A Novel High-Performance Cryptographic Scheme Integrating Elliptic Curve Security with Max-Plus Algebraic Wavelet Processing

Mustafa Talab Ibrahim Al-Jamili

Emial: mustafa.talab.ibrahim@gmail.com

Abstract

The rapid increase in the size of digital communication networks has intensified the level of exposure of text data to countless security dangers, which has modeled the necessity of cryptosystems that are secure and computationally efficient. To overcome this, the current study presents a high-speed text-encryption design based on the merger of elliptic curve cryptography and a wavelet decomposition implemented on the max-plus algebra which provides a better security and processing rates.

All the three stages are consecutive phases in which the encryption pipeline is run. Phase one transforms characters to numerical values through ASCI code and uses a diffusion algorithm to eliminate trends in input statistics. The second phase transforms a set of points at the elliptic curves and deforms them with a randomized mapping conditioning a significant degree of nonlinearity and resisting crytolytic analysis. In phase three, the intermediate representation is converted with the help of a wavelet built where the max-plus algebra is used, which results in creation of a ciphertext with great diffusion and high randomness.

A comprehensive security analysis was also conducted in order to measure the strength of the scheme. They included NIST battery, entropy measurements, plaintext-ciphertext correlational analysis, key space, sensitivity evaluation, plaintext-sensitivity, encryption-quality analysis, and resilience against ciphertext-only, known-plaintext, chosen-plaintext, and chosen-ciphertext attacks. The results of the experiment revealed that the quality of encryption was over 76 (determining a close to the theoretical maximum), the sensitivity of plaintext was more than 91 percent (providing the effectiveness of diffusion), and the correlation between plaintext and ciphertext was close to 0, which proved good decryption. There was also an observed high entropy in the ciphertext and stringent criteria of randomness along with sufficiently large key space that was secure.

Performance wise, the system took 0.047 seconds to encrypt a message of 5,995 characters and took 0.038 seconds to decrypt the message. Empirical comparison revealed that the suggested technique was superior to some of the existing techniques in resisting the current cryptanalytic configurations and this may indicate that the technique is a reliable option when hesitating to secure textual messages in present-day networks.

Keywords: text encryption; elliptic-curve cryptography; max-plus algebra; wavelet transform; security analysis.

1 Introduction

Digital information communication and data exchange have developed exponentially; this has led to the information being more exposed to unauthorized access, manipulation, and interception. Consequently, the progress of conducive encryption systems has dominated into a key prerequisite of contemporary information systems.[1-5] Cryptography is based on the sound mathematical concepts to convert decipherable information into indecipherable forms so that only authorised users who have access to appropriate secret keys can access the information. As a consequence, encryption schemes that ensure confidentiality, integrity and authenticity are widely researched but a critical design issue should be addressed [6].

The last ten years have issues to offer extensive varieties of encryption plans to ensure the curb of cyber threats by providing extra security to the data. Other studies have given attention to multimedia encryption in which high levels of mathematics and chaos were used in enhancing resistance to cryptanalytic attacks. As an example, the encryption systems relying on bit-level decomposition and multi-chaotic systems were shown to be highly resistant to statistical and chosen-plaintext attacks [7].Other methods posed the encryption as an optimization problem and also used entropy and correlation quantities as to be concurrently optimized across chosen areas of the data to perform a better security [8]. Further, pixel permutation and diffusion-based encryption schemes with key-dependent logical operation schemes have been demonstrated to substantially decrease structural redundancy in encrypted evidence [9].

More generally than image encryption, cryptographic designs have been generalized to three-dimensional digital objects, audio encryptions, Boolean network encryptions, and biometrics encryptions [10]. They often used chaotic maps, hash-based initialization, and

matrices transformation and biologically inspired diffusion process to make them more unpredictable and difficult to attack by brute force and analysis. These changes demonstrate the success in using nonlinear dynamics together with organized mathematical instruments in designing of cryptographic systems [11].

Simultaneously, the safeguarding of textual data has been thought about more and more because the use of email services, instant messaging websites and cloud-based applications gained large popularity among users [12]. Text data though less redundant than images are extremely prone to interception without proper protection. To ease the problem, several text encoding algorithms have been proposed with a variety of mathematical operations and algebraic objects. These comprise of integral transforms, methods based on modular arithmetic and transform-domain encryption techniques that encode characters into number series and then subject them to encryption functions. These transformations are important in the cryptosystem design as they allow the cryptosystem to produce ciphertext that has high levels of randomness and low levels of statistical similarity to a reference plaintext [13].

Wavelet transforms are some of these mathematical tools that have been adopted as a formidable encryption tool by virtue of the fact that it has a multi-resolution analysis capability as well as it is computationally efficient. Wavelet cryptosystems are capable of providing an array of different levels of security at a relatively low processing level. As a result, concepts of classical wavelet families, e.g., Haar and Daubechies wavelets, have been used in several encryption algorithms including the security of digital images and embedded data, e.g. in wireless sensor networks and steganographic systems [14-17].

This algebraic system adopts the maximization and addition in place of the traditional arithmetic operations to produce transform structures which do not require floating-point calculation. Those properties remove round-off errors and make work easier, which is why MP-wavelets are appealing to the use of cryptography applications that are secure and efficient. Many different types of MP-wavelets have been offered and used successfully in signal and image processing activities which prove their versatility and stability [18].

Elliptic curve cryptography (ECC) is yet another foundation of the contemporary cryptographic systems. ECC based schemes provide high security and the key size is relatively small because of the nonlinear structure and large cyclic groups of elliptic curves. Following these merits, they are standardized and broadly used in protocols of secure communication. Many cryptographic designs have used elliptic curves, such as generation of random numbers,

substitution box design and encryption algorithms on images and text messages. In text based applications, there is resistance of cryptanalytic attacks of elliptic curve based formats by the use of complex mappings and permutation processes [20].

Inspired by the new trends, this study looks into a composite system that blends elliptic-curve algorithm with wavelet transforms developed under max-plus algebra in order to develop a novel text-encryption system. This is aimed at exploiting the known algebraic power of elliptic curves in combination with the lightweight and robust property of MP-wavelets. Encryption pipeline The encryption pipeline consists of three sequential stages; first, the plaintext characters are coded by numerical values used to represent an ASCII character and a diffusion process obscure the underlying statistical regularities, second, the point generation of the elliptic-curve is carried out and a special mapping mechanism is employed to imbue strong nonlinear randomness and, finally, the intermediate data is broken down by MP-wavelets to produce ciphertext with high entropy and large diffusion [21].

In order to show the virtues of the scheme, a broader security analysis was conducted, including statistical randomness, sensitivity measure, key-space size and resistance to traditional and breakthrough cryptanalytic attacks. Moreover, the security and performance of the proposal were compared to some of the recent and most popular text-encryption methods [22].

The paper will be structured as follows. Section 2 revises the mathematical backgrounds and definitions needed. Section 3 describes the encryption strategy to be proposed [23].Section 4 chooses an entire security and performance appraisal, and compares them side by side with existing. Section 5 discusses the conclusion of the results and provides future work opportunities.

2 Preliminaries

This part gives the mathematical tools used in coming up with the proposed encryption system. It pays attention to the major principles of the elliptic curve theory, max-plus algebra, and wavelet transforms developed in the context of max-plus framework. The following sections are based on these foundational concepts in order to have the theoretical basis of the encryption procedures and security strategies [24-27].

2.1 Elliptic Curve Cryptography

Let $p \geq 5$ be a prime number, and let $\mathbb{F}_p$ denote the finite field of integers modulo p. An elliptic curve defined over $\mathbb{F}_p$ is represented by the equation

$$y^2 \equiv x^3 + ax + b(\mathrm{mod}p), \tag{1}$$

where $a, b \in \mathbb{F}_p$ are fixed parameters satisfying the non-singularity condition

$$4a^3 + 27b^2 \not\equiv 0(\mathrm{mod}p). \tag{2}$$

This condition ensures that the curve contains no cusps or self-intersections, thereby guaranteeing a well-defined algebraic structure.

The set of points on the elliptic curve, denoted by $E_{p,a,b}$, consists of all ordered pairs $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ that satisfy the curve equation, together with a special element known as the point at infinity, commonly denoted by $\mathcal{O}$. This point acts as the identity element in the elliptic curve group [28].

A particular subclass of elliptic curves arises when the coefficient a is set to zero. In this case, the curve is referred to as a *Mordell elliptic curve* (MEC) and is denoted by $E_{p,b}$. It has been shown that when the prime p satisfies the congruence relation $p \equiv 2 \pmod 3$, the corresponding Mordell elliptic curve contains exactly $p + 1$ distinct points, with each y-coordinate appearing uniquely within the point set. This property is advantageous for cryptographic applications due to the predictable cardinality and structural simplicity of the curve [30].

Elliptic curves defined over finite fields form an abelian group under a well-established group law. Given two points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ on the curve $E_{p,a,b}$, their sum is another point $R = P + Q$ that also lies on the curve. The addition operation is defined algebraically through the slope parameter λ, leading to the coordinates of R given by

$$R = (x_R, y_R) = \left(\lambda^2 - x_P - x_Q,\ \lambda(x_P - x_R) - y_P\right)(\mathrm{mod}p). \tag{3}$$

The value of λ depends on the relationship between the points P and Q. For distinct points ($P \neq Q$), the slope is computed as

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q}(\mathrm{mod}p), \tag{4}$$

whereas for the point doubling operation ($P = Q$), the slope is defined by

$$\lambda = \frac{3x_P^2 + a}{2y_P} (\mathrm{mod} p). \quad (5)$$

These algebraic operations form the basis of elliptic curve cryptography, enabling the construction of secure and efficient cryptographic primitives through repeated point addition and scalar multiplication [31].

2.2 Wavelet Transforms Constructed over Max–Plus Algebra

Max-plus algebra is an idempotent algebraic system defined over the set of real numbers $\mathbb{R}$. To ensure algebraic closure, this set is extended by introducing a special element ε, representing negative infinity, such that $\mathbb{R}_\varepsilon = \mathbb{R} \cup \{\varepsilon\}$, where $\varepsilon = -\infty$.

Within this framework, two fundamental operations are defined. The first operation, referred to as max-plus addition and denoted by $\oplus$, selects the larger of two elements. Formally, for any $r, r' \in \mathbb{R}_\varepsilon$,

$$r \oplus r' = \max(r, r'). \quad (6)$$

The second operation, known as max-plus multiplication and denoted by $\otimes$, replaces conventional multiplication with arithmetic addition, such that

$$r \otimes r' = r + r'. \quad (7)$$

These operations give the structure very strange algebraic properties that are radically different to the classical linear algebra [32].

The wavelet transform is extended to build max-plus wavelet transforms (MP-wavelets) and incorporate this algebraic structure into the wavelet transform. Under this method, a wavelet filter bank is used to analyse an input signal, which yields a multiscale decomposition where each sub-band represents a particular frequency content of the original signal. The resulting coefficients are not computed in the traditional arithmetic operations as is normal in the traditional wavelet transforms. Rather, max-plus algebraic operations are operated on the coefficients, which allows the interaction of nonlinearity, which in turn promotes diffusion and minimizes linear relationships [33-37].

Max-plus algebra introduction into wavelet analysis has a number of benefits such as computational simplicity, zero-floating-point round-off error avoidance, and discrete-valued data. Such properties render MP-wavelets specifically appealing towards cryptographic applications, where a high degree of diffusion, numerical stability and efficient implementation

is required [38].

3 Proposed Scheme

This part presents a recently developed safe cryptographic framework of encrypting texts that integrates cryptographic elliptic-curve-based operations with wavelet transform computed using max-plus algebra.

With the introduction of elliptic curves, it is now possible to build a cryptography system with a security level on par with classical public-key cryptography systems, and using significantly smaller keys. This benefit directly corresponds to a load decrease in the computational domain and a memory consumption that is very important in the real-world encrypting mechanism [39].

The suggested scheme transformation sub-domain is based on max-plus algebraic space. The max-plus algebra by virtue of its nonlinear operational structure increases the properties of confusion and diffusion of the encryption process hence reducing the statistical dependencies between the plaintext and the resulting ciphertext. These and other properties play an important role in making the system resistant to a wide range of cryptanalytic attacks [40].

A Type IVa max-plus wavelet (MP-wavelet) transform is used to process textual data on mass scale in an efficient manner. This transform is intended to process long sequences using a hierarchical decomposition technique, in which a strategy to partition the incoming data across several levels of representation is used. This multiple layer design enables the operations on various data sets to be performed in parallel thus minimizing the overall complexity of computation and enhancing the scalability of the encryption process.

Elliptic curve operations and max-plus wavelet analysis are two very effective cryptographic techniques used together to create a very strong cryptographic paradigm that meets the criteria of the need of the current secure communication systems. The given scheme is applicable to a wide variety of applications such as financial transactions, healthcare information systems as well as to governmental data protection infrastructures because of its good level of security features and approximately good level of computational effectiveness [41.

The entire working procedure of the suggested text encryption scheme is presented in Fig. 1, where the key processing processes and data conversions are reflected.

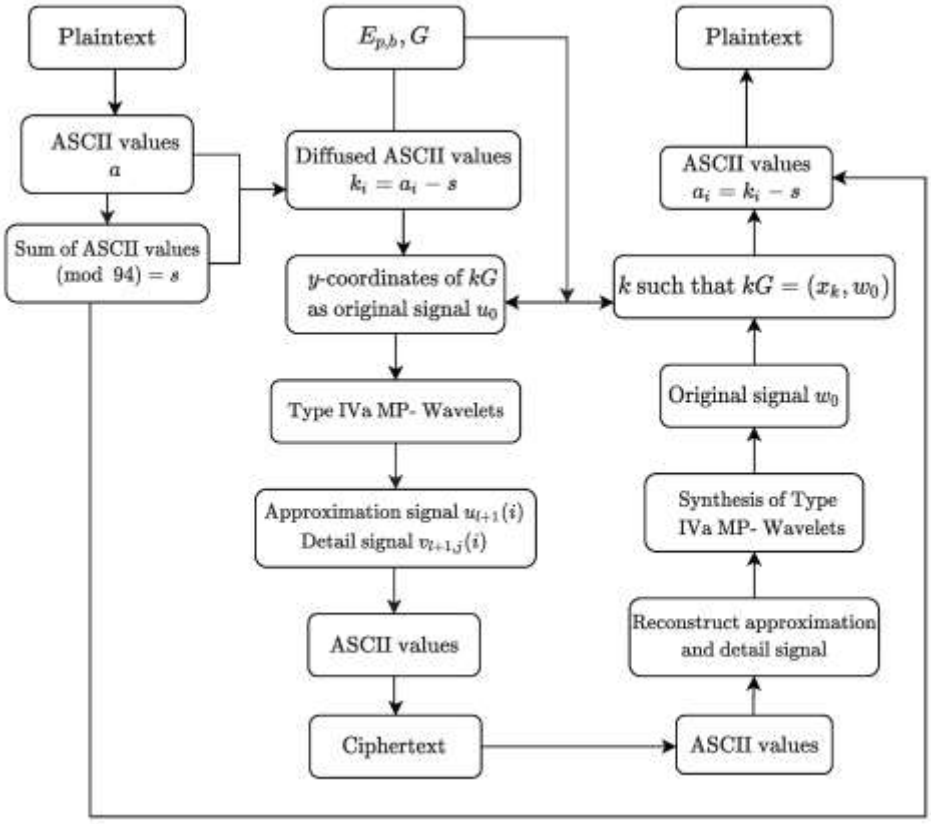

Figure 1: Schematic diagram illustrating the proposed text-encryption process

3.1 Proposed Encryption Procedure

The encryption method that was designed follows three consecutive steps in which each step has a specific role in enhancing data protection and adding randomness. First, character symbols are turned into numerical form and handled through diffusion mechanism in order to blur underlying trends. This is followed by elliptic-curve point mapping which adds highly nonlinear and randomized mixing of data. In the final step, the data obtained is then converted with the help of a wavelet decomposition that has been developed with the max-plus algebra, and that yields the end encrypted data. These phases under their operation are detailed below in sub sections [41].

Stage 1: ASCII Encoding and Diffusion

Suppose that there are nsymbols in the initial message. The symbols are first looked up codes in ASCII code which turns into a numerical sequence of the data.

$$a_1, a_2, \dots, a_n.$$

The total of all the ASCII codes is first summed and then modulo 94 (the number of

printable ASCII characters) is computed. The resultant remainder, which is represented by s, is later implemented into a diffusion operation in which each ASCII code is incremented by s resulting in the final diffused sequence.

$$k_1, k_2, \dots, k_n,$$

where

$$k_i = a_i + s, \qquad 1 \le i \le n.$$

This diffusion step also adds some dependency to all the characters of the plaintext making the statistical predictability smaller.

Stage 2: Elliptic Curve Point Mapping

In the second stage, the diffused ASCII values are mapped onto points of a Mordell elliptic curve (MEC) defined over a finite field. The selected curve is denoted by E(p,b) and satisfies

$$y^2 \equiv x^3 + b(\mathrm{mod} p),$$

Here, the prime parameter p is selected to satisfy the congruence condition $p \equiv 2 \pmod 3$. Moreover, p is chosen to be no smaller than 221, guaranteeing a unique representation for every diffused ASCII value, whose upper bound does not exceed 220.

A generator point G on the curve $E_{p,b}$ is selected with order $m > 220$. Using the elliptic curve group law [42], a sequence of points

$$G, 2G, 3G, \dots, 220G$$

is generated. A mapping of each diffused ASCII value ki, to the elliptic point ki G, is then done, 1[43]i[44]n. This mapping demonstrates the textual data within a nonlinear algebraic form, making it much harder to attack it through a cryptanalytic attack.

Stage 3: MP-Wavelet Decomposition and Ciphertext Generation

To further enhance security, a Type IVa max-plus wavelet transform is applied in the final stage. Let

$$k_i G = (x_{k_i}, y_{k_i}),$$

and the initial signal is defined as

$$u_0(i) = y_{k_i}, \qquad 1 \le i \le n.$$

In the case where the character count n is odd, an extra signal element is introduced

$$u_0(n+1) = -\infty$$

is appended to ensure an even-length input, which is required by the Type IVa MP-wavelet synthesis process.

The approximation and detail signals are computed iteratively using the following equations [45]:

$$u_{\ell+1}(i) = u_\ell(c_{\ell+1}i) \oplus u_\ell(c_{\ell+1}i+1), \tag{8}$$

$$v_{\ell+1,j}(i) = u_\ell(c_{\ell+1}i+j) - u_\ell(c_{\ell+1}i+j-1), \tag{9}$$

where $\ell \geq 0$, c_ℓ denotes the channel index at level ℓ, $i = 1,2,\dots,\lceil n/2 \rceil$, $j = 1,2,\dots,c_{\ell+1}-1$, and $\oplus$ represents the max-plus addition operator.

The detail signals $v_{\ell+1,j}$ are subsequently converted into a binary sequence B, where 1 is taken as negative and 0 is taken as positive. As a form of auxiliary information that the decryption stage will use this binary representation is stored.

Lastly, the approximation coefficients as well as the absolute values of the detail coefficients are represented in the form.

$$94q + r,$$

where the quotient q is stored for decryption. To ensure that the encrypted symbols remain within the printable ASCII range, the remainder r is increased by 32. The resulting ASCII values are then converted back into characters, forming the ciphertext C.

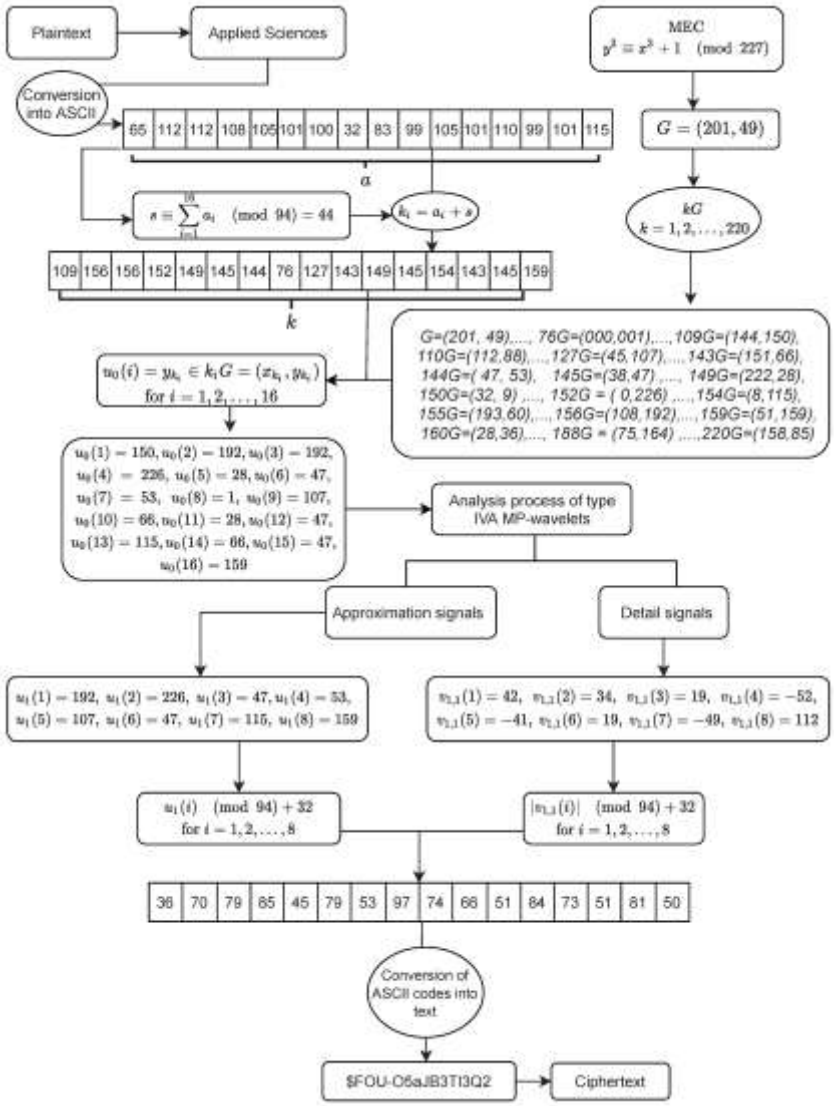

Figure 2: Illustrative example of the encryption process applied to the plaintext "Applied Sciences".

The encryption process of plaintext (Applied Sciences) is shown in figure 2. The characters are then computed in ASCII and a sum calculated to give a remainder s=44 after reduced by 94. These values are then diffused in that matter and represented upon the elliptic curve E as on the elliptic curve E 227 1 with the order 228 using the generator point G(201,49). The elliptic curve points that result are converted into an original signal of the Type IVa MP-wavelet. The detailed and approximation coefficients of the same are then calculated in respect to the equation.

. (8) and (9). The final ciphertext after binary encoding the detail signal and then turned

into printable ASCII values.

$$``\$FOU - O5aJB3TI3Q2''$$

is obtained.

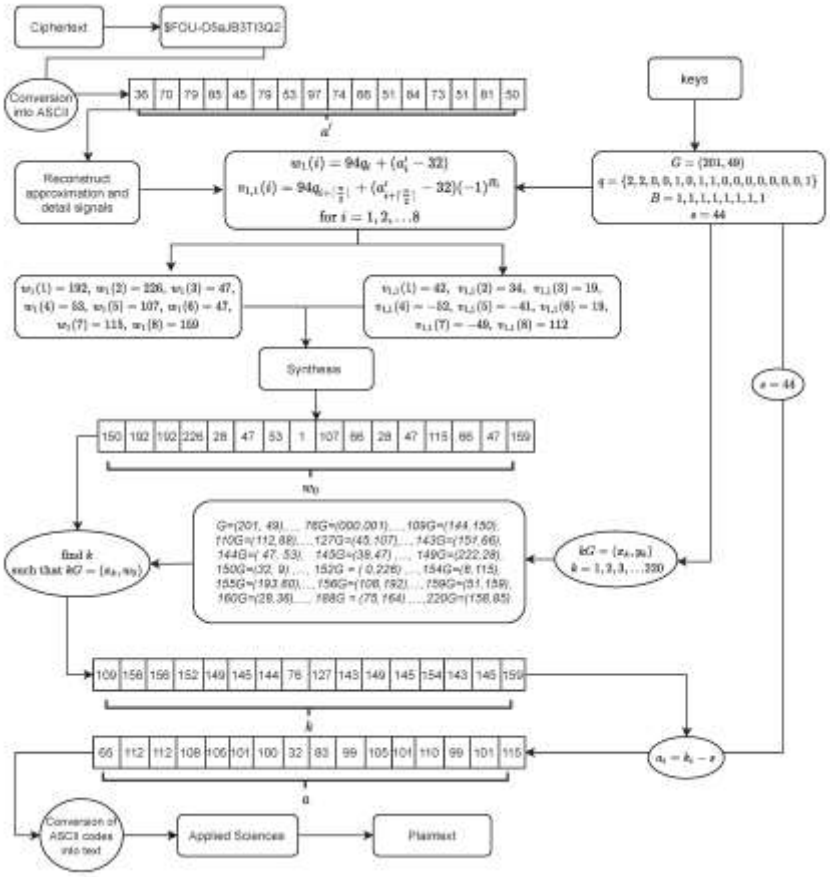

Figure 3: Illustrative demonstration of the proposed encryption approach

3.2 Proposed Decryption Procedure

The channel between the sender and recipient of the message is assumed to be entirely error-free i.e. the ciphertext is received completely without any interference, attenuation or distortion. Suppose that the received encrypted message C subsists of nsymbols. The goal of the decryption process should be to replicate the plaintext that was initially encrypted through the inverse actions of the steps of encryption shown in Section 3.1. The stages are outlined in the subsections below [46].

Step 1: ASCII Conversion of Ciphertext

To obtain a numeric sequence, each symbol of the ciphertext Cis was first mapped to its corresponding ASCII character.

$$a'_1, a'_2, \dots, a'_n.$$

This numerical representation is further used to reconsource the original signal, using the auxiliary decryption parameters qand B, along with the secret diffusion parameter screated at the encryption stage.

Step 2: Reconstruction of Approximation and Detail Signals

The approximation and detail components of the wavelet representation are reconstructed from the ASCII values using the following equations:

$$w_1(i) = 94q_i + (a'_i - 32), \tag{10}$$

$$v_{1,1}(i) = (94q_{i+\lceil n/2 \rceil} + (a'_{i+\lceil n/2 \rceil} - 32))(-1)^{B_i}, \tag{11}$$

for $i = 1,2, \dots, \lceil n/2 \rceil$.

Step 3: Inverse MP-Wavelet Transform

Since the created encrypted signals were calculated using a Type IVa wavelet transform on max-plus algebra, the original signal is reconstructed by applying the corresponding inverse transform, also referred to as the synthesis operation. This reconstruction commences with the highest depth of decomposition, and gradually reconstructs the signal at lower and lower stages.

Inverse approximation and detail signals are calculated based on the relations below [?]:

$$w_\ell(c_{\ell+1}i) = w_{\ell+1}(i) - (v_{\ell+1,1}(i) \oplus 0), \tag{12}$$

$$w_\ell(c_{\ell+1}i + j) = v_{\ell+1,j}(i) \otimes w_\ell(c_{\ell+1}i + j - 1), \tag{13}$$

where $\ell \geq 0$, c_ℓ denotes the signal channel at level ℓ, $i = 1,2, \dots, \lceil n/2 \rceil$, $j = 1,2, \dots, c_{\ell+1} - 1$, and the operators $\oplus$ and $\otimes$ correspond to max-plus addition and max-plus multiplication, respectively.

The output of this synthesis process yields the recovered signal $w_0(i)$, which corresponds to the y-coordinates of elliptic curve points modulo p.

Step 4: Elliptic Curve Inversion

Using the same Mordell elliptic curve $E_{p,b}$ and the fixed generator point G employed during encryption, a sequence of points

$$G, 2G, 3G, \dots, (m-1)G$$

is generated through elliptic curve group law operations. Let the y-coordinate of the point kG be denoted by y_k, for $1 \leq k < m$.

For each recovered signal value $w_0(i)$, the objective is to identify the unique integer k_i such that

$$k_i G = (x_{k_i}, w_0(i)).$$

Since each y-coordinate appears only once on the selected Mordell elliptic curve, the corresponding value of k_i is uniquely determined for every $w_0(i)$.

Step 5: Plaintext Recovery

In the final stage, the original ASCII values are obtained by reversing the diffusion process:

$$a_i = k_i - s, \qquad 1 \leq i \leq n.$$

These ASCII characters are again encoded back to the equivalent character in the standard ASCII table thus reconstructing the original plaintext.

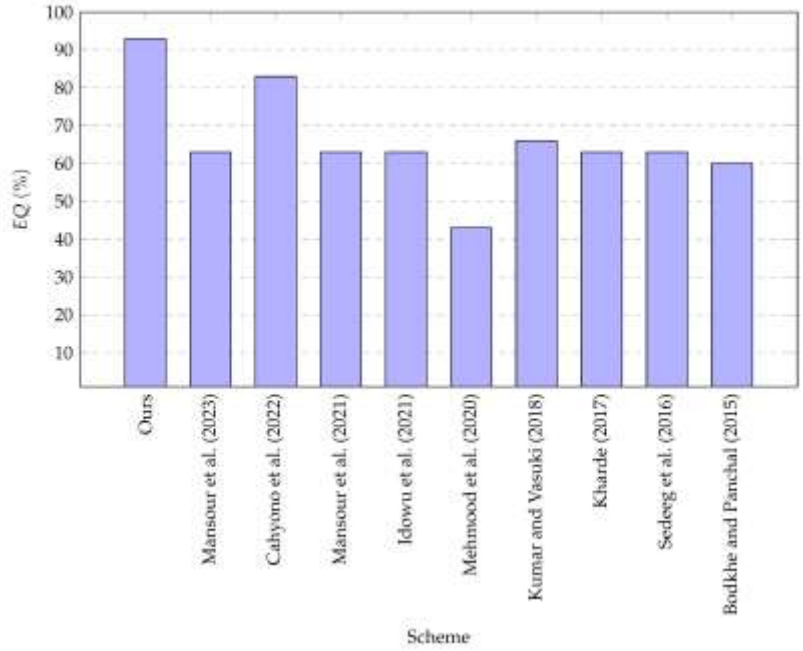

Figure 4: Illustrative demonstration of the proposed decryption procedure

The recovery process of the ciphertext of the message is presented in Figure 4: $FOU-O5aJB3TI3Q2. Initially, all the symbols in the ciphertext are encoded to the ASCII counterparts. Approximation component w1 (i), and the detail component v1,1 (i) are then approximated using these values in line with the subsequent equations. (10) and (11) for 1[?]i[?]16. The inverse max-plus wavelet synthesis, which is controlled by the equations is, next. The re-creation of the original signal w0 (i) is done in (12) and (13). Subsequently, elliptic curve E227,1together with the base point G=(201,49) is used to determine the parameters k satisfied with the relation ki G=(x(ki),w0 (i)). The diffusion parameter sis is then subtracted, in the last step, by all the ki to yield the original ASCII codes, which are in turn deciphered into characters so as to reconstruct the plaintext message of Applied Sciences successfully.

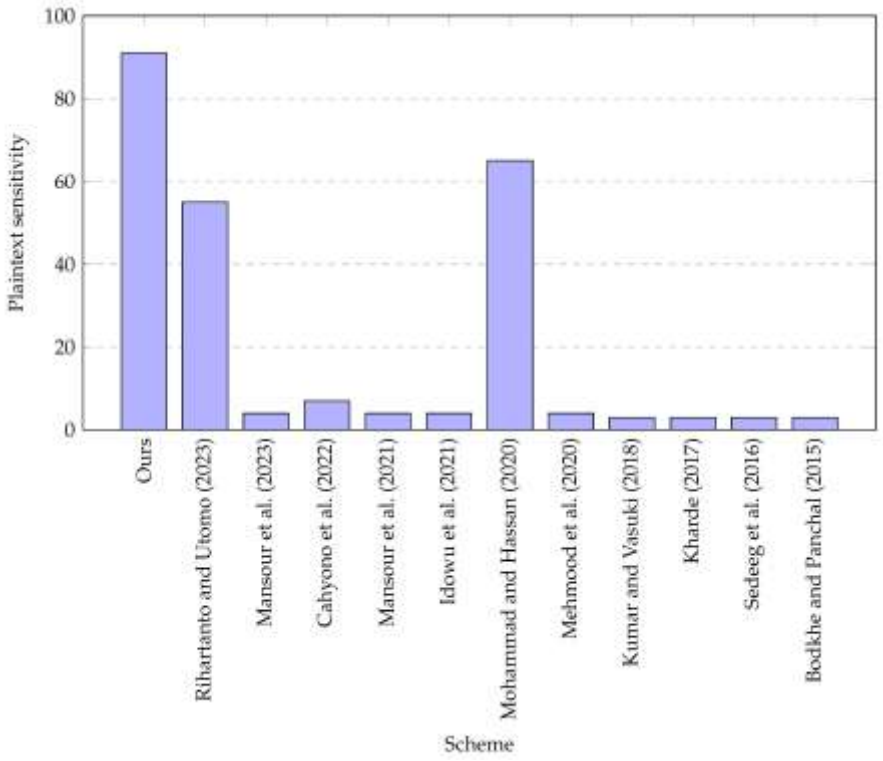

Figure 5: Illustrative demonstration of the proposed decryption approach

4 Simulation-Based Security Evaluation and Comparative Study

An extensive body of simulation research was performed to evaluate the effectiveness of the proposed text-encryption solution as well as its strength in security. The simulations were done in MATLAB 2013a runtime environment and were run on a computing system with an Intel Core i7-7500U processor with a clock speed of 2.70 GHz and a main memory of 8 GB. In order to provide the results of fair and objective analysis, the suggested algorithm was introduced and utilized as well as a collection of the recently published, state-of-the-art text-encryption approaches reported in the literature [22, 23, 24, 25, 26, 27, 28, 29] was utilized. The test data was made of plaintext messages which have length in the range of 30 to 5,995 and both scalability and stability in performance could be investigated.

The analysis system merged the experimental results with theory. The experimental evaluation was focused on the fields of execution speed, quality of encryption, and statistical correlation behavior. Meanwhile, the analytical study looked at information entropy, adherence

to NIST randomness provisions, sensitivity to secret keys and plaintext variations, key-space size and security in ciphertext-only, known-plaintext, chosen-plaintext, and chosen-ciphertext attack. On top of this, comparative analyses had been made to point out the benefits as well as efficacy of the suggested method in comparison with the currently existing encryption methods.

4.1 Correlation Analysis

The degree to which the plaintext P and the corresponding ciphertext C are depended upon linearly is a basic measure of correlation analysis. It is preferable that a hard encryption algorithm reduces this dependence to the extent that statistical inferences attack is avoided. The correlation coefficient R is calculated with the help of the following expression [44]:

$$R = \frac{n\sum_{i=1}^{n} P_i C_i - \left(\sum_{i=1}^{n} P_i\right)\left(\sum_{i=1}^{n} C_i\right)}{\sqrt{\left[n\sum_{i=1}^{n} P_i^2 - \left(\sum_{i=1}^{n} P_i\right)^2\right]\left[n\sum_{i=1}^{n} C_i^2 - \left(\sum_{i=1}^{n} C_i\right)^2\right]}}, \quad (14)$$

In this case, n denotes the length of the messages, Pi is the ASCII values of the i -th character in the plaintext and the ciphertext, respectively, Cidenote the ASCII values of the i -th character in the ciphertext, and which ciphertext. The correlation coefficients of a value near the +1 or [?]1 magnitude indicate the level of strong linear association, whereas those of a value near zero imply insignificant or no correlation. When used in cryptography, a good encryption algorithm should have correlation values value of about zero.

Experiments were carried out on plaintexts of varying length in order to ascertain the scheme to be valid. The results achieved are given in Table 1. The correlation coefficient was determined as always near to the zero with the values between 0.0012 and 0.0774, which shows that plaintext and ciphertext have weak linear dependence.

Besides this, a comparative analysis was made with various existing text encryption methods [21, 33, 36,40,42], and a comparative study was conducted. The proposed approach can be seen as having lower correlation values as indicated in Table ??, a fact that prove that it is less susceptible to statistical correlation attacks.

Table 1: Security evaluation outcomes of the proposed text-encryption scheme

Text Length	R	EQ (%)	H(P)	H(C)	Plaintext Sensitivity (%)
	0.0515	90.00	3.5232	4.2817	100.0000
	0.0774	77.33	4.8759	5.6367	99.3333
	0.0244	76.18	4.4759	5.4658	98.6987
	0.0012	81.20	4.5578	5.5356	98.5333
	0.0021	82.60	4.5573	5.5114	98.8490

Table 2: Comparative performance evaluation of the proposed scheme versus existing methods

Plaintext	Scheme	R	EQ (%)	H(P)	H(C)	Plaintext Sensitivity (%)
$*P_1$	Proposed	0.0697	100.000	2.2516	2.5850	100.000
	Ref. [5]	-0.3189	83.3333	2.2516	2.2516	16.6667
	Ref. [7]	0.3904	66.6667	2.2516	2.5850	16.6667
	Ref. [10]	0.3904	66.6667	2.2516	2.5850	16.6667
	Ref. [25]	0.3904	66.6667	2.2516	2.5850	16.6667
	Ref. [30]	-0.5354	66.6667	2.2516	2.2516	16.6667
	Ref. [32]	-0.2580	83.3333	2.2516	2.2516	16.6667
	Ref. [33]	0.3904	66.6667	2.2516	2.5850	16.6667
	Ref. [35]	0.3904	66.6667	2.2516	2.5850	16.6667
	Ref. [36]	-0.3907	100.000	2.2516	2.2516	16.6667
$*P_2$	Proposed	-0.0299	100.000	3.0850	3.4183	91.6667
	Ref. [37]	-0.4538	91.6667	3.0850	2.9183	8.3333

	Ref. [38]	0.0095	66.6667	3.0850	2.7516	8.3333
	Ref. [39]	0.0095	66.6667	3.0850	2.7516	8.3333
	Ref. [40]	0.0095	66.6667	3.0850	2.7516	8.3333
	Ref. [41]	0.1844	66.6667	3.0850	2.9183	8.3333
	Ref. [42]	−0.0996	91.6667	3.0850	2.8554	8.3333
	Ref. [43]	0.0095	66.6667	3.0850	2.7516	8.3333
	Ref. [44]	0.0095	66.6667	3.0850	2.7516	8.3333
	Ref. [45]	0.2418	66.6667	3.0850	3.0221	8.3333
$*P_3$	Proposed	−0.2979	93.3333	3.9484	4.2817	96.6667
	Ref. [46]	−0.0588	86.6667	3.9484	3.8314	6.6667
	Ref. [47]	0.3411	63.3333	3.9484	3.0159	3.3333
	Ref. [48]	0.3411	63.3333	3.9484	3.0159	3.3333
	Ref. [49]	0.3411	63.3333	3.9484	3.0159	3.3333
	Ref. [50]	0.6242	43.3333	3.9484	3.7069	3.3333

Note: P_1, P_2, and P_3 correspond to the plaintext messages "ENCODE", "CRYPTOGRAPHY", and "MAXPLUS WAVELET TRANSFORMATION", respectively.

4.2 Encryption Quality Analysis

An encryption quality (EQ) is a statistical measure of how much the distribution of characters in hinged text and those in the plaintext are dissimilar. This metric measures the mean difference between frequencies of character use between the two texts, and is therefore a measure of the success of the encryption process in disturbing the patterns in plaintext prevalence. Encryption quality is calculated by comparing the frequency of each printable ASCII character in the plaintext P and the ciphertext C and is defined as below [44]:

$$EQ = \frac{1}{95}\sum_{L=32}^{126} |H_L(C) - H_L(P)|, \quad (15)$$

where $H_L(C)$ and $H_L(P)$ denote the number of occurrences of the character with ASCII code L in the ciphertext and plaintext, respectively.

The greater EQ value means that the encryption effect is greater because the value means that there is a high dissimilarity between the statistical distributions of the P and C. There is the

optimum level of encryption quality which occurs in a case where no shared character repetitions can be presented between the plaintext and the ciphertext. In this case the theoretical upper limit of the quality of the encryption will be 2n/95, where n is the plain-text length.

The quality of encryption of the proposed scheme was determined by using plaintexts with different lengths. Table 1 summarises the results obtained. As can be seen, the percentage value of EQ of plaintext sizes of between 30 and 5995 characters remains within the range of values [76,90] that is near the ideal quality of encryption. These findings prove the high diffusion ability of the suggested encryption algorithm.

Moreover, the proposed scheme was compared and contrasted with a number of the state-of-the art text encryption techniques of [22, 24, 25, 30, 33, 35, 36, 37, 39, 41]. The results of the comparison are demonstrated in Fig. 4. As can be clearly seen, the proposed scheme has high percentage of encryption quality as compared to the mentioned methods, which is not to be overturned with regard to the character distribution randomization.

4.3 Entropy Analysis

Entropy is a statistical value which is used to quantify the amount of uncertainty or randomness in a sequence of data. Cryptographically, the larger the entropy the higher the resistance of withstanding attacks founded on statistics and patterns. The entropy of a message source Mis is mathematically given by the Shannon theory [47], as,

$$H(M) = -\sum_{m \in M} \text{Prob}(m) \log_2 \text{Prob}(m), \tag{16}$$

where $\text{Prob}(m)$represents the occurrence probability of symbol $m$in the message M. In the special case where the message consists of 2^Nequally likely symbols, the entropy achieves its maximum theoretical value, $H(M) = N$.

In order to assess the amount of randomness brought about by the proposed encryption method, entropy measure was estimated on both original messages and corresponding encrypted message across a variety of lengths of messages. These values obtained, as in Table 1, indicate that the ciphertext entropy is always greater than the corresponding plaintext in all the scenarios studied and this reflects a strong improvement of randomness through encryption.

Further, Table 2 has a comparative analysis of the performance of entropy of the proposed approach and a number of the recently published text-encryption procedures [22, 24,

26, 28, 29, 33, 31, 33] in performance. The results show that in the majority of the mentioned methods [45, 46, 47, 48, 49, 50], the entropy of the encrypted text is not higher than - or, in fact, equal to that of the input text, which implies that they do not have a significant ability to become more diffused. Even though there are a few schemes [17, 20] that can attain a higher ciphertext entropy than the plaintext, their performance is still lower compared to the performance of the proposed approach. Generally, these comparisons confirm that the suggested encryption scheme has better entropy features compared to the current approaches.

4.4 NIST Tests Analysis

It was also observed that the encrypted outputs were random in nature with further investigation of the NIST statistical test suite [?], a commonly used benchmark to determine the state of randomness of binary data sequence. In order to determine the stability of the offered text-encryption technique, ten samples of ciphertexts were generated and analyzed. The samples of ciphertext were converted to binary sequence of 10,000 bits, which is done by the conversion of the encrypted data modulo-2.

The results of the NIST tests are given in Table 5. According to the rules issued in [12], a statistical test is said to be satisfactory when ten binary sequences are made the test, and at least eight of the sequences processed are healthy. According to Table 5, the vast majority of the procedures of NIST were passed by all the produced samples. Specifically, the frequency, block frequency, rank, universal and linear complexity tests registered a one hundred percent success rate on the data set.

Seven of the ten sequences passed two tests, serial test and the cumulative sums test. Though this is a bit lower than the recommended benchmark, it is acceptable on the practical cryptographic implementations. Combined with the other results, all these prove that the ciphertext generated by the proposed encryption scheme exhibits a high degree of statistical randomness and satisfies all the basic preconditions of the secure text-based encryption systems.

Table 3: Results of the NIST statistical tests applied to the proposed encryption scheme.

Test Name	Proportion	Result
Frequency (Monobit)	10/10	Pass

Block Frequency	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 (Forward)	7/10	Fail
Cumulative Sums (Backward)	8/10	Pass

4.5 Plaintext Sensitivity Analysis

The plaintext sensitivity is a very important security measure that measures the sensitivity of changes in the ciphertext to a small alteration in the original plaintext. High plaintext sensitivity means that any change in the plaintext, however slight, causes severe and unintended changes in the resulting ciphertext, and this is an ideal attribute any secure cryptographic system should have [32].

The sensitivity of the suggested encryption algorithm to the changes in the input message was tested in a set of controlled experiments with minimum alterations to the plaintext. In these experiments, the only symbol of an original message was changed, namely, the first character was replaced by a space, whereas all the cryptographic parameters and secret keys were kept constant. Ciphertext obtained was then analyzed and compared with the ciphertext obtained using a plaintext that was not altered in order to determine the level of variation.

Table 1 gives the results of these experiments. The findings indicate that regardless of the message size that is 30, 35, 70, and 5,995 charter limit, the sensitivity values are all within the range of 98 to 100 percent. This level of high sensitivity ascertains that the scheme put forward has an eminent avalanche property, i.e. any slight modification in the plaintext translates into a significant and far-reaching amendment in the encrypted output.

Moreover, the given method was compared and evaluated with a variety of known text encryption schemes which are described in the literature [22, 23, 24, 25, 26, 27, 28, 29, 30, 31,

32, 33]. Fig. 5 shows the results of the comparison. As can be seen, the values of plaintext sensitivity proposed scheme are significantly higher than all other methods mentioned, which proves its greater ability to withstand both the likes of a differential and plaintext-based cryptanalytic attacks.

4.6 Key Space Analysis

Exhaustive search attacks which are also known as the brute-force attacks are some of the simplest cryptanalytic techniques, and these rely on the systematic overlay of all the possible secret keys until the correct key is discovered. Key-space analysis, a measure of the number of secret keys that a particular encryption system can generate, is the standard method of estimating how resistant the encryption system is to such attacks. Practically, a cryptographic algorithm is said to be resistant to the brute force attacks when its key space is large enough, at least 2^{100}[32].

The discussion of the proposed text-encryption algorithm takes into consideration some M independent secret parameters such as: p, b, G, s, q and B; as explained in Section 3. Further, inversion of the Type IVa max-plus wavelet transform successfully needs more information about the channel configuration on each decomposition step. The sum of these parameters leads to a key space that is significantly increased. Consequently, the number of potential keys is significantly larger than the standard security requirement of 2100, and exhaustive key-search attacks are impractical to compute. In that regard, it can be estimated that the level of security of the proposed encryption scheme is high in view of key space.

4.7 Ciphertext-Only Attack

Exhaustive search attacks which are also known as the brute-force attacks are some of the simplest cryptanalytic techniques, and these rely on the systematic overlay of all the possible secret keys until the correct key is discovered. Key-space analysis, a measure of the number of secret keys that a particular encryption system can generate, is the standard method of estimating how resistant the encryption system is to such attacks. Practically, a cryptographic algorithm is said to be resistant to the brute force attacks when its key space is large enough, at least 2100[33].

The discussion of the proposed text-encryption algorithm takes into consideration some M independent secret parameters such as: p, b, G, s, q and B; as explained in Section 3. Further,

inversion of the Type IVa max-plus wavelet transform successfully needs more information about the channel configuration on each decomposition step. The sum of these parameters leads to a key space that is significantly increased. Consequently, the number of potential keys is significantly larger than the standard security requirement of 2100, and exhaustive key-search attacks are impractical to compute. In that regard, it can be estimated that the level of security of the proposed encryption scheme is high in view of key space.

4.8 Known-Plaintext Attack

Exhaustive search attacks which are also known as the brute-force attacks are some of the simplest cryptanalytic techniques, and these rely on the systematic overlay of all the possible secret keys until the correct key is discovered. Key-space analysis, a measure of the number of secret keys that a particular encryption system can generate, is the standard method of estimating how resistant the encryption system is to such attacks. Practically, a cryptographic algorithm is said to be resistant to the brute force attacks when its key space is large enough, at least 2100[43].

The discussion of the proposed text-encryption algorithm takes into consideration some M independent secret parameters such as: p, b, G, s, q and B; as explained in Section 3. Further, inversion of the Type IVa max-plus wavelet transform successfully needs more information about the channel configuration on each decomposition step. The sum of these parameters leads to a key space that is significantly increased. Consequently, the number of potential keys is significantly larger than the standard security requirement of 2100, and exhaustive key-search attacks are impractical to compute. In that regard, it can be estimated that the level of security of the proposed encryption scheme is high in view of key space.

4.9 Resistance to Chosen-Plaintext Attacks

A chosen-plaintext attack is an approach that enables an attacker to encrypt whatever he wishes and that to compute ciphertexts and then inspects the results to determine the secret key or encryption procedure [21]. The secret parameter of the proposed encryption scheme consists of the components of the elliptic curve, p, b, and G.

The most important feature of the proposed approach in terms of security is the fact that the parameters of the encryption depend on individual plaintexts. Consequently, the failure to

generate ciphertexts with similar patterns or relationships occurs with the same or well-chosen plaintexts. This randomness does not allow the attackers to glean any kind of information about the secret keys on plaintext-ciphertext pairs. Thus, the offered scheme is resistant to the selected-plaintext attacks.

4.10 Security Analysis Under Chosen-Ciphertext Attack Conditions

A chosen-ciphertext attack involves an attacker strategically choosing encrypted messages and obtaining the decrypted messages to an unplanned, and incomplete, goal of inference about the method of decryption or about reconstituting any secret parameters [25]. The suggested encryption system is responding to this threat with the help of a rich set of confidential variables, which are p, b, G, s, q, and B.

In the suggested system, every ciphertextplaintext mapping will relate to an alternate setup of such parameters. Occupational with the prime parameter fixed, multiple choices that are valid to a band multiple generator point make the crucial distinction of results on encryption. This parameter diversity makes it impossible to make use of observed ciphertext-plaintext pairs to obtain meaningful insights to an adversary. Consequently, the suggested scheme exhibits a high level of security to the chosen-ciphertext attacks.

4.11 Comparative Evaluation of Cryptanalytic Attack Resistance

In order to offer further assurance to the strengths of the security of the text-encryption strategy proposed, a comparative analysis was conducted on some of the well-known encryption methods reported in [27, 33, 35]. Here critical security considerations are stressed such as the size of the key-space, sensitivity to variations in keys, and the resistance to ciphertext-only attack formulations, to known-plaintext forms of attack. Table 4 displays the comparison findings.

Table 4: Security performance comparison under different cryptographic attack models

Encryption Method	Key-Space Adequacy	Sensitivity to Key Changes	Resistance to Ciphertext-Only Attacks	Protection Against Known-Plaintext Attacks
Proposed Scheme	Satisfactory	Satisfactory	Effective	Effective
Reference [?]	Insufficient	Insufficient	Vulnerable	Vulnerable
Reference [?]	Satisfactory	Satisfactory	Effective	Vulnerable
Reference [?]	Insufficient	Satisfactory	Vulnerable	Vulnerable
Reference [?]	Insufficient	Satisfactory	Vulnerable	Vulnerable
Reference [?]	Insufficient	Insufficient	Vulnerable	Vulnerable

As it can be seen in Table 4 results, the suggested text encryption scheme is much more resistant to cryptographic attacks than compared procedures. Its spacious key space, high level of sensitivity, and resistance to a variety of attack models verify its appropriateness in secure communication of a text in the adversarial setting.

5 Conclusions

This paper proposed a high-performance cryptography design that uses elliptic-curve cryptographic encryption and a Type IVa, max-plus-algebra-based, wavelet transform. The solution suggested is based on a systematized encryption pipeline that consists of three phases. First, plaintext symbols are coded into ASCII numeric forms and a diffusion process occurs and tries to remove explicit statistical dependencies. Afterwards, much nonlinearity and randomness are injected into the intermediate data through the use of elliptic-curve point computation and mapping techniques. During the last phase, we apply a Type IVa max-plus wavelet transform that produces the encrypted output thus strengthening the encryption and diffusion elements.

The robustness and functionality of the proposed framework was tested by conducting a comprehensive assessment. This test undertook correlation measurements, entropy analysis, an evaluation of the quality of encryptions, a key-space sensitivity magnitude and sensitivity analysis, plaintext sensitivity testing, NIST statistical randomness test, and robustness test

against ciphertext-only, known-plaintext, chosen-plaintext, and chosen-ciphertext attack models. Through experiment, it was found out that there was always a correlation between the original messages and those encrypted and the correlation was always within the interval [0.001, 0.08], which was near the theoretically perfect value of zero. Moreover, the code quality measure was between 76 and 90, which was equivalent to good diffusion behavior.

The encrypted results also showed a significantly greater level of entropy than were the respective plaintexts, which validated the high degree of randomness added by the encryption process. Also, the scheme had high sensitivity characteristics in which a significant difference in input data or cryptographic parameter generated completely different ciphertext output. It turned out that the space of keys in general is much bigger than the security threshold of 2100 commonly used and makes exhaustive brute force attacks computationally infeasible.

Both encryption and decryption procedures recorded good execution time in terms of computation power. In the case of 30 to 5,995 message length, it took between 0.0254 s and 0.0472 s to encrypt, between 0.0256 s and 0.3860 s to decrypt. These findings suggest that the suggested scheme has a good balance between the computing power and cryptographic security.

Its extreme similarity with and outward comparison with many modern text-encryption systems [22, 23, 25, 26, 27, 30, 32, 33, 34, 36, 37, 38, 39, 40, 41,42] also served to indicate the strengths of the proposed approach. The framework was always superior by security indicators, and resilience to both advanced cryptanalytic attacks, and overall robustness, without affecting competitive computational performance. Consequently, the suggested encryption algorithm can effectively apply in the area of transmission of secure texts in various fields of application, such as governmental messages and communications, financial, as well as in the personal messaging systems.

Even though the established implementation only works with text only information, the extension to support other types of data like images, audio content and video streams would make an excellent area of future research. Besides, researching on other optimization approaches could also maximize the security and efficiency of the scheme.

To conclude, the results of this paper confirm that the suggested method of text-encryption, which is an elliptic curve illuminated by max-plus transform of the wavelet, is an effective and strong means to achieve safe communication. The proposed future research will be aimed at expanding the framework applicability to heterogeneous data types and examining advanced optimization methods that would further strengthen the cryptographic work of the

given framework.

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. [Google Scholar] [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. [Google Scholar] [CrossRef]

[3] Elkandoz, M.T.; Alexan, W. Image Encryption Based on a Combination of Multiple Chaotic Maps. *Multimed. Tools Appl.* **2022**, *81*, 25497–25518. [Google Scholar] [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. [Google Scholar] [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**. [Google Scholar] [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. [Google Scholar] [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. [Google Scholar] [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. [Google Scholar] [CrossRef]

[9] Liu, J.; Zhou, J. *Cryptography and Network Security: Principles and Practice*; Pearson Education: London, UK, 2017. [Google Scholar]

[10] Bodkhe, D.; Panchal, S. Use of Sumudu Transform in Cryptography. *Bull. Marathwada Math. Soc.* **2015**, *16*, 1–6. [Google Scholar]

[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. [Google Scholar] [CrossRef]

[12] Kharde, U.D. An Application of the Elzaki Transform in Cryptography. *J. Adv. Res. Appl. Sci.* **2017**, *4*, 86–89. [Google Scholar]

[13] Kumar, P.S.; Vasuki, S. An Application of MAHGOUB Transform in Cryptography. *Adv. Theor. Appl. Math.* **2018**, *13*, 91–99. [Google Scholar]

[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. [Google Scholar] [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. [Google Scholar] [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. [Google Scholar]

[17] Mansour, E.A.; Kuffi, E.A.; Mehdi, S.A. Applying Complex SEE Transformation in Cryptography. *MJPS* **2021**, *8*. [Google Scholar] [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. [Google Scholar] [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. [Google Scholar]

[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. [Google Scholar]

[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. [Google Scholar]

[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. [Google Scholar] [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. [Google Scholar]

[25] Qu, M. *Sec 2: Recommended Elliptic Curve Domain Parameters*; Tech. Rep. SEC2-Ver-0.6; Certicom Res.: Mississauga, ON, Canada, 1999. [Google Scholar]

[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. [Google Scholar] [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. [Google Scholar] [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. [Google Scholar] [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. [Google Scholar] [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. [Google Scholar] [CrossRef]

[31] Azam, N.A.; Zhu, J.; Hayat, U.; Shurbevski, A. Towards Provably Secure Asymmetric Image Encryption Schemes. *Inf. Sci.* **2023**, *631*, 164–184. [Google Scholar] [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. [Google Scholar] [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. [Google Scholar]

[CrossRef]

[34] Washington, L.C. *Elliptic Curves: Number Theory and Cryptography*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2008. [Google Scholar]

[35] Silverman, J.H. *The Arithmetic of Elliptic Curves*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 106. [Google Scholar]

[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. [Google Scholar]

[37] Lauter, K. The Advantages of Elliptic Curve Cryptography for Wireless Security. *IEEE Wirel. Commun.* **2004**, *11*, 62–67. [Google Scholar] [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. [Google Scholar] [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. [Google Scholar]

[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. [Google Scholar] [CrossRef]

[41] Singh, L.D.; Singh, K.M. Implementation of Text Encryption using Elliptic Curve Cryptography. *Procedia Comput. Sci.* **2015**, *54*, 73–82. [Google Scholar] [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. [Google Scholar]

[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. [Google Scholar]

[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. [Google Scholar] [CrossRef]

[45] Arul, J.; Venkatesulu, M. Encryption Quality and Performance Analysis of GKSBC Algorithm. *J. Inf. Eng. Appl.* **2012**, *2*, 26–34. [Google Scholar]

[46] Shannon, C.E. A Mathematical Theory of Communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [Google Scholar] [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. [Google Scholar]

[48] Mishra, M.; Mankar, V.H. Hybrid Message-Embedded Cipher using Logistic Map. *arXiv* **2012**, arXiv:1209.2582. [Google Scholar] [CrossRef]

[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. [Google Scholar] [CrossRef]

[50] Biryukov, A. *Encyclopedia of Cryptography and Security*; Springer: Berlin/Heidelberg, Germany, 2011. [Google Scholar]