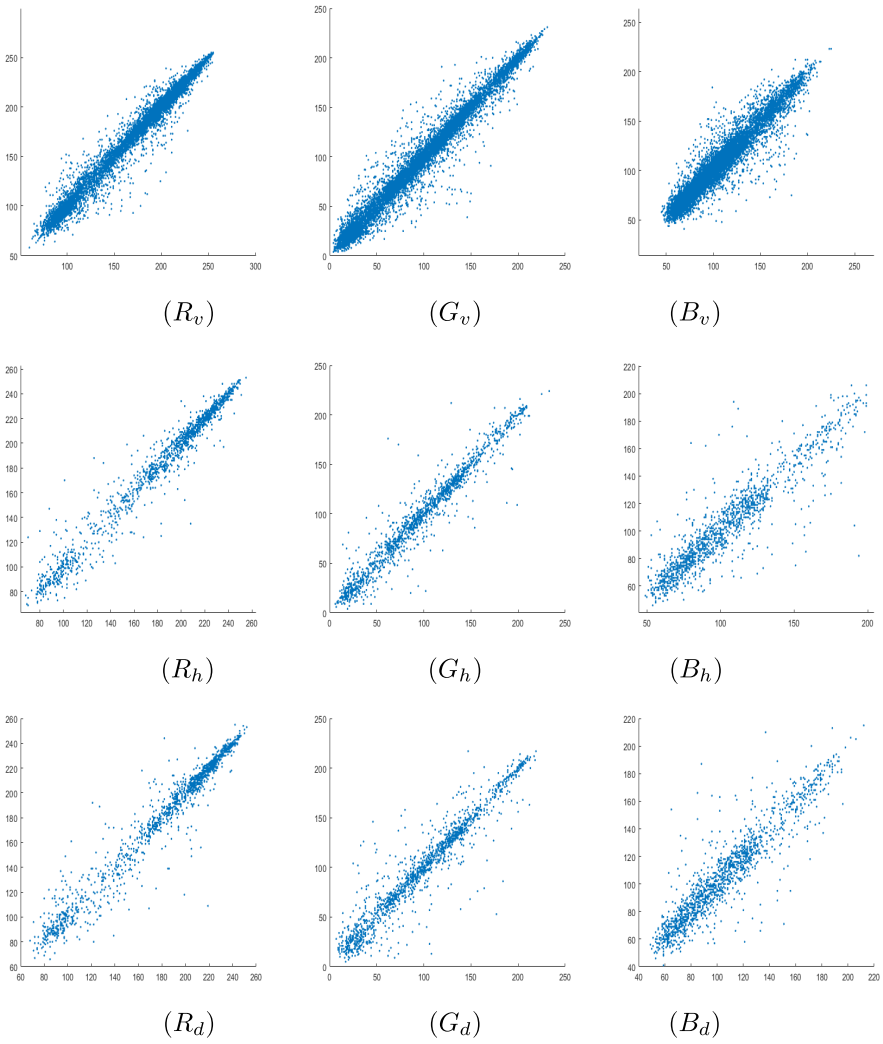


FIGURE 5. Correlation plots of two adjacent pixels of red channel(R), green channel(G) and blue channel(B) of the original RGB image of lena from first to third row illustrate that: vertical, horizontal and diagonal adjacent pixels of each channel respectively.

is as follows:

$$NPCR = \frac{1}{M \times N}\left[\sum_{m,n} E(m,n)\right] \times 100\% \tag{6.3}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{m,n} \frac{I_1(m,n) - I_2(m,n)}{255}\right] \times 100\% \tag{6.4}$$

where I_1 and I_2 are the ciphered images analogous to one byte differing from the original plain images, and $E(m, n)$ is of size $M \times N \times 3$ defined by

$$E(m,n) = \begin{cases} 1, & if \quad I_1(m,n) = I_2(m,n) \\ 0, & otherswise \end{cases} \tag{6.5}$$

The NPCR and UACI analysis results are shown in Table 8. From Table 8, we can conclude that the proposed work has greater security against differential attacks.

G. OCCLUSION ATTACK

An occluded attack is one in which an attacker purposefully creates or manipulates occlusions (obstructions or coverings) in the ciphered image or during the deciphering procedure in the context of image encryption and decryption. The decryption process can be hampered or misled by these occlusions, or they can be exploited to conceal particular areas of interest in the image. How an occlusion attack might operate in the encryption and decryption of images is as follows:

1) OCCLUSIONS INTRODUCED DURING ENCRYPTION

The attacker may add or overlay specific occlusions to the plaintext image before encryption to change it. These occlusions could be noise, random patterns, or pictures intended to obstruct the original information. These occlusions would subsequently be present in the encrypted image.

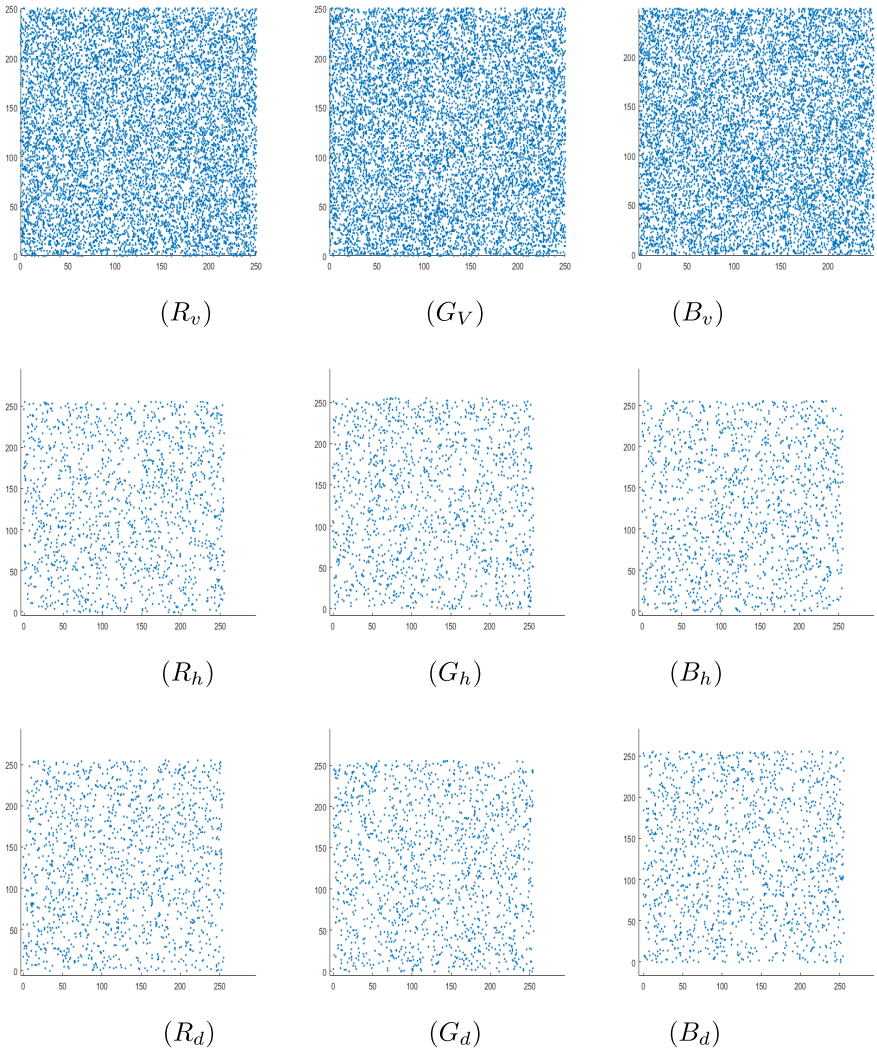


FIGURE 6. Correlation plots of two adjacent pixels of red channel(R), green channel(G) and blue channel(B) of the ciphered image of lena from first to third row illustrate that: vertical, horizontal and diagonal adjacent pixels of each channel respectively.

2) OCCLUSIONS INTRODUCED DURING TRANSMISSION

Attackers might occasionally interfere with the encrypted image as it is transmitted over a network. They could contribute extra information or make noise that looks like occlusions.

3) OCCLUSIONS INTRODUCED AFTER DECRYPTION

Attackers may alter the decryption process or the ciphered (encrypted image) to introduce occlusions. To deceive or hide the decoded image, it may entail changing pixel values, adding noise, or adding more content.

Image encryption and decryption systems must have strong security measures and cryptographic approaches that can identify and reduce the impact of occlusions in order to protect against occluded attacks. We modify the ciphered images in a number of ways before deciphering them, as shown in FIGURE 7, to test the suggested encryption scheme's resistance against the occluded attacks. The occluded encrypted images are presented in FIGURE 7$(a - h)$, and the matching decrypted images are shown in FIGURE 7$(i - p)$. The resulting deciphered photographs illustrate that the recommended encryption technique is able to keep the data in the images, even though 20% data of the encrypted image is changed during transmission.

H. PEAK SIGNAL TO NOISE RATIO(PSNR)

Peak Signal-to-Noise Ratio (PSNR), a crucial statistic in image encryption and decryption, provides a numerical assessment of how well the quality of the decrypted image is preserved from the original image, mathematically defined as:

$$PSNR \doteq 10.\log_{10}(\frac{Maxpixelvalue^2}{\sqrt{MSE}}), \qquad (6.6)$$

TABLE 6. Results of the proposed scheme's correlation coefficient comparison with various existing techniques in three layers.

		Image	Original color Image			Ciphered Image		
			R	G	B	R	G	B
Proposed scheme	lena	Vertical	0.9894	0.9817	0.9563	0.0005	-0.0012	0.0005
		Diagonal	0.9711	0.9437	0.9313	-0.0001	-0.0043	-0.00003
		Horizontal	0.9767	0.9725	0.9396	-0.0085	0.-0.0025	-0.0017
	Baboon	Vertical	0.8628	0.7717	0.8774	0.0021	-0.0008	0.0028
		Diagonal	0.8435	0.7430	0.8466	-0.00035	0.00087	0.0014
		Horizontal	0.9201	0.8564	0.9085	-0.0.0066	0.-0.0033	0.0098
	Pepper	Vertical	0.9672	0.9834	0.9672	-0.0025	0.0007	-0.0021
		Diagonal	0.9651	0.9834	0.9515	-0.0059	0.0038	0.0063
		Horizontal	0.9625	0.9675	0.9651	0.0026	0.0015	-0.0008
Ref. [35]	Lena	Vertical	0.9803	0.9594	0.9224	0.0203	-0.0025	0.0006
		Diagonal	0.9668	0.9433	0.9099	-0.0073	-0.0131	0.0111
		Horizontal	0.9813	0.9691	0.9455	0.0092	0.0002	0.0076
Ref. [36]	Lena	Vertical	0.9682	0.9755	0.9642	0.0031	0.0001	0.0022
		Diagonal	0.9377	0.9474	0.9217	0.0007	0.0017	0.0007
		Horizontal	0.9651	0.7202	0.9572	0.0049	0.0054	0.00053
Ref. [37]	Lena	Vertical	0.9508	0.9370	0.9171	-0.0013	-0.0051	-0.0078
		Diagonal	0.9259	0.9111	0.8867	-0.0025	-0.0103	0.0099
		Horizontal	0.9777	0.9607	0.9496	0.0090	0.0027	-0.0155
Ref. [38]	Lena	Vertical	0.9635	0.9642	0.9280	-0.0141	-0.0134	-0.0486
		Diagonal	0.8993	0.9075	0.8449	0.0464	0.0189	-0.0501
		Horizontal	0.9278	0.9278	0.8867	-0.0362	-0.0089	-0.0105

TABLE 7. The results of the proposed scheme's NPCR and UACI analyses are compared to those of some current methods.

		NPCR%			UACI%			Average
		R	G	B	R	G	B	
Proposed scheme		99.960	99.966	99.963	34.9709	33.0386	33.7423	33.9262
		99.979	99.985	99.982	33.4044	33.7832	35.6901	34.2925
		99.981	99.982	99.977	33.7500	32.9338	33.0931	33.2589
		99.970	99.679	99.984	34.4891	33.0523	32.3105	33.2839
Ref. [35]	Lena	99.653	99.652	99.651	33.4572	33.4715	33.4715	33.4384
Ref. [36]	Lena	99.650	99.644	99.662	33.4462	33.4131	33.4399	33.4330
Ref. [37]	Lena	99.630	99.602	99.601	33.60	33.30	33.40	—

where MSE(mean square error) is defined as:

$$MSE \doteq \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{i=1}^{M} [I(i,j) - I'(i,j)], \qquad (6.7)$$

where $I(i,j)$ and $I'(i,j)$ denotes the pixels values of the unencrypted and encrypted images.

Using a comparison between the original and the decrypted image, PSNR measures the quality of the image, while MSE (Mean Squared Error) gauges the average squared difference between comparable pixels. A more faithful decryption method, as indicated by a greater PSNR value, results in a restored image with little loss or distortion. This metric is essential for maintaining image integrity and secure transmission in various practicality, including secure communications, and multimedia content protection. A higher PSNR score often denotes a stronger encryption technique and shows that only a small amount of data was lost while deciphering the image, as given in Table 8.

TABLE 8. PNSR values of the suggested scheme of original(O) vs decrypted image(D) and original image(O) vs ciphered image(C).

Test Images	PSNR(O-D)	PSNR(O-C)
Lena	∞	8.63
Baboon	∞	8.78
Pepper	∞	8.09

I. COMPUTATIONAL COMPLEXITY

Time and space complexity are two ways to define computational complexity. Time complexity involves determining the amount of time required to solve a problem with a given dimension. The technique involves multiple image processing steps on an input, including channel splitting, bit-wise XOR operations, random permutation, and substitution using S-boxes. The time complexity of this algorithm primarily relies on the input image's size ('N') and the creation of various intermediate data structures during bit-wise operations, substitutions, and permutations. The resulting time complexity from these operations can be expressed as $O(N + 3n + 3m + 3k + p + q)$, where 'n' denotes the size of permutation or random number data, 'm' represents the size of S-boxes, 'k' signifies the size of data resulting from substitutions, 'p' stands for the size of the 'key', and 'q' accounts for the total number of elements involved in bit-wise XOR and concatenation. Moreover, the memory required to store the input image and its channels, along with the various intermediate matrices generated during S-box operations, substitutions, and permutations, significantly influences the algorithm's space complexity.

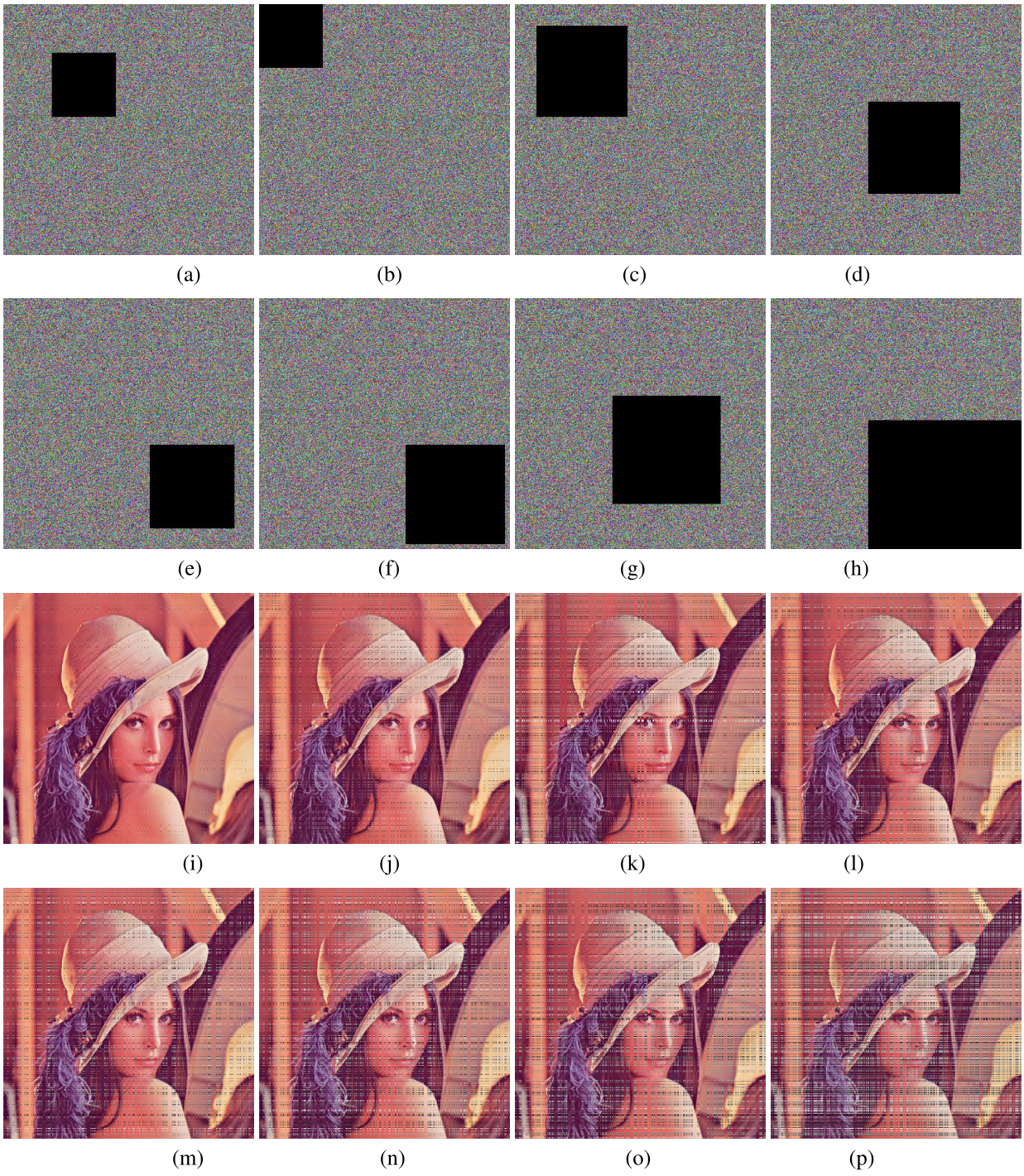


FIGURE 7. Occlusion attack: *Fig*. 9(*a* – *h*) obstructed encrypted images, *Fig*. 9(*i* – *p*) decrypted images corresponding to obstructed encrypted images.

The space complexity is approximately $O(N+6n+m+3k+p+3q)$, where 'N' represents the image size and 'n', 'm', 'k', 'p', and 'q' denote the sizes of intermediate data structures generated at different stages of the process. Additionally, the proposed scheme takes eighteen seconds on a normal PC for encryption, and on a high-speed PC, it may take less time.

VII. COMPARISON AND DISCUSSION

Table 9 reveals that the non-linearity (NL) of the constructed S-boxes is higher than that of various well-known existing S-boxes, including those referenced in the following list: [26], [27], [28], [29], [30], [31], [32], [33]. The proposed S-boxes provide resistance against linear attacks, and their Linear Approximation Probability (LAP) values are comparable

TABLE 9. A comparison between the suggested S-boxes and several high-quality S-boxes.

S-boxes	NL(avr)	SAC	BIC-SAC	BIC	DP	LP
$\mathbb{S}_{13}^{2520}$	107.5	0.5048	0.5018	103.143	0.0390625	0.148438
$\mathbb{S}_{11}^{820}$	107.25	0.509033	0.5026	103.643	0.046875	0.125
$\mathbb{S}_{1342}^{3043}$	107	0.508301	0.5002	103.429	0.0390625	0.1328
Ref. [26]	106.7	0.4988	0.5010	106.25	0.96875	0.5
Ref. [27]	106.7	0.5034	0.5015	103.78	0.0390625	0.140625
Ref. [28]	106.5	0.4995	0.4992	104.29	0.0390625	0.132813
Ref. [29]	105.5	0.4937	0.5013	105.7	0.1250	0.1170
Ref. [30]	103	0.5020	0.4998	102.93	0.039063	0.140625
Ref. [31]	105.8	0.4976	0.5032	104.5	0.0390625	0.1250
Ref. [32]	103	0.4961	0.5043	104.13	0.0390625	0.136719
‘ Ref. [33]	100	0.4812	0.4967	101.93	0.0625	0.179688

TABLE 10. A comparison between the suggested S-boxes and several high-quality S-boxes.

S-boxes	NL(min)	LAP	DAP	SAC(max)	SAC(min)	BIC(min)
$\mathbb{S}_{13}^{2520}$	104	0.1484	0.0391	0.5938	0.4219	0.4668
$\mathbb{S}_{11}^{820}$	106	0.125	0.0469	0.6094	0.3594	0.4746
$\mathbb{S}_{1342}^{3043}$	106	0.1328	0.0391	0.6094	0.4219	0.4766
Ref. [1]	106	0.1328	0.0391	0.5938	0.4531	0.4648
Ref. [3]	100	0.1328	0.0547	0.6094	0.4219	0.4746
Ref. [8]	74	0.2109	0.0547	0.6875	0.1094	0.4023
Ref. [9]	102	0.1484	0.0391	0.6094	0.375	0.4707
Ref. [10]	103	0.1328	0.0391	0.5703	0.4414	0.4961
Ref. [11]	104	0.0391	0.0391	0.625	0.3906	0.4707
Ref. [18]	104	0.109	0.0469	0.593	0.39	0.454
Ref. [24]	106	0.1406	0.0391	0.5938	0.4375	0.4648

to those of all currently existing S-boxes. The suggested S-boxes' differential approximation probability (DAP) values are 0.50, which is nearly optimal. Consequently, the suggested S-boxes induce strong data diffusion and possess the ability to resist differential attacks. Moreover, the strict avalanche criterion (SAC) and bit independence criterion (BIC) values of the suggested S-boxes are lower than or equivalent to those of a few well-known existing S-boxes. As a result, the suggested method can generate high-quality S-boxes. Additionally, the proposed image encryption scheme exhibits strong resistance to both statistical and differential attacks. The aforementioned sections, including image analysis, demonstrate the robustness of our suggested technique against these attacks. This cryptographic technique is an exemplar of efficiency, encompassing an extensive range of experiments, from security against a variety of attacks such as differentials and occlusions to entropy and histogram evaluations. Its exceptional effectiveness in securing data integrity across a range of operational environments is defined by its capacity to strike a balance between strong security, processing power, and resilience against a multitude of threats. An essential metric for assessing the feasibility and practicality of an encryption technique is operating efficiency. Naturally, an algorithm with a quick running time is more widely accepted. The newly suggested technique takes only 18 seconds to encrypt an image of size 512×512, has no issue with space, and stands against all the well-known linear and differential attacks. Therefore, the newly suggested technique is efficient for real-time implementation. Tables 9 and 10 present a comparative analysis of the proposed S-box scheme with existing published work.

VIII. CONCLUSION

This study discusses a revolutionary S-box construction approach. Prey-predator map output values are employed in the logistic map according to the proposed technique, which uses the EC's x and y coordinates over the finite prime field. Over the elliptic curve $E_r^p(a, b)$, an s-box is built, denoted by the symbol $\mathbb{S}_a^b$. Numerous cryptographic tests can be conducted on the newly constructed S-boxes to assess their quality. Based on the experimental results of the suggested S-boxes, a comparison with several high-quality S-boxes has also been performed. The experimental findings demonstrate that the suggested technique allows for the creation of high-quality S-boxes.

The selection of parameters a, b, and r, where $r > 0$ and both a and b are members of the finite prime field, constitutes the key element of the suggested technique. By varying the values of p, a, b, and r, multiple S-boxes can be generated. Image encryption can also be performed using the proposed S-boxes. The suggested method can also be employed to construct discrete dynamical systems with more robust S-boxes from a cryptographic perspective. The proposed image encryption technique ensures the secure transmission of digital images. The proposed method is primarily based on elliptic curves and chaotic maps. In this method, the color image is divided into three channels: red (R), green (G), and blue (B). The proposed three S-boxes are used for substitution in each channel separately, inducing confusion in the encryption process. For the confusion component, the substituted channels are permuted using a random sequence of numbers generated through an elliptic curve. The final step of image encryption involves the bitwise

XOR operation of the key generated using a logistic map with the permuted channels individually, combining all three encrypted color channels of the test image to obtain the ciphered image. The decryption process is the reverse of the proposed encryption technique. The proposed techniques withstand various differential, linear, and statistical attacks. Furthermore, in comparison with some published work, the proposed technique exhibits better performance.

The videos consist of a continuous flow of images. The future work of the proposed technique can also find applications in video encryption as well as audio encryption. Additionally, the hardware implementation of the proposed technique presents an interesting avenue for future research.

REFERENCES

[1] U. Hayat, N. A. Azam, and M. Asif, "A method of generating 8 × 8 substitution boxes based on elliptic curves," *Wireless Pers. Commun.*, vol. 101, no. 1, pp. 439–451, Jul. 2018.

[2] N. A. Azam, U. Hayat, and I. Ullah, "Efficient construction of a substitution box based on a mordell elliptic curve over a finite field," *Frontiers Inf. Technol. Electron. Eng.*, vol. 20, no. 10, pp. 1378–1389, Oct. 2019.

[3] G. Tang, X. Liao, and Y. Chen, "A novel method for designing S-boxes based on chaotic maps," *Chaos, Solitons Fractals*, vol. 23, no. 2, pp. 413–419, Jan. 2005.

[4] A. Gautam, G. S. Gaba, R. Miglani, and R. Pasricha, "Application of chaotic functions for construction of strong substitution boxes," *Indian J. Sci. Technol.*, vol. 8, no. 28, pp. 1–5, Oct. 2015.

[5] 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.*, vol. 2, Aug. 2010, pp. 1033–1037.

[6] J. Kim and R. C.-W. Phan, "Advanced differential-style cryptanalysis of the NSA's skipjack block cipher," *Cryptologia*, vol. 33, no. 3, pp. 246–270, Jul. 2009.

[7] G. Chen, Y. Chen, and X. Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic baker maps," *Chaos, Solitons Fractals*, vol. 31, no. 3, pp. 571–579, Feb. 2007.

[8] G. Chen, "A novel heuristic method for obtaining S-boxes," *Chaos, Solitons Fractals*, vol. 36, no. 4, pp. 1028–1036, May 2008.

[9] 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.

[10] D. E. S. Cipher, "Linear cryptanalysis method for," in *Proc. Adv. CryptologyEUROCRYPT, Workshop Theory Appl. Cryptograph. Techn*, vol. 765. Lofthus, Norway. Cham, Switzerland: Springer, May 1993, p. 386, May 2003.

[11] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, Aug. 1985, pp. 523–534.

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

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

[14] I. Hussain, N. A. Azam, and T. Shah, "Stego optical encryption based on chaotic S-box transformation," *Opt. Laser Technol.*, vol. 61, pp. 50–56, Sep. 2014.

[15] J. Daemen and V. Rijmen. (1999). *AES Proposal: Rijndael (Version 2)*. [Online]. Available: NISTAESwebsitecsrc.nist.gov/encryption/aes

[16] N. Ferguson, R. Schroeppel, and D. Whiting, "A simple algebraic representation of Rijndael," in *Proc. Int. Workshop Sel. Areas Cryptogr.* Berlin, Germany: Springer, Aug. 2001, pp. 103–111.

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

[18] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an EC," *Signal Process.*, vol. 155, pp. 391–402, Sep. 2019.

[19] G. Gong, T. A. Berson, and D. R. Stinson, "EC pseudorandom sequence generators," in *Proc. Int. Workshop Sel. Areas Cryptogr.* Berlin, Germany: Springer, Aug. 1999, pp. 34–48.

[20] M. Caragiu, R. A. Johns, and J. Gieseler, "Quasi-random structures from ECs," *J. Algebra, Number Theory Appl.*, vol. 6, pp. 561–571, Sep. 2006.

[21] R. R. Farashahi, B. Schoenmakers, and A. Sidorenko, "Efficient pseudo-random generators based on the DDH assumption," in *Proc. Int. Workshop Public Key Cryptogr.* Berlin, Germany: Springer, Apr. 2007, pp. 426–441.

[22] O. Reyad and Z. Kotulski, "On pseudo-random number generators using elliptic curves and chaotic systems," *Appl. Math. Inf. Sci.*, vol. 9, no. 1, pp. 31–38, Jan. 2015.

[23] 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.

[24] S. A. Vanstone, "Elliptic curve cryptosystem—The answer to strong, fast public-key cryptography for securing constrained environments," *Inf. Secur. Tech. Rep.*, vol. 2, no. 2, pp. 78–87, Jan. 1997.

[25] S. Hussain, S. S. Jamal, T. Shah, and I. Hussain, "A power associative loop structure for the construction of non-linear components of block cipher," *IEEE Access*, vol. 8, pp. 123492–123506, 2020.

[26] S. S. Jamal, T. Shah, and A. Attaullah, "A group action method for construction of strong substitution box," *3D Res.*, vol. 8, no. 2, pp. 1–10, Jun. 2017.

[27] 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.

[28] T. Farah, R. Rhouma, and S. Belghith, "A novel method for designing S-box based on chaotic map and teaching–learning-based optimization," *Nonlinear Dyn.*, vol. 88, no. 2, pp. 1059–1074, Apr. 2017.

[29] M. Khan and T. Shah, "A novel construction of substitution box with Zaslavskii chaotic map and symmetric group," *J. Intell. Fuzzy Syst.*, vol. 28, no. 4, pp. 1509–1517, 2015.

[30] A. Anees and Z. Ahmed, "A technique for designing substitution box based on van der pol oscillator," *Wireless Pers. Commun.*, vol. 82, no. 3, pp. 1497–1503, Jun. 2015.

[31] G. Liu, W. Yang, W. Liu, and Y. Dai, "Designing S-boxes based on 3-D four-wing autonomous chaotic system," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1867–1877, Dec. 2015.

[32] M. A. Gondal, A. Raheem, and I. Hussain, "A scheme for obtaining secure S-boxes based on chaotic Baker's map," *3D Res.*, vol. 5, no. 3, p. 17, Sep. 2014.

[33] M. Khan, T. Shah, and S. I. 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, Apr. 2016.

[34] J. C. H. Castro, J. M. Sierra, A. Seznec, A. Izquierdo, and A. Ribagorda, "The strict avalanche criterion randomness test," *Math. Comput. Simul.*, vol. 68, no. 1, p. 17, 2005.

[35] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Process., Image Commun.*, vol. 80, Feb. 2020, Art. no. 115670.

[36] X. Li, L. Wang, Y. Yan, and P. Liu, "An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems," *Optik*, vol. 127, no. 5, pp. 2558–2565, Mar. 2016.

[37] X.-Y. Wang, H.-L. Zhang, and X.-M. Bao, "Color image encryption scheme using CML and DNA sequence operations," *Biosystems*, vol. 144, pp. 18–26, Jun. 2016.

[38] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

[39] X. Wang, Y. Zhao, H. Zhang, and K. Guo, "A novel color image encryption scheme using alternate chaotic mapping structure," *Opt. Lasers Eng.*, vol. 82, pp. 79–86, Jul. 2016.

[40] K. M. Faraoun, "Fast encryption of RGB color digital images using a tweakable cellular automatonbased schema," *Opt. Laser Technol.*, vol. 64, Sep. 2014, Art. no. 145155.

[41] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011.

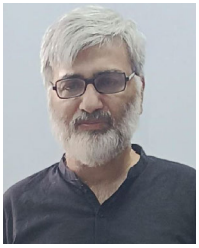
[42] A. F. Weister and S. E. Tavares, "On the design of S-boxes," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, Aug. 1985, pp. 523–534.

[43] C. Adams and S. Tavares, "The structured design of cryptographically good s-boxes," *J. Cryptol.*, vol. 3, no. 1, pp. 27–41, Jan. 1990.

[44] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. With Appl.*, vol. 59, no. 10, pp. 3320–3327, May 2010.

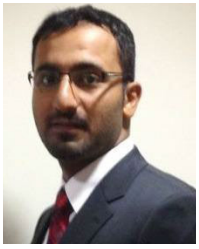
[45] K.-W. Wong, B. S.-H. Kwok, and W.-S. Law, "A fast image encryption scheme based on chaotic standard map," *Phys. Lett. A*, vol. 372, no. 15, pp. 2645–2652, Apr. 2008.
[46] M. Usamaa, M. Khana, K. Alghathbar, and C. Lee, "Chaos-based secure satellite image cryptosystem," *Comput. Math. Appl.*, vol. 60, Jul. 2010, Art. no. 326337.
[47] C. Li, S. Li, G. Chen, and W. A. Halang, "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence," *Image Vis. Comput.*, vol. 27, no. 8, pp. 1035–1039, Jul. 2009.
[48] H. Li, S. Yu, W. Feng, Y. Chen, J. Zhang, Z. Qin, Z. Zhu, and M. Wozniak, "Exploiting dynamic vector-level operations and a 2D-enhanced logistic modular map for efficient chaotic image encryption," *Entropy*, vol. 25, no. 8, p. 1147, Jul. 2023.
[49] H. Wen, Y. Huang, and Y. Lin, "High-quality color image compression-encryption using chaos and block permutation," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 8, Sep. 2023, Art. no. 101660.
[50] K. Qian, W. Feng, Z. Qin, J. Zhang, X. Luo, and Z. Zhu, "A novel image encryption scheme based on memristive chaotic system and combining bidirectional bit-level cyclic shift and dynamic DNA-level diffusion," *Frontiers Phys.*, vol. 10, Aug. 2022, Art. no. 963795.
[51] H. Wen and Y. Lin, "Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding," *Expert Syst. Appl.*, vol. 237, Mar. 2024, Art. no. 121514.
[52] H. Wen and Y. Lin, "Cryptanalyzing an image cipher using multiple chaos and DNA operations," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 7, Jul. 2023, Art. no. 101612.
[53] W. Feng, Z. Qin, J. Zhang, and M. Ahmad, "Cryptanalysis and improvement of the image encryption scheme based on feistel network and dynamic DNA encoding," *IEEE Access*, vol. 9, pp. 145459–145470, 2021.
[54] Q. Liu and L. Liu, "Color image encryption algorithm based on DNA coding and double chaos system," *IEEE Access*, vol. 8, pp. 83596–83610, 2020.
[55] Z. Azimi and S. Ahadpour, "Color image encryption based on DNA encoding and pair coupled chaotic maps," *Multimedia Tools Appl.*, vol. 79, nos. 3–4, pp. 1727–1744, Jan. 2020.
[56] D. Shah and T. Shah, "Binary Galois field extensions dependent multimedia data security scheme," *Microprocessors Microsyst.*, vol. 77, Sep. 2020, Art. no. 103181.
[57] J. Rosenthal, "A polynomial description of the Rijndael advanced encryption standard," *J. Algebra Appl.*, vol. 2, no. 2, pp. 223–236, 2003.
[58] N. A. Azam, "A novel fuzzy encryption technique based on multiple right translated AES gray S-boxes and phase embedding," *Secur. Commun. Netw.*, 2017.
[59] K. Kazlauskas and J. Kazlauskas, "Key-dependent S-box generation in AES block cipher system," *Informatica*, vol. 20, no. 1, pp. 23–34, 2009.
[60] G. Manjula and H. S. Mohan, "Constructing key dependent dynamic S-Box for AES block cipher system," in *Proc. 2nd Int. Conf. Appl. Theor. Comput. Commun. Technol. (ICATCCT)*, Jul. 2016, pp. 613–617.
[61] S. Katiyar and N. Jeyanthi, "Pure dynamic S-box construction," *Int. J. Comput.*, vol. 1, 2016.
[62] M. K. Balajee and J. M. Gnanasekar, "Evaluation of key dependent S-box based data security algorithm using Hamming distance and balanced output," *Tem J.*, vol. 5, no.1 p. 67, 2016.
[63] B. Rahnama, Y. Kıran, and R. Dara, "Countering AES static S-box attack," in *Proc. 6th Int. Conf. Secur. Inf. Netw.*, Nov. 2013, pp. 256–260.
[64] P. Agarwal, A. Singh, and A. Kilicman, "Development of key-dependent dynamic S-boxes with dynamic irreducible polynomial and affine constant," *Adv. Mech. Eng.*, vol. 10, no. 7, 2018, Art. no. 1687814018781638.
[65] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

TANVEER QAYYUM received the M.Sc. degree in mathematics from The University of Azad Jammu & Kashmir, Muzaffarabad, Pakistan, in 2018, and the M.Phil. degree in pure mathematics from Quaid-i-Azam University, Islamabad, Pakistan, in 2021. He is currently a Ph.D. Scholar with the Department of Mathematics, Quaid-i-Azam University. His current research interests include elliptic curve cryptography and chaotic cryptography.



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, error-correcting codes, and cryptography.

ALI YAHYA HUMMDI received the Ph.D. degree from The University of Sheffield, U.K., in 2022. He is currently an Assistant Professor with the Department of Mathematics, King Khalid University, Abha, Saudi Arabia. His research interests include non-commutative Noetherian rings and their modules (especially rings of differential operators and D-modules), dimension (the Krull dimension and the Gelfand-Kirillov dimension), graded and filtered algebras, and cryptography.



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, University of Colorado Colorado Springs (UCCS), Colorado Springs, USA, in 2018. He is currently an Associate 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. He received multiple research awards from UCCS, UT, and SACM for his outstanding research articles. His research interests include software-defined networking, artificial intelligence, cloud computing, the IoT, and cybersecurity.

ZAID BASSFAR received the B.S. degree in computer science, in 2007, the M.S. degree in information technology and communication, in 2010, and the Ph.D. degree in web applications, in 2014. Since 2020, he has been an Associate Professor with the College of Computer and Information Technology, University of Tabuk. His research interests include web applications, virtual reality, emerging technology, virtual learning, e-learning, m-learning, multimedia, and human–computer interaction.