A Novel Image Encryption Scheme Based on Elliptic Curves over Finite Rings

Umar Hayat 1,*, Ikram Ullah 1, Naveed Ahmed Azam 2,• and Sumaira Azhar 1

1 Department of Mathematics, Quaid-i-Azam University, Islamabad 45320, Pakistan; ikram.ullah@math.qau.edu.pk (I.U.); 03141713011@student.qau.edu.pk (S.A.)
2 Department of Applied Mathematics and Physics, Graduate School of Informatics, Kyoto University, Kyoto 606-8503, Japan
* Correspondence: umar.hayat@qau.edu.pk (U.H.); azam@amp.i.kyoto-u.ac.jp (N.A.A.)

Abstract: Image encryption based on elliptic curves (ECs) is emerging as a new trend in cryptography because it provides high security with a relatively smaller key size when compared with well-known cryptosystems. Recently, it has been shown that the cryptosystems based on ECs over finite rings may provide better security because they require the computational cost for solving the factorization problem and the discrete logarithm problem. Motivated by this fact, we proposed a novel image encryption scheme based on ECs over finite rings. There are three main steps in our scheme, where, in the first step, we mask the plain image using points of an EC over a finite ring. In step two, we create diffusion in the masked image with a mapping from the EC over the finite ring to the EC over the finite field. To create high confusion in the plain text, we generated a substitution box (S-box) based on the ordered EC, which is then used to permute the pixels of the diffused image to obtain a cipher image. With computational experiments, we showed that the proposed cryptosystem has higher security against linear, differential, and statistical attacks than the existing cryptosystems. Furthermore, the average encryption time for color images is lower than other existing schemes.

Keywords: elliptic curve; finite ring; total order; substitution box; image encryption

1. Introduction

In this modern era, the transmission of images over public networks is an indispensable task. Therefore, distributing secret images in a secure way is essential. Encryption schemes take plain-text data as an input and convert it into an unreadable form using secret keys. Then, an authorized person uses the secret keys to acquire the original data. Recently, S-box-based encryption algorithms have gained special attention [1]. An S-box is used to create confusion; therefore, researchers are not only trying to improve the existing S-box schemes, but are also proposing new ones. Many authors (see, for example, [2,3]) have observed that the S-box used in the well-known cryptosystem, the advanced encryption standard (AES), is vulnerable because the AES cryptosystem uses a static S-box. Furthermore, it also has low algebraic complexity.

The role of an S-box is vital in a cryptosystem. Therefore, researchers are trying to generate S-boxes which are cryptographically secure. One way is to improve the security of the AES cryptosystem. That is why Cui and Cao [4] enhanced the algebraic complexity of an AES S-box to make it secure against algebraic attacks. Similarly, Liu et al. [5] proposed an improved AES S-box that has reliable security against algebraic and differential attacks. Tran et al. [6] presented the Gray S-box for the AES, which is secure against algebraic and interpolation attacks. In addition to this, many other techniques are used to design S-boxes with the desired security. For example, Silva-Garcia et al. [7] developed a novel chaos-based cryptosystem, which generates an S-box to resist linear attacks. Ibrahim and Alhabi [1] used a Henon map to generate secure and dynamic S-boxes. Özkaynak [8] proposed robust S-boxes using different chaotic systems. Due to their higher security, EC-based cryptosystems...
have gained the interest of researchers. Miller [9] presented an EC-based cryptosystem with high security and a small key size. Cheon et al. [10] used hyperelliptic curves to obtain a lower bound on the nonlinearity of Boolean functions. Hayat et al. [11,12] employed ECs over finite fields and rings to design secure S-boxes. It is analyzed that the S-box generators over finite rings generate dynamic S-boxes with reasonable time complexity.

Furthermore, the pixels have high correlation and the data size is large in an image. Therefore, to develop secure cryptosystems for the delivery of secret images is a common interest of researchers. Many techniques, such as fuzzy theory [13] and chaotic maps [14–25], are used to develop encryption schemes.

Recently, chaos-based schemes have received more attention due to their easy implementation and fast execution [26]. Similarly, chaotic maps have some unique characteristics, such as ergodicity, unpredictability, random behavior, and sensitivity to initial parameters, which are required for a good cryptosystem [27]. Therefore, a number of image encryption schemes are proposed based on sine maps [28,29], cat maps [30], and some other chaotic maps [31]. Huang et al. [32] developed an encryption scheme with better confusion creation capability using the Rivest–Shamir–Adleman (RSA) algorithm and Arnold map. Similarly, Ye et al. [33] designed an effective and secure image cryptosystem based on the RSA technique and a fractional-order chaotic system. On the other hand, there exist chaotic encryption schemes which are not secure. Chen et al. [30] developed an image encryption algorithm using a 3D chaotic cat map, which has short period and hence, is vulnerable to the chosen plain-text attack [34]. Similarly, the scheme developed by Sui et al. [31] is based on logistic maps; however, logistic maps are insecure due to the small key space [14].

Related work: Like chaotic maps, elliptic curves (ECs) are highly sensitive to the initial parameters, and a number of EC-based algorithms have been developed for cryptographic applications [9,35–48]. Zhang and Wang [40] used the group law for the generation of a public key and encrypted digital images by combining a chaotic system and elliptic curve cryptography (ECC). Abdelfatah [41] presented a digital signature scheme using the group law. Abbas et al. [42] proposed a chaotic encryption algorithm using an addition operator over the points of the EC. El-Latif et al. [49] developed an efficient encryption scheme using a cyclic EC and a generalized logistic map; basically, an EC-based sequence and a chaotic sequence are combined to generate a keystream for encryption. Toughi et al. [30] generated a sequence of numbers using ECs, which are then used in the generation of keys to propose an encryption algorithm. Hayat et al. [51] proposed a twofold image encryption scheme. Firstly, a plain image is masked by EC-based random numbers, and then permuted by an S-box generated using an EC. Reyad et al. [52] modulated random sequences using ECs and chaotic maps. It is experimentally proved that all the above schemes are highly secure. In addition, ECs provide more security to a cryptosystem than chaotic maps [35,54], but it is important to mention that the scheme in [49] first generates a sequence of scalars. Each scalar is then mapped to a scalar multiple of a point of a cyclic EC. To compute a scalar multiple of a point lying on an EC is not simple; it involves the group law, consisting of many complex calculations. Similarly, the scheme in [52] also uses group operations to generate random numbers from the points of ECs. Thus, the schemes of [40–42,44,49,52] are time-consuming due to the use of the group law. The scheme in [51] avoids the group law to generate ECs, but each plain image requires the generation of two ECs. Moreover, trials are required for the generation of ECs to ensure the encryption of an image because the said scheme does not output an S-box for all parameters. These facts slow the execution time of the scheme. The algorithm in [37] does not generate triads for all images of the same size, but generates an EC for each image, which enhances the execution time.

In all the above-discussed EC-based schemes, finite fields are used to obtain the desired security. The security of such cryptosystems based on ECs over finite fields essentially depends on the computational cost for solving the discrete logarithm problem [55]. Recently, Diaz et al. [55] pointed out that the cryptosystems based on ECs over finite rings are more secure as compared to the cryptosystems based on ECs over finite fields. Their claim follows from the fact that the computational cost of breaking such cryptosystems based on ECs over
finite rings depends on solving the factorization problem \cite{56} and the discrete logarithm problem. Our research contribution aims to develop a cryptosystem that is based on a ring of integers and that has higher resistance against modern attacks than the existing schemes of Ecs over finite fields. In this work, we propose:

1. A new S-box generator that can generate a good S-box based on an EC over a finite ring of integers;
2. An image encryption algorithm using the aforementioned S-box generator.

The current work is novel in the sense that:
- It is based on a ring of integers rather than on a finite field;
- It avoids the traditional way (group law) of generating an EC. Furthermore, it imposes a bound on the y-coordinate of the EC, which is not the case in \cite{12,51}, and one does not have to check all the possible values over the underlying structure. So, the current S-box generator is comparatively efficient for a possible S-box;
- It generates cryptographically strong S-boxes;
- The time complexity of the proposed scheme is dependent on the chosen bound on the y-coordinate of the EC;
- Unlike the case in \cite{37,51,57}, each input image does not need the computation of a new EC for the confusion phase;
- It can encrypt a number of images with better security against differential, statistical, key and plain-text attacks;
- The run-time of the proposed scheme to encrypt color images is very low.

The rest of the paper is organized as follows: Section 2 contains the related notions of Ecs. In Section 3, the proposed S-box algorithm and its analysis is described. In Section 4, the proposed image encryption scheme is presented. In Section 5, the decryption of the proposed scheme is reported. The security analysis is conducted in Section 6. An application of the proposed scheme to color images is shown in Section 7. Lastly, the conclusion is drawn in Section 8.

2. Related Notions of Ecs

Let \( \{ p_i \}_{i \in \Omega} \) be a set of primes for any indexing set \( \Omega \). Then, for \( k \geq 2 \), \( n = \prod_{i=1}^{k} p_i \) is a composite integer and, hence, \( \mathbb{Z}_n \) is a ring. As for each prime \( p_i \), \( \mathbb{F}_p \) represents a finite field. Thus, for primes \( p_i \), \( 1 \leq i \leq k \), we say that \( \mathbb{F}_p \) is a finite field related to the ring \( \mathbb{Z}_n \).

For any two integers, \( a, b \in \mathbb{Z}_n \), with the condition that \( 4a^3 + 27b^2 \in \mathbb{Z}_n \setminus \{0\} \), the EC \( E_{n,a,b} \) represents the set of points \( \{(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n | y^2 = x^3 + ax + b \ (\text{mod} \ n)\} \cup \{\infty\} \), where \( \infty \) is the neutral point lying at each vertical line passing through the EC, and \( 4a^3 + 27b^2 \) is the discriminant of \( E_{n,a,b} \). The condition on the discriminant is imposed so that the EC \( E_{n,a,b} \) has no singular point. The integers \( n, a \) and \( b \) are known as the parameters of \( E_{n,a,b} \). For \( a = 0 \), the Ecs are known as Mordell elliptic curves (MECs); we denote them by \( E_{n,b} \) and \( \#E_{n,b} \) denotes the number of points on the MEC \( E_{n,b} \). There is a bijection \cite{56} between \( E_{n,b} \) and \( E_{p_1 b} \times \ldots \times E_{p_k b} \), which maps \( (x, y) \in E_{n,b} \) to \( (x \ (\text{mod} \ p_1), y \ (\text{mod} \ p_1)) \times \ldots \times (x \ (\text{mod} \ p_k), y \ (\text{mod} \ p_k)) \in E_{p_1 b} \times \ldots \times E_{p_k b} \). Consequently, an EC \( E_{p_i b} \) may be deduced from \( E_{n,b} \) by mapping \( (x, y) \in E_{n,b} \) to \( (x \ (\text{mod} \ p_i), y \ (\text{mod} \ p_i)) \) and, hence, for each \( p_i \) we have a surjective map from \( E_{n,b} \) to \( E_{p_i b} \). Let \( f : E_{n,b} \to E_{p_1 b} \times \ldots \times E_{p_k b} \) and \( g : E_{a,b} \to E_{p_i b} \) represent the former bijective and surjective maps, respectively; then, mathematically, \( f \) and \( g \) are given by:

\[
\begin{align*}
    f(x, y) &= (x \ (\text{mod} \ p_1), y \ (\text{mod} \ p_1)) \times \ldots \times (x \ (\text{mod} \ p_k), y \ (\text{mod} \ p_k)) , \\
    g(x, y) &= (x \ (\text{mod} \ p_i), y \ (\text{mod} \ p_i)).
\end{align*}
\]

The MECs play an important role in cryptography. Azam et al. \cite{58} defined different total orders, named as natural ordering \((\prec_N)\) and diffusion ordering \((\prec_D)\), on the points of MECs. For details, the readers are referred to \cite{58}.
3. The Proposed S-Box and Its Analysis

The proposed encryption scheme in Section 4 requires an S-box generator to obtain the desired level of confusion. For the construction of an S-box, we need the parameters \( n, b, \) and \( t \). It is mentioned that \( n = \prod_{i=1}^{k} p_i \), where each \( p_i \) is a prime and \( k \) is a positive integer.

In principle, \( n \) may be assigned any value. We choose \( n \) as a product of primes because, in the masking phase for each prime \( p_i \), we need the EC over the related prime field \( \mathbb{F}_{p_i} \).

The parameters \( n, b \) are used to generate the EC \( E_{n,b} \) over the ring of integers \( \mathbb{Z}_n \), where \( t \) is used as an upper bound on the \( y \)-coordinate of the EC \( E_{n,b} \). Here, upper bound \( t \) means that we compute such \((x, y) \in E_{n,b}\) for which \( y \leq t \). The \( y \)-coordinate is kept bounded, so that we compute \((x, y) \in E_{n,b}\) for all \( x \in \mathbb{Z}_n \) and particular values of \( y \) instead of all \( y \in \mathbb{Z}_n \). This is conducted in order to reduce the time of execution. After the generation of the EC \( E_{n,b} \), the points of \( E_{n,b} \) need to be arranged by some ordering. The points may be arranged according to any ordering, but the ordering \( \prec \) is capable of generating S-boxes with high cryptographic properties. Therefore, we use \( \prec \) to sort the points of \( E_{n,b} \). Then, we construct an \( m \times m \) S-box \( \sigma(n, t) \) by extracting the first \( 2^m \) different values \( y_i < 2^m \) of the \( y \)-coordinate of the ordered \( E_{n,b} \). Mathematically, the S-box is generated according to the following function:

\[
\sigma(n, t) : [0, 2^m - 1] \rightarrow [0, 2^m - 1]
\]

defined by:

\[
\sigma(n, t)(i) = y_i,
\]

where \((x, y_i) \in E_{n,b}\) for some \( x \in \mathbb{Z}_n \) and \( \sigma(n, t)(r) \neq y_i \) for \( r < i \). The S-box construction is clearly described in the following steps:

Step 1. To generate an \( m \times m \) S-box, select three integers \( n, b, \) and \( t \) such that \( n > 2^m, 0 < b < n \) and \( 2^m \leq t \leq n; \)

Step 2. Choose primes \( p_i \) for a finite \( k \geq 2 \) in such a way that \( n = \prod_{i=1}^{k} p_i; \)

Step 3. For each \( y \in [0, t] \) and \( x \in [0, n - 1] \), compute all the points \((x, y)\) such that \( y^2 \equiv x^3 + b \pmod{n} \); i.e., compute \( E_{n,b} \);

Step 4. If the set \([0, 2^m - 1]\) is contained in the \( y \)-coordinates of the points \((x, y) \in E_{n,b}\), then proceed to Step 5. Otherwise, change \( p_i \) for some \( i \) and repeat Steps 1–3;

Step 5. Arrange the points of \( E_{n,b} \) by applying the ordering \( \prec \);

Step 6. Construct the S-box \( \sigma(n, t) : [0, 2^m - 1] \rightarrow [0, 2^m - 1] \), such that \( \sigma(n, t)(i) = y_i \), where \((x, y_i) \in E_{n,b}\) for some \( x \in [0, n - 1] \) with the constraint that \( y_i < 2^m \) and \( \sigma(n, t)(i) \neq \sigma(n, t)(j) \) for \( j < i \).

For parameters \( n = 2491, p_1 = 47, p_2 = 53, b = 716, \) and \( t = 255 \), an \( 8 \times 8 \) S-box generated by the proposed method on an EC \( E_{2491,716} \) is shown in Table 1.

Table 1. The S-box \( \sigma(2491, 255) \) generated by the proposed algorithm.

| \( n \) | \( b \) | \( t \) | \( \sigma(n, t) \) |
|---|---|---|---|
| 29 | 221 | 121 | 55 | 244 | 223 | 215 | 53 | 14 | 115 | 131 | 96 | 11 | 143 | 145 | 238 |
| 136 | 3 | 181 | 138 | 137 | 248 | 61 | 189 | 140 | 64 | 20 | 182 | 70 | 134 | 124 | 49 |
| 141 | 50 | 19 | 191 | 164 | 125 | 22 | 179 | 118 | 237 | 202 | 66 | 10 | 167 | 38 | 83 |
| 40 | 193 | 230 | 234 | 175 | 9 | 159 | 158 | 229 | 34 | 251 | 205 | 249 | 180 | 197 | 81 |
| 218 | 110 | 195 | 116 | 27 | 150 | 94 | 87 | 157 | 62 | 48 | 226 | 117 | 75 | 217 | 99 |
| 86 | 1 | 68 | 90 | 165 | 130 | 242 | 163 | 32 | 203 | 72 | 51 | 89 | 235 | 37 | 120 |
| 113 | 77 | 239 | 188 | 5 | 201 | 162 | 60 | 149 | 192 | 211 | 59 | 161 | 88 | 155 | 6 |
| 233 | 222 | 106 | 8 | 178 | 245 | 209 | 123 | 204 | 199 | 76 | 153 | 122 | 194 | 184 | 100 |
| 246 | 228 | 107 | 142 | 26 | 207 | 232 | 104 | 227 | 198 | 73 | 154 | 186 | 172 | 152 | 12 |
| 57 | 56 | 65 | 58 | 44 | 69 | 46 | 74 | 92 | 101 | 174 | 160 | 82 | 220 | 112 | 200 |


3.1. Analysis of the Proposed S-Box

The cryptographic strength of the proposed S-box is analyzed by well-known tests, which are described as follows.

3.1.1. Linear Attacks

A cryptosystem is secure if it can strongly resist attackers to exploit the linear relations of inputs and outputs. The immunity of an \( n \times n \) S-box \( S \) against linear attacks is evaluated by its non-linearity \( \text{NL}(S) \) [59], linear approximation probability \( \text{LAP}(S) \) [60], and algebraic complexity \( \text{AC}(S) \) [61].

For a chosen \( n \), the \( \text{NL}(S) \) represents the minimum Hamming distances between the S-box \( S \) and all the corresponding affine functions. Similarly, the \( \text{LAP}(S) \) is the approximation of the relation lying between the inputs and outputs, and the \( \text{AC}(S) \) represents the number of non-zero terms in the polynomial representation of the S-box \( S \). Mathematically, the \( \text{NL}(S) \) and \( \text{LAP}(S) \) are computed by Equations (1) and (2), respectively:

\[
\text{NL}(S) = \min_{\alpha \neq 0, \beta, \lambda} \# \{ x \in \mathbb{F}_2^n : \alpha \cdot S(x) \neq \beta \cdot x \oplus \lambda \}, \tag{1}
\]

\[
\text{LAP}(S) = \frac{1}{2^n} \left\{ \max_{\alpha, \beta \neq 0} \left\{ \# \{ x \in \mathbb{F}_2^n \mid x \cdot \alpha = S(x) \cdot \beta - 2^{n-1} \} \right\} \right\}, \tag{2}
\]

where \( \alpha, \beta \in \mathbb{F}_2^n \), and “.” denotes the dot product. The resistance to linear attacks is greater if the \( \text{NL}(S) \) is close to \( 2^n - 1 - 2^{(n/2)-1} \), the \( \text{LAP}(S) \) is low, and the \( \text{AC}(S) \) tends to \( 2^n - 1 \).

The values of the \( \text{NL} \), \( \text{LAP} \), and \( \text{AC} \) for the S-box shown in Table 1 are 106, 0.0156, and 254, respectively. Moreover, from Table 2, it follows that the \( \text{NL} \) of the proposed S-box is greater than those of \([51,62–66]\) and equal to \( \text{NL} \) of the S-boxes in \([8,12,37,48,58]\). Similarly, the \( \text{LAP} \) of the new S-box is less than the \( \text{LAP} \) of the S-boxes in \([8,12,37,48,51,58,62–66]\). The \( \text{AC} \) of the presented S-box is greater than the \( \text{AC} \) of the S-boxes proposed in \([51,58,64,65]\) and equal to that of the S-boxes \([37,62,63,66]\). From the above discussion, it is obvious that the proposed S-box is highly secure against linear attacks, compared to the S-boxes in \([37,51,58,62–66]\), while the security of the proposed S-box against linear attacks is comparable with the S-boxes in \([8,12,48]\).

Table 1. Comparison of the S-boxes generated by the proposed algorithm and some recent algorithms.

| Scheme   | NL     | LAP    | AC     | DAP    | SAC (min) | SAC (max) | BIC (min) | BIC (max) |
|----------|--------|--------|--------|--------|-----------|-----------|-----------|-----------|
| Proposed | 106    | 0.0156 | 254    | 0.0469 | 0.4063    | 0.5938    | 0.4688    | 0.5293    |
| Ref. [37] | 106    | 0.1484 | 254    | 0.0234 | 0.3906    | 0.6094    | 0.4727    | 0.5254    |
| Ref. [58] | 106    | 0.1328 | 253    | 0.0391 | 0.3750    | 0.5938    | 0.4688    | 0.5254    |
| Ref. [62] | 104    | 0.0469 | 254    | 0.0391 | 0.4063    | 0.6250    | 0.4668    | 0.5234    |
| Ref. [63] | 101    | 0.0664 | 254    | 0.0391 | 0.4219    | 0.5781    | 0.4668    | 0.5195    |
| Ref. [64] | 104    | 0.0625 | 253    | 0.0391 | 0.4219    | 0.5938    | 0.4766    | 0.5391    |
| Ref. [65] | 100    | 0.0391 | 253    | 0.0469 | 0.4063    | 0.6094    | 0.4473    | 0.5332    |
| Ref. [8]  | 106    | 0.0703 | 255    | 0.0391 | 0.3906    | 0.6094    | 0.4707    | 0.5332    |
| Ref. [66] | 102    | 0.0781 | 254    | 0.0469 | 0.4219    | 0.6406    | 0.4766    | 0.5332    |
| Ref. [51] | 104    | 0.1328 | 253    | 0.0391 | 0.4063    | 0.5938    | 0.4668    | 0.5430    |
| Ref. [12] | 106    | 0.148  | 255    | 0.0470 | 0.4063    | 0.6250    | 0.4710    | 0.5390    |
| Ref. [48] | 106    | 0.148  | 254    | 0.0390 | 0.4220    | 0.5940    | 0.4710    | 0.5330    |
3.1.2. Differential Attacks

Differential attacks are used to study the differences of outputs for the corresponding differences of inputs to obtain useful information. For an S-box \( S \), the differential approximation probability \( \text{DAP}(S) \) [67] measures the strength of \( S \) to thwart the differential attackers. The mathematical representation of \( \text{DAP}(S) \) is given by:

\[
\text{DAP}(S) = \frac{1}{2^n} \left\{ \max_{\Delta x, \Delta y} \{ \# \{ x \in \mathbb{F}_2^n \mid S(x \oplus \Delta x) = S(x) \oplus \Delta y \} \} \right\},
\]

where \( \Delta x, \Delta y \in \mathbb{F}_2^n \), and “\( \oplus \)” stands for the bit-wise addition in \( \mathbb{F}_2 \). Thus, the S-box \( S \) possesses higher security if the \( \text{DAP}(S) \) is close to \( 1/2^n \). The \( \text{DAP} \) value of the S-box depicted in Table 1 is 0.0469. From Table 2, it is also evident that the \( \text{DAP} \) value of the proposed S-box is equal to the \( \text{DAP} \) values of the S-boxes displayed in [12,65,66], and comparable to the \( \text{DAP} \) of the S-boxes in [8,37,48,51,62–66]. Thus, the strength of the presented S-box against differential attacks is comparable to strength of the S-boxes in [8,12,37,48,51,58,62–66].

3.1.3. Analysis of Boolean Functions

The Boolean functions of an S-box are used to create confusion/diffusion in a cryptosystem. Two approaches, strict avalanche criterion (SAC) [68] and bit independence criterion (BIC) [68], are used to analyze the Boolean functions. The SAC calculates the change that occurred in the output bits due to the inversion of one bit in a set of input bits. The BIC determines the dependence level of a pair of output bits on inverting an input bit. For an \( n \times n \) S-box \( S \), two matrices, \( M(S) = [m_{ij}] \) and \( B(S) = [b_{ij}] \), compute the SAC(S) and the BIC(S), respectively:

\[
m_{ij} = \frac{1}{2^n} \left( \sum_{x \in \mathbb{F}_2^n} w( S_i(x \oplus a_j) \oplus S_i(x) ) \right),
\]

(4)

\[
b_{ij} = \frac{1}{2^n} \left( \sum_{1 \leq r \neq i \leq n} w( S_j(x \oplus a_j) \oplus S_i(x) \oplus S_r(x + a_j) \oplus S_r(x) ) \right),
\]

(5)

where \( w(y) \) represents the number of non-zero symbols in \( y \), \( a_j \in \mathbb{F}_2^n \) with \( w(a_j) = 1 \), and \( S_i \) denotes the \( i \)-th Boolean function of the S-box \( S \). An S-box creates enough confusion/diffusion if all off-diagonal entries of \( M(S) \) and \( B(S) \) are close to 0.5. The minimum (SAC (min)) and maximum (SAC (max)) of the off-diagonal values of \( M(S) \) for the S displayed in Table 1 are 0.4063 and 0.5938, respectively. Furthermore, it follows from Table 2 that the SAC (min) value of the designed S-box is greater than the SAC (min) values of the S-boxes designed in [8,37,58], and that the SAC (max) value of the new S-box is less than or equal to that of the S-boxes in [8,12,37,58]. So, the confusion-creation capability of the S-box in Table 1 is greater than that of the S-boxes in [8,37,58]. The SAC (min) value of the presented S-box is equal to the SAC (min) values of the S-boxes in [12,62,65], and the SAC (max) value is less than that of the S-boxes in [12,62,65]. This reveals that the proposed scheme generates S-boxes with higher confusion than the schemes in [12,62,65]. The SAC values indicate that the confusion-creation capability of the new S-box is equal to the S-box in [51] and comparable to that of [48,66]. Now, the minimum (BIC (min)) and maximum (BIC (max)) of the off-diagonal values of \( B(S) \) for \( S \) in Table 1 are 0.4688 and 0.5938, respectively. Table 2 reveals that the BIC (min) of the proposed S-box is comparable with that of the S-boxes in [8,12,37,48,51,58,62–66], and the BIC (max) value of the current S-box is less than that of the S-boxes in [8,12,48,51,64–66]. Thus, the proposed scheme generates S-boxes with diffusion-creation capabilities comparable to the S-boxes in [8,12,37,48,51,58,62–66].
4. The Proposed Encryption Scheme

Suppose we want to encrypt an image $I$ of size $u \times v$ over the symbol set $[0, 2^m - 1]$, and $I(i, j)$ represents the pixel lying at the intersection of the $i$-th row and the $j$-th column. Furthermore, let $S_1$ denote the sum of all pixel values of $I$. Then, the proposed encryption scheme consists of the following steps.

4.1. Generation of Keys

To encrypt an image of size $u \times v$, we need to generate an EC $E_{n,b}$, over a ring $\mathbb{Z}_n$, for $n = \prod_{i=1}^{k} p_i$. For the sake of convenience, we take $k = 2$ and $n \geq uv$, so that we choose primes $p_1, p_2$ and integers $b, t \in \mathbb{Z}_n$ to generate $E_{n,b}$. Thus, $p_1, p_2, b$ and $t$ are chosen in such a way that there exists at least $uv$ points $(x, y) \in E_{n,b}$, where $y$ is attaining each value in the interval $[0, 2^m - 1]$. This condition is imposed to ensure the generation of an S-box using points of the EC $E_{n,b}$. We further choose an integer value $\ell_1$ as a key. The use of the key $\ell_1$ is explained in Section 4.4(i). The parameters $p_1, p_2, b, t$, and $\ell_1$ are all secret keys.

4.2. Masking Phase

Before masking an image $I$, we first arrange the points of the EC $E_{n,b}$ according to the ordering $\prec_D$. After ordering, we assume that $(x_i, y_i) \in E_{n,b}$ stands for the $i$-th point of the EC $E_{n,b}$. The reason for this is that the $\prec_D$ diffuses the $y$-coordinates of the points lying on an EC, because, over a ring of integers $\mathbb{Z}_n$, if $(x, y) \in E_{n,b}$, then, for such an $x$, there are at least two values $y_1, y_2$ of $y$ in $\mathbb{Z}_n$ such that $(x, y_1), (x, y_2) \in E_{n,b}$. The masking phase of an image $I$ takes place as follows:

(i) Generate a row matrix $M$ from $(x_i, y_i) \in E_{n,b}$ of length $2(#E_{n,b})$ such that, for $1 \leq i \leq #E_{n,b}$, we have:

$$M(j) = \begin{cases} x_i, & \text{if } j \text{ is odd} \\ x_i + y_i, & \text{otherwise} \end{cases}$$

The purpose of constructing matrix $M$ is to design a sequence from both coordinates of $E_{n,b}$. The elements of the said sequence are used to hide the pixel values of an image $I$;

(ii) Choose a submatrix $N$, which consists of the first $uv$ entries of the matrix $M$ because only the $uv$ values are needed to hide the pixel values. The chosen $n$ should not be less than $uv$; otherwise, in Section 4.3(i), the construction of $M_2$ with size $u \times v$ will not be possible;

(iii) The sensitivity to the plain image is necessary for a secure cryptosystem. For this purpose, transform the entries of $N$ by the pixel value $I(1, 1)$ to obtain the matrix $B$, given by:

$$B(i) = N(i) + I(1, 1).$$

There is no restrictions on pixel or the number of pixels. Any number of arbitrary pixels may be used for transformation. For the sake of convenience, only one pixel value $I(1, 1)$ is fixed;

(iv) For the sake of simplicity, reshape the matrix $B$ to construct a matrix with $u$ rows and $v$ columns. By reshaping $B$, we mean that $B$ is divided into $v$ blocks such that each block contains $u$ entries and the $i$-th block represents the $i$-th column of the matrix $B$, so that the corresponding values of both $B$ and $I$ are combined to hide the pixel values of the image $I$;

(v) To obtain the masked image $M_I$, mask the pixels of image $I$ using Equation (7):

$$M_I(i, j) = I(i, j) + B(i, j) \pmod{2^m}.$$
Since there is a one–one correspondence between \( E_{n,b} \) and \( E_{p_1,b} \times E_{p_2,b} \), \( E_{n,b} \) may be mapped onto \( E_{p_1,b} \) and \( E_{p_2,b} \) respectively, via the following maps:

\[
(x, y) \rightarrow (x \mod p_1, y \mod p_1), \quad (8)
\]

\[
(x, y) \rightarrow (x \mod p_2, y \mod p_2). \quad (9)
\]

These two ECs, \( E_{p_1,b} \) and \( E_{p_2,b} \), are used to alter the pixels of an image. The S-box generated on \( E_{n,b} \) is used to create the confusion in the encrypted image. The steps of the said procedure are explained in the following phase.

4.3. Diffusion Phase

The steps of this phase are explained as follows:

(i) For \( 1 \leq i \leq \#E_{n,b} \), construct two row matrices, \( M_k, k = 1, 2 \), due to the all points \((x_i, y_i) \in E_{p_k,b}\) for both primes \( p_k, k = 1, 2 \), respectively, such that:

\[
M_1(j) = \begin{cases} 
    x_{1i}, & \text{if } j \text{ is odd} \\
    x_{1i} + y_{1i}, & \text{otherwise},
\end{cases}
\]

and:

\[
M_2(j) = y_{1i}.
\]

In fact, we want to generate two sequences using ECs \( E_{p_1,b} \) and \( E_{p_2,b} \). Both sequences consist of integer values, which are further used to alter the pixel values of the masked image \( M_1 \) in Section 4.3(v) and to permute the image \( P \) in Section 4.4(iii), respectively;

(ii) Take submatrices \( N_{ik}, k = 1, 2 \) containing the first \( uv \) entries of \( M_{ik}, k = 1, 2 \), respectively, so as to choose the sequences of length that are equal to that of the number of pixels in the image \( I \);

(iii) Modify the sizes of above constructed matrices, so that \( N_{ik}, k = 1, 2 \) has \( u \) rows and \( v \) columns. The reason for generating such matrices has been explained previously;

(iv) Apply the modulo \( 2^m \) operator to \( N_{ik}, k = 1, 2 \) to generate the matrices \( B_{ik}, k = 1, 2 \), consisting of \( m \)-bit integers. Since for encrypting \( m \)-bit images, \( m \)-bit sequences are needed;

(v) Convert the elements of \( M_1 \) and \( B_{ik}, k = 1, 2 \) into the binary format and generate the image \( X_1 \) by diffusing the pixels of \( M_1 \) by the following equation:

\[
X_1(i, j) = M_1 \oplus B_1(i, j), \quad (10)
\]

where \( \oplus \) is a logical operator (XOR operation by binary bit) known as exclusive disjunction.

4.4. Confusion Phase

For a secure cryptographic algorithm, it is necessary to have a desired level of confusion. For the current cryptosystem, the confusion phase consists of the following steps:

(i) Choose a secret key \( \ell_1 \) to construct a shifting parameter \( \ell_2 \), such that \( \ell_2 = S_1 + \ell_1 \) (mod \( 2^m \)); then, give a circular shift to the S-box \( \sigma(n, t) \) to design a new S-box \( \sigma'(n, t, \ell_2) \). The shifting parameter, the secret key \( \ell_1 \), and \( S_1 \) are linked in order to enhance the sensitivity to the plain image \( I \);

(ii) Permute the pixels of the image \( X_1 \) using the S-box \( \sigma'(n, t, \ell_2) \) as follows:

\[
P(i, j) = \sigma(n, t, \ell_2)X_1(i, j). \quad (11)
\]

In the coming encryption of a \( 4 \times 4 \) hypothetical image, the first entry of \( X_1 \) is 2. Then, \( \sigma(n, t, \ell_2)(2) \) represents the third entry of the S-box \( \sigma(n, t, \ell_2) \), which is 1. That is, \( \sigma(n, t, \ell_2)(r) \) stands for the \( (r + 1) \)-th element of the S-box \( \sigma(n, t, \ell_2) \);
(iii) In order to obtain the scrambled image \( X_2 \), repeat Section 4.3(v) using \( P \) in place of \( M \), and replacing \( B_1(i, j) \) with \( B_2(i, j) \), such that:

\[
X_2(i, j) = P \oplus B_2(i, j);
\]  

(12)

(iv) Finally, to obtain the encrypted image \( C \) with the desired level of confusion, permute the image \( X_2 \) as follows:

\[
C(i, j) = \sigma(n, t, \ell_2)X_2(i, j).
\]  

(13)

The flowchart of the proposed encryption scheme is shown in Figure 1.

---

We theoretically derive the time complexity of the proposed scheme in Theorem 1.

**Theorem 1.** Let \( I \) be a plain image of size \( u \times v \), and let \( n \geq uv \) be a positive integer; then, the time complexity of the proposed scheme is \( O(\max\{nt, (#E_{n,b}) \log (#E_{n,b})\}) \), where \( t \leq n \) is an integer such that \( E_{n,b} \) is computed for all \( x \in [0, n - 1] \) and \( y \leq t \).

**Proof.** In the key generation phase (Section 4.1), to compute all \((x, y) \in E_{n,b}\), we need to check for each \( x \in [0, n - 1] \), \( t \) values of \( y \in [0, t - 1] \), such that \( y^2 \equiv x^3 + b \pmod{n} \). Thus, the computation of \( E_{n,b} \) takes \( O(nt) \) time. Further, the ordering of the points of the EC \( E_{n,b} \) needs \( O((#E_{n,b}) \log (#E_{n,b})) \) time. In Section 4.2(i), we can see that \( #M = 2(#E_{n,b}) \); therefore, \( M \) can be constructed in \( O(n) \) time. As \( #N = #B = uv \), we can design \( N, B \) by a
for loop, executing \( uv \) times. Furthermore, \( B \) can be reshaped by two nested loops, such that one loop executes \( u \) times, while the other executes \( v \) times. In a similar way, we can add two matrices of the same order by two nested loops. Thus, the time complexity of Section 4.2(ii)–(v) is \( O(uv) \). From the chosen keys, we have \( n \geq uv \) and \( \#E_{n,b} \leq n \), so that the complexity of the masking phase is \( O\left(\max\{nt, (\#E_{n,b}) \log(\#E_{n,b})\}\right) \).

Now, we can map the EEC \( E_{n,b} \) on the ECEs \( E_{p_1,a,b} \) and \( E_{p_2,a,b} \) in \( O(n) \) time. In the diffusion phase (Section 4.3(i)), \( \#M_k = 2(\#E_{n,b}) \) and \( \#N_k = \#B_k = uv \) for \( k = 1, 2 \). Therefore, Section 4.3(i)–(v) takes \( O(\#E_{n,b}) \) and \( O(uv) \) time, respectively.

In the confusion phase (Section 4.4(i)), the time required to compute \( S_I \) is \( O(uv) \) and \( \ell_2 \) can be computed in constant time. Since \( X_I \) has \( uv \) entries, we can implement Section 4.4(ii)–(iv) in \( O(uv) \) time, using two nested loops executing \( u \) and \( v \) times, respectively.

Clearly, \( nt > n \) and \( n \geq uv \); thus, the above discussion implies that the time complexity for the presented scheme is \( O\left(\max\{nt, (\#E_{n,b}) \log(\#E_{n,b})\}\right) \). 

As the time complexity is dependent on the parameter \( t \), that is, the time is controllable with \( t \), the current scheme is effective, particularly when a large dataset of images is to be encrypted.

The whole process is illustrated by the encryption of a 4-bit hypothetical image, as shown in Figure 2.

![Figure 2. Encryption of a 4 x 4 image by the proposed scheme.](image-url)
5. Decryption

The decryption process takes place by reversing all the steps of the encryption process. The receiver will need the keys $p_1, p_2, b, t$, and $\ell_1$ to generate the inverse S-box $\sigma^{-1}(n, t, \ell_2)$ and the matrices $B_k, k = 1, 2$. Then, by the use of Equations (6), (7), and (10)–(13), one can obtain the original image $I$.

6. Security Analysis

In this section, some well-known metrics are described, which are generally used to measure the security level of new algorithms. The security of the proposed encryption scheme is evaluated by performing experiments on all-gray images of different sizes, taken from the USC-SIPI database [69]. The database consists of square images of size $w \times w, w = 256, 512, 1024$. The plain images of Lena and Clock, along with their encrypted images, are shown in Figure 3. The experiments are performed by taking the parameters $p_1 = p_2 = 1031, b = 7, t = 1031^2$ and $\ell_1 = 80 - S_I$, using MATLAB 2016a on a personnel machine equipped with a 1.8 GHz processor, 6 GB RAM, and Windows 10 operating system. The security strength of the encryption algorithm is analyzed in the following subsections.

![Figure 3.](image)

Figure 3. (a,e) Plain images; (b,f) masked images; (c,g) diffused images; (d,h) encrypted images of Lena and Clock, respectively.

6.1. Differential Attacks Analysis

The cryptographic strength of an encryption scheme against differential attacks is analyzed by two measures: the number of pixels’ change rate (NPCR) and the unified average changing intensity (UACI). In an encryption algorithm, the change of one pixel of a plain image has an influence on the encrypted image. The NPCR is a criterion used to measure the influence of a change in a plain image on the ciphers. The UACI criterion measures the average intensity difference between two different images. If $I$ and $I'$ are any two plain images of the same dimension $u \times v$, and $C_I$ and $C_{I'}$ are the respective cipher images of $I$ and $I'$, then NPCR and UACI are calculated by Equations (14) and (15), as given by:

$$\text{NPCR} = \sum_{i=1}^{u} \sum_{j=1}^{v} \frac{\tau(i,j)}{u \times v}, \quad (14)$$

$$\text{UACI} = \sum_{i=1}^{u} \sum_{j=1}^{v} \frac{|C_I(i,j) - C_{I'}(i,j)|}{255 \times u \times v}, \quad (15)$$
where \( \tau(i,j) = 0 \) if \( C_I(i,j) = C_I'(i,j) \), and \( \tau(i,j) = 1 \), otherwise. For 8-bit images with \( w = 256, 512, 1024 \), the theoretical values of NPCR are 99.5693, 99.5893, 99.5994, respectively. Unlike NPCR, the expected ranges of UACI are [33.2824, 33.6447], [33.3730, 33.5541], and [33.4183, 33.5088], respectively [18]. We randomly choose \( i \) and \( j \), and a random value is assigned to the pixel \( I(i,j) \) for each image \( I \) of the database. The random values of \( i, j \) and \( I(i,j) \) for images of size \( w = 256 \) are shown in Figure 4a. Then, the NPCR and UACI results for the current scheme are computed for each image of the database for a randomly chosen pixel value \( I(i,j) \); the graphical results are shown in Figure 4b,c, where the average values of NPCR and UACI are 99.60 and 33.32, respectively, which are close enough to the expected values.

Moreover, we randomly changed one pixel value of some images, and compared the results of the NPCR and UACI tests with the results of the recent schemes in [14–18,28,51,57,70,71], as shown in Tables 3 and 4, respectively. The pass ratio for the proposed scheme in Table 3 is higher than that of the schemes in [14,15,17,28,51], and equal to that of the schemes in [16,18,57,70,71]. Similarly, the pass ratio for the proposed scheme in Table 4 is higher than that of the schemes in [15–17,51,57,70] and equal to that of the schemes in [14,18,28,71]. It follows that the proposed scheme has better performance against differential attacks than the schemes in [14–17,28,51,57], and has comparable performance to the schemes in [18,71].

![Figure 4.](image)

Figure 4. (a) Random values of \( i, j \) and \( I(i,j) \); (b–d) NPCR, UACI, and entropy results, respectively, for the whole image database.
Comparison of entropy results due to the proposed algorithm and some other schemes, where

\[
H(I) = - \sum_{i=1}^{k} p(x_i) \log_2(p(x_i)),
\]

where \(p(x_i)\) represents the probability of a pixel value \(x_i\), and \(k\) is the total number of gray values in an image \(I\). For an 8-bit encrypted image, the ideal value of entropy is 8, which corresponds to the highest level of uncertainty. Thus, for a cryptographically strong encryption scheme, the value of \(H(I)\) should be close to 8. The entropy results for the current scheme are computed for each image of the database as shown in Figure 4d. The entropy for images of size \(w = 256, 512, 1024\) are lying in the ranges \([7.9966, 7.9977], [7.9991, 7.9995]\), and \([7.9998, 7.99987]\), respectively. In all cases, the entropy approaches the optimal value. Consequently, the proposed encryption scheme is capable of providing high randomness in a cipher.

The comparison of the entropy results is carried out in Table 5. It is clear from Table 5 that the information entropy for the presented scheme is higher than that of \([15–17,19,20,28,46,51,57]\) and comparable to that of the schemes in \([14,18,41,72]\). Thus, our scheme generates encrypted images having more randomness than the techniques in \([15–17,19,20,28,46,51,57]\).
6.3. Histogram

A histogram of an image represents the frequency distribution of the gray values. If each pixel value occurs with almost equal frequency in an image, then the histogram of that image is said to be uniform. The histogram of an ordinary image is always highly nonuniform, while a properly encrypted image has a uniform histogram. Figure 5a,c depicts the histograms of the plain images in Figure 3a,e, respectively, and Figure 5b,d shows the histograms of the cipher images in Figure 3d,h, respectively.

![Histograms of plain and encrypted images](image)

**Figure 5.** Histograms of plain and encrypted images: (a,c) histogram of the plain images in Figure 3a,e, respectively; (b,d) histogram of the encrypted images in Figure 3d,h, respectively.

It is evident from the histograms that the proposed scheme encrypts an image in such a way that it does not reveal any secret information of the former.

6.4. Correlation

A pixel of an ordinary image has high correlation with adjacent pixels. A good encryption scheme breaks the correlation among the pixels of an encrypted image. The correlation coefficient between datasets $x$ and $y$ of the same size $M$ is determined by:

$$C_{xy} = \frac{\sum_{i=1}^{M} (x_i - E[x])(y_i - E[y])}{\sqrt{\sum_{i=1}^{M} (x_i - E[x])^2 \sum_{i=1}^{M} (y_i - E[y])^2}}, \quad (17)$$

where $x_i \in x$ and $y_i \in y$ and $E[x] = \frac{1}{M} \sum_{i=1}^{M} x_i$. The horizontal, diagonal, off-diagonal, and vertical correlation coefficients among the pixels of each image in the database encrypted by the proposed scheme are computed as shown in Figure 6. The average values of correlation in Figure 6a–d are $-0.00012$, $-0.00038$, $-0.00026$, and $-0.00004$, respectively. From these results, it follows that the proposed scheme makes the correlation close to zero in all directions. So, the proposed method is capable of disrupting the correlation of pixels in ciphers.
In addition, a random sample of 2560 pairs of pixels is selected along the horizontal, diagonal, off-diagonal, and vertical directions from both the plain image and the cipher image of Lena\(_{512 \times 512}\). The correlation distribution between the adjacent gray values before and after encryption is shown in Figure 7.

It follows from Figure 7a–d that adjacent pixels of the plain image are in high correlation, but Figure 7e–h indicates that the proposed scheme successfully weakens the correlation of the pixels.

The correlation results for encrypted image of Lena\(_{512 \times 512}\) and Barbara\(_{512 \times 512}\) are compared with other schemes in Table 6. It can be observed that the results for the Lena image of the current scheme are better than all the compared schemes. Similarly, the results for the Barbara image encrypted by the proposed scheme are better than that of the schemes in [19,41,51,72], and comparable to the results of [16,57]. Thus, our scheme generates encrypted images with more randomness than the other techniques listed in Table 6.

Figure 6. Correlation among the adjacent pixels of each encrypted image in the databases: (a) horizontal; (b) diagonal; (c) off-diagonal; (d) vertical correlation.

Figure 7. Correlation distribution of adjacent pixels of plain image along the (a) horizontal, (b) diagonal, (c) off-diagonal, and (d) vertical directions, respectively; correlation distribution of adjacent pixels of cipher image along the (e) horizontal, (f) diagonal, (g) off-diagonal, and (h) vertical directions, respectively.
Table 6. Comparison of correlation results along all the three directions for the Lena and Barbara images, due to the proposed algorithm and some other schemes.

| Scheme     | Lena Horizontal | Lena Vertical | Lena Diagonal | Barbara Horizontal | Barbara Vertical | Barbara Diagonal |
|------------|-----------------|---------------|---------------|--------------------|-----------------|------------------|
| Proposed   | −0.0006         | −0.00009      | −0.0005       | 0.0007             | 0.0014          | −0.0005          |
| Ref. [14]  | −0.0026         | −0.0054       | 0.0082        | −                 | −               | −                |
| Ref. [28]  | −0.0353         | 0.0286        | −0.0249       | −                  | −               | −                |
| Ref. [15]  | −0.0011         | −0.0020       | 0.0064        | −                  | −               | −                |
| Ref. [16]  | 0.0027          | 0.0003        | 0.0012        | 0.0005             | 0.0068          | 0.0003           |
| Ref. [17]  | −0.0005         | −0.0011       | −0.0015       | −                  | −               | −                |
| Ref. [18]  | 0.0039          | 0.0059        | −0.0050       | −                  | −               | −                |
| Ref. [19]  | −0.0013         | 0.0080        | −0.0094       | −0.0047            | 0.0007          | 0.0060           |
| Ref. [20]  | −0.0005         | 0.0012        | 0.0007        | −                  | −               | −                |
| Ref. [51]  | 0.0009          | 0.0097        | −0.0013       | −0.0016            | 0.0038          | 0.0014           |
| Ref. [57]  | −0.0003         | −0.0005       | 0.0005        | −0.0002            | 0.0003          | −0.0006          |
| Ref. [46]  | 0.0023          | 0.0029        | 0.0021        | −                  | −               | −                |
| Ref. [72]  | 0.0019          | −0.0024       | 0.0011        | −0.0024            | 0.0031          | −0.0013          |
| Ref. [41]  | 0.0019          | −0.0006       | −0.0014       | −0.00007           | −0.0022         | 0.0007           |

6.5. Key Space

Key space is a set consisting of the all possible secret keys for a cryptosystem. Generally, for a good cryptosystem, the size of a key space should be at least $2^{128}$. The five keys $p_1, p_2, b, t$, and $\ell_1$ are introduced by the proposed scheme. The least number of bits to store a key required by the proposed algorithm is 29. Thus, the size of our key space is $2^{145}$, which is much larger than $2^{128}$. Hence, the described scheme has the capability to resist brute-force attacks in an efficient way.

6.6. Key Sensitivity

This is an important feature of a cryptographically strong cryptosystem. Key sensitivity is also necessary to resist brute-force attacks. If a small change in a key leads to a significant change in the cipher, then the cryptosystem is said to be sensitive to the keys. For this purpose, we decrypted the Lena image by changing a single key; the results are shown in Figure 8b–d.

![Figure 8](image_url)

(a) (b) (c) (d)

Figure 8. Decrypted image with (a) actual keys; (b) $p_1 = p_2 = 257$; (c) $b = 8$; (d) $\ell_1 = \ell_1 + 1$.

Moreover, slightly changing the keys $b$ and $p$ change the coordinates of the ECs $E_{257,1}$, $E_{257,2}$, and $E_{263,1}$; these are shown in Figure 9a,b, respectively.

Figure 9 shows the sensitivity of the masking phase to the parameters of the ECs. From Figures 8 and 9, it follows that slight changes in a key lead to very different results. Hence, our proposed scheme is highly sensitive to the keys.
6.7. Plain-Text Attacks

There are two types of plain-text attacks, i.e., known plain-text attacks and chosen plain-text attacks. In known plain-text attacks, the attacker knows about a string of the plain text, along with the relevant string of the cipher text. In chosen plain-text attacks, the adversary has a partial access to the encryption scheme. That is, the adversary can obtain the ciphered string for a chosen plain-text string. For this purpose, attackers use all-black or all-white images to obtain information about the encryption scheme [50], so that a secure encryption scheme encrypts all-black and all-white images with optimal results. The efficiency of the current scheme is visible from Table 7 and Figure 10.

Table 7. Analysis of the proposed encryption technique against plain-text attacks.

| Plain Image  | NPCR (%) | UACI (%) | Correlation of Cipher Image | Entropy  |
|--------------|----------|----------|----------------------------|----------|
|               |          |          | Hor. | Ver. | Diag. |               |          |
| All-black     | 99.62    | 33.42    | 0.0046 | 0.0036 | −0.0040 | 7.9974         |
| All-white     | 99.62    | 33.49    | 0.0062 | 0.0037 | 0.0012 | 7.9974         |

Figure 9. (a) Two ECs generated for a small change in the key b; (b) points of ECs for two different primes.

Figure 10. (a,e) Plain images; (b,f) masked images; (c,g) diffused images; (d,h) encrypted images of all-black and all-white images, respectively; (i,k) histograms of (a,e), respectively; (j,l) histograms of (d,h), respectively.
Table 7 and Figure 10 indicate that the current scheme not only randomizes the all-white and all-black images, but also weakens the pixels’ correlation and makes the pixels’ distribution uniform in the encrypted images. Thus, the proposed scheme is highly secure against both kinds of plain-text attacks.

7. An Application to Encryption of Color Images

In this section, we apply the proposed scheme to the color images. We encrypted images of Female_{256×256}, Lena_{512×512}, and San Francisco_{1024×1024} using the parameters $p_1 = p_2 = 1031, b = 7, l = 1031^2$, and $l_1 = 80 - S_I$, where $l$ stands for the R (Red), G (Green), and B (Blue) components of an image, respectively. The plain and encrypted images of Female_{256×256}, Lena_{512×512}, and San Francisco_{1024×1024} are shown in Figure 11.

The NPCR and UACI results are computed by randomly changing a pixel value in each channel. It can be observed from Table 8 that the NPCR and UACI results of each channel for the tested color images lie in the expected range. Similarly, the entropy results of the R, G, and B components also belong to the expected ranges for each of the color images.

| Image        | Size   | NPCR (%) | UACI (%) | Entropy |
|--------------|--------|----------|----------|---------|
| Female       | 256×256| 99.61    | 99.57    | 33.32   | 33.33   | 33.28   | 7.9974 | 7.9972 | 7.9971 |
| Lena         | 512×512| 99.61    | 99.66    | 33.41   | 33.45   | 33.44   | 7.9992 | 7.9992 | 7.9994 |
| San Francisco| 1024×1024| 99.67   | 99.67    | 33.48   | 33.45   | 33.48   | 7.9998 | 7.9998 | 7.9998 |

The experimental results of the color Lena_{512×512} are compared with the results of the schemes in [7,28,29,73–78], as shown in Tables 9 and 10.
Table 9. Comparison of NPCR and UACI results for the color image of Lena_{512×512}.

| Scheme  | Image  | NPCR (%) | UACI (%) |
|---------|--------|----------|----------|
|         |        | R        | G        | B        | Average | R        | G        | B        | Average |
| Proposed| Lena   | 99.61    | 99.66    | 99.63    | 99.64   | 33.41    | 33.45    | 33.44    | 33.44   |
| Ref. [73]|       | 99.63    | 99.62    | 99.65    | 99.63   | 33.60    | 33.50    | 33.55    | 33.55   |
| Ref. [74]|       | 99.62    | 99.64    | 99.60    | 99.62   | 33.43    | 33.45    | 33.43    | 33.44   |
| Ref. [75]|       | 99.56    | 99.63    | 99.63    | 99.61   | 35.46    | 33.22    | 33.02    | 33.90   |
| Ref. [76]| Lena   | 99.63    | 99.63    | 99.57    | 99.61   | 33.49    | 33.38    | 33.47    | 33.45   |
| Ref. [77]|       | 99.61    | 99.61    | 99.61    | 99.61   | 33.43    | 33.50    | 33.38    | 33.38   |
| Ref. [28]|       | 99.62    | 99.63    | 99.59    | 99.61   | 33.44    | 33.53    | 33.48    | 33.48   |
| Ref. [29]|       | 99.60    | 99.60    | 99.60    | 99.60   | 33.55    | 33.50    | 33.46    | 33.50   |
| Ref. [78]|       | 99.69    | 99.70    | 99.50    | 99.63   | 33.36    | 33.58    | 33.38    | 33.38   |
| Ref. [7] |    | 99.61    | 99.62    | 99.61    | 99.61   | 33.51    | 33.45    | 33.39    | 33.45   |

The results in Table 9 reveal that the NPCR values for the R, G, and B components of Lena_{512×512} are greater than the theoretical value (99.5893). Apart from this, the R component’s NPCR value is greater than the values of the schemes in [29,75], equal to that of [7,77], and comparable with [28,74,76]. The NPCR value of the G plane is greater than all the NPCR results of to the schemes in [7,28,29,73–77]. Similarly, the NPCR results of the B component is better than the results of [7,28,29,74–78]. In addition, the average NPCR value resulting from the current scheme is greater than the NPCR results of all the listed schemes in Table 9. The UACI results of the R, G, and B components of the current scheme lie in the expected range. Furthermore, the UACI results of the new scheme for all the three components are better than the results of the schemes in [7,73,75,78] and comparable to that of the schemes in [28,29,74,76,77]. It follows that the proposed scheme is better in performance against the differential attacks than the schemes in [7,28,70,73–78].

Table 10. Comparison of the Entropy results for the color image of Lena_{512×512}.

| Scheme  | Image  | Entropy |
|---------|--------|---------|
|         |        | R       | G       | B       | Average |
| Proposed| Lena   | 7.9992  | 7.9992  | 7.9994  | 7.9993  |
| Ref. [73]|       | 7.9994  | 7.9993  | 7.9993  | 7.9993  |
| Ref. [74]|       | 7.9912  | 7.9914  | 7.9915  | 7.9914  |
| Ref. [75]|       | 7.9278  | 7.9744  | 7.9705  | 7.9576  |
| Ref. [76]| Lena   | 7.9992  | 7.9993  | 7.9994  | 7.9993  |
| Ref. [77]|       | 7.9895  | 7.9894  | 7.9894  | 7.9894  |
| Ref. [28]|       | 7.9993  | 7.9993  | 7.9993  | 7.9993  |
| Ref. [29]|       | 7.9993  | 7.9992  | 7.9993  | 7.9993  |
| Ref. [78]|       | 7.9992  | 7.9994  | 7.9993  | 7.9993  |
| Ref. [7] |       | 7.9993  | 7.9994  | 7.9994  | 7.9994  |
| Ref. [43]|       | 7.9993  | 7.9994  | 7.9993  | 7.9993  |

Table 10 reveals that the entropy value of the R component is greater than that in [74,75,77] and equal to the values of [76,78]. The entropy value of the G component is also greater than that in [74,75,77] and equal to the value of [29]. Similarly, the entropy result of the B component is greater than the results of [28,29,43,73–75,77,78] and equal to that of [7,76]. In addition, the average entropy value resulting from the current scheme is better than that of the schemes in [73–75,77] and equal to that of the results of [28,29,43,76,78]. This discussion indicates that the current scheme generates encrypted color images with higher randomness than the schemes in [74,75,77], and the randomness of the encrypted images in current scheme and the schemes in [29,78] is comparable.
The histograms of the channels of the plain Lena$_{512 \times 512}$ and the encrypted Lena$_{512 \times 512}$ are shown in Figure 12a–f, respectively.

Figure 12 confirms that the histograms of the encrypted channels are uniform and, hence, the presented scheme encrypts color images having high resistance against the statistical attacks.

![Histograms of plain Lena and encrypted Lena](image)

**Figure 12.** (a–c) Histogram of the plain R, G, and B channels of the color Lena$_{512 \times 512}$, respectively; (d–f) histogram of the encrypted R, G, and B channels of the color Lena$_{512 \times 512}$, respectively.

In Table 11, the correlation of the adjacent pixels of three different encrypted images with different sizes is shown. It is evident that the proposed scheme encrypts any image in such a way that it weakens the correlation between two adjacent pixels of any channel.

**Table 11.** Correlation coefficients of two adjacent pixels in encrypted color images.

| Image    | Size     | Correlation | Horizontal | Diagonal | Vertical |
|----------|----------|-------------|------------|----------|----------|
|          |          | R | G | B | R | G | B | R | G | B |
| Female   | 256 x 256| 0.000177 | 0.00240 | 0.00253 | 0.00143 | 0.00256 | 0.00354 | 0.00097 | 0.00113 | 0.00027 |
| Lena     | 512 x 512| -0.00035 | -0.00221 | 0.00084 | 0.00108 | 0.00002 | 0.00007 | 0.00200 | 0.00133 | -0.00026 |
| San Francisco | 1024 x 1024 | -0.00059 | -0.00067 | 0.00125 | 0.00083 | -0.00013 | 0.00002 | 0.00158 | -0.00031 | 0.00120 |

Along with other properties, a good encryption scheme should be highly efficient. Different color images with different sizes are encrypted using the current scheme. To demonstrate the efficiency of the current scheme, the encryption times (sec) for the said three images are computed, since we use a pre-computed EC over the ring of integers as an input for all input images. While computing the encryption time, the time taken by the inputs is not taken under the consideration. The encryption time of the current scheme is compared with the time of some recent schemes [28,78,79], as shown in Figure 13. The results for the schemes in [28,78,79] are available in Table 3 of [80].
For images of size $w = 256,512$, the performance of our scheme is comparable with that of [28], and for $w = 1024$, the new scheme is highly efficient, compared to the scheme of [28]. Similarly, in Figure 13, the plots of [78,79] are overlapping, but our scheme is more efficient than [78,79] for images of all sizes.

Thus, the presented scheme is capable of efficiently encrypting color images as well, and can be used for the good encryption of color images.

8. Conclusions

We proposed a new S-box generator and an image encryption algorithm. We employed an EC over a ring of integers instead of a finite field. The presented S-box is highly resistive against linear attacks when compared to the S-boxes generated by the ECs over finite fields in [37,51,58] and the S-boxes of [62–66]. The confusion-creation capability of the proposed S-box is higher than that of the S-boxes in [8,37,58].

Furthermore, our encryption scheme has better performance against differential attacks than that of the EC-based schemes [51,57] and the schemes in [14–17,28], and provides encrypted images with higher randomness than the schemes in [15–17,19,20,28,51,57]. The current scheme is also used for different color images. The presented scheme is able to encrypt color images with low run-times and higher security when compared with [78,79], while the scheme in [51] discusses the novelty regarding only gray images. Furthermore, for relatively large images, the run-time of the current scheme is very low, compared to the schemes in [28,78,79]. The future directions consist of the following works:

(i) To improve the current scheme for the simultaneous encryption of all channels of a color image; (ii) To optimize the current scheme for a text-encryption algorithm; (iii) To generate random numbers based on ECs over rings and employ the sequence of random numbers in text encryption; (iv) To generate random binary sequences using ECs over a ring of integers and experimentally prove their cryptographic strength.

Author Contributions: Conceptualization, U.H. and N.A.A.; Funding acquisition, N.A.A. and S.A.; Methodology, U.H., I.U., N.A.A. and S.A.; Software, U.H., I.U., N.A.A. and S.A.; Supervision, U.H. and N.A.A.; Writing—original draft, I.U. and S.A.; Writing—review & editing, U.H. and N.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by the HEC project NRPU-7433 and the QAU project URF-2015.

Conflicts of Interest: The authors declare no conflict of interest.
Abbreviations

The following abbreviations are used in this manuscript:

ECs  Elliptic curves
S-box  Substitution box

References

1. Ibrahim, S.; Alharbi, A. Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography. *IEEE Access* 2020, 8, 194289–194302. [CrossRef]

2. Murphy, S.; Robshaw, M.J. Essential algebraic structure within the AES. In Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology, Berlin/Heidelberg, Germany, 18–22 August 2002; pp. 1–16.

3. Rosenthal, J. A polynomial description of the Rijndael Advanced Encryption Standard. *J. Algebra Its Appl.* 2003, 2, 223–236. [CrossRef]

4. Cui, L.; Cao, Y. A new S-box structure named Affine-Power-Affine. *Int. J. Innov. Comput. Inf. Control* 2007, 3, 751–759.

5. Liu, J.; Wei, B.; Cheng, X.; Wang, X. An AES S-box to increase complexity and cryptographic analysis. In Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA’05) Volume 1 (AINA Papers), Taipei, Taiwan, 25–30 March 2005; Volume 1, pp. 724–728.

6. Tran, M.T.; Bui, D.K.; Duong, A.D. Gray S-box for advanced encryption standard. In Proceedings of the 2008 International Conference on Computational Intelligence and Security, Suzhou, China, 13–17 December 2008; Volume 1, pp. 253–258.

7. Silva-Garcia, V.M.; Flores-Carapia, R.; Gonzalez-Ramirez, M.D.; Vega-Alvarado, E.; Villarreal-Cervantes, M.G. Cryptosystem Based on the Elliptic Curve With a High Degree of Resistance to Damage on the Encrypted Images. *IEEE Access* 2020, 8, 218777–218792. [CrossRef]

8. Özkanayık, F. Construction of robust substitution boxes based on chaotic systems. *Neural Comput. Appl.* 2019, 31, 3317–3326. [CrossRef]

9. Miller, V.S. Use of elliptic curves in cryptography. In Proceedings of the Conference on the Theory and Application of Cryptographic Technique, Linz, Austria, 9–11 April 1985; pp. 417–426.

10. Cheon, J.H.; Chee, S.; Park, C. S-boxes with controllable nonlinearity. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999; pp. 286–294.

11. Hayat, U.; Azam, N.A.; Asif, M. A method of generating $8 \times 8$ substitution boxes based on elliptic curves. *Wirel. Pers. Commun.* 2018, 101, 439–451. [CrossRef]

12. Hayat, U.; Azam, N.A.; Gallegos-Ruiz, H.R.; Naz, S.; Batool, L. A Truly Dynamic Substitution Box Generator for Block Ciphers Based on Elliptic Curves Over Finite Rings. *Arab. J. Sci. Eng.* 2021, 46, 8887–8899. [CrossRef]

13. Azam, N.A. A novel fuzzy encryption technique based on multiple right translated AES gray S-boxes and phase embedding. *Secur. Commun. Netw.* 2017, 2017, 5790189. [CrossRef]

14. Liu, L.; Miao, S. A new simple one-dimensional chaotic map and its application for image encryption. *Multimed. Tools Appl.* 2018, 77, 21445–21462. [CrossRef]

15. Liu, L.; Miao, S.; Hu, H.; Cheng, M. N-phase logistic chaotic sequence and its application for image encryption. *IET Signal Process.* 2016, 10, 1096–1104. [CrossRef]

16. Wang, X.; Feng, L.; Li, R.; Zhang, F. A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model. *Nonlinear Dyn.* 2019, 95, 2797–2824. [CrossRef]

17. Tang, J.; Yu, Z.; Liu, L. A delay coupling method to reduce the dynamical degradation of digital chaotic maps and its application for image encryption. *Multimed. Tools Appl.* 2019, 78, 24765–24788. [CrossRef]

18. Talhaoui, M.Z.; Wang, X.; Midoun, M.A. Fast image encryption algorithm with high security level using the Bülban chaotic map. *J. Real-Time Image Process.* 2020, 18, 85–98. [CrossRef]

19. Ismail, S.M.; Said, L.A.; Radwan, A.G.; Madian, A.H.; Abu-Elyazeed, M.F. Generalized double-humped logistic map-based medical image encryption. *J. Adv. Res.* 2018, 10, 85–98. [CrossRef] [PubMed]

20. Wang, M.; Wang, X.; Zhao, T.; Zhang, C.; Xia, Z.; Yao, N. Spatiotemporal Chaos in Improved Cross Coupled Map Lattice and Its Application in a Bit-level Image Encryption Scheme. *Inf. Sci.* 2020, 544, 1–24. [CrossRef]

21. Hua, Z.; Zhou, Y.; Huang, H. Cosine-transform-based chaotic system for image encryption. *Inf. Sci.* 2019, 480, 403–419. [CrossRef]

22. Lambić, D.; Janković, A.; Ahmad, M. Security analysis of the efficient chaos pseudo-random number generator applied to video encryption. *J. Electron. Test.* 2018, 34, 709–715. [CrossRef]

23. Ahmad, M.; Alam, M.Z.; Umayya, Z.; Khan, S.; Ahmad, F. An image encryption approach using particle swarm optimization and chaotic map. *Int. J. Inf. Technol.* 2018, 10, 247–255. [CrossRef]

24. Zhang, Y. A new unified image encryption algorithm based on a lifting transformation and chaos. *Inf. Sci.* 2020, 547, 307–327. [CrossRef]

25. Zhang, Y. The fast image encryption algorithm based on lifting scheme and chaos. *Inf. Sci.* 2020, 520, 177–194. [CrossRef]

26. Tong, X.J.; Wang, Z.; Zhang, M.; Liu, Y.; Xu, H.; Ma, J. An image encryption algorithm based on the perturbed high-dimensional chaotic map. *Nonlinear Dyn.* 2015, 80, 1493–1508. [CrossRef]
| Page | Reference |
|------|-----------|
| 27. | Wang, X.; Zhao, J.; Zhang, Z. A chaotic cryptosystem based on multi-one-dimensional maps. *Mod. Phys. Lett. B* 2009, 23, 183–189. [CrossRef] |
| 28. | Hua, Z.; Jin, F.; Xu, B.; Huang, H. 2D Logistic-Sine-coupling map for image encryption. *Signal Process.* 2018, 149, 148–161. [CrossRef] |
| 29. | Hua, Z.; Zhou, Y.; Pun, C.M.; Chen, C.P. 2D Sine Logistic modulation map for image encryption. *Inf. Sci.* 2015, 297, 80–94. [CrossRef] |
| 30. | Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic Cat maps. *Chaos Solitons Fractals* 2004, 21, 749–761. [CrossRef] |
| 31. | Sui, L.; Duan, K.; Liang, J.; Hei, X. Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps. *Opt. Express* 2014, 22, 10605–10621. [CrossRef] |
| 32. | Huang, X.L.; Dong, Y.X.; Jiao, K.X.; Ye, G.D. Asymmetric pixel confusion algorithm for images based on RSA and Arnold transform. *Front. Inf. Technol. Electron. Eng.* 2020, 21, 1783–1794. [CrossRef] |
| 33. | Ye, G.; Jiao, K.; Wu, H.; Pan, C.; Huang, X. An asymmetric image encryption algorithm based on a fractional-order chaotic system and the RSA public-key cryptosystem. *Int. J. Bifurc. Chaos* 2020, 30, 2050233. [CrossRef] |
| 34. | Wang, X.; Liu, L.; Zhang, Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Opt. Lasers Eng.* 2015, 66, 10–18. [CrossRef] |
| 35. | Amara, M.; Siad, A. Elliptic curve cryptography and its applications. In Proceedings of the International Workshop on Systems, Signal Processing and Their Applications, WOSSPA, Tipaza, Algeria, 9–11 May 2011; pp. 247–250. |
| 36. | Azam, N.A.; Hayat, U.; Ullah, I. An Injective S-Box Design Scheme over an Ordered Isomorphic Elliptic Curve and Its Characterization. *Secur. Commun. Netw.* 2018, 2018, 3421725. [CrossRef] |
| 37. | Ullah, I.; Hayat, U.; Bustamante, M.D. Image Encryption Using Elliptic Curves and Rossby/Drift Wave Triads. *Entropy* 2020, 22, 454. [CrossRef] [PubMed] |
| 38. | Sadkhan, S.B.; Hameed, N.F. Proposed Developments of Elliptic Curves Cryptosystem. *J. Qudisiyah Pure Sci.* 2019, 15, 79–86. |
| 39. | Obaid, O.A.; Al Saffar, N.F.H. Image Encryption Based on Menezes Vastone Elliptic Curve Cryptosystem. *Solid State Technol.* 2020, 63, 5256–5265. |
| 40. | Zhang, X.; Wang, X. Digital image encryption algorithm based on elliptic curve public cryptosystem. *IEEE Access* 2018, 6, 70025–70034. [CrossRef] |
| 41. | Abdelfatah, R.I. Secure image transmission using chaotic-enhanced elliptic curve cryptography. *IEEE Access* 2019, 8, 3875–3890. [CrossRef] |
| 42. | Abbas, A.M.; Alharbi, A.A.; Ibrahim, S. A Novel Parallelizable Chaotic Image Encryption Scheme Based on Elliptic Curves. *IEEE Access* 2021, 9, 54978–54991. [CrossRef] |
| 43. | Diaz, E.A.H.; Meana, H.M.P.; García, V.M.S. Encryption of RGB images by means of a novel cryptosystem using elliptic curves and chaos. *IEEE Lat. Am. Trans.* 2020, 18, 1407–1415. [CrossRef] |
| 44. | Ali, T.S.; Ali, R. A novel medical image signcryption scheme using TLTS and Henon chaotic map. *IEEE Access* 2020, 8, 71974–71992. [CrossRef] |
| 45. | Shafique, A.; Ahmed, J.; Rehman, M.U.; Hazzazi, M.M. Noise-Resistant Image Encryption Scheme for Medical Images in the Chaos and Wavelet Domain. *IEEE Access* 2021, 9, 59108–59130. [CrossRef] |
| 46. | Li, X.; Xiao, D.; Mou, H.; Lu, D.; Peng, M. A Compressive Sensing Based Image Encryption and Compression Algorithm With Identity Authentication and Blind Signcryption. *IEEE Access* 2020, 8, 211676–211690. [CrossRef] |
| 47. | Azhar, S.; Azam, N.A.; Hayat, U. Text Encryption Using Pell Sequence and Elliptic Curves with Provable Security. *Comput. Contin.* 2022, 71, 4972–4989. [CrossRef] |
| 48. | Murtaza, G.; Azam, N.A.; Hayat, U. Designing an Efficient and Highly Dynamic Substitution-Box Generator for Block Ciphers Based on Finite Elliptic Curves. *Secur. Commun. Netw.* 2021, 2021, 3367521. [CrossRef] |
| 49. | Abd El-Latif, A.A.; Niu, X. A hybrid chaotic system and cyclic elliptic curve for image encryption. *AEU-Int. J. Electron. Commun.* 2013, 67, 136–143. [CrossRef] |
| 50. | Toughi, S.; Fathi, M.H.; Sekhavat, Y.A. An image encryption scheme based on elliptic curve pseudo random and advanced encryption system. *Signal Process.* 2017, 141, 217–227. [CrossRef] |
| 51. | Hayat, U.; Azam, N.A. A novel image encryption scheme based on an elliptic curve. *Signal Process.* 2019, 155, 391–402. [CrossRef] |
| 52. | Reyad, O.; Kotulski, Z.; Abd-Elhafiez, W. Image encryption using chaos-driven elliptic curve pseudo-random number generators. *Appl. Math. Inf. Sci* 2016, 10, 1283–1292. [CrossRef] |
| 53. | Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; Wiley: Hoboken, NJ, USA, 2012. |
| 54. | Jia, N.; Liu, S.; Ding, Q.; Wu, S.; Pan, X. A New Method of Encryption Algorithm Based on Chaos and ECC. *J. Inf. Hiding Multimed. Signal Process.* 2016, 7, 637–643. |
| 55. | Duran Diaz, R.; Hernandez Encinas, L.; Munoz Masque, J. A group law on the projective plane with applications in Public Key Cryptography. *Mathematics* 2020, 8, 734. [CrossRef] |
| 56. | Meyer, B.; Müller, V. A public key cryptosystem based on elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ equivalent to factoring. In *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, Saragossa, Spain, 12–16 May 1996; pp. 49–59. |
57. Azam, N.A.; Ullah, I.; Hayat, U. A Fast and Secure Public-key Image Encryption Scheme Based on Mordell Elliptic Curves. Opt. Lasers Eng. 2020, 137, 106371. [CrossRef]
58. Azam, N.A.; Hayat, U.; Ullah, I. Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field. Front. Inf. Technol. Electron. Eng. 2019, 20, 1378–1389. [CrossRef]
59. Adams, C.; Tavares, S. The structured design of cryptographically good S-boxes. J. Cryptol. 1990, 3, 27–41. [CrossRef]
60. Matsui, M. Linear cryptanalysis method for DES cipher. In Workshop on the Theory and Application of Cryptographic Techniques; Springer: Berlin/Heidelberg, Germany, 1993; pp. 386–397.
61. Sakalli, M.T.; Aslan, B.; Buluş, E.; Mesut, A.; Büyüksaraçoğlu, F.; Karaahmetoğlu, O. On the algebraic expression of the AES S-Box like S-Boxes. In Proceedings of the International Conference on Networked Digital Technologies. Prague, Czech Republic, 7–9 July 2010; pp. 213–227.
62. Ye, T.; Zhimao, L. Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. Nonlinear Dyn. 2018, 94, 2115–2126. [CrossRef]
63. Özkaynak, F.; Çelik, V.; Özer, A.B. A new S-box construction method based on the fractional-order chaotic Chen system. Signal, Image Video Process. 2017, 11, 659–664. [CrossRef]
64. Çavuşoğlu, Ü.; Zengin, A.; Pehlivan, I.; Kaçar, S. A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. Nonlinear Dyn. 2017, 87, 1081–1094. [CrossRef]
65. Belazi, A.; Abd El-Latif, A.A. A simple yet efficient S-box method based on chaotic sine map. Optik 2017, 130, 1438–1444. [CrossRef]
66. Liu, L.; Zhang, Y.; Wang, X. A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. Appl. Sci. 2018, 8, 2650. [CrossRef]
67. Biham, E.; Shamir, A. Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. 1991, 4, 3–72. [CrossRef]
68. Webster, A.; Tavares, S.E. On the design of S-boxes. In Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Linz, Austria, 9–11 April 1985; pp. 523–534.
69. USC-SIPI Image Database. Available online: http://sipi.usc.edu/database/database.php (accessed on 29 December 2020).
70. Zhou, Y.; Bao, L.; Chen, C.P. Image encryption using a new parametric switching chaotic system. Signal Process. 2013, 93, 3039–3052. [CrossRef]
71. Xian, Y.; Wang, X. Fractal sorting matrix and its application on chaotic image encryption. Inf. Sci. 2021, 547, 1154–1169. [CrossRef]
72. Luo, Y.; Ouyang, X.; Liu, J.; Cao, L. An image encryption method based on elliptic curve elgamal encryption and chaotic systems. IEEE Access 2019, 7, 38507–38522. [CrossRef]
73. Patro, K.A.K.; Acharya, B. An efficient colour image encryption scheme based on 1D chaotic maps. J. Inf. Secur. Appl. 2019, 46, 23–41.
74. Kumar, M.; Sathish, G.; Alphonce, M.; Lahcen, R.A.M. A new RGB image encryption using generalized heat equation associated with generalized Vigenere-type table over symmetric group. Multimed. Tools Appl. 2019, 78, 28025–28061. [CrossRef]
75. Kadir, A.; Hamdulla, A.; Guo, W.Q. Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. Optik 2014, 125, 1671–213. [CrossRef]
76. Li, S.; Ding, W.; Yin, B.; Zhang, T.; Ma, Y. A novel delay linear coupling logistics map model for color image encryption. Entropy 2018, 20, 463. [CrossRef] [PubMed]
77. Wu, X.; Kurths, J.; Kan, H. A robust and lossless DNA encryption scheme for color images. Multimed. Tools Appl. 2018, 77, 12349–12376. [CrossRef]
78. Zhou, Y.; Bao, L.; Chen, C.P. A new 1D chaotic system for image encryption. Signal Process. 2014, 97, 172–182. [CrossRef]
79. Chai, X.; Chen, Y.; Broyle, L. A novel chaos-based image encryption algorithm using DNA sequence operations. Opt. Lasers Eng. 2017, 88, 197–213. [CrossRef]
80. Hua, Z.; Zhu, Z.; Yi, S.; Zhang, Z.; Huang, H. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. Inf. Sci. 2021, 546, 1063–1083. [CrossRef]