entropy

MDPI

Article

Image Encryption Using Elliptic Curves and Rossby/Drift Wave Triads

Ikram Ullah [1], Umar Hayat [1,*] and Miguel D. Bustamante [2,*]

[1] Department of Mathematics, Quaid-i-Azam University, Islamabad 45320, Pakistan; ikram.ullah@math.qau.edu.pk

[2] School of Mathematics and Statistics, University College Dublin, Belfield, Dublin 4, Ireland

* Correspondence: umar.hayat@qau.edu.pk (U.H.); miguel.bustamante@ucd.ie (M.D.B)

Received: 4 March 2020; Accepted: 14 April 2020; Published: 16 April 2020

Abstract: We propose an image encryption scheme based on quasi-resonant Rossby/drift wave triads (related to elliptic surfaces) and Mordell elliptic curves (MECs). By defining a total order on quasi-resonant triads, at a first stage we construct quasi-resonant triads using auxiliary parameters of elliptic surfaces in order to generate pseudo-random numbers. At a second stage, we employ an MEC to construct a dynamic substitution box (S-box) for the plain image. The generated pseudo-random numbers and S-box are used to provide diffusion and confusion, respectively, in the tested image. We test the proposed scheme against well-known attacks by encrypting all gray images taken from the USC-SIPI image database. Our experimental results indicate the high security of the newly developed scheme. Finally, via extensive comparisons we show that the new scheme outperforms other popular schemes.

Keywords: quasi-resonant Rossby/drift wave triads; Mordell elliptic curve; pseudo-random numbers; substitution box

1. Introduction

The exchange of confidential images via the internet is usual in today's life, even though the internet is an open source that is unsafe and unauthorized persons can steal useful or sensitive information. Therefore it is essential to be able to share images in a secure way. This goal is achieved by using cryptography. Traditional cryptographic techniques such as data encryption standard (DES) and advanced encryption standard (AES) are not suitable for image transmission because image pixels are usually highly correlated [1,2]. By contrast, DES and AES are ideal techniques for text encryption [3], so researchers are trying to develop such techniques to meet the demand for reliable image delivery.

A number of image encryption schemes have been developed using different approaches [4–14]. Hua et al. [12] developed a highly secure image encryption algorithm, where pixels are shuffled via the principle of the Josephus problem and diffusion is obtained by a filtering technology. Wu et al. [13] proposed a novel image encryption scheme by combining a random fractional discrete cosine transform (RFrDCT) and the chaos-based Game of Life (GoL). In their scheme, the desired level of confusion and diffusion is achieved by GoL and an XOR operation, respectively. "Confusion" entails hiding the relation between input image, secret keys and the corresponding cipher image, and "diffusion" is an alteration of the value of each pixel in an input image [1].

One of the dominant trends in encryption techniques is chaos-based encryption [15–20]. The reason for this dominance is that the chaos-based encryption schemes are highly sensitive to the initial parameters. However, there are certain chaotic cryptosystems that exhibit a lower security level due to the usage of chaotic maps with less complex behavior (see [21]). This problem is addressed in [22] by introducing a cosine-transform-based chaotic system (CTBCS) for encrypting images with higher

security. Xu et al. [23] suggested an image encryption technique based on fractional chaotic systems and verified experimentally the higher security of the underlying cryptosystem. Ahmad et al. [24] highlighted certain defects of the above-mentioned cryptosytem by recovering the plain image without the secret key. Moreover, they proposed an enhanced scheme to thwart all kinds of attacks.

The chaos-based algorithms also use pseudo-random numbers and substitution boxes (S-boxes) to create confusion and diffusion [25,26]. Cheng et al. [25] proposed an image encryption algorithm based on pseudo-random numbers and AES S-box. The pseudo-random numbers are generated using AES S-box and chaotic tent maps. The scheme is optimized by combining the permutation and diffusion phases, but the image is encrypted in rounds, which is time consuming. Belazi et al. [26] suggested an image encryption algorithm using a new chaotic map and logistic map. The new chaotic map is used to generate a sequence of pseudo-random numbers for masking phase. Then eight dynamic S-boxes are generated. The masked image is substituted in blocks via aforementioned S-boxes. The substituted image is again masked by another pseudo-random sequence generated by the logistic map. Finally, the encrypted image is obtained by permuting the masked image. The permutation is done by a sequence generated by the map function. This algorithm fulfills the security analysis but performs slowly due to the four cryptographic phases. In [27], an image encryption method based on chaotic maps and dynamic S-boxes is proposed. The chaotic maps are used to generate the pseudo-random sequences and S-boxes. To break the correlation, pixels of an input image are permuted by the pseudo-random sequences. In a second phase the permuted image is decomposed into blocks. Then blocks are encrypted by the generated S-boxes to get the cipher image. From histogram analysis it follows that the suggested technique generates cipher images with a nonuniform distribution.

Similar to the chaotic maps, elliptic curves (ECs) are sensitive to input parameters, but EC-based cryptosystems are more secure than those of chaos [28]. Toughi et al. [29] developed a hybrid encryption algorithm using elliptic curve cryptography (ECC) and AES. The points of an EC are used to generate pseudo-random numbers and keys for encryption are acquired by applying AES to the pseudo-random numbers. The proposed algorithm gets the promising security but pseudo-random numbers are generated via the group law, which is time consuming. In [3], a cyclic EC and a chaotic map are combined to design an encryption algorithm. The developed scheme overcomes the drawbacks of small key space but is unsafe to the known-plaintext/chosen-plaintext attack [30]. Similarly, Hayat et al. [31] proposed an EC-based encryption technique. The stated scheme generates pseudo-random numbers and dynamic S-boxes in two phases, where the construction of S-box is not guaranteed for each input EC. Therefore, changing of ECs to generate an S-box is a time-consuming work. Furthermore, the generation of ECs for each input image makes it insufficient.

Based on the above discussion, we propose an improved image encryption algorithm, based on quasi-resonant Rossby/drift wave triads [32,33] (triads, for short) and Mordell elliptic curves (MECs). The triads are utilized in the generation of pseudo-random numbers and MECs are employed to create dynamic S-boxes. The proposed scheme is novel in that it introduces the technique of pseudo-random numbers generation using triads, which is faster than generating pseudo-random numbers by ECs. Moreover, the scheme does not require to separately generate triads for each input image of the same size. In the present scheme, MECs are used opposite to [31], in the sense that now, for each input image, the generation of a dynamic S-box is guaranteed [34]. Finally, extensive performance analyses and comparisons reveal the efficiency of the proposed scheme.

This paper is organized as follows. Preliminaries are described in Section 2. In Section 3, the proposed encryption algorithm is explained in detail. Section 4 provides the experimental results as well as a comparison between the proposed method and other existing popular schemes. Lastly, conclusions are presented in Section 5.

2. Preliminaries

Barotropic vorticity equation: The barotropic vorticity equation (in the so-called β-plane approximation) is one of the simplest two-dimensional models of the large-scale dynamics of a

shallow layer of fluid on the surface of a rotating sphere. It is described in mathematical terms by the partial differential equation

$$\frac{\partial}{\partial t}(\nabla^2\psi - F\psi) + \left(\frac{\partial\psi}{\partial x}\frac{\partial\nabla^2\psi}{\partial y} - \frac{\partial\psi}{\partial y}\frac{\partial\nabla^2\psi}{\partial x}\right) + \gamma\frac{\partial\psi}{\partial x} = 0, \tag{1}$$

where $\psi(x,y,t) \in \mathbb{R}$ represents the geopotential height, γ is the Coriolis parameter, a real constant measuring the variation of the Coriolis force with latitude (x represents longitude and y represents latitude) and F is a non-negative real constant representing the inverse of the square of the deformation radius. We assume periodic boundary conditions: $\psi(x+2\pi,y,t) = \psi(x,y+2\pi,t) = \psi(x,y,t)$ for all $x,y,t \in \mathbb{R}$. In the literature Equation (1) is also known as the Charney–Hasegawa–Mima equation (CHM) [35–39]. This equation accepts harmonic solutions, known as Rossby waves, which are solutions of both the linearized form and the whole (nonlinear) form of Equation (1). A Rossby wave solution is given explicitly by the parameterized function $\psi_{(k,l)}(x,y,t) = \Re\{A\,e^{i(kx+ly-\omega(k,l)t)}\}$, where $A \in \mathbb{C}$ is an arbitrary constant, $\omega(k,l) = -\frac{\gamma k}{k^2+l^2+F}$ is the so-called dispersion relation, and $(k,l) \in \mathbb{Z}^2$ is called the wave vector. For simplicity, we take $\gamma = -1$ and $F = 0$ in what follows [32,33].

Resonant triads: As Equation (1) is nonlinear, modes with different wave vectors tend to couple and exchange energy. If the nonlinearity is weak, this exchange happens to be quite slow and is more efficient amongst groups of modes that are in *resonance*. To the lowest order of nonlinearity in Equation (1), approximate solutions known as resonant triad solutions can be constructed via linear combinations of the form

$$\psi(x,y,t) = \Re\{A_1\,e^{i(k_1x+l_1y-\omega(k_1,l_1)t)} + A_2\,e^{i(k_2x+l_2y-\omega(k_2,l_2)t)} + A_3\,e^{i(k_3x+l_3y-\omega(k_3,l_3)t)}\},$$

where A_1, A_2, A_3 are slow functions of time (they satisfy a closed system of ODEs, not shown here), and the wave vectors $(k_1,l_1), (k_2,l_2)$ and (k_3,l_3) satisfy the Diophantine system of equations:

$$k_1 + k_2 = k_3, \quad l_1 + l_2 = l_3 \quad \text{and} \quad \omega_1 + \omega_2 = \omega_3, \tag{2}$$

for $\omega_i = \omega(k_i,l_i), i = 1,2,3$. A set of three wavevectors satisfying Equations (2) is called a resonant triad. Solutions can be found analytically via a rational transformation to elliptic surfaces (see below).

Quasi-resonant triads and detuning level: If, in (2), the equation $\omega_1 + \omega_2 = \omega_3$ is replaced by the inequality $|\omega_1 + \omega_2 - \omega_3| \leq \delta^{-1}$, for a large positive number δ, then the triad becomes a quasi-resonant triad and δ^{-1} is known as the detuning level of the quasi-resonant triad. It is possible to construct quasi-resonant triads via downscaling of resonant triads that have very large wave vectors [32]. For simplicity, in what follows we simply call a quasi-resonant triad a triad and denote it by Δ. Finally, to avoid over-counting of triads we will impose the condition $k_3 > 0$.

Rational transformation: In [32], wave vectors are explicitly expressed in terms of rational variables X, Y and D as follows:

$$\frac{k_1}{k_3} = \frac{X}{Y^2+D^2}, \quad \frac{l_1}{k_3} = \left(\frac{X}{Y}\right)\left(1 - \frac{D}{Y^2+D^2}\right), \quad \frac{l_3}{k_3} = \frac{D-1}{Y}. \tag{3}$$

In the case $F = 0$, the rational variables X, Y, D lie on an elliptic surface. The transformation is bijective and its inverse mapping is given by:

$$X = \frac{k_3(k_1^2+l_1^2)}{k_1(k_3^2+l_3^2)}, \quad Y = \frac{k_3(k_3l_1 - k_1l_3)}{k_1(k_3^2+l_3^2)}, \quad D = \frac{k_3(k_3k_1 - l_1l_3)}{k_1(k_3^2+l_3^2)}. \tag{4}$$

New parameterization: In [40], Kopp parameterized the resonant triads and in terms of parameters u and t it follows by [40] (Equation (1.22)) that:

$$\frac{k_1}{k_3} = (t^2+u^2)(t^2-2u+u^2)/(1-2u), \tag{5}$$

$$\frac{l_3}{k_3} = \big(u(2u-1)+(t^2+u^2)(t^2-2u+u^2)\big)/\big(t(1-2u)\big), \tag{6}$$

$$\frac{l_1}{k_3} = (t^2+u^2)\big((2u-1)+u(t^2-2u+u^2)\big)/\big(t(1-2u)\big). \tag{7}$$

In 2019, Hayat et al. [33] found a new parameterisation of X, Y and D in terms of auxiliary parameters a, b and hence $\frac{k_1}{k_3}$, $\frac{l_3}{k_3}$ and $\frac{l_1}{k_3}$ are given by:

$$\frac{k_1}{k_3} = \frac{\big(a^2+b(2-3b)+1\big)^3}{(a^2-3b^2-2b+1)\big(2(11-3a^2)b^2+(a^2+1)^2-16ab+9b^4\big)}, \tag{8}$$

$$\frac{l_3}{k_3} = \frac{6(a^2+a-1)b^2-(a+1)^2(a^2+1)+4ab-9b^4}{(a^2-3b^2-1)(a^2-3b^2-2b+1)}, \tag{9}$$

$$\frac{l_1}{k_3} = \frac{\big(a^2+b(2-3b)+1\big)}{(a^2-3b^2-1)(a^2-3b^2-2b+1)\big(2(11-2a^2)b^2+(a^2+1)^2-16ab+9b^4\big)} \times[a^6+2a^5+a^4(-9b^2-6b+3)-4a^3(3b^2+2b-1)+3a^2(3b^2+2b-1)^2 +2a(9b^4+12b^3+14b^2-4b+1)-(3b^2+1)^2(3b^2+6b-1)]. \tag{10}$$

Elliptic curve (EC): Let $\mathbb{F}_p$ be a finite field for any prime p, then an EC E_p over $\mathbb{F}_p$ is defined by

$$y^2 \equiv x^3+bx+c \pmod{p}, \tag{11}$$

where $b, c \in \mathbb{F}_p$. The integers b, c and p are called parameters of an EC. The number of all $(x, y) \in \mathbb{F}_p^2$ satisfying the congruence (11) is denoted by $\#E_p$.

Mordell elliptic curve (MEC): In the special but important case $b = 0$, the above EC is known as an MEC and is represented by

$$y^2 \equiv x^3+c \pmod{p}. \tag{12}$$

For $p \equiv 2 \pmod 3$, there are exactly $p+1$ points $(x, y) \in \mathbb{F}_p^2$ satisfying the congruence (12), see [41] for further details.

If points on E_p are ordered according to some total order $\prec$ then E_p is said to be an ordered EC. Recall that total order is a binary relation which possesses the reflexive, antisymmetric and transitive properties. Azam et al. [42] introduced a total order known as a natural ordering on MECs given by

$$(x_1, y_1) \prec (x_2, y_2) \Leftrightarrow \begin{cases} \text{either } x_1 < x_2, \text{ or} \\ x_1 = x_2 \text{ and } y_1 < y_2, \end{cases}$$

and generated efficient S-boxes using the aforesaid ordering. We will use natural ordering to generate S-boxes. Thus from here on E_p stands for a naturally ordered MEC unless it is specified otherwise.

3. The Proposed Encryption Scheme

The proposed encryption scheme is based on pseudo-random numbers and S-boxes. The pseudo-random numbers are generated using quasi-resonant triads. To get an appropriate level of diffusion we need to properly order the Δs. For this purpose we define a binary relation $\lesssim$ as follows.

3.1. Ordering on Quasi-Resonant Triads

Let Δ, Δ' represent the triads $(k_i, l_i), (k_i', l_i'), i = 1, 2, 3$, respectively, then

$$\Delta \lesssim \Delta' \Leftrightarrow \begin{cases} \text{either } a < a', \text{ or} \\ a = a' \text{ and } b < b', \text{ or} \\ a = a', b = b' \text{ and } k_3 \leq k_3', \end{cases}$$

where a, b and a', b' are the corresponding auxiliary parameters of Δ and Δ', respectively.

Lemma 1. *If T denotes the set of Δs in a box of size L, then $\lesssim$ is a total order on T.*

Proof. The reflexivity of $\lesssim$ follows from $a = a, b = b$ and $k_3 = k_3$ and hence $\Delta \lesssim \Delta$. As for antisymmetry we suppose $\Delta \lesssim \Delta'$ and $\Delta' \lesssim \Delta$. Then, by definition $a \leq a'$ and $a' \leq a$, which imply $a = a'$. Thus we are left with two results: $b \leq b'$ and $b' \leq b$, which imply $b = b'$. Thus, we obtain the results $k_3 \leq k_3'$ and $k_3' \leq k_3$, which ultimately give $k_3 = k_3'$. Solving Equations (8)–(10) for the obtained values, we get $k_1 = k_1', l_3 = l_3'$ and from Equation (2) it follows that $l_2 = l_2'$. Consequently $\Delta = \Delta'$ and $\lesssim$ is antisymmetric. As for transitivity, let us assume $\Delta \lesssim \Delta'$ and $\Delta' \lesssim \Delta''$. Then $a \leq a'$ and $a' \leq a''$, implying $a \leq a''$. If $a < a''$, then transitivity follows. If $a = a''$, then $a' = a''$ too. Thus, $b \leq b'$ and $b' \leq b''$, so $b \leq b''$. If $b < b''$, then transitivity follows. If $b = b''$, then $b' = b''$ too. Thus, $k_3 \leq k_3'$ and $k_3' \leq k_3''$, implying $k_3 \leq k_3''$ and hence transitivity follows: $\Delta \lesssim \Delta''$. □

Let $\overset{*}{T}$ stand for the set of Δs ordered with respect to the order $\lesssim$. The main steps of the proposed scheme are explained as follows.

3.2. Encryption

A. Public parameters: In order to exchange the useful information the sender and receiver should agree on the public parameters described as below:

(1) Three sets: choose three sets $\mathcal{A}_i = [A_i, B_i], i = 1, 2, 3$ of consecutive numbers with unknown step sizes, where the end points $A_i, B_i, i = 1, 2, 3$ are rational numbers.
(2) A total order: select a total order $\prec$ so that the triads generated by the above-mentioned sets may be arranged with respect to that order.

Suppose that P represents an image of size $m \times n$ to be encrypted, and the pixels of P are arranged in column-wise linear ordering. Thus, for positive integer $i \leq mn$, $P(i)$ represents the i-th pixel value in linear ordering. Define S_P as the sum of all pixel values of the image P. Then the proposed scheme chooses the secret keys in the following ways.

B. Secret keys: To generate confusion and diffusion in an image, the sender chooses the secret keys as follows.

(1) Step size: select positive integers a_i, b_i to construct the step sizes $\alpha_i = \frac{a_i}{b_i}$ of $\mathcal{A}_i, i = 1, 2$. Additionally, choose a non-negative integer a_3 as a step size of $\mathcal{A}_3$ in such a way that $\prod_{i=1}^{3} n_i \geq mn$, where $\#\mathcal{A}_i = n_i$ represents the number of elements in $\mathcal{A}_i$.
(2) Detuning level: fix some posive integer δ to find the detuning level δ^{-1} allowed for the triads.
(3) Bound: select a positive integer L such that $|k_i|, |l_i| \leq L$ for $i = 1, 2, 3$. This condition is imposed in order to bound the components of the triad wave vectors. Furthermore, choose an integer t to find $r = \lfloor S_P / t \rceil$, where $\lfloor \cdot \rceil$ gives the nearest integer when S_P is divided by t. The reason for choosing such a t is to generate key-dependent S-boxes and the integer r is used to diffuse the components of triads.
(4) A prime: select a prime $p \geq 257$ such that $p \equiv 2 \pmod 3$ as a secret key for computing nonzero $c \equiv S_P + t \pmod p$ to generate an S-box $\zeta_{E_p}(p, t, S_P)$ on the E_p. The S-box construction technique is made clear in Algorithm 1, and the S-box generated for $p = 1607, t = 182$ and $S = 0$

by Algorithm 1 is shown in Table 1. Furthermore, the cryptographic properties of the said S-box are evaluated in Sections 4.1 and 4.2.

Algorithm 1: Construction of 8×8 S-box.

/* B is a set of points (x, y) satisfying E_p, $B(i)$ is i-th point of B and y_i stands for y-component of point $B(i)$. */

Input : A prime $p \equiv 2 \pmod 3$ and two integers t and S such that $c = S + t$ and $S + t \not\equiv 0 \pmod p$.

Output: An S-box $\zeta_{E_p}(p, t, S)$.

$B := \emptyset$;
$Y := [0, (p-1)/2]$;
$i \leftarrow 0$;
for $x \in [0, p-1]$ **do**
  for $y \in Y$ **do**
    if $y^2 \equiv x^3 + c \pmod p$ **then**
      $i \leftarrow i + 1$; $B(i) := (x, y)$;
      if $y \neq 0$ **then**
        $i \leftarrow i + 1$; $B(i) := (x, p - y)$;
        break;
  $Y = Y - \{y\}$;
$\zeta_{E_p}(p, t, S) = \{y_i \in B(i) : 0 \leq y_i < 256\}$.

Table 1. The obtained S-box $\zeta_{E_{1607}}(1607, 182, 0)$.

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

The positive integers $a_1, b_1, a_2, b_2, a_3, \delta, L, S_P, t$ and p are secret keys. Here it is mentioned that the parameters $a_1, b_1, a_2, b_2, a_3, \delta$ and L are used to generate mn triads in a box of size L. The generation of triads is explained step by step in Algorithm 2. These triads along with keys S_P and t are used to generate the sequence $\beta_{\underset{T}{*}}(t, S_P)$ of pseudo-random numbers.

Algorithm 2: Generating quasi-resonant triads.

```
/* T is a set containing the Quasi-resonant triads, while m and n are the
   dimensions of an input image.                                          */
```

Input : Three sets $\mathcal{A}_i, i = 1,2,3$, inverse detuning level δ, bound L, two positive integers m and n.

Output: Quasi-resonant triads

$T := \emptyset$;
$c_1 \leftarrow 0, c_2 \leftarrow 1$;
for $a \in \mathcal{A}_1$ **do**
  for $b \in \mathcal{A}_2$ **do**
    $c_1 \leftarrow c_1 + 1$;
    Calculate and store the values of $k_1'(c_1), l_3'(c_1)$, and $l_1'(c_1)$ for each pair (a, b) using Equations (8)–(10).
for $c_2 \in [1, c_1]$ **do**
  for $k_3 \in \mathcal{A}_3$ **do**
    $k_1 = \lfloor (k_1'(c_2) * k_3) \rceil, l_3 = \lfloor (l_3'(c_2) * k_3) \rceil$ and $l_1 = \lfloor (l_1'(c_2) * k_3) \rceil$;
    $k_2 = k_3 - k_1, l_2 = l_3 - l_1$ and $\omega_i = k_i/(k_i^2 + l_i^2), i = 1,2,3$;
    $\omega_4 = \omega_3 - \omega_2 - \omega_1$;
    if $|\omega_4| < \delta^{-1}$ *and* $0 < |k_i|, |l_i| < L, i = 1,2,3$ **then**
      $T := T \cup \{\Delta\}$;
    if #T=mn **then**
      break;
  break;
Sort T with respect to the ordering $\lesssim$ to get $\overset{*}{T}$.

Thus Δ_j represents the j-th triad in ordered set $\overset{*}{T}$. Moreover, $(k_{ji}, l_{ji}), i = 1,2,3$ are the components of Δ_j . In Algorithm 3, the generation of $\beta_{\overset{*}{T}}(t, S_P)$ is interpreted.

Algorithm 3: Generating the proposed pseudo-random sequence.

Input : An ordered set $\overset{*}{T}$, an integer t and a plain image P.

Output: Random numbers sequence $\beta_{\overset{*}{T}}(t, S_P)$.

$Tr(j) := |rk_{j1}| + |l_{j1}| + |k_{j2}|$;
$\beta_{\overset{*}{T}}(t, S_P)(j) = (Tr(j) + S_P) \pmod{256}$;

The proposed sequence $\beta_{\overset{*}{T}}(t, S_P)$ is cryptographically a good source of pseudo-randomness because triads are highly sensitive to the auxiliary parameters (a, b) [33] and inverse detuning level δ. It is shown in [32] that the intricate structure of clusters formed by triads depends on the chosen δ, and the size of the clusters increases as the inverse detuning level increases. Moreover, the generation of triads is rapid due to the absence of modular operation.

C. Performing diffusion. To change the statistical properties of an input image, a diffusion process is performed. While performing the diffusion, the pixel values are changed using the sequence $\beta_{\overset{*}{T}}(t, S_P)$. Let M_P denote the diffused image for a plain image P. The proposed scheme alters the pixels of P according to:

$$M_P(i) = \beta_{\overset{*}{T}}(t, S_P)(i) + P(i) \pmod{256}. \tag{13}$$

D. Performing confusion. A nonlinear function causes confusion in a cryptosystem, and nonlinear components are necessary for a secure data encryption scheme. The current scheme uses the dynamic S-boxes to produce the confusion in an encrypted image. If C_P stands for the encrypted image of P, then confusion is performed as follows:

$$C_P(i) = \zeta_{E_p}(p, t, S_P)(M_P(i)). \tag{14}$$

Lemma 2. *If* $\#\mathcal{A}_i = n_i, i = 1, 2, 3$ *and* p *is a prime chosen for the generation of an S-box, then the time complexity of the proposed encryption scheme is* $max\{\mathcal{O}(n_1n_2n_3), p^2\}$.

Proof. The computation of all possible values of k_1', l_3' and l_1' in Algorithm 2 takes $\mathcal{O}(n_1n_2)$ time. Similarly the time complexity for generating $\overset{*}{T}$ is $\mathcal{O}(c_1n_3)$ but c_1 executes n_1n_2 times. Thus the time required by $\overset{*}{T}$ and hence by $\beta_{\overset{*}{T}}(t, S_P)$ is $\mathcal{O}(n_1n_2n_3)$. Additionally, Algorithm 1 shows that the proposed S-box can be constructed in $\mathcal{O}(p^2)$ time. Thus the time complexity of the proposed scheme is $\max\{\mathcal{O}(n_1n_2n_3), p^2\}$. □

Example 1. *In order to have a clear picture of the proposed cryptosystem, we explain the whole procedure using the following hypothetical* 4×4 *image. For example, let* I *represent the plain image of* $Lena_{256\times256}$*, and let* P *be the subimage of* I *consisting of the intersection of the first four rows and the first four columns of* I *as shown in Table 2, whereas the column-wise linearly ordered image* P *is shown in Table 3.*

Table 2. Plain image P.

162	162	162	163
162	162	162	163
162	162	162	163
160	163	160	159

Table 3. Linear ordering of image P.

$P(1)$	$P(5)$	$P(9)$	$P(13)$
$P(2)$	$P(6)$	$P(10)$	$P(14)$
$P(3)$	$P(7)$	$P(11)$	$P(15)$
$P(4)$	$P(8)$	$P(12)$	$P(16)$

We have $S_P = 2589$ and $c = 247$ and the values of other parameters are described in Section 4.3. The corresponding 16 triads are obtained by Algorithm 2 as shown in Table 4.

Table 4. The corresponding set $\overset{*}{T}$ for image P.

Δ_j	k_1	l_1	k_2	l_2	k_3	l_3	Δ_j	k_1	l_1	k_2	l_2	k_3	l_3
Δ_1	−1128	1152	1529	668	401	1820	Δ_9	−1240	1267	1681	735	441	2002
Δ_2	−1142	1167	1548	676	406	1843	Δ_{10}	−1254	1282	1700	743	446	2025
Δ_3	−1156	1181	1567	685	411	1866	Δ_{11}	−1268	1296	1719	751	451	2047
Δ_4	−1170	1195	1586	694	416	1889	Δ_{12}	−1282	1310	1738	760	456	2070
Δ_5	−1184	1210	1605	701	421	1911	Δ_{13}	−1296	1325	1757	768	461	2093
Δ_6	−1198	1224	1624	710	426	1934	Δ_{14}	−1310	1339	1776	776	466	2115
Δ_7	−1212	1238	1643	719	431	1957	Δ_{15}	−1325	1353	1796	785	471	2138
Δ_8	−1226	1253	1662	726	436	1979	Δ_{16}	−1339	1368	1815	793	476	2161

From $S_P = 2589$ and $t = 2$, it follows that $r = 1295$ and hence by application of Algorithm 3 the terms of $\beta_{\overset{*}{T}}(2, 2589)$ are listed in Table 5. Moreover, the S-box $\zeta_{E_{293}}(293, 2, 2589)$ is constructed by Algorithm 1, giving the mapping $\zeta_{E_{293}}(293, 2, 2589) : \{0, 1, \ldots, 255\} \to \{0, 1, \ldots, 255\}$, which maps the list $(0, \ldots, 255)$ to the list

(80, 213, 29, 113, 180, 2, 119, 174, 10, 103, 190, 120, 173, 99, 194, 126, 167, 42, 251, 78, 215, 84, 209, 93, 200, 130, 163, 32, 17, 117, 176, 62, 231, 110, 183, 56, 237, 75, 218, 127, 166, 73, 220, 13, 91, 202, 28, 129, 164, 118, 175, 69, 224, 50, 243, 100, 193, 137, 156, 89, 204, 12, 63, 230, 74, 219, 4, 131, 162, 134, 159, 123, 170, 90, 203, 70, 223, 87, 206, 59, 234, 145, 148, 58, 235, 57, 236, 65, 228, 15, 112, 181, 52, 241, 76, 217, 60, 233, 121, 172, 68, 225, 51, 242, 135, 158, 41, 252, 21, 142, 151, 26, 25, 40, 253, 96, 197, 136, 157, 9, 116, 177, 122, 171, 45, 248, 115, 178, 102, 191, 67, 226, 95, 198, 143, 150, 133, 160, 98, 195, 3, 94, 199, 30, 104, 189, 132, 161, 8, 64, 229, 144, 149, 140, 153, 14, 85, 208, 20, 6, 109, 184, 125, 168, 92, 201, 19, 53, 240, 31, 66, 227, 35, 82, 211, 108, 185, 139, 154, 33, 16, 86, 207, 128, 165, 5, 71, 222, 38, 255, 23, 0, 81, 212, 1, 141, 152, 111, 182, 138, 155, 49, 244, 22, 106, 187, 105, 188, 36, 54, 239, 46, 247, 43, 250, 97, 196, 27, 11, 24, 44, 249, 83, 210, 61, 232, 39, 254, 7, 72, 221, 77, 216, 47, 246, 107, 186, 48, 245, 55, 238, 124169, 34, 79, 214, 88, 205, 114, 179, 37, 18, 146, 147, 101, 192).

Table 5. Pseudo-random sequence for plain image P.

$\beta_{\overset{*}{T}}(2,2589)(1) = 188$	$\beta_{\overset{*}{T}}(2,2589)(5) = 126$	$\beta_{\overset{*}{T}}(2,2589)(9) = 65$	$\beta_{\overset{*}{T}}(2,2589)(13) = 3$
$\beta_{\overset{*}{T}}(2,2589)(2) = 108$	$\beta_{\overset{*}{T}}(2,2589)(6) = 47$	$\beta_{\overset{*}{T}}(2,2589)(10) = 241$	$\beta_{\overset{*}{T}}(2,2589)(14) = 180$
$\beta_{\overset{*}{T}}(2,2589)(3) = 29$	$\beta_{\overset{*}{T}}(2,2589)(7) = 224$	$\beta_{\overset{*}{T}}(2,2589)(11) = 162$	$\beta_{\overset{*}{T}}(2,2589)(15) = 115$
$\beta_{\overset{*}{T}}(2,2589)(4) = 206$	$\beta_{\overset{*}{T}}(2,2589)(8) = 144$	$\beta_{\overset{*}{T}}(2,2589)(12) = 83$	$\beta_{\overset{*}{T}}(2,2589)(16) = 35$

Hence by the respective application of Equation (13) and the S-box $\zeta_{E_{293}}(293, 2, 2589)$, the pixel values of diffused image M_{P} and encrypted image C_{P} are shown in Tables 6 and 7, respectively.

Table 6. Diffused image M_{P}.

94	32	227	166
14	209	147	87
191	130	68	22
110	51	243	194

Table 7. Encrypted image C_{P}.

76	231	254	19
194	54	161	65
0	67	162	209
151	69	34	1

3.3. Decryption

In our scheme the decryption process can take place by reversing the operations of the encryption process. One should know the inverse S-box $\zeta^{-1}_{E_p}(n, t, S_{\mathrm{P}})$ and the pseudo-random numbers $\beta_{\overset{*}{T}}(t, S_{\mathrm{P}})$. Assume the situation when the secret keys $a_1, b_1, a_2, b_2, a_3, \delta$, L, S_{P}, t and p are transmitted by a secure channel, so that the set $\overset{*}{T}$ is obtained using keys $a_1, b_1, a_2, b_2, a_3, \delta$ and L, and hence the S-box $\zeta^{-1}_{E_p}(p, t, S_{\mathrm{P}})$ and the pseudo-random numbers $\beta_{\overset{*}{T}}(t, S_{\mathrm{P}})$ can be computed by S_{P}, t and p. Finally, the receiver gets the original image P by applying the following equations:

$$M_{\mathrm{P}}(i) = \zeta^{-1}_{E_p}(p, t, S_{\mathrm{P}})(\mathrm{C}_{\mathrm{P}}(i)), \tag{15}$$

$$P(i) = M_{\mathrm{P}}(i) - \beta_{\overset{*}{T}}(t, S_{\mathrm{P}})(i) \pmod{256}. \tag{16}$$

4. Security Analysis

In this section the cryptographic strength of both the S-box construction technique and encryption scheme are analyzed in detail.

4.1. Evaluation of the Designed S-Box

An S-box with good cryptographic properties ensures the quality of an encryption technique. Generally, some standard tests such as nonlinearity (NL), linear approximation probability (LAP), strict avalanche criterion (SAC), bit independence criterion (BIC) and differential approximation probability (DAP) are used to evaluate the cryptographic strength of an S-box.

The NL [43] and the LAP [44] are outstanding features of an S-box, used to measure the resistance against linear attacks. The NL measures the level of nonlinearity and the LAP finds the maximum imbalance value of an S-box. The optimal value of the nonlinearity is 112. A low value of LAP corresponds to a high resistance. The minimum NL and the LAP values for the displayed S-box are 106 and 0.1484, respectively. This ensures that the proposed S-box is immune to linear attacks. Webster and Tavares [45] developed the concepts of the SAC and the BIC, which are used to find the confusion and diffusion creation potential of an S-box. In other words, the SAC criterion measures the change in output bits when an input bit is altered. Similarly, the BIC criterion explores the correlation in output bits when change in a single input bit occurs. The average values of the SAC and the BIC for the constructed S-box are 0.4951 and 0.4988, respectively, which are close to the optimal value 0.5. Thus, both tests are satisfied by the suggested S-box. The DAP [46] is another important feature used to analyze the capability of an S-box against differential attacks. The lowest value of DAP for an S-box implies the highest security to the differential attacks. Our DAP result is 0.0234, which is good enough to resist differential cryptanalysts.

4.2. Performance Comparison of the S-Box Generation Algorithm

After performing the rigorous analyses, the S-box constructed by the current algorithm is compared with some cryptographically strong S-boxes developed by recent schemes, as shown in Table 8.

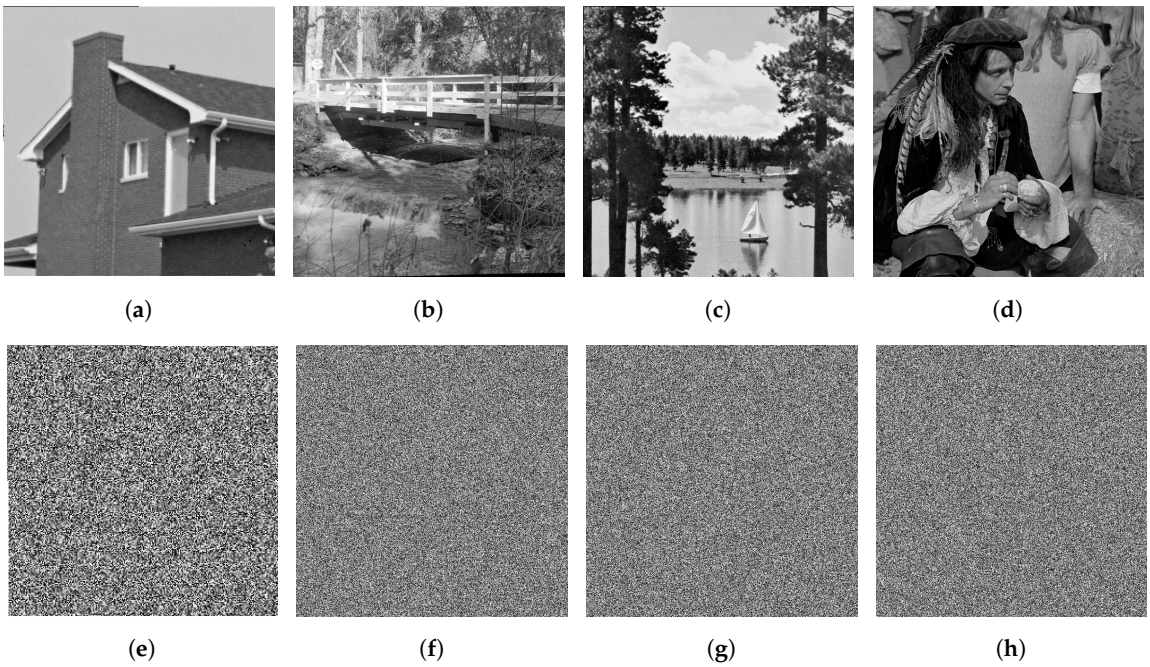
Table 8. Comparison table of the proposed S-box $\zeta_{E_{1607}}(1607, 182, 0)$.

S-Boxes	NL	LAP	SAC			BIC			DAP
			(min)	(avg)	(max)	(min)	(avg)	(max)	
Ours	106	0.1484375	0.390625	0.49511719	0.609375	0.47265625	0.49888393	0.52539063	0.0234375
Ref. [31]	104	0.1484375	0.421900	-	0.6094	0.4629	-	0.5430	0.0469
Ref. [47]	104	0.1328125	0.40625	0.49755859	0.625	0.46679688	0.50223214	0.5234375	0.0234375
Ref. [48]	101	0.140625	0.421875	0.49633789	0.578125	0.46679688	0.49379185	0.51953125	0.03125
Ref. [49]	104	0.140625	0.421875	0.50390625	0.59375	0.4765625	0.50585938	0.5390625	0.0234375
Ref. [50]	100	0.140625	0.40625	0.50097656	0.609375	0.44726563	0.50634766	0.53320313	0.03125
Ref. [51]	106	0.140625	0.390625	0.49414063	0.609375	0.47070313	0.50132533	0.53320313	0.0234375
Ref. [52]	102	0.140625	0.421875	0.49804688	0.640625	0.4765625	0.50746373	0.53320313	0.0234375
Ref. [53]	104	0.0391	0.3906	-	0.6250	0.4707	-	0.53125	0.0391
Ref. [54]	104	0.0547000	0.4018	0.4946	0.5781	0.4667969	0.4988839	0.5332031	0.0391
Ref. [55]	108	0.1328	0.40625	0.4985352	0.59375	0.46484375	0.5020229	0.52734375	0.0234375

From Table 8 it follows that the NL of $\zeta_{E_{1607}}(1607, 182, 0)$ is greater than the S-boxes in [31,47–50,52–54], equal to that of [51] and less than the S-box developed in [55], which indicates that $\zeta_{E_{1607}}(1607, 182, 0)$ is highly nonlinear in comparison to the S-boxes in [31,47–50,52–54]. Additionally, the LAP of $\zeta_{E_{1607}}(1607, 182, 0)$ is comparable to all the S-boxes in Table 8. The SAC (average) value of $\zeta_{E_{1607}}(1607, 182, 0)$ is greater than the S-boxes in [51,54], and the SAC (max) value is less than or equal to the S-boxes in [31,47,50–53]. Similarly the BIC (min) value of $\zeta_{E_{1607}}(1607, 182, 0)$ is closer to the optimal value 0.5 than that of [31,47,48,50,51,53–55], and the BIC (max) value of the new S-box is better than that of the S-boxes in [31,49–55]. Thus the confusion/diffusion creation capability of $\zeta_{E_{1607}}(1607, 182, 0)$ is better than [31,50–53,55]. The DAP value of our suggested S-box $\zeta_{E_{1607}}(1607, 182, 0)$ is lower than the DAP of the S-boxes presented in [31,48,50,53,54] and equal to that of [47,49,51,52,55]. Thus from the above discussion it follows that the newly designed S-box shows high resistance to linear as well as differential attacks.

4.3. Evaluation of the Proposed Encryption Technique

In this section the current scheme is implemented on all gray images of the USC-SIPI Image Database [56]. The USC-SIPI database contains images of size $m \times m$, m = 256,512,1024. Furthermore, some security analyses that are explained one by one in the associated subsections are presented. To validate the quality of the proposed scheme, the experimental results are compared with some other encryption schemes. The parameters used for the experiments are $A_1 = A_2 = -1.0541, A_3 = 401, B_1 = B_2 = -0.8514$ and $B_3 = 691, 3036, 5071$ for m = 256,512,1024, respectively; $a_1 = 2, b_1 = 1000, a_2 = 19, b_2 = 1000, a_3 = 5, \delta = 1000, t = 2, p = 293, L$ = 90,000 and S_P varies for each P. The experiments were performed using Matlab R2016a on a personal computer with a 1.8 GHz Processor and 6 GB RAM. All encrypted images of the database along with histograms are available at [57]. Some plain images, $\text{House}_{256\times256}$, $\text{Stream}_{512\times512}$, $\text{Boat}_{512\times512}$ and $\text{Male}_{1024\times1024}$ and their cipher images are displayed in Figure 1.



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

(**e**) (**f**) (**g**) (**h**)

Figure 1. (**a**–**d**) Plain images House, Stream, Boat and Male; (**e**–**h**) cipher images of the plain images (**a**–**d**), respectively.

4.3.1. Statistical Attack

A cryptosystem is said to be secure if it has high resistance against statistical attacks. The strength of resistance against statistical attacks is measured by entropy, correlation and histogram tests. All of these tests are applied to evaluate the performance of the discussed scheme.

(1) Histogram. A histogram is a graphical way to display the frequency distribution of pixel values of an image. A secure cryptosystem generates cipher images with uniform histograms. The histograms of the encrypted images using the proposed method are available at [57]. However, the respective histograms for the images in Figure 1 are shown in Figure 2. The histograms of the encrypted images are almost uniform. Moreover, the histogram of an encrypted image is totally different from that of the respective plain image, so that it does not allow useful information to the adversaries, and the proposed algorithm can resist any statistical attack.

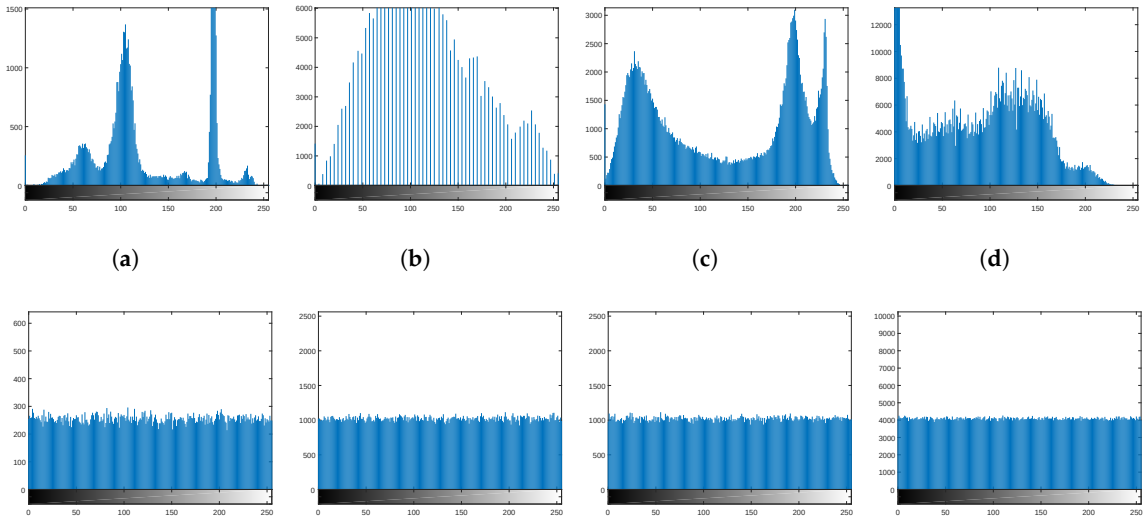


Figure 2. (**a**–**d**) Histograms of Figure 1**a**–**d**; (**e**–**h**) histograms of Figure 1**e**–**h**.

(2) Entropy. Entropy is a standout feature to measure the disorder. Let I be a source of information over a set of symbols N. Then the entropy of I is defined by:

$$\mathrm{H}(I) = \sum_{i=1}^{\#N} p(I_i) \log_2 \frac{1}{p(I_i)}, \tag{17}$$

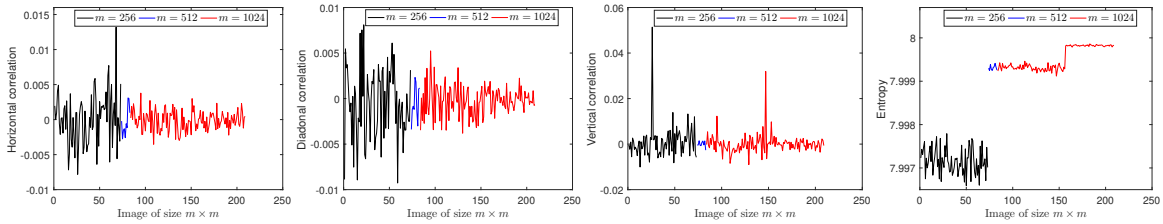
where $p(I_i)$ is the probability of occurrence of symbol i. The ideal value of $\mathrm{H}(I)$ is $\log_2(\#N)$, if all symbols of N occur in I with the same probability. Thus, an image I emanating 256 gray levels is highly random if $\mathrm{H}(I)$ is close to 8 (notice, however, that this definition of entropy does not take into account pixel correlations). The entropy results for all images encrypted by the suggested technique are shown in Figure 3, where the minimum, average and maximum values are 7.9966, 7.9986 and 7.9999, respectively. These results are close to 8, and hence the developed mechanism is secure against entropy attacks.

(3) Pixel correlation. A meaningful image has strong correlation among the adjacent pixels. In fact, a good cryptosystem has the ability to break the pixel correlation and bring it close to zero. For any two gray values x and y, the pixel correlation can be computed as:

$$C_{xy} = \frac{E\big[(x - E[x])(y - E[y])\big]}{\sqrt{K[x]K[y]}}, \tag{18}$$

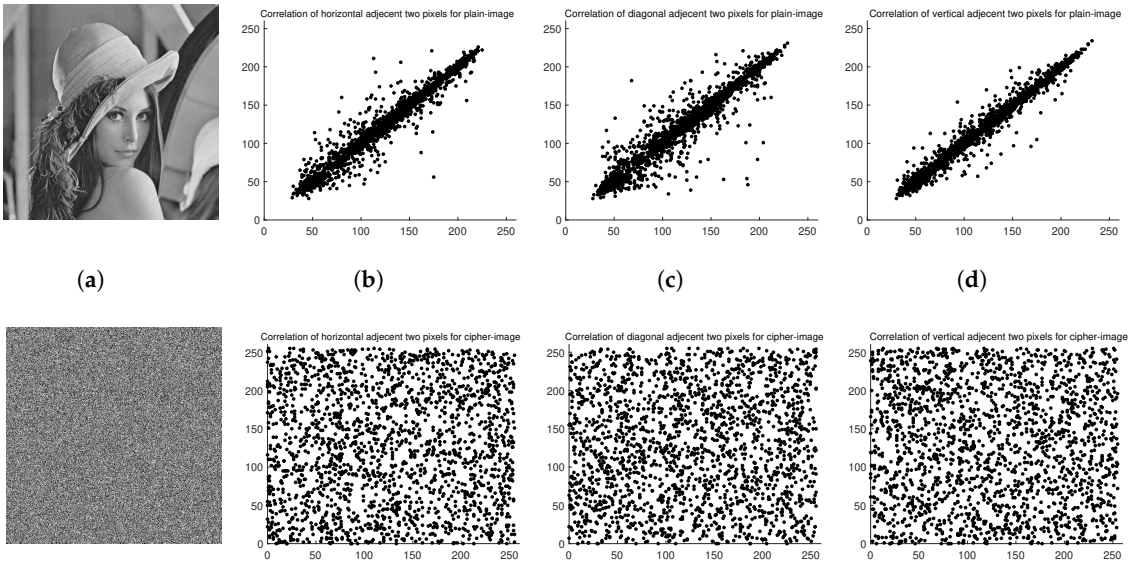
where $E[x]$ and $K[x]$ denote expectation and variance of x, respectively. The range of C_{xy} is -1 to 1. The gray values x and y are in low correlation if C_{xy} is close to zero. As the pixels may be adjacent in horizontal, diagonal and vertical directions, the correlation coefficients of all encrypted images along all three directions are shown in Figure 3, where the respective ranges of C_{xy} are $[-0.0078, 0.0131]$, $[-0.0092, 0.0080]$ and $[-0.0100, 0.0513]$. These results show that the presented method is capable of reducing the pixel correlation near to zero.

In addition, 2000 pairs of adjacent pixels of the plain image and cipher image of $\mathrm{Lena}_{512\times512}$ are randomly selected. Then correlation distributions of the adjacent pixels in all three directions are shown in Figure 4, which reveals the strong pixel correlation in the plain image but a weak pixel correlation in the cipher image generated by the current scheme.



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

Figure 3. (**a**–**c**) The horizontal, diagonal and vertical correlations among pixels of each image in USC-SIPI database; (**d**) the entropy of each image in USC-SIPI database.



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

(**e**) (**f**) (**g**) (**h**)

Figure 4. (**b**–**d**) The distribution of pixels of the plane image (**a**) in the horizontal, diagonal and vertical directions; (**f**–**h**) the distribution of pixels of the cipher image (**e**) in the horizontal, diagonal and vertical directions.

4.3.2. Differential Attack

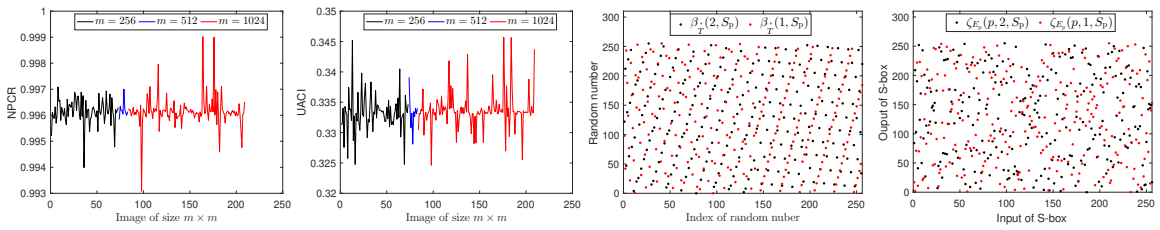
In differential attacks the opponents try to get the secret keys by studying the relation between the plain image and cipher image. Normally attackers encrypt two images by applying a small change to these images, then compare the properties of the corresponding cipher images. If a minor change in the original image can cause a significant change in the encrypted image, then the cryptosystem has a high security level. The two tests NPCR (number of pixels change rate) and UACI (unified average changing intensity) are usually used to describe the security level against differential attacks. For two plain images P and $P^{'}$ different at only one pixel value, let C_{P} and $C_{\mathrm{P}'}$ be the cipher images of P and $P^{'}$, respectively, then NPCR and UACI are calculated as:

$$\mathrm{NPCR} = \sum_{u=1}^{m}\sum_{v=1}^{n}\frac{\tau(u,v)}{m \times n}, \tag{19}$$

$$\mathrm{UACI} = \sum_{u=1}^{m}\sum_{v=1}^{n}\frac{|C_{\mathrm{P}}(u,v) - C_{\mathrm{P}'}(u,v)|}{255 \times m \times n}, \tag{20}$$

where $\tau(u,v) = 0$ if $C_{\mathrm{P}}(u,v) = C_{\mathrm{P}'}(u,v)$ and $\tau(u,v) = 1$, otherwise. The expected values of NPCR and UACI for 8-bit images are 0.996094 and 0.334635, respectively [13]. We applied the above two tests to each image of the database by randomly changing the pixel value of each image. The experimental results are

shown in Figure 5, giving average values of NPCR and UACI of 0.9961 and 0.3334, respectively. It follows from the obtained results that our scheme is capable of resisting a differential attack.



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

Figure 5. (**a**,**b**) The NPCR and UACI results for each image in the USC-SIPI database; (**c**) First 256 pseudo-random numbers and (**d**) two S-boxes generated for $\text{Lena}_{512\times512}$ with a small change in an input key t.

4.3.3. Key Analysis

For a secure cryptosystem it is essential to perform well against key attacks. A cryptosystem is highly secure against key attacks if it has key sensitivity and large key space and strongly opposes the known-plaintext/chosen-plaintext attack. The proposed scheme is analyzed against key attacks as follows.

(1) Key sensitivity. Attackers usually use slightly different keys to encrypt a plain image and then compare the obtained cipher image with the original cipher image to get the actual keys. Thus, high key sensitivity is essential for higher security. That is, cipher images of a plain image generated by two slightly different keys should be entirely different. The difference of the cipher images is quantified by Equations (19) and (20). In experiments we encrypted the whole database by changing only one key, while other keys remain unchanged. The key sensitivity results are shown in Table 9, where the average values of NPCR and UACI are 0.9960 and 0.3341, respectively, which specify the remarkable difference in the cipher images. Moreover, our cryptosytem is based on the pseudo-random numbers and S-boxes. The sensitivity of pseudo-random numbers sequences $\beta^*_T(2, S_P)$ and $\beta^*_T(1, S_P)$ and S-boxes $\zeta_{E_p}(p, 2, S_P)$ and $\zeta_{E_p}(p, 1, S_P)$ for $\text{Lena}_{512\times512}$ is shown in Figure 5.

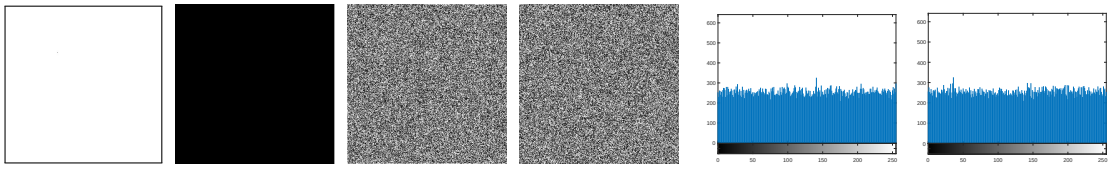
Table 9. Difference between two encrypted images when key $t = 2$ is changed to $t = 1$. NPCR: number of pixels change rate; UACI: unified average changing intensity.

Image	NPCR(%)	UACI(%)	Image	NPCR(%)	UACI(%)	Image	NPCR(%)	UACI(%)
Female	99.62	33.39	House	99.62	33.23	Couple	99.56	33.30
Tree	99.59	33.35	Beans	99.64	33.23	Splash	99.60	33.97

(2) Key space. In order to resist a brute force attack, key space should be sufficiently large. For any cryptosystem, key space represents the set of all possible keys required for the encryption process. Generally, the size of the key space should be greater than 2^{128}. In the present scheme the parameters $a_1, b_1, a_2, b_2, a_3, \delta, L, S_P, t$ and p are used as secret keys, and we store each of them in 28 bits. Thus the key space of the proposed cryptosystem is 2^{280} which is larger than 2^{128} and hence capable to resist a brute force attack.

(3) Known-plaintext/chosen-plaintext attack. In a known-plaintext attack, the attacker has partial knowledge about the plain image and cipher image, and tries to break the cryptosystem, while in a chosen-plaintext attack the attacker encrypts an arbitrary image to get the encryption keys. An all-white/black image is usually encrypted to test the performance of a scheme against these powerful attacks [29,58]. We analyzed our scheme by encrypting an all-white/black image of size 256×256. The results are shown in Figure 6 and Table 10, revealing that the encrypted

images are significantly randomized. Thus the proposed system is capable of preventing the above mentioned attacks.



(**a**) (**b**) (**c**) (**d**) (**e**) (**f**)

Figure 6. (**a**) All-white; (**b**) all-black; (**c**,**d**) cipher images of (**a**,**b**); (**e**,**f**) histograms of (**c**,**d**).

Table 10. Security analysis of all-white/black encrypted images by the proposed encryption technique.

Plain Image	Entropy	Correlation of Plain Image			NPCR (%)	UACI (%)
		Hori.	Diag.	Ver.		
All-white	7.9969	0.0027	0.0020	−0.0090	99.60	33.45
All-black	7.9969	−0.0080	0.0035	0.0057	99.62	33.41

4.4. Comparison and Discussion

Apart from security analyses, the proposed scheme is compared with some well-known image encryption techniques. The gray scale images of $\text{Lena}_{256\times256}$ and $\text{Lena}_{512\times512}$ are encrypted using the presented method, and experimental results are listed in Table 11.

Table 11. Comparison of the proposed encryption scheme with several existing cryptosystems for image $\text{Lena}_{m\times m}$, m = 256,512.

Size m	Algorithm	Entropy	Correlation			NPCR (%)	UACI(%)	#	Dynamic
			Hori.	Diag.	Ver.			S-Boxes	S-Boxes
256	**Ours**	7.9974	0.0001	−0.0007	−0.0001	99.91	33.27	1	Yes
	Ref. [31]	7.9993	0.0012	0.0003	0.0010	99.60	33.50	1	Yes
	Ref. [3]	7.9973	-	-	-	99.50	33.30	0	-
	Ref. [27]	7.9046	0.0164	−0.0098	0.0324	98.92	32.79	>1<50	Yes
	Ref. [26]	7.9963	−0.0048	−0.0045	−0.0112	99.62	33.70	8	Yes
	Ref. [59]	7.9912	−0.0001	0.0091	0.0089	100	33.47	0	-
	Ref. [60]	7.9974	0.0020	0.0020	0.0105	99.59	33.52	0	-
512	**Ours**	7.9993	0.0001	0.0042	0.0021	99.61	33.36	1	Yes
	Ref. [25]	7.9992	0.0075	0.0016	0.0057	99.61	33.38	1	No
	Ref. [29]	7.9993	−0.0004	0.0001	−0.0018	99.60	33.48	1	No
-	Ref. [61]	7.9970	−0.0029	0.0135	0.0126	99.60	33.48	0	-
	Ref. [62]	7.9994	0.0018	−0.0012	0.0011	99.62	33.44	>1	Yes
	Ref. [2]	7.9993	0.0032	0.0011	−0.0002	99.60	33.47	>1	Yes

It is deduced that our scheme generates cipher images with comparable security. Furthermore, we remark that the scheme in [29] generates pseudo-random numbers using group law on EC, while the proposed method generates pseudo-random numbers by constructing triads using auxiliary parameters of elliptic surfaces. Group law consists of many operations, which makes the pseudo-random number generation process slower than the one we present here. The scheme in [26] decomposes an image to eight blocks and uses dynamic S-boxes for encryption purposes. The computation of multiple S-boxes takes more time than computing only one S-box. Similarly the techniques in [2,27] use a set of S-boxes and encrypt an image in blocks, while our newly developed scheme encrypts the whole image using only one dynamic S-box. Thus, our scheme is faster than the schemes in [2,27]. The security system in [61] uses a chaotic system to encrypt blocks of an image. The results in Table 11 reveal that our proposed system is cryptographically stronger than

the scheme in [61]. The algorithms in [3,59] combine chaotic systems and different ECs to encrypt images. It follows from Table 11 that the security level of our scheme is comparable to that of the schemes in [3,59]. The technique in [60] uses double chaos along with DNA coding to get good results, as shown in Table 11, but the results obtained by the new scheme are better than that of [60]. Similarly the technique in [31] encrypts images using ECs but does not guarantee an S-box for each set of input parameters, thus making our scheme faster and more robust than the scheme developed in [31].

Furthermore, the following facts put our scheme in a favorable position:

(i) Our scheme uses a dynamic S-box for each input image while the S-box used in [29] is a static one, which is vulnerable [63] and less secure than a dynamic one [64].
(ii) The presented scheme guarantees an S-box for each image, which is not the case in [31].
(iii) To get random numbers, the described scheme generates triads for all images of the same size, while in [31] the computation of an EC for each input image is necessary, which is time consuming.
(iv) The scheme in [26] uses eight dynamic S-boxes for a plain image, while the current scheme uses only one dynamic S-box for each image to get the desired cryptographic security.

5. Conclusions

An image encryption scheme based on quasi-resonant triads and MECs was introduced. The proposed technique constructs triads to generate pseudo-random numbers and computes an MEC to construct an S-box for each input image. The pseudo-random numbers and S-box are then used for altering and scrambling the pixels of the plain image, respectively. As for the advantages of our proposed method, firstly triads are based on auxiliary parameters of elliptic surfaces, and thus pseudo-random numbers and S-boxes generated by our method are highly sensitive to the plain image, which prevents adversaries from initiating any successful attack. Secondly, generation of triads using auxiliary parameters of elliptic surfaces consumes less time than computing points on ECs (we find a 4x speed increase for a range of image resolutions $m \in [128, 512]$), which makes the new encryption system relatively faster. Thirdly, our algorithm generates the cipher images with an appropriate security level.

In summary, all of the above analyses imply that the presented scheme is able to resist all attacks. It has high encryption efficiency and less time complexity than some of the existing techniques. In the future, the current scheme will be further optimized by means of new ideas to construct the S-boxes using the constructed triads, so that we will not need to compute an MEC for each input image.

Author Contributions: All authors contributed equally to this work. All authors have read and agree to the published version of the manuscript.

Funding: This research is funded through the HEC project NRPU-7433.

Acknowledgments: We thank Gene Kopp for useful comments and suggestions.

Conflicts of Interest: The authors declare no conflict of interest. The funding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

MEC	Mordell elliptic curve
S-box	Substitution box
EC	Elliptic curves

References

1. Mahmud, M.; Lee, M.; Choi, J.Y. Evolutionary-Based Image Encryption using RNA Codons Truth Table. *Optics Laser Technol.* **2020**, *121*, 105818. [CrossRef]

2. Zhang, X.; Mao, Y.; Zhao, Z. An Efficient Chaotic Image Encryption Based on Alternate Circular S-boxes. *Nonlinear Dyn.* **2014**, *78*, 359–369. [CrossRef]
3. El-Latif, A.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]
4. Yang, Y.G.; Pan, Q.X.; Sun, S.J.; Xu, P. Novel Image Encryption Based on Quantum Walks. *Sci. Rep.* **2015**, *5*, 1–9. [CrossRef] [PubMed]
5. Zhong, H.; Chen, X.; Tian, Q. An Improved Reversible Image Transformation using K-Means Clustering and Block Patching. *Information* **2019**, *10*, 17. [CrossRef]
6. Li, C.; Lin, D.; Lü, J. Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits. *IEEE MultiMedia* **2017**, *24*, 64–71. [CrossRef]
7. Hua, Z.; Yi, S.; Zhou, Y. Medical Image Encryption using High-Speed Scrambling and Pixel Adaptive Diffusion. *Signal Process.* **2018**, *144*, 134–144. [CrossRef]
8. Xie, E.Y.; Li, C.; Yu, S.; Lü, J. On the Cryptanalysis of Fridrich's Chaotic Image Encryption Scheme. *Signal Process.* **2017**, *132*, 150–154. [CrossRef]
9. 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]
10. Luo, Y.; Tang, S.; Qin, X.; Cao, L.; Jiang, F.; Liu, J. A Double-Image Encryption Scheme Based on Amplitude-Phase Encoding and Discrete Complex Random Transformation. *IEEE Access* **2018**, *6*, 77740–77753. [CrossRef]
11. Li, J.; Li, J.S.; Pan, Y.Y.; Li, R. Compressive Optical Image Encryption. *Sci. Rep.* **2015**, *5*, 10374. [CrossRef] [PubMed]
12. Hua, Z.; Xu, B.; Jin, F.; Huang, H. Image Encryption using Josephus Problem and Filtering Diffusion. *IEEE Access* **2019**, *7*, 8660–8674. [CrossRef]
13. Wu, J.; Cao, X.; Liu, X.; Ma, L.; Xiong, J. Image Encryption using the Random FrDCT and the Chaos-Based Game of Life. *J. Modern Opt.* **2019**, *66*, 764–775. [CrossRef]
14. Yousaf, A.; Alolaiyan, H.; Ahmad, M.; Dilbar, N.; Razaq, A. Comparison of Pre and Post-Action of a Finite Abelian Group Over Certain Nonlinear Schemes. *IEEE Access* **2020**, *8*, 39781–39792. [CrossRef]
15. Ismail, S.M.; Said, L.A.; Radwan, A.G.; Madian, A.H.; Abu-ElYazeed, M.F. A Novel Image Encryption System Merging Fractional-Order Edge Detection and Generalized Chaotic Maps. *Signal Process.* **2020**, *167*, 107280. [CrossRef]
16. Tang, Z.; Yang, Y.; Xu, S.; Yu, C.; Zhang, X. Image Encryption with Double Spiral Scans and Chaotic Maps. *Secur. Commun. Netw.* **2019**, *2019*, 8694678. [CrossRef]
17. Abdelfatah, R.I. Secure Image Transmission using Chaotic-Enhanced Elliptic Curve Cryptography. *IEEE Access* **2019**, *8*, 3875–3890. [CrossRef]
18. Yu, J.; Guo, S.; Song, X.; Xie, Y.; Wang, E. Image Parallel Encryption Technology Based on Sequence Generator and Chaotic Measurement Matrix. *Entropy* **2020**, *22*, 76. [CrossRef]
19. Zhu, S.; Zhu, C.; Wang, W. A Novel Image Compression-Encryption Scheme Based on Chaos and Compression Sensing. *IEEE Access* **2018**, *6*, 67095–67107. [CrossRef]
20. ElKamchouchi, D.H.; Mohamed, H.G.; Moussa, K.H. A Bijective Image Encryption System Based on Hybrid Chaotic Map Diffusion and DNA Confusion. *Entropy* **2020**, *22*, 180. [CrossRef]
21. Zhou, Y.; Bao, L.; Chen, C.P. Image Encryption using a New Parametric Switching Chaotic System. *Signal Process.* **2013**, *93*, 3039–3052. [CrossRef]
22. Hua, Z.; Zhou, Y.; Huang, H. Cosine-Transform-Based Chaotic System for Image Encryption. *Inf. Sci.* **2019**, *480*, 403–419. [CrossRef]
23. Xu, Y.; Wang, H.; Li, Y.; Pei, B. Image Encryption Based on Synchronization of Fractional Chaotic Systems. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 3735–3744. [CrossRef]
24. Ahmad, M.; Shamsi, U.; Khan, I.R. An Enhanced Image Encryption Algorithm using Fractional Chaotic Systems. *Procedia Comput. Sci.* **2015**, *57*, 852–859. [CrossRef]
25. Cheng, P.; Yang, H.; Wei, P.; Zhang, W. A Fast Image Encryption Algorithm Based on Chaotic Map and Lookup Table. *Nonlinear Dyn.* **2015**, *79*, 2121–2131. [CrossRef]
26. Belazi, A.; El-Latif, A.A.A.; Belghith, S. A Novel Image Encryption Scheme Based on Substitution-Permutation Network and Chaos. *Signal Process.* **2016**, *128*, 155–170. [CrossRef]
27. Rehman, A.U.; Khan, J.S.; Ahmad, J.; Hwang, S.O. A New Image Encryption Scheme Based on Dynamic S-boxes and Chaotic Maps. *3D Res.* **2016**, *7*, 7. [CrossRef]

28. Jia, N.; Liu, S.; Ding, Q.; Wu, S.; Pan, X. A New Method of Encryption Algorithm Based on Chaos and ECC. *J. Inf. Hiding Multimedia Signal Process.* **2016**, *7*, 637–643.
29. 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]
30. Liu, H.; Liu, Y. Cryptanalyzing an Image Encryption Scheme Based on Hybrid Chaotic System and Cyclic Elliptic Curve. *Opt. Laser Technol.* **2014**, *56*, 15–19. [CrossRef]
31. Hayat, U.; Azam, N.A. A Novel Image Encryption Scheme Based on an Elliptic Curve. *Signal Process.* **2019**, *155*, 391–402. [CrossRef]
32. Bustamante, M.D.; Hayat, U. Complete Classification of Discrete Resonant Rossby/Drift Wave Triads on Periodic Domains. *Commun. Nonlinear Sci. Numer Simul.* **2013**, *18*, 2402–2419. [CrossRef]
33. Hayat, U.; Amanullah, S.; Walsh, S.; Abdullah, M.; Bustamante, M.D. Discrete Resonant Rossby/Drift Wave Triads: Explicit Parameterisations and a Fast Direct Numerical Search Algorithm. *Commun. Nonlinear Sci. Numer. Simul.* **2019**, *79*, 104896. [CrossRef]
34. 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]
35. Charney, J.G. On the scale of atmospheric motions. *Geophys. Public* **1948**, *17*, 3–17.
36. Hasegawa, A.; Mima, K. Pseudo-three-dimensional turbulence in magnetized nonuniform plasma. *Phys. Fluids* **1978**, *21*, 87–92. [CrossRef]
37. Connaughton, C.P.; Nadiga, B.T.; Nazarenko, S.V.; Quinn, B.E. Modulational instability of Rossby and drift waves and generation of zonal jets. *J. Fluid Mech.* **2010**, *654*, 207–231. [CrossRef]
38. Harris, J.; Connaughton, C.; Bustamante, M.D. Percolation Transition in the Kinematics of Nonlinear Resonance Broadening in Charney–Hasegawa–Mima Model of Rossby Wave Turbulence. *New J. Phys.* **2013**, *15*, 083011. [CrossRef]
39. Galperin, B.; Read, P.L. (Eds.) *Zonal Jets: Phenomenology, Genesis, and Physics*; Cambridge University Press: Cambridge, UK, 2019.
40. Kopp, G.S. The Arithmetic Geometry of Resonant Rossby Wave Triads. *SIAM J. Appl. Algebra Geomet.* **2017**, *1*, 352–373. [CrossRef]
41. Washington, L.C. *Elliptic Curves Number Theory and Cryptography, Discrete Mathematics and Its Applications*, 2nd ed.; Chapman and Hall/CRC, University of Maryland College Park: College Park, MD, USA, 2003.
42. Azam, N.A.; Hayat, U.; Ullah, I. Efficient Construction of S-boxes Based on a Mordell Elliptic Curve Over a Finite Field. *Front. Inf. Technol. Electron. Eng.* **2019**, *20*, 1378–1389. [CrossRef]
43. Adams, C.; Tavares, S. The Structured Design of Cryptographically Good S-boxes. *J. Cryptol.* **1990**, *3*, 27–41. [CrossRef]
44. Matsui, M. Linear cryptanalysis method of DES cipher. In *Advances in Cryptology, Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques (EURO-CRYPT-93), Lofthus, Norway, 23–27 May 1993*; Springer: Berlin/Heidelberg, Germany, 1994; pp. 386–397.
45. Webster, A.; Tavares, S.E. On the design of S-boxes. In *Conference on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1985; pp. 523–534.
46. Biham, E.; Shamir, A. Differential Cryptanalysis of DES-like Cryptosystems. *J. Cryptol.* **1991**, *4*, 3–72. [CrossRef]
47. 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]
48. 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]
49. 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]
50. Belazi, A.; El-Latif, A.A.A. A Simple yet Efficient S-box Method Based on Chaotic Sine Map. *Optik* **2017**, *130*, 1438–1444. [CrossRef]
51. Özkaynak, F. Construction of robust substitution boxes based on chaotic systems. *Neural Comput. Appl.* **2019**, *31*, 3317–3326. [CrossRef]
52. 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]

53. Hayat, U.; Azam, N.A.; Asif, M. A Method of Generating 8 × 8 Substitution Boxes Based on Elliptic Curves. *Wirel. Pers. Commun.* **2018**, *101*, 439–451. [CrossRef]
54. Wang, X.; Çavuşoğlu, Ü.; Kacar, S.; Akgul, A.; Pham, V.T.; Jafari, S.; Alsaadi, F.E.; Nguyen, X.Q. S-box Based Image Encryption Application using a Chaotic System without Equilibrium. *Appl. Sci.* **2019**, *9*, 781. [CrossRef]
55. Alzaidi, A.A.; Ahmad, M.; Ahmed, H.S.; Solami, E.A. Sine-Cosine Optimization-Based Bijective Substitution-Boxes Construction using Enhanced Dynamics of Chaotic Map. *Complexity* **2018**, *2018*, 9389065. [CrossRef]
56. USC-SIPI Image Database. Available online: http://sipi.usc.edu/database/database.php (accessed on 21 February 2020).
57. Available online: https://github.com/ikram702314/Results (accessed on 15 April 2020).
58. Wang, X.; Zhao, H.; Hou, Y.; Luo, C.; Zhang, Y.; Wang, C. Chaotic Image Encryption Algorithm Based on Pseudo-Random Bit Sequence and DNA Plane. *Modern Phys. Lett. B* **2019**, *33*, 1950263. [CrossRef]
59. Wu, J.; Liao, X.; Yang, B. Color Image Encryption Based on Chaotic Systems and Elliptic Curve ElGamal Scheme. *Signal Process.* **2017**, *141*, 109–124. [CrossRef]
60. Wan, Y.; Gu, S.; Du, B. A New Image Encryption Algorithm Based on Composite Chaos and Hyperchaos Combined with DNA Coding. *Entropy* **2020**, *22*, 171. [CrossRef]
61. Tong, X.J.; Zhang, M.; Wang, Z.; Ma, J. A Joint Color Image Encryption and Compression Scheme Based on Hyper-Chaotic System. *Nonlinear Dyn.* **2016**, *84*, 2333–2356. [CrossRef]
62. Zhang, Y.; Xiao, D. An Image Encryption Scheme Based on Rotation Matrix Bit-Level Permutation and Block Diffusion. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 74–82. [CrossRef]
63. Rosenthal, J. A Polynomial Description of the Rijndael Advanced Encryption Standard. *J. Algebra. Its Appl.* **2003**, *2*, 223–236. [CrossRef]
64. Kazlauskas, K.; Kazlauskas, J. Key-Dependent S-box Generation in AES Block Cipher system. *Informatica* **2009**, *20*, 23–34.