applied sciences

MDPI

Article

An Efficient and Secure Cryptographic Algorithm Using Elliptic Curves and Max-Plus Algebra-Based Wavelet Transform

Kanza Abdul Sattar [1], Takreem Haider [1,2], Umar Hayat [1,3] and Miguel D. Bustamante [4,*]

[1] Department of Mathematics, Quaid-i-Azam University, Islamabad 45320, Pakistan; kanzasattar@math.qau.edu.pk (K.A.S.); tahaider@iu.edu (T.H.); umar.hayat@qau.edu.pk or u.hayat@surrey.ac.uk (U.H.)
[2] Department of Computer Science, Indiana University Bloomington, Bloomington, IN 47408, USA
[3] Department of Computer Science, University of Surrey, Guildford GU2 7XH, UK
[4] School of Mathematics and Statistics, University College Dublin, Belfield, Dublin 4, Ireland
* Correspondence: miguel.bustamante@ucd.ie

Abstract: With the advent of communication networks, protecting data from security threats has become increasingly important. To address this issue, we present a new text encryption scheme that uses a combination of elliptic curve cryptography and max-plus algebra-based wavelet transform to provide enhanced security and efficiency. The proposed encryption process consists of three main phases. In the first phase, the plaintext is encoded using ASCII characters, followed by the introduction of diffusion in its representation. In the second phase, points are computed on an elliptic curve, and a mapping method is applied to introduce randomness into the data. Finally, in the third phase, the output is decomposed using a max-plus algebra-based wavelet transform to generate the ciphertext. We conduct a comprehensive security analysis of our scheme that includes NIST analysis, entropy analysis, correlation analysis, key space, key sensitivity, plaintext sensitivity, encryption quality, ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, and chosen-ciphertext attack. The findings indicate that the proposed scheme exhibits excellent encryption quality, surpassing a value of 76, which is closer to the ideal value. Moreover, the sensitivity of the plaintext is greater than 91%, indicating its high sensitivity. The correlation between the plaintext and ciphertext is very close to the ideal value of zero. The encrypted texts exhibit a high level of randomness and meet the necessary criteria for a strong key space. These characteristics contribute to its superior security, providing protection against various cryptographic attacks. Additionally, the encryption process for a 5995-character plaintext only takes 0.047 s, while decryption requires 0.038 s. Our results indicate that the proposed scheme offers high levels of security while maintaining reasonable computational efficiency. Thus, it is suitable for secure text communication in various applications. Moreover, when compared with other state-of-the-art text encryption methods, our proposed scheme exhibits better resistance to modern cryptanalysis.

Keywords: text encryption; elliptic curve; max-plus algebra; security analysis

Citation: Sattar, K.A.; Haider, T.; Hayat, U.; Bustamante, M.D. An Efficient and Secure Cryptographic Algorithm Using Elliptic Curves and Max-Plus Algebra-Based Wavelet Transform. *Appl. Sci.* **2023**, *13*, 8385. https://doi.org/10.3390/app13148385

Academic Editor: Mostafa Fouda

Received: 25 May 2023
Revised: 8 July 2023
Accepted: 11 July 2023
Published: 20 July 2023

1. Introduction

With the increasing amount of data being shared electronically, the need for secure encryption schemes has become more critical than ever. Encryption schemes use mathematical functions to scramble data in a way that can only be decoded by authorized parties with the right decryption key. Designing a robust encryption scheme is essential for ensuring the confidentiality, integrity, and authenticity of sensitive information transmitted over networks or stored on devices.

Numerous encryption schemes have been designed with the aim of reducing the likelihood of cyberattacks by ensuring the security of data. Zhu et al. [1] analyzed the security aspects concerning an image encryption system that relies on bit-plane extraction and multi chaos. They presented an algorithm that offers robust security and is highly

resilient against chosen-plaintext attacks. Haider et al. [2] developed an image encryption method utilizing an optimization approach. The underlying objective function of this approach considers both entropy and correlation, where a specific region called the core is chosen within the original image, and a parameter is computed to optimize the objective function over this core. Elkandoz [3] presented a novel method for encrypting images that incorporates both confusion and diffusion. This approach involves reorganizing the pixels of the image to generate a shuffled variant, followed by the process of diffusion achieved by XoRing the pixels using a secret key. Wu et al. [4] introduced a novel encryption method that employs a two-dimensional logistic nested infinite collapse technique to securely transmit audio data via the internet. Gao et al. [5] created a novel encryption technique for ensuring safe communication in asynchronous updating Boolean networks. The algorithm employs chaos-inspired approaches and an asynchronous updating mechanism. Their work made significant advances, such as the development of a unique two-dimensional completely parameterized sine map and an encoding method. These components enable the network to be transformed into a Boolean matrix and propagated as an image. Xu et al. [6] developed a method for securing 3D image files by altering the starting state of a discrete system with the SHA-256 hash algorithm. To scramble and spread the coordinate values inside an image file, they used chaotic sequences, the Arnold matrix, and a DNA diffusion technique. Gao et al. [7] designed a face encryption technique that utilizes chaos. The proposed algorithm is composed of three components: key generation through the application of hash and a two-dimensional logistic tent modular map, the extraction of facial images, and the encryption of the facial images. Furthermore, Gao et al. [8] introduced a novel encryption approach designed specifically for three-dimensional models. The proposed technique involves the utilization of a two-dimensional chaotic system, formed by combining the logistic map and infinite collapse. Additionally, they [8] incorporated the principles of semi-tensor product theory into their encryption method.

Nowadays, the security of text messages has gained significant attention due to the major concerns of users regarding the privacy and security of their communication channels, such as email and messaging apps, which are vulnerable to interception and hacking. Various schemes for securing text data have been developed, using a range of transformations including wavelet transforms, max-plus algebra-based wavelet transforms, and different mathematical structures, such as elliptic curves. In the design of cryptosystems, various types of transformations are significant, as they enable the conversion of plain data into encrypted data that are challenging to understand without having access to the secret key used for encryption [9]. Many researchers have used different types of transformations to design text encryption schemes [10–18]. Sedeeg et al. [11] presented an encryption approach that encrypts plaintext with the Aboodh transform and then decrypts it with the inverse Aboodh transform. Kharde [12] developed a novel technique for encoding plaintext messages using Elzaki transform and decoding the messages using the inverse transform. Kumar et al. [13] presented a technique for encrypting and decrypting a message that employs an integral approach based on Mahgoub transformation and a modulo operator to ensure congruence. Mehmood et al. [15] created a unique cryptographic idea that employs a natural transition to improve information security, particularly for sensitive data. The technique encodes and decodes sensitive data using a newly created mathematical algorithm that performs computations with either mod 26 or mod 63. Idowu et al. [16] presented a mathematical method for encrypting and decrypting data, using a transform known as the Kamal transform to encrypt the plaintext and its inverse transform for decryption. The congruence modulo operator is used as a security measure for protecting the sensitive data from unauthorized access. In addition, Mansour et al. [18] used the SEE integral transform for producing a distinct sequence from an algebraic equation obtained by applying the transform to the numerical values of the message letters. This SEE integral transform functions as a symmetrical cryptosystem that can be employed to encode plaintext, and its inverse is utilized to decipher the received cipher text and restore it to its original state. Furthermore, Mansour et al. [17] developed a scheme that is based on a

complex Sadiq–Emad–Eman (SEE) integral transform. This method involves utilizing the complex SEE conversion to encode a message, and then decrypting the resulting ciphertext to recover the original information.

The use of wavelet transforms in designing cryptosystems provides numerous notable advantages [19]. They allow for the creation of encryption schemes that are both secure and efficient, with low computational complexity. Furthermore, such encryption schemes can be made robust against attacks by using the multiple layers of security provided by wavelet transforms. There exist numerous cryptographic algorithms in the literature that rely on wavelet transforms as a key component, for instance, [20–22]. Goswami et al. [20] suggested a cryptographic technique that involves implementing the Daubechies wavelet transform. Shankar and Elhoseny [21] applied the Haar wavelet transform to safeguard images in wireless sensor networks. Sivasankari and Krishnaveni [22] enhanced the protection of images through steganography, utilizing optimal wavelet coefficients.

Max-plus algebra is a mathematical structure that involves two operations, namely maximization and addition, on the set of real numbers. This algebraic structure has been employed in various fields, such as cryptography. Incorporating max-plus algebra into the development of a cryptosystem has the potential to enhance its security and increase its ability to withstand attacks [14]. The application of max-plus algebra in wavelet transforms has led to the creation of various types of wavelet transforms, known as MP-wavelets. Nobuhara et al. [23] proposed three such types, namely Type I, Type II, and Type III, which use max-plus algebra in conjunction with the Haar wavelet transform. More recently, Kannoth and Kumar [24] suggested a multi-image enhancement method that employs MP-wavelets. One of the benefits of MP-wavelets is that they do not require floating-point calculations, which eliminates the problem of round-off errors. Additionally, MP-wavelets are simple and efficient to compute.

The use of elliptic curves (ECs) in cryptography is widespread due to their favorable mathematical properties, such as being non-linear and having a large group order, which makes them resilient to numerous cryptographic attacks. They have been standardized by the National Institute of Standards and Technology (NIST) and are extensively used in modern cryptographic systems [25]. Several researchers developed cryptographic algorithms based on ECs, such as the random numbers generator [26,27], the substitution box generator [28–30], image encryption [2,31,32], and text encryption [33]. Azhar et al. [33] presented a text encryption algorithm, where the Pell sequence and elliptic curves serve as the foundation for the proposed approach. Initially, the plaintext is diffused by shifting the symbols in a cyclic manner, making the resulting text meaningless. In the second step, the diffused plaintext is concealed from potential attackers through the use of the Pell sequence, a weight function, and a binary sequence to translate each element of the diffused plaintext into real numbers. The third step involves generating permutations over elliptic curves to further obscure the encoded, diffused plaintext.

The focus of our research is to investigate how elliptic curves can be incorporated into the max-plus algebra-based wavelet transform. The aim is to improve the performance of the transform by utilizing the mathematical properties of elliptic curves. For our purpose, we design a novel text encryption scheme based on ECs and MP wavelets. The proposed text encryption scheme involves three primary phases. The initial phase uses ASCII characters for encoding the plaintext, which enables us to represent the data in a standardized way. Additionally, we introduce diffusion in the representation, which adds randomness to the data and makes it more difficult to anticipate the pattern of the data. In the second stage, we generate points on an elliptic curve, followed by applying a mapping approach to enhance the level of randomness into the data, thereby increasing the security of the encryption process. This stage incorporates an extra layer of complexity that further increases the difficulty for a potential attacker to decrypt the encoded information. In the third and final phase, we break down the output using MP wavelets. This procedure involves breaking down the information into smaller portions and employing a specific mathematical method to generate encrypted text. This final stage yields a secure result

that can be safely transmitted or stored without any concern of unauthorized access. Moreover, we conduct a thorough security analysis of our scheme and compare it to various state-of-the-art schemes.

This paper is structured as follows: Section 2 includes some introductory material. In Section 3, we introduce a new scheme for encrypting text. Section 4 contains a comprehensive evaluation of the security of our proposed scheme, along with a thorough comparison with existing text encryption schemes [10–18]. Finally, in Section 5, we provide concluding remarks.

2. Preliminaries

This section provides an introduction to elliptic curves, max-plus algebra, and max-plus wavelet transforms. These concepts are used in later sections to design our encryption scheme.

2.1. Elliptic Curve (EC)

For a prime $p \geq 5$, the elliptic curve denoted by $E_{p,a,b}$ defined over a prime field $\mathbb{F}_p$ can be expressed by an equation in the form $y^2 \equiv x^3 + ax + b \pmod{p}$, where a and b are integers modulo p, and the discriminant $4a^3 + 27b^2$ is not equal to zero modulo p. The set of points on this curve includes a point at infinity denoted by δ and all points (x, y) within $\mathbb{F}_p \times \mathbb{F}_p$ that satisfy the equation $y^2 \equiv x^3 + ax + b \pmod{p}$.

An EC $E_{p,a,b}$ with coefficient $a = 0$ is known as the Mordell elliptic curve (MEC). We denote MEC by $E_{p,b}$. According to Washington [34], a MEC having $p \equiv 2 \pmod{3}$ has precisely $p + 1$ distinct points and does not contain any duplicate y coordinates.

The group law [35] of an elliptic curve allows the addition of two points on the curve to generate a third point that also lies on the curve. This is performed by using the formula for adding two points, P and Q, on the EC $E_{p,a,b}$. The resulting point is denoted by R and its coordinates are calculated using the formula: $\mathrm{R} = (\lambda^2 - x_\mathrm{P} - x_\mathrm{Q}, \lambda(x_\mathrm{P} - x_\mathrm{Q}) - y_\mathrm{P})$, where λ is calculated based on whether the points P and Q are the same or different. If they are different, λ is calculated as $(y_\mathrm{P} - y_\mathrm{Q})/(x_\mathrm{P} - x_\mathrm{Q})$. If they are the same, λ is calculated as $(3{x_\mathrm{P}}^2 + a)/(2y_\mathrm{P})$.

2.2. Max-Plus Algebra-Based Wavelet Transforms (MP Wavelets)

The max-plus algebra [36], works on the set of real numbers $\mathbb{R}$. This set is expanded by adding an element ϵ such that $\mathbb{R}_\epsilon = \mathbb{R} \cup \epsilon$, where ϵ is equal to negative infinity $-\infty$. The max-plus algebra uses two operations, namely, max-plus addition represented by $\oplus$ and max-plus multiplication represented by $\otimes$. When performing max-plus addition on any two elements r and r' in $\mathbb{R}_\epsilon$, the result is the maximum of r and r'. On the other hand, max-plus multiplication of r and r' involves adding the two elements together.

MP wavelets [23] use the max-plus algebra as the fundamental mathematical basis in their wavelet transform. Initially, the input signal is decomposed into several wavelets through a wavelet filter bank, where each wavelet indicates a distinct frequency constituent of the input signal. Then, the wavelet coefficients are subjected to mathematical operations using max-plus algebra.

3. Proposed Scheme

In this section, we explain our designed scheme for encrypting text using elliptic curves and the max-plus algebra-based wavelet transform. The proposed method utilizing elliptic curves offers comparable security to traditional cryptosystems but with significantly shorter key lengths, resulting in improved efficiency in terms of computational resources and storage requirements. The transformation works within the framework of max-plus algebra, which possesses characteristics that strengthen the confusion and diffusion properties of encryption schemes. The Type IVa MP wavelet transform possesses the capability to effectively manage extensive amounts of data. By employing a hierarchical breakdown, it performs operations on sequences or signals, enabling parallel processing and decreasing

the computational complexity of the encryption procedure. The combination of these techniques is a powerful tool in modern cryptography and possesses a diverse range of applications in various fields, such as finance, healthcare, and government [37]. Figure 1 illustrates the flowchart of our designed text encryption scheme.

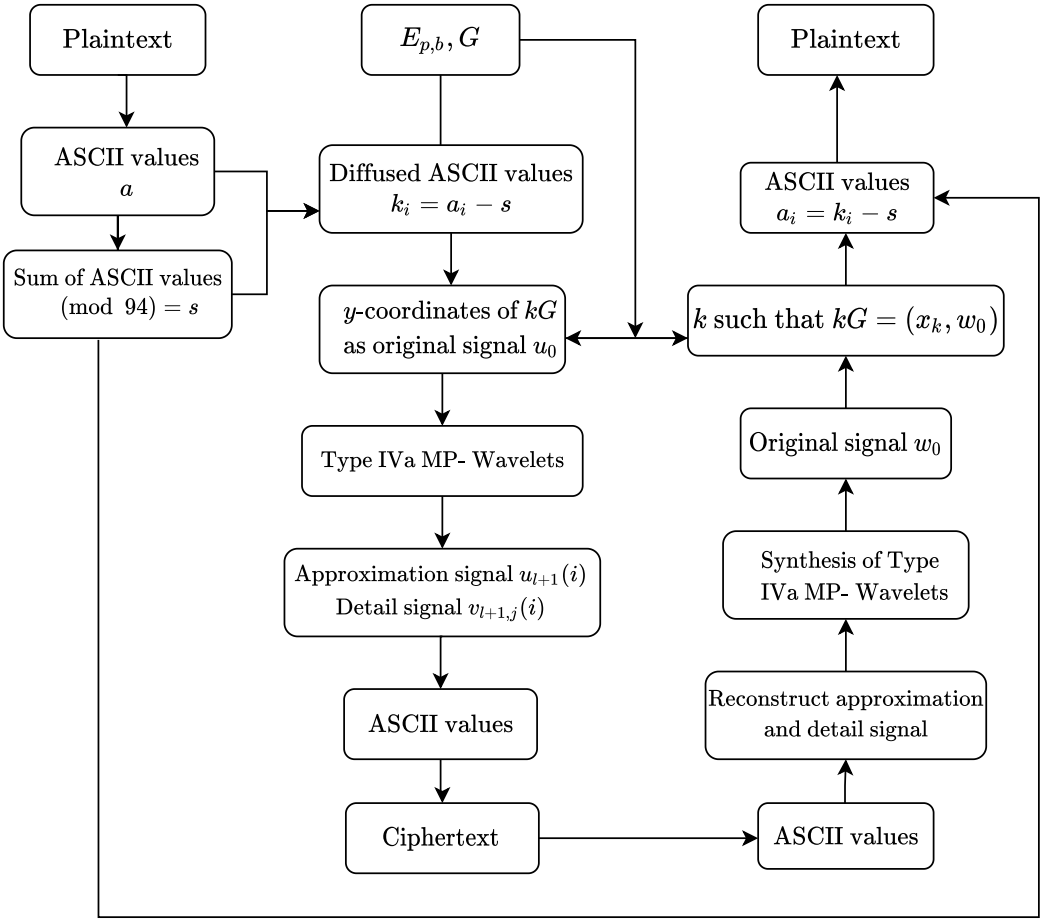

Figure 1. Flowchart of our proposed text encryption scheme.

3.1. Encryption Algorithm

Our algorithm comprises three primary stages. The first stage involves encoding the plaintext using ASCII characters and inducing diffusion in its representation. In the second stage, we compute points on an elliptic curve and apply a mapping method to create randomness in the data. Finally, in the third stage, we decompose the output using a max-plus algebra-based wavelet transform and generate a ciphertext. We provide a comprehensive explanation of these stages as follows.

In the first stage, the plaintext is encoded using ASCII characters, and then a process of diffusion is applied to the ASCII representation of the plaintext. Suppose the plaintext contains n characters. Convert each character into its corresponding ASCII code and denote them as $a_1, a_2, \ldots, a_n$. Compute the sum of these ASCII codes, take the result modulo 94, as there are a total of 94 printable ASCII characters, and let s be the remainder. Then, add s to each ASCII code of the plaintext to obtain the diffused ASCII values $k_1, k_2, \ldots, k_n$, where for $1 \leq i \leq n$, $k_i = a_i + s$.

During the second stage, we first generate points over an elliptic curve. To do so, we use a MEC, denoted by $E_{p,b}$, which satisfies the equation $y^2 \equiv x^3 + b \pmod{p}$ where $p \equiv 2 \pmod{3}$. We assume that the value of p is at least 221 because the standard ASCII table shows that ASCII character codes range from 0 to 127, and since the maximum value for s is 93, the biggest possible diffused value is 220. Select any point G on the $E_{p,b}$ whose order is greater than 220. Let the order of point G be m. To generate a sequence of points $2G, 3G, \ldots, 220G$ over an elliptic curve $E_{p,b}$, we start with a point $G = (x, y)$. We use the group law [35] operations to compute the subsequent points $1G, 2G, \ldots, 220G$. We consider each diffused ASCII value k_i and map it to a specific point k_iG on the curve $E_{p,b}$, where $k_i \leq 220$, and $1 \leq i \leq n$.

In the third stage, we apply Type IVa MP wavelet for improving the security and robustness of our designed text encryption process. For $1 \leq i \leq n$, let $k_iG = (x_{k_i}, y_{k_i})$, then compute the original signal as $u_0(i) = y_{k_i}$. If the total number of characters n is even, then we set $u_0(i) = y_{k_i}$. On the other hand, if n is odd, we set $u_0(i) = y_{k_i}$ and add an extra signal $u_0(i+1) = -\infty$. We add this extra signal because the Type IVa MP-wavelet synthesis process requires an even number of signals. This is because the synthesis process involves dividing the input signals into two parts: approximation and detail signals. We use Equations (1) and (2) to compute the approximation and detail signal, respectively [14]:

$$u_{\ell+1}(i) = u_\ell(c_{\ell+1}i) \oplus u_\ell(c_{\ell+1}i + 1), \tag{1}$$

$$v_{\ell+1,j}(i) = u_\ell(c_{\ell+1}i + j) - u_\ell(c_{\ell+1}i + j - 1), \tag{2}$$

where $\ell \geq 0$, c_ℓ represents the channel of a signal at level ℓ, $i = 1, 2, \ldots, \lceil \frac{n}{2} \rceil$, $j = 1, 2, \ldots, c_{\ell+1} - 1$, and $\oplus$ represents max-plus addition.

Next, we create a binary representation of the detail signals $v_{\ell+1,j}$ by assigning 1 to negative values and 0 to positive values. This binary encoding denoted by B is used in the decryption process.

Finally, the ASCII code for the encrypted message is obtained by transforming both the approximation signals and the absolute value of detail signals into the form of $94q + r$. The quotient q is used in the decryption process. To ensure that all ASCII codes are printable, we increase r by 32. Note that any ASCII code with a value of 32 or more is considered printable. The ciphertext C is generated by the obtained ASCII codes into a text.

Figure 2 illustrates an example of the encryption process of our designed text encryption scheme. To encrypt the text "Applied Sciences", each character of the plaintext is first converted into its corresponding ASCII value. The sum of these ASCII values is then calculated, and the modulo 94 of the result is obtained. In this case, the remainder s is found to be 44. The next step involves adding s to each ASCII value of the plaintext, resulting in diffused ASCII values. For the encryption procedure, a specific elliptic curve, denoted as $E_{227,1}$, is chosen, along with a point $G = (201, 49)$ on this curve, having an order of 228. By utilizing the group law operations, a sequence of points $1G, 2G, \ldots, 220G$ is generated. Each diffused ASCII value is mapped to an elliptic curve point on the selected curve. Subsequently, the y coordinates of these points are extracted, representing the original signal $u_0(i)$, where $1 \leq i \leq 16$, for the Type IVa MP wavelet. The approximation signal $u_1(i)$ and the detail signal $v_{1,1}(i)$ for Type IVa MP-wavelet are then computed using Equations (1) and (2), respectively, for $1 \leq i \leq 16$. The detail signal $v_{1,1}(i)$ is converted into binary form, where negative values are assigned 1 and positive values are assigned 0. Additionally, both the approximation signal and the absolute value of the detail signal are transformed into the form $94q + r$. The remainder r is increased by 32, yielding the ASCII codes of the ciphertext. Finally, these ASCII codes are converted back into text, resulting in the ciphertext "$FOU-O5aJB3TI3Q2".

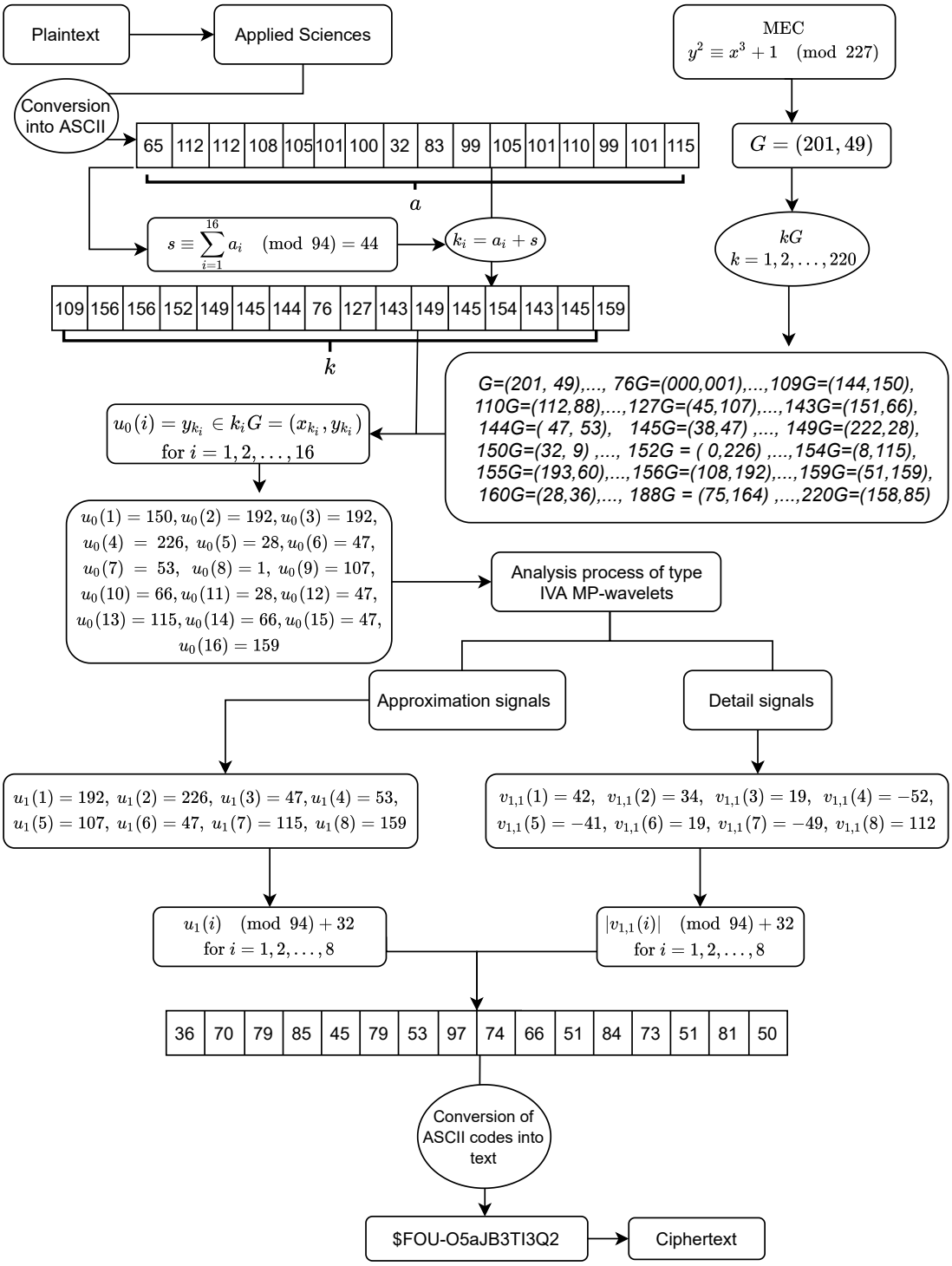

Figure 2. An illustrative example of the proposed encryption algorithm.

3.2. Decryption Algorithm

Suppose that the communication channel between the sender and receiver is free of any noise or interference, and the receiver obtains the ciphertext C of n characters without any errors or distortion. The decryption process involves the following steps.

The initial step is to convert each character of the ciphertext C, which is a string of n characters, into its corresponding ASCII code; we denote it as $a'_1, a'_2, \ldots, a'_n$. This conversion facilitates the reconstruction of the original signal by using the ASCII codes, the decryption keys q and B, and secret key s described in Section 3.1.

The next step is to reconstruct the approximation and detail signals from the ASCII codes using Equations (3) and (4), respectively. These equations enable the calculation of the values of the approximation signal $w_1(i)$ and the detail signal $v_{1,1}(i)$:

$$w_1(i) = 94q_i + (a'_i - 32), \tag{3}$$

$$v_{1,1}(i) = (94q_{i+\lceil \frac{n}{2} \rceil} + (a'_{i+\lceil \frac{n}{2} \rceil} - 32))(-1)^{B_i}, \tag{4}$$

where $i = 1, 2, \ldots, \lceil \frac{n}{2} \rceil$.

Since we generate the ciphertext using the Type IVa MP wavelets, in the decryption process, we apply the inverse transform process to obtain the original signal. To do so, we use the synthesis process, which starts from the highest-frequency level and works its way down to the original signal. We use Equations (5) and (6) to compute the inverse approximation and detail signal, respectively [14]:

$$w_\ell(c_{\ell+1}i) = w_{\ell+1}(i) - (v_{\ell+1,1}(i) \oplus 0), \tag{5}$$

$$w_\ell(c_{\ell+1}i + j) = v_{\ell+1,j}(i) \otimes w_\ell(c_{\ell+1}i + j - 1), \tag{6}$$

where $\ell \geq 0$, c_ℓ represents the channel of a signal at level ℓ, $i = 1, 2, \ldots, \lceil \frac{n}{2} \rceil$, $j = 1, 2, \ldots, c_{\ell+1} - 1$, and we use the symbols $\oplus$ and $\otimes$ to denote the operations of max-plus addition and max-plus multiplication, respectively.

Next, using a MEC $E_{p,b}$ and a fixed point G on the curve, we generate a sequence of points $2G, 3G, \ldots, (m-1)G$ on the curve $E_{p,b}$ using the group law operations. We assume that for each point kG, where $1 \leq k < m$, the y-coordinate of the point is denoted by y_k. Our goal is to find a particular value of k_i for each $w_0(i)$ such that $k_iG = (x_{k_i}, w_0(i))$, where $w_0(i)$ is the resultant signal obtained after applying the modulo operation with respect to p to the output received during the synthesis process. In other words, we are looking for a value of k that generates a point on the curve with the same x-coordinate as G but with a y-coordinate equal to $w_0(i)$. Since $w_0(i)$ exists only once on the MEC, there will be only one corresponding value of k_i for each $w_0(i)$.

Finally, we subtract s from each value k_i to obtain the original ASCII codes a_i. The original ASCII codes a_i obtained from the previous step can be converted back into their corresponding plaintext characters using the ASCII table. After performing all these steps, we obtain the original plaintext.

Figure 3 illustrates an example of the decryption process of the proposed scheme. The decryption process for the ciphertext "$FOU-O5aJB3TI3Q2" involves the following steps. Initially, each character of the ciphertext is converted into its corresponding ASCII value. Subsequently, the approximation signal $w_1(i)$ and the detail signal $v_{1,1}(i)$ are reconstructed using Equations (3) and (4), respectively, where $1 \leq i \leq 16$. The inverse transform process, also known as the synthesis process, is then applied to obtain the original signal $w_0(i)$ by utilizing Equations (5) and (6). Next, by using the elliptic curve $E_{227,1}$ and a point $G = (201, 49) \in E_{227,1}$, a sequence of points $1G, 2G, \ldots, 227G$ is generated using group law operations. The value k_i is determined for each signal $w_0(i)$ such that $k_iG = (x_{k_i}, w_0(i))$. Finally, in the last step, s is subtracted from each value of k_i to retrieve the original ASCII codes. These ASCII codes are converted back into text, resulting in the recovery of the original plaintext "Applied Sciences".

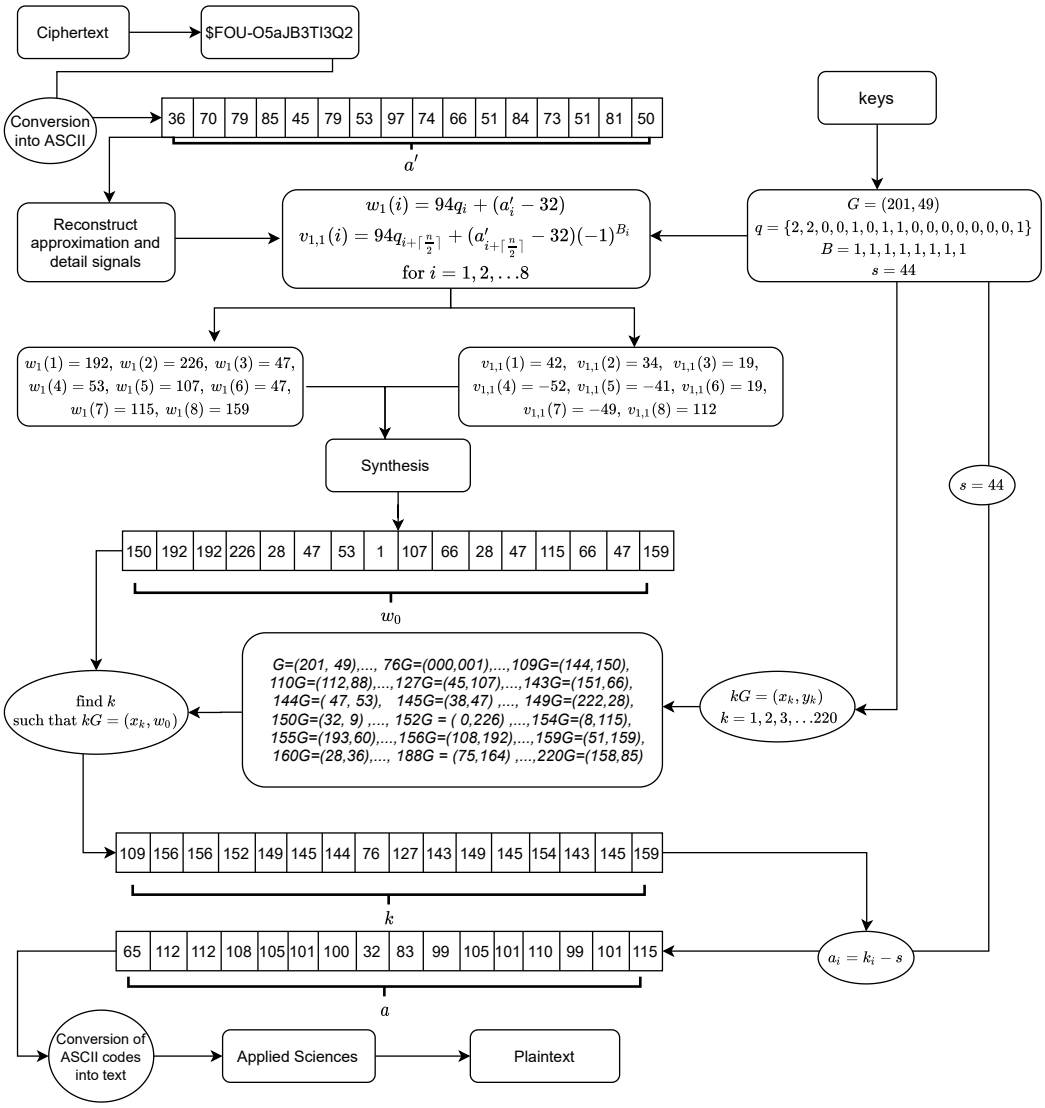

Figure 3. An illustrative example of the proposed decryption algorithm.

4. Simulation Experiments: Security Analysis and Comparison

We conducted simulation experiments using Matlab 2013a on a machine with an Intel Core i7-7500U processor running at 2.70 GHz and 8 GB of RAM to assess the effectiveness of the proposed encryption algorithm. To ensure a fair comparison, we performed experiments with the state-of-the-art schemes [10–18,38–44] in our system and tested it on different texts of various sizes, ranging from 30 to 5995.

We conducted both analytical and empirical evaluations of the proposed text encryption scheme. The empirical study focuses on the correlation analysis, running time, and encryption quality. On the other hand, the analytical study includes entropy analysis, NIST analysis, key sensitivity analysis, plaintext sensitivity analysis, key space analysis, ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, and chosen ciphertext attack. Furthermore, we compared our text encryption scheme with the state-of-the-art text encryption schemes [10–18,38–44].

4.1. Correlation Analysis

The aim of conducting a correlation analysis is to evaluate how much of a linear connection exists between the plaintext P and the ciphertext C. The correlation coefficient R is computed using the formula given below [45]:

$$R = \frac{n\sum_{i=1}^{n}(P_iC_i) - \sum_{i=1}^{n}P_i\sum_{i=1}^{n}C_i}{\sqrt{\left(n\sum_{i=1}^{n}P_i^2 - (\sum_{i=1}^{n}P_i)^2\right)\left(n\sum_{i=1}^{n}C_i^2 - (\sum_{i=1}^{n}C_i)^2\right)}}, \quad (7)$$

where n represents the length of the text, and P_i and C_i represent the ASCII codes for the i-th character of the plaintext and ciphertext, respectively. When the correlation coefficient is near 1 or -1, there is a strong linear relationship between the ciphertext and plaintext. Conversely, when the correlation coefficient is close to 0, the ciphertext and plaintext have a weak linear relationship. A good encryption algorithm should have a weak linear relationship between the ciphertext and plaintext.

We conducted experiments on different texts to evaluate the performance of the proposed scheme and summarized the results in Table 1, which shows that the correlation coefficient ranges from 0.001 to 0.08. Additionally, we compared the correlation analysis of our scheme with several state-of-the-art schemes [10–18]. As presented in Table 2, the proposed scheme exhibits a weaker linear association than the schemes [10–18].

Table 1. Security analysis of the proposed text encryption scheme.

Number of Characters in P	R	EQ (%)	$H(P)$	$H(C)$	**Plaintext Sensitivity**
30	0.0515	90.00	3.5232	4.2817	100.000
300	0.0774	77.33	4.8759	5.6367	99.3333
999	0.0244	76.18	4.4759	5.4658	98.6987
3000	0.0012	81.20	4.5578	5.5356	98.5333
5995	0.0021	82.60	4.5573	5.5114	98.8490

Table 2. Comparison of the proposed text encryption scheme with the state-of-the-art schemes.

[1] **Plaintext**	**Scheme**	R	EQ (%)	$H(P)$	$H(C)$	**Plaintext Sensitivity**
P_1	Proposed	0.0697	100.000	2.2516	2.5850	100.000
	Ref. [14]	−0.3189	83.3333	2.2516	2.2516	16.6667
	Ref. [18]	0.3904	66.6667	2.2516	2.5850	16.6667
	Ref. [17]	0.3904	66.6667	2.2516	2.5850	16.6667
	Ref. [16]	0.3904	66.6667	2.2516	2.5850	16.6667
	Ref. [15]	−0.5354	66.6667	2.2516	2.2516	16.6667
	Ref. [13]	−0.2580	83.3333	2.2516	2.2516	16.6667
	Ref. [12]	0.3904	66.6667	2.2516	2.5850	16.6667
	Ref. [11]	0.3904	66.6667	2.2516	2.5850	16.6667
	Ref. [10]	−0.3907	100.000	2.2516	2.2516	16.6667
P_2	Proposed	−0.0299	100.000	3.0850	3.4183	91.666
	Ref. [14]	−0.4538	91.6667	3.0850	2.9183	8.3333
	Ref. [18]	0.0095	66.6667	3.0850	2.7516	8.3333
	Ref. [17]	0.0095	66.6667	3.0850	2.7516	8.3333
	Ref. [16]	0.0095	66.6667	3.0850	2.7516	8.3333
	Ref. [15]	0.1844	66.6667	3.0850	2.9183	8.3333
	Ref. [13]	−0.0996	91.6667	3.0850	2.8554	8.3333
	Ref. [12]	0.0095	66.6667	3.0850	2.7516	8.3333
	Ref. [11]	0.0095	66.6667	3.0850	2.7516	8.3333
	Ref. [10]	0.2418	66.6667	3.0850	3.0221	8.3333

Table 2. *Cont.*

[1] Plaintext	Scheme	R	EQ (%)	$H(P)$	$H(C)$	Plaintext Sensitivity
P_3	Proposed	−0.2979	93.3333	3.9484	4.2817	96.666
	Ref. [14]	−0.0588	86.6667	3.9484	3.8314	6.6667
	Ref. [18]	0.3411	63.3333	3.9484	3.0159	3.3333
	Ref. [17]	0.3411	63.3333	3.9484	3.0159	3.3333
	Ref. [16]	0.3411	63.3333	3.9484	3.0159	3.3333
	Ref. [15]	0.6242	43.3333	3.9484	3.7069	3.3333
	Ref. [13]	0.0223	66.6667	3.9484	3.0799	3.3333
	Ref. [12]	0.3411	63.3333	3.9484	3.0159	3.3333
	Ref. [11]	0.3411	63.3333	3.9484	3.0159	3.3333
	Ref. [10]	0.3588	60.0000	3.9484	2.8115	3.3333

[1] P_1, P_2, and P_3 represents the plaintext messages ENCODE, CRYPTOGRAPHY, and MAXPLUS WAVELET TRANSFORMATION, respectively.

4.2. Computation Time

An encryption algorithm that is considered good must achieve a balance between security and efficiency. It should be robust enough to withstand attacks and safeguard confidential information, while also being fast enough to perform its function promptly according to the intended use case. To assess the scalability of our scheme, we measure the amount of time it takes to carry out the encryption and decryption procedures.

The experiments were conducted on a machine with an Intel Core i7-7500U processor running at 2.70 GHz and 8 GB of memory. We conducted experiments on various texts with different sizes to analyze the computation time of our scheme. The results for the encryption and decryption time are presented in Table 3. From Table 3, we can observe that when the number of characters in the plaintext is between 30 and 5995, the encryption time ranges from 0.0254 to 0.0472 s, and the decryption time ranges from 0.0256 to 0.3860 s. These findings suggest that our proposed scheme is effective for cryptographic purposes.

Table 3. Computation time of the proposed text encryption scheme.

Number of Characters in P	Time (Seconds)	
	Encryption	Decryption
30	0.0254	0.0256
300	0.0294	0.0432
999	0.0320	0.0956
3000	0.0372	0.2050
5995	0.0472	0.3860

We conducted a comparison of the computational time between our proposed scheme and several state-of-the-art text encryption schemes [14,41–43]. The results of our comparison are presented in Table 4, which demonstrate that our proposed method is significantly faster than the existing schemes [14,41–43]. For example, when encrypting and decrypting a 1126-character text, our proposed method only takes 0.0272 s and 0.0926 s, respectively, whereas the method by Murillo et al. [42] requires 0.14 s for encryption and 0.109 s for decryption. On the other hand, the results of the schemes by Cahyono et al. [14], Singh and Singh [41], and Vigila et al. [43] are based on texts fewer than 1126 characters, but they still require more time for encryption and decryption when compared with the proposed scheme. These results show that our scheme is more efficient than those schemes [14,41–43].

Table 4. Computation time comparison of the proposed scheme with the state-of-the-art text encryption schemes.

Scheme	Number of Characters in P	Time (Seconds)	
		Encryption	Decryption
Proposed	1126	0.0272	0.0926
Ref. [14]	999	0.2650	0.3590
Ref. [41]	409	0.0930	0.1400
Ref. [42]	1126	0.1400	0.1090
Ref. [43]	409	1.9500	0.8300

4.3. Encryption Quality Analysis

To analyze the encryption quality EQ, the frequency of letters in both the plaintext P and ciphertext C are compared. This analysis determines the average number of letter changes, which can be mathematically expressed as [45]

$$EQ = \frac{\sum_{L=32}^{126} |H_L(C) - H_L(P)|}{95}, \tag{8}$$

where the number of times that a letter with ASCII code L appears in C and P is denoted as $H_L(C)$ and $H_L(P)$, respectively. If the encryption quality of a cryptographic algorithm is high, then it is considered better. The highest possible encryption quality is achieved when there are no repeated letters between P and C. The encryption quality can reach a maximum of $2n/95$, where n represents the length of P.

Table 1 displays the results obtained from testing the encryption quality of the proposed scheme on various texts. Table 1 shows that for the text size ranging from 30 to 5995, the percentage (%) of EQ lies in the range [76, 90], which is closer to the optimal percentage. Thus, the proposed scheme can encrypt the text with good encryption quality. We also compared EQ of the proposed scheme with the state-of-the-art schemes [10–18], and the results are shown in Figure 4, which shows that the proposed scheme has better encryption quality than the schemes [10–18].

4.4. Entropy Analysis

The degree of randomness in data is commonly measured by a fundamental criterion called information entropy. To calculate the entropy H of a message source M, Shannon [46] proposed the following equation:

$$H(M) = -\sum_{m \in M} \text{Prob}(m) \log_2 \text{Prob}(m), \tag{9}$$

where Prob denotes the probability of the symbol m in M. If there are 2^N possible symbols for encrypting a message M, then the optimal amount of entropy $H(M) = N$.

By examining texts of various sizes, we calculated the entropy and displayed the results in Table 1. The results demonstrate that the entropy of the ciphertext is higher than that of the plaintext. Furthermore, Table 2 presents a comparison of entropy between the proposed scheme and some state-of-the-art schemes [10–18]. Our evaluation reveals that the entropy of the ciphertext is lower than that of the plaintext in the schemes [10–13,16–18], whereas in [14,15], the entropy of the ciphertext is higher than that of the plaintext but not as high as in the proposed scheme. Therefore, the proposed scheme outperforms [10–18] in terms of entropy.

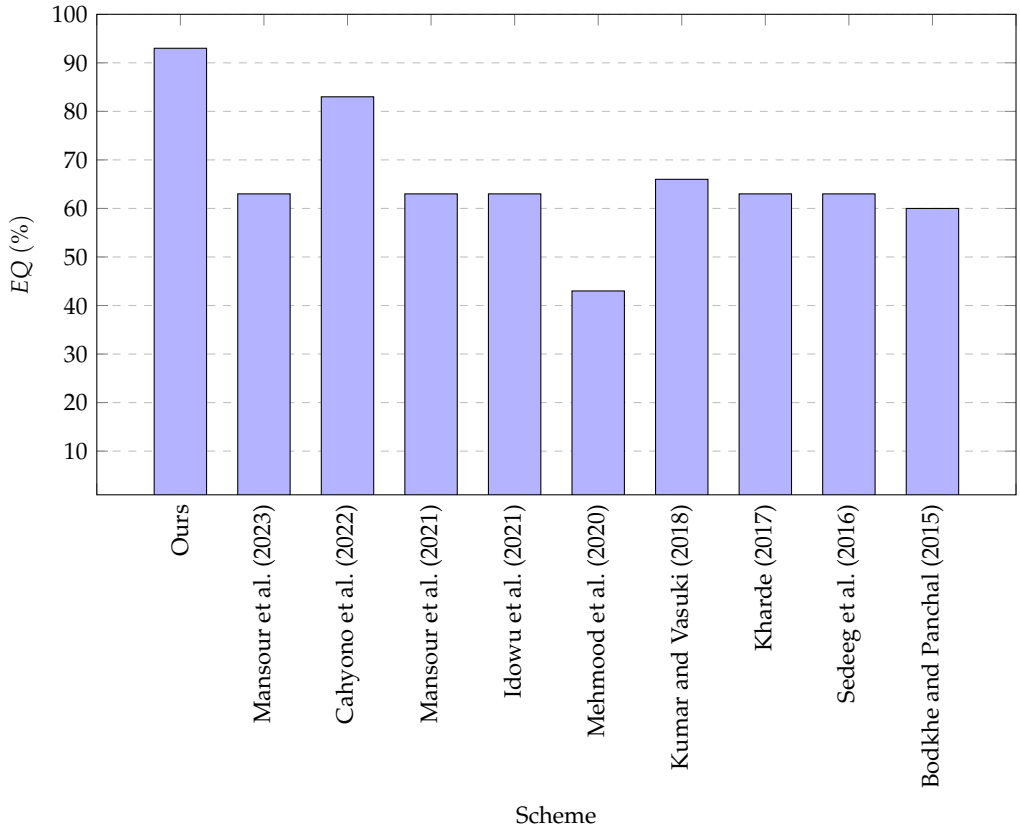

Figure 4. Comparison of the percentage of encryption quality of the proposed scheme with the state-of-the-art schemes [10–18].

4.5. NIST Tests Analysis

The NIST statistical test suite [47] is a set of statistical tests used to evaluate the degree of randomness in the data. To validate the effectiveness of our text encryption method, we utilized the NIST test suite to assess the randomness of 10 sequences obtained from the cipher texts generated from the proposed scheme. Each sequence consists of 10,000 binary bits obtained by applying modulo 2 on the generated cipher texts.

The results of the NIST tests are presented in Table 5. According to the information provided in [47], the minimum pass rate for each statistical test listed in Table 5 is approximately 8 when considering a sample of 10 binary sequences. Our findings, as shown in Table 5, indicate that all sequences generated by our proposed method successfully passed all the NIST tests listed in Table 5, with the exception of the serial test and cumulative sum test. These two tests passed in 7 out of 10 sequences, which is close to the acceptable passing threshold of 8. Therefore, it can be concluded that the proposed text encryption scheme has the ability to generate cipher text with a high level of randomness.

Table 5. Results of NIST tests.

Test Name	Proportion	Results
Frequency (monobit)	10/10	Pass
Frequency (block)	10/10	Pass
Longest run	9/10	Pass
Rank	10/10	Pass
Non-overlapping template	9/10	Pass
Overlapping template	10/10	Pass
Universal	10/10	Pass
Linear complexity	10/10	Pass
Serial	7/10	Fail
Cumulative sums 1	7/10	Fail
Cumulative sums 2	8/10	Pass

4.6. Key Sensitivity Analysis

The term key sensitivity [48] refers to the proportion of alteration in the modified ciphertext compared to the original ciphertext. The modified ciphertext is created by encrypting the plaintext using an adjusted key. A cryptographic algorithm is considered to have higher key sensitivity when the percentage of change is more significant.

To determine the key sensitivity of the proposed scheme, modifications are made to the original keys with respect to EC equation $y^2 \equiv x^3 + b \pmod{p}$, the prime p, and the point G on the EC to create a modified key. The results obtained from these modifications are presented in Table 6. The result shows that even minor changes to any of the parameters b, p, and G result in a completely distinct modified ciphertext.

Table 6. Key sensitivity analysis of the proposed text encryption scheme.

Key Sensitivity			
Plaintext → Applied Sciences Original key → $y^2 \equiv x^3 + 1 \pmod{227}$, $G = (201, 49)$ Original ciphertext C → \$FOU-O5aJB3TI3Q2			
Modified key			Modified ciphertext
$y^2 = x^3 + b$	p	G	C'
$y^2 = x^3 + 1$	227	(193, 60)	dd*F>*TG‘caj4a6,
$y^2 = x^3 + 1$	239	(206, 48)	A@BHhBlO!%9GG9$F
$y^2 = x^3 + 7$	227	(203, 22)	!!Q“wQ$QbZI$6IAt

4.7. Plaintext Sensitivity Analysis

Plaintext sensitivity [48] refers to the extent of change in the modified ciphertext compared to the original ciphertext. By modifying one character in the original plaintext, we obtain the modified ciphertext. A cryptographic algorithm is considered to have a better plaintext sensitivity when it is deemed to possess better sensitivity towards plaintext. We performed experiments to evaluate the sensitivity of the suggested cryptographic algorithm towards plaintext by changing the first character of the original plaintext to a space character. The results presented in Table 1 indicate that the plaintext sensitivity of different text sizes, ranging from 30 to 5995, lies in the interval [98, 100]. This indicates that the proposed scheme has a higher sensitivity towards plaintext. In addition, we compared the plaintext sensitivity of the proposed scheme with the state-of-the-art schemes [10–18,38,44]. The results are shown in Figure 5, which depicts that the proposed scheme has better plaintext sensitivity than the other schemes [10–18,38,44].

4.8. Key Space Analysis

Cryptanalysts often use brute-force attacks to decipher encrypted messages. To assess the vulnerability of an encryption system to such attacks, key space analysis is used. Key space refers to the range of unique secret keys that can be generated by an encryption scheme. An encryption scheme can be considered secure if its key space is equal to or greater than 2^{100} [49].

The proposed encryption scheme employs six secret keys, namely the parameters p, a, G, s, q, and B, which are explained in detail in Section 3. Furthermore, the decryption key for the Type IVa MP wavelets consists of the number of channels at all levels. These details indicate that the key space of our proposed text encryption scheme based on ECs and MP-wavelets is significantly larger than 2^{100}, meaning that the scheme has a large key space. As a result, it would be difficult for an attacker to use the brute-force method to attack the algorithm.

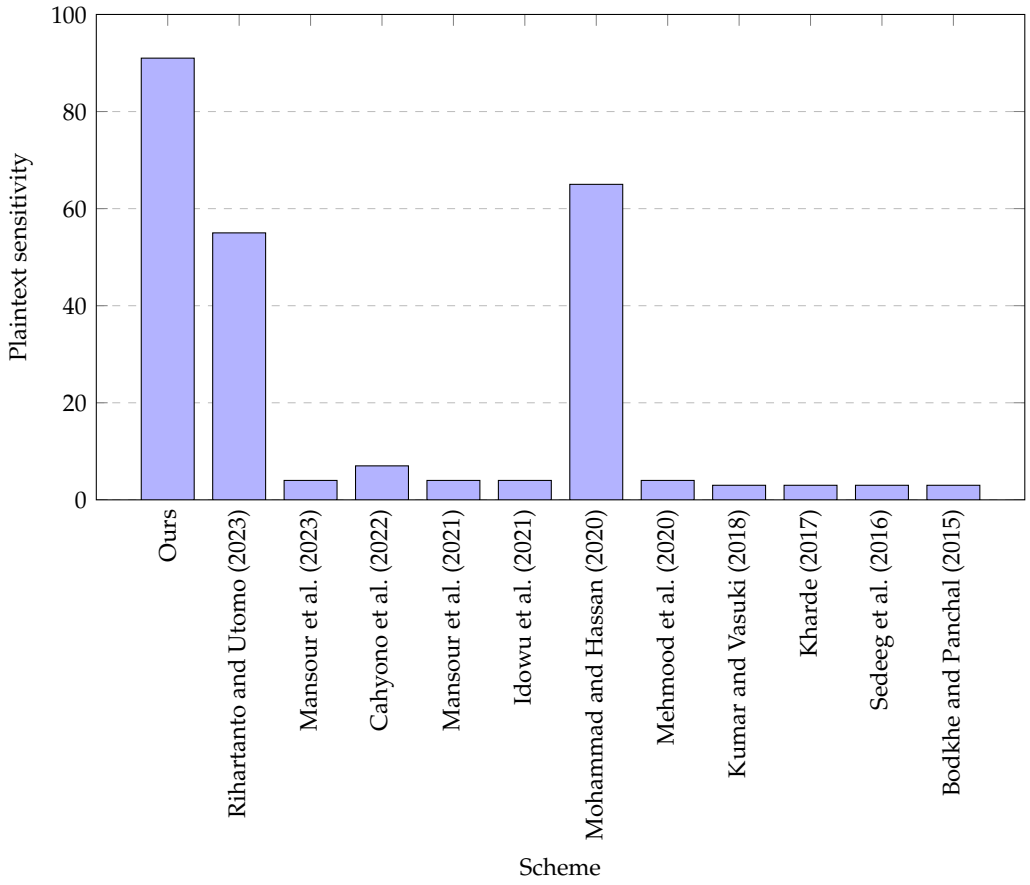

Figure 5. Comparison of the plaintext sensitivity of the proposed scheme with the state-of-the-art schemes [10–18,38,44].

4.9. Ciphertext-Only Attack

A ciphertext-only attack [50] arises when a cryptographer obtains certain ciphertexts and endeavors to acquire the confidential keys and eventually the plaintext. However, without the secret keys of the proposed scheme, the cryptanalyst cannot reveal the plaintext. Moreover, as explained earlier, the key space of the proposed scheme is at least 2^{100}, making it extremely time consuming to conduct a brute-force attack to decrypt the ciphertext without the keys. Thus, the proposed scheme is considered secure against ciphertext-only attacks.

4.10. Known-Plaintext Attack

A known-plaintext attack [50] is a cryptographic attack, where an attacker has access to some pairs of plaintext and its corresponding ciphertext, aiming to discover the secret key. As our cryptographic algorithm is based on an elliptic curve, it is crucial for the attacker to possess extensive knowledge about the specific curve being used. Our algorithm offers a wide range of options for the prime p. Additionally, for each prime value, there are numerous possible values of b, and for each b, there are vast options of point G on the corresponding elliptic curve. Therefore, for an attacker to succeed, they would need to exhaustively try all possible primes and, for each prime, use all b, then for each b, iterate through all points on the elliptic curve. This process is highly time consuming and presents a significant computational challenge. As a result, the proposed text encryption scheme exhibits a high level of security against the known-plaintext attack.

4.11. Chosen-Plaintext Attack

In a chosen-plaintext attack [50], the attacker can select a particular plaintext and observe the resulting ciphertext. The objective is to examine the obtained pairs of plaintext

and ciphertext to gain information about the secret encryption key or to understand the encryption process, which can compromise the security of the system. In the proposed scheme, the secret encryption keys consist of elliptic curve parameters denoted as p, b, and G. It is important to note that for each plaintext, there is a variation in the values of p, b, and G. As a result, the attacker cannot deduce any information about the secret key based solely on the plaintext–ciphertext pairs. This characteristic demonstrates that the proposed scheme is secure against chosen-plaintext attacks.

4.12. Chosen-Ciphertext Attack

The chosen-ciphertext attack [50] allows the attacker to select a ciphertext and observe its corresponding plaintext. The objective of this attack is to obtain information about the decryption algorithm or secret key. Our proposed algorithm ensures that attackers are unable to extract any information about the secret key through the ciphertext–plaintext pairs. In the proposed scheme explained in Section 3, the secret keys consist of parameters, namely p, b, G, s, q, and B. Each ciphertext–plaintext pair in this scheme has distinct elements for all components of the key. For example, when dealing with a prime value p, there are numerous possible options for b, and for each chosen b, the resulting ciphertext is entirely different. Consequently, the attacker cannot extract any information about the secret key from any given ciphertext–plaintext pair. Hence, the proposed scheme ensures security against the chosen-ciphertext attack.

4.13. Comparative Analysis of Cryptographic Attacks

We conducted a security analysis of our proposed text encryption scheme and compared its performance with existing encryption schemes [14,38–40,44]. The results are presented in Table 7, which outlines the evaluation of both the proposed scheme and the existing schemes in terms of key spacing, key sensitivity, the ciphertext-only attack, and the known-plaintext attack. The results from Table 7 indicate that the proposed scheme offers superior security against cryptographic attacks when compared with the text encryption schemes [14,38–40,44].

Table 7. Comparison of security performance against different cryptograhic attacks.

Scheme	Key Space	Key Sensitivity	Ciphertext Only Attack	Known-Plaintext Attack
Proposed	Pass	Pass	Pass	Pass
Ref. [38]	Fail	Fail	Fail	Fail
Ref. [14]	Pass	Pass	Pass	Fail
Ref. [44]	Fail	Pass	Fail	Fail
Ref. [39]	Fail	Pass	Fail	Fail
Ref. [40]	Fail	Fail	Fail	Fail

5. Conclusions

We proposed a novel scheme for text encryption that combines elliptic curve cryptography and a Type IVa MP wavelet to enhance security and improve efficiency. The proposed approach involves three distinct phases: in the first phase, the plaintext is encoded using ASCII characters, and its representation is then subjected to diffusion; in the second phase, points on an elliptic curve are computed, and a mapping technique is applied to introduce randomization into the data; finally, in the third phase, the resulting output is decomposed using a Type IVa MP wavelet to generate the ciphertext.

To examine the robustness of the proposed scheme and determine its reliability for secure text communication in various applications, we rigorously analyzed its security through a range of tests, including NIST analysis, entropy analysis, correlation analysis, key space analysis, key sensitivity analysis, plaintext sensitivity analysis, encryption quality analysis, ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, and chosen ciphertext attack.

The experimental results demonstrate that the correlation coefficient between the plaintext and ciphertext ranges from 0.001 to 0.08, indicating that it is very close to the ideal value of zero. Moreover, the percentage of encryption quality falls within the range of [76, 90], which is closer to the optimal percentage. The results also illustrate that the entropy of the ciphertext is significantly higher than that of the plaintext. Additionally, even minor changes to the input parameters lead to entirely different modified ciphertexts. The proposed text encryption scheme possesses a key space that is significantly larger than the acceptable value of 2^{100}, implying that the scheme has a substantial key space. Consequently, an attacker would face a challenging task when attempting to decrypt the text using the brute-force method. Furthermore, the results depict that the encryption and decryption times vary between 0.0254 and 0.0472 s, and 0.0256 and 0.3860 s, respectively, for plaintext lengths ranging from 30 to 5995 characters. These results provide compelling evidence that our designed encryption scheme is highly effective for cryptographic purposes.

We compared our proposed encryption scheme with existing text encryption schemes to gain a broader understanding of its performance in comparison to the state-of-the-art schemes [10–18,38–44]. We can list the following advantages of our approach:

- Our results indicate that the designed scheme offers a high level of security, while maintaining reasonable computational efficiency, making it well suited for secure text communication in various contexts, including sensitive government communications, financial transactions, and personal messaging.
- Additionally, the analysis performed depicts that our proposed scheme offers better resistance to modern cryptanalysis than the existing state-of-the-art text encryption schemes [10–18,38–40].

As for disadvantages of our current approach, we can list the following:

- The designed encryption scheme is currently limited to text data, but it could be advantageous to broaden its application to include other types of data, such as images, audios, and videos.
- Moreover, the results obtained by the proposed encryption scheme are not fully optimized. It would be useful to apply an optimization algorithm to attain an optimal level of security.

In conclusion, further research could be carried out to analyze the potential of incorporating different data formats into the proposed framework, and to evaluate its effectiveness in terms of security and computational efficiency.

Author Contributions: Conceptualization, U.H., M.D.B. and K.A.S.; Methodology, U.H., K.A.S. and T.H.; Software, K.A.S. and T.H.; Supervision, U.H.; Writing—original draft T.H. and K.A.S.; Writing—review and editing, U.H. and M.D.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

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

References

1. Zhu, S.; Zhu, C. Security Analysis and Improvement of an Image Encryption Cryptosystem Based on Bit Plane Extraction and Multi Chaos. *Entropy* **2021**, *23*, 505. [CrossRef]
2. Haider, T.; Azam, N.A.; Hayat, U. A Novel Image Encryption Scheme Based on ABC Algorithm and Elliptic Curves. *Arab. J. Sci. Eng.* **2022**, 1–21. [CrossRef]
3. Elkandoz, M.T.; Alexan, W. Image Encryption Based on a Combination of Multiple Chaotic Maps. *Multimed. Tools Appl.* **2022**, *81*, 25497–25518. [CrossRef]
4. Wu, R.; Gao, S.; Wang, X.; Liu, S.; Li, Q.; Erkan, U.; Tang, X. AEA-NCS: An Audio Encryption Algorithm Based on a Nested Chaotic System. *Chaos Solitons Fractals* **2022**, *165*, 112770. [CrossRef]
5. Gao, S.; Wu, R.; Wang, X.; Liu, J.; Li, Q.; Wang, C.; Tang, X. Asynchronous Updating Boolean Network Encryption Algorithm. *IEEE Trans. Circuits Syst. Video Technol.* **2023**. [CrossRef]

6. Xu, J.; Zhao, C.; Mou, J. A 3D Image Encryption Algorithm Based on the Chaotic System and the Image Segmentation. *IEEE Access* **2020**, *8*, 145995–146005. [CrossRef]
7. Gao, S.; Wu, R.; Wang, X.; Liu, J.; Li, Q.; Tang, X. EFR-CSTP: Encryption for Face Recognition Based on the Chaos and Semi-Tensor Product Theory. *Inf. Sci.* **2023**, *621*, 766–781. [CrossRef]
8. Gao, S.; Wu, R.; Wang, X.; Wang, J.; Li, Q.; Wang, C.; Tang, X. A 3D Model Encryption Scheme Based on a Cascaded Chaotic System. *Signal Process.* **2023**, *202*, 108745. [CrossRef]
9. Liu, J.; Zhou, J. *Cryptography and Network Security: Principles and Practice*; Pearson Education: London, UK, 2017.
10. Bodkhe, D.; Panchal, S. Use of Sumudu Transform in Cryptography. *Bull. Marathwada Math. Soc.* **2015**, *16*, 1–6.
11. Sedeeg, A.K.H.; Abdelrahim Mahgoub, M.M.; Saif Saeed, M.A. An Application of the New Integral Aboodh Transform in Cryptography. *Pure Appl. Math. J.* **2016**, *5*, 151–154. [CrossRef]
12. Kharde, U.D. An Application of the Elzaki Transform in Cryptography. *J. Adv. Res. Appl. Sci.* **2017**, *4*, 86–89.
13. Kumar, P.S.; Vasuki, S. An Application of MAHGOUB Transform in Cryptography. *Adv. Theor. Appl. Math.* **2018**, *13*, 91–99.
14. Subiono, J.C.; Cahyono, J.; Adzkiya, D.; Davvaz, B. A Cryptographic Algorithm using Wavelet Transforms over Max-Plus Algebra. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 627–635. [CrossRef]
15. Mehmood, A.; Farid, G.; Javed, R.; Ahsan, M.K. A New Mathematical Exponential Cryptology Algorithm by using Natural Transformation. *Int. J. Math. Anal.* **2020**, *14*, 187–193. [CrossRef]
16. Idowu, A.E.; Saheed, A.; Adekola, O.R.; Omofa, F.E. An Application of Integral Transform Based Method in Cryptograph. *Asian J. Pure Appl. Math.* **2021**, *3*, 13–18.
17. Mansour, E.A.; Kuffi, E.A.; Mehdi, S.A. Applying Complex SEE Transformation in Cryptography. *MJPS* **2021**, *8*. [CrossRef]
18. Mansour, E.A.; Kuffi, E.A.; Mehdi, S.A. Applying SEE Integral Transform in Cryptography. *IEEE Trans. Circuits Syst. Video Technol.* 2023, *in press*.
19. Tedmori, S.; Al-Najdawi, N. Image Cryptographic Algorithm Based on the Haar Wavelet Transform. *Inf. Sci.* **2014**, *269*, 21–34. [CrossRef]
20. Goswami, D.; Rahman, N.; Biswas, J.; Koul, A.; Tamang, R.L.; Bhattacharjee, D.A. A Discrete Wavelet Transform Based Cryptographic Algorithm. *Int. J. Comput. Sci. Netw. Secur.* **2011**, *11*, 178–182.
21. Shankar, K.; Elhoseny, M. An Optimal Haar Wavelet with Light Weight Cryptography Based Secret Data Hiding on Digital Images in Wireless Sensor Networks. In *Secure Image Transmission in Wireless Sensor Network (WSN) Applications*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 65–81.
22. Sivasankari, A.; Krishnaveni, S. Optimal Wavelet Coefficients Based Steganography for Image Security with Secret Sharing Cryptography Model. In *Cybersecurity and Secure Information Systems*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 67–85.
23. Nobuhara, H.; Trieu, D.B.K.; Maruyama, T.; Bede, B. Max-Plus Algebra-Based Wavelet Transforms and their FPGA Implementation for Image Coding. *Inf. Sci.* **2010**, *180*, 3232–3247. [CrossRef]
24. Kannoth, S.; Sateesh Kumar, H.C. Multi-Image Enhancement Technique using Max-Plus Algebra-Based Morphological Wavelet Transform. In Proceedings of the Advances in Signal Processing and Intelligent Recognition Systems: 4th International Symposium SIRS 2018, Bangalore, India, 19–22 September 2018; Revised Selected Papers 4; Springer: Berlin/Heidelberg, Germany, 2019; pp. 421–432.
25. Qu, M. *Sec 2: Recommended Elliptic Curve Domain Parameters*; Tech. Rep. SEC2-Ver-0.6; Certicom Res.: Mississauga, ON, Canada, 1999.
26. Ullah, I.; Azam, N.A.; Hayat, U. Efficient and Secure Substitution Box and Random Number Generators over Mordell Elliptic Curves. *J. Inf. Secur. Appl.* **2021**, *56*, 102619. [CrossRef]
27. 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]
28. Khan, M.A.M.; Azam, N.A.; Hayat, U.; Kamarulhaili, H. A Novel Deterministic Substitution Box Generator over Elliptic Curves for Real-Time Applications. *J. King Saud-Univ. Comput. Inf. Sci.* **2023**, *35*, 219–236. [CrossRef]
29. Azam, N.A.; Hayat, U.; Ayub, M. A Substitution Box Generator, its Analysis, and Applications in Image Encryption. *Signal Process.* **2021**, *187*, 108144. [CrossRef]
30. 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]
31. Azam, N.A.; Zhu, J.; Hayat, U.; Shurbevski, A. Towards Provably Secure Asymmetric Image Encryption Schemes. *Inf. Sci.* **2023**, *631*, 164–184. [CrossRef]
32. Azam, N.A.; Murtaza, G.; Hayat, U. A Novel Image Encryption Scheme Based on Elliptic Curves and Coupled Map Lattices. *Optik* **2023**, *274*, 170517. [CrossRef]
33. Azhar, S.; Azam, N.A.; Hayat, U. Text Encryption Using Pell Sequence and Elliptic Curves with Provable Security. *Comput. Cont.* **2022**, *71*, 4972–4989. [CrossRef]
34. Washington, L.C. *Elliptic Curves: Number Theory and Cryptography*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2008.
35. Silverman, J.H. *The Arithmetic of Elliptic Curves*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 106.
36. Baccelli, F.; Cohen, G.; Olsder, G.J.; Quadrat, J.P. *Synchronization and Linearity: An Algebra for Discrete Event Systems*; Wiley: Hoboken, NJ, USA, 1992.
37. Lauter, K. The Advantages of Elliptic Curve Cryptography for Wireless Security. *IEEE Wirel. Commun.* **2004**, *11*, 62–67. [CrossRef]

38. Rihartanto, R.; Utomo, D.S.B.; Februariyanti, H.; Susanto, A.; Khafidhah, W. Bit-Based Cube Rotation for Text Encryption. *Int. J. Electr. Comput. Eng.* **2023**, *13*, 709. [CrossRef]
39. Muchsin, H.N.N.; Sari, D.E.; Setiadi, D.R.I.M.; Rachmawanto, E.H. Text Encryption using Extended Bit Circular Shift Csipher. In Proceedings of the 2019 Fourth International Conference on Informatics and Computing (ICIC), Semarang, Indonesia, 16–17 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 8138–8143.
40. Chandra, S.; Mandal, B.; Alam, S.S.; Bhattacharyya, S. Content Based Double Encryption Algorithm using Symmetric Key Cryptography. *Procedia Comput. Sci.* **2015**, *57*, 1228–1234. [CrossRef]
41. Singh, L.D.; Singh, K.M. Implementation of Text Encryption using Elliptic Curve Cryptography. *Procedia Comput. Sci.* **2015**, *54*, 73–82. [CrossRef]
42. Murillo-Escobar, M.; Abundiz-Pérez, F.; Cruz-Hernández, C.; López-Gutiérrez, R. A Novel Symmetric Text Encryption Algorithm Based on Logistic Map. In Proceedings of the International Conference on Communications, Signal Processing and Computers, Guilin, China, 5–8 August 2014; Volume 4953.
43. Vigila, S.M.C.; Muneeswaran, K. Implementation of Text Based Cryptosystem using Elliptic Curve Cryptography. In Proceedings of the 2009 First International Conference on Advanced Computing, Chennai, India, 13–15 December 2009; pp. 82–85.
44. Mohammed, S.D.; Hasan, T.M. Cryptosystems using an Improving Hiding Technique Based on Latin Square and Magic Square. *Indones. J. Electr. Eng. Comput. Sci.* **2020**, *20*, 510–520. [CrossRef]
45. Arul, J.; Venkatesulu, M. Encryption Quality and Performance Analysis of GKSBC Algorithm. *J. Inf. Eng. Appl.* **2012**, *2*, 26–34.
46. Shannon, C.E. A Mathematical Theory of Communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [CrossRef]
47. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; Technical report; Booz-Allen and Hamilton Inc.: McLean, VA, USA, 2001.
48. Mishra, M.; Mankar, V.H. Hybrid Message-Embedded Cipher using Logistic Map. *arXiv* **2012**, arXiv:1209.2582.
49. Seyedzadeh, S.M.; Norouzi, B.; Mosavi, M.R.; Mirzakuchaki, S. A Novel Color Image Encryption Algorithm Based on Spatial Permutation and Quantum Chaotic Map. *Nonlinear Dyn.* **2015**, *81*, 511–529. [CrossRef]
50. Biryukov, A. *Encyclopedia of Cryptography and Security*; Springer: Berlin/Heidelberg, Germany, 2011.