Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print) 2521-3520 (electronic)

ORIGINAL ARTICLE *OPEN ACCESS*

Dynamics Data Encryption Based on Chaotic Functions and Elliptic Curves: Application to Text Data

Joel Kinganga [a], Nathanael Kasoro [a], and Alain Musesa [a]

[a] *Department of Mathematics, Statistics and Computer Science, Faculty of Science, University of Kinshasa, Kinshasa, Democratic Republic of the Congo*

CORRESPONDANCE
Joel Kinganga
joel.kinganga@unikin.ac.cd

ARTICLE INFO
Received: October 20, 2024
Revised: February 19, 2025
Accepted: March 01, 2025
Published: March 30, 2025

ABSTRACT: ***Background:*** *Given the vast amount of data generated daily on the Internet, numerous cryptosystems have been developed to ensure data confidentiality using symmetric, asymmetric, or hybrid encryption techniques. However, many of these systems suffer from limitations such as slow execution times and large key sizes.* ***Objective:*** *This paper presents a novel cryptosystem for text data encryption that integrates elliptic curve cryptography with chaotic functions to enhance data confidentiality and security.* ***Methods:*** *The proposed system utilizes elliptic curve points and pseudo-random numbers generated from a hybrid chaotic map (a fusion of the logistic map, sine map, and piecewise linear chaotic map) to derive short key sizes. Various analyses, including frequency histograms, correlation coefficients, and key sensitivity tests, are conducted to demonstrate the system's robustness and reliability.* ***Results:*** *The analyses confirm that the fusion of chaotic functions makes the system highly sensitive to initial conditions, thus providing strong protection against unauthorized access.* ***Conclusions:*** *By integrating elliptic curve cryptography with chaotic functions, the proposed cryptosystem effectively addresses the limitations of existing systems, offering enhanced data confidentiality and security through the use of short key sizes and strong sensitivity to initial conditions.*

KEYWORDS: *Elliptic curve cryptography; Chaotic functions; Data encryption; Hybrid cryptosystems; Key sensitivity analysis*

INTRODUCTION

The field of data security, particularly cryptography, has become increasingly important in recent decades due to the rapid growth of information technologies and the expanding number of networked users. Cryptography, originally developed to ensure the confidentiality of messaging and data, is now essential for protecting sensitive information in computer applications. Its primary purpose is to allow two parties to exchange information securely over an unsecured channel, ensuring that any third party intercepting the data cannot decipher it.

Information is encrypted and decrypted using sophisticated algorithms, as demonstrated in [1] and [2], where hybrid encryption methods combining symmetric and asymmetric techniques are employed to secure data. Recent research has made significant advancements in encryption technologies. Studies such as [3]–[7] focus on protecting images using asymmetric encryption methods to prevent unauthorized access. In [8], data security is enhanced through the use of fractal structures, where a fusion of Phoenix and Landa fractals, termed PLFF, is employed to encrypt images. The encryption keys are generated using a pseudo-random number sequence (PRN). Additional cryptographic systems incorporating both symmetric and asymmetric techniques have been proposed in [9]–[11], highlighting new methods for securing text data. Simple encryption systems, such as those in [12], utilize permutation matrices and XOR operations with symmetric keys to encrypt texts, allowing for flexible key sizes. In [13], a novel encryption system is introduced that leverages Fermat's theorem and dynamic keys, resulting in ciphered texts that differ in size from the original. Further innovations include the algorithm in [14], which employs two Clifford attractors to enhance text security during

transmission, offering new features for online text exchange. Due to its efficient key length, elliptic curve cryptography was selected in [15] to reduce the computational burden associated with other encryption methods while resisting modern cryptographic attacks.

This paper proposes an asymmetric cryptographic system for text data encryption, integrating chaotic sequences with elliptic curves. The system fuses three chaotic maps to generate pseudo-random numbers, creating confusion during data encryption, as outlined in [7], [16]. These chaotic maps also generate coefficients for the elliptic curve equation, while private keys are derived using the discrete logarithm principle.

The paper is structured as follows: the introduction provides context for the study, followed by a section on tools and methods used. The third section details the proposed algorithm, while the final section presents the results and discussions, concluding with insights into the system's performance and robustness.

MATERIALS AND METHODS

Our proposed cryptosystem integrates elliptic curve cryptography (ECC) with chaotic functions to create a hybrid encryption system. The elliptic curves provide a secure asymmetric framework based on the discrete logarithm problem, while chaotic functions introduce randomness and sensitivity to initial conditions, enhancing security. The chaotic map used in our system is a fusion of the logistic map, sine map, and piecewise linear chaotic map, generating pseudo-random numbers for key generation and encryption processes.

The practical implementation of a data encryption system requires the use of a number of tools. The proposed algorithm was implemented using Python, which facilitated the generation of diagrams and analysis. The following subsections describe the chaotic functions and elliptic curves employed in our system.

Chaotic Functions

A system is said to be chaotic when it is deterministic, unpredictable, and non-linear. Determinism and unpredictability are linked to sensitivity to initial conditions. Two closely related initial conditions can lead to vastly different outcomes, highlighting the inherent unpredictability of chaotic systems. These systems are highly applicable in cryptography due to their complexity and unpredictability. Chaotic systems, while deterministic, produce outputs that are extremely difficult to predict without precise knowledge of the initial conditions. Additionally, chaotic systems exhibit strange attractors, which generate both continuous and discrete chaotic signals. In our work, we focus on the discrete signals for encryption purposes.

The Logistics Card

In cryptographic applications, the most widely used card is the logistic card. Its equation is given in Equation 1. It generates non-uniform sequences in the histogram.

$$X_{n+1} = rX_n(1 - X_n) \tag{1}$$

In this function, as explained in [17], [18], r is a positive number in the range 1 to 4. The quantity X_n is between 0 and 1. Chaotic behavior occurs at r values of 3.6 and above. In Figure 1, we find the bifurcation diagram of the quantity X_n as a function of r.

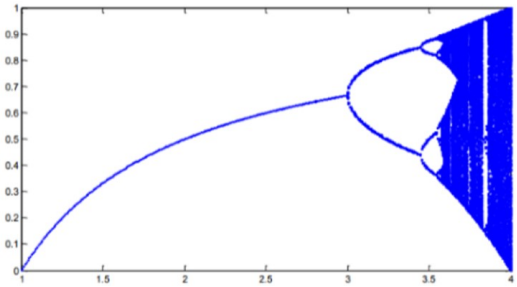

Figure 1. Logistic map bifurcation diagram

This sequence is much more popular due to its simple representation, efficient implementation, and good dynamic behavior. As in [19], its equation can be described by Equations 2 and 3.

$$X_n = r\frac{X_n}{2} \rightarrow if, X_n \leq 0.5 \tag{2}$$

$$X_n = r\frac{1 - X_n}{2} \rightarrow if, X_n \geq 0.5 \tag{3}$$

where: $X_n \in (0, 1)$ with $n \in N, X_0$ initial. The control parameter r takes values in the range $(0, 0.5)$. The piecewise linear chaotic sequence has good confusion as explained in [20], and can generate a good random sequence required by cryptographic systems.

The Sine Map

Equation 4 is the equation of the sine map.

$$X_{n+1} = Y \sin(\pi X_n) \tag{4}$$

As mentioned in [21], chaotic behavior is manifested directly with $Y = 1$. This manifestation is similar to the Logistic function. In the vicinity of $x = 0.5$, the sine map is quadratic and identical to the logistic recurrence. Its evolution towards chaos and its probabilistic distribution by period doubling is almost identical. As explained in [22], the sine map differs somewhat from the logistic map in that the periodic windows are wider than those of the logistic map, and once the period is doubled, the bifurcations appear earlier.

Elliptic Curves

Koblitz and Miller were the first to apply elliptic curves in cryptography. This method relies on the difficulty of solving the discrete logarithm problem within the group of points on an elliptic curve. By definition, as noted in [23]–[26], an elliptic curve E over a field K is the set of projective points satisfying the Weierstrass Equation 5

$$E = y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{5}$$

In [27], we read that if we make the change of variables $y = X/Z$ and $y = Y/Z$ to have a homogeneous equation, the elliptic curve will be considered as the set of affine points satisfying the Weierstrass equation. Equation 6 is the form of the Weiestrass equation.

$$E = y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{6}$$

An elliptic curve is represented by $E_p(a, b)$, with a and b cornered $mod\ p$ and p is a prime number. The Elliptic curve E used for cryptography, in Weierstrass form over a prime field F_p, is as follows: $E : y^2 = x^3 + ax + b\ mod\ p.a$, b $F_p = 2, 3$. One condition must be satisfied for this curve. It is that of $4\alpha^3 + 27b^2 \neq 0$. If this condition is satisfied, then the elliptic curve will be called a non-singular elliptic curve and will have a total of 3 distinct curve roots suitable for ECC. The elliptic group coming from the curve $E_p(a, b)$ will be composed of all points (x, y) that will satisfy the curve E, including a point O called the point at infinity.

A few arithmetic operations on an elliptic curve have made curves more efficient in cryptography. These operations are performed on two different points on the curve, or even on a single point on the curve, and generate a new point on the curve.

Adding Points

Adding two points on the elliptic curve gives a new point on the curve. Let there be two points P and Q. Two points on the curve, adding these two points on the curve, we find the point R. [14] Schematically, when adding two points, we draw a straight-line joining points P and Q and extend the line to another point that touches the curve called R. This addition of points on the elliptic curve is defined as follows:

$$P + Q = R \tag{7}$$

Let $P(x_p, y_p)$ and $Q(x_q, y_q)$ be two points on the curve, their sum gives $R(x_r, y_r)$.

The coordinates of point R are given by:

$$x_r = \lambda^2 - x_p - s_q \tag{8}$$

$$y_r = \lambda(x_p - x_r) - y_p \tag{9}$$

With

$$\lambda = \frac{(y_q - y_p)}{(x_q - x_p)}, if P \neq Q \tag{10}$$

Point Doubling

The doubling of points is nothing more than an addition of the points of the curve, if P and R two points of the curve, point to the same point on the curve, then the slope of the curve λ is calculated as shown in this section. [15] In general, the doubling point of the function λ of the elliptic curve is defined as follows:

$$R = 2P = P + P = (x_3, y_3) \tag{11}$$

$$\lambda = \frac{3x_1^2 + a}{2y_2} \tag{12}$$

$$x_3 \equiv (\lambda^2 - 2x_1)(\mathrm{mod}\, p) \tag{13}$$

$$y_3 \equiv (\lambda x_1 - \lambda x_3 - y_1)(\mathrm{mod}\, p) \tag{14}$$

Point Multiplication

On an elliptic curve, only scalar multiplication is possible on points. It's the same as point addition, perhaps a doubling of points, for n times, it's applied, and calculated nP where the positive scalar value is n.

$$R = nP = (P + P + P + ... + P)n\text{times} \tag{15}$$

On an elliptic curve, the operation that naturally applies is modular arithmetic. This operation guarantees that calculation on the curve is possible. To move elliptic curves from the real numbers to the finite field, mathematical calculations directly require modulo p, where p is a prime number.

Encryption / Decryption with Elliptic Curves

To encrypt a message, 2 people must first transform the message into a point Pm belonging to the elliptic curve E. Each character in the message will be converted into an ASCII hexadecimal code, for example. The encryption function is given by Equations 16 and 17:

$$E_k = E(F_p) \rightarrow E(F_p) \tag{16}$$

$$P \rightarrow E_k(P) = P + K \tag{17}$$

the decryption function will be denoted by:

$$D_k : E(F_p) \rightarrow E(F_p) \tag{18}$$

$$c \rightarrow D_k(c) = P = c - k \tag{19}$$

Proposed System

1 Proposed Chaotic Map

Chaotic maps differ significantly from conventional random number generators. While traditional generators produce sequences that cannot be reproduced once generated, chaotic systems can regenerate the same sequence if the same function and initial conditions are applied. In our proposed system, we have merged three chaotic functions: the logistic function, the sine function, and the piecewise linear chaotic function. This fusion enhances the complexity and unpredictability of the generated sequences, making them highly suitable for cryptographic applications. Figure 2 illustrates

the chaotic behavior resulting from the merger of these functions, including some generated values and the corresponding bifurcation diagram.

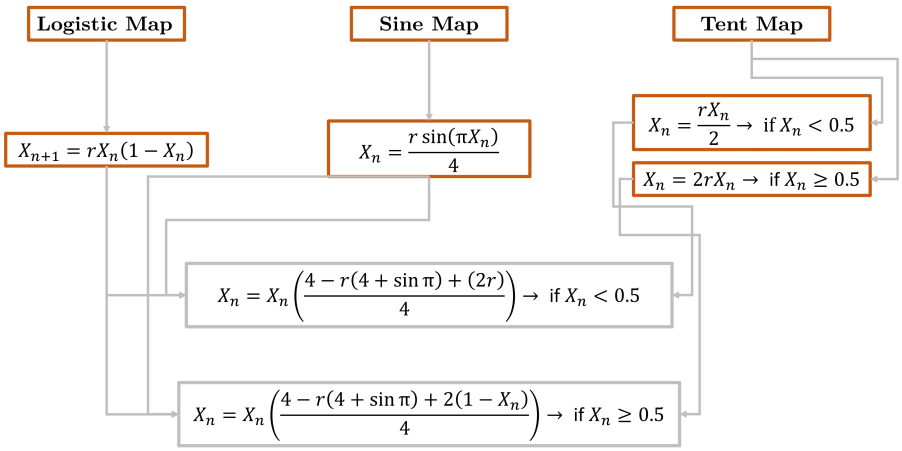

Figure 2. Merging three chaotic functions

The following data displays the data obtained after executing the fusion of our 3 proposed chaotic functions.

$$[0.5, 5.001592652916487, 9.507168206395846, 18.521907222377415,$$
$$36.558563929533136, 72.64624041079874, 144.85033094492852,$$
$$289.3160100408738, 578.3624100753365, 1156.6853854402693,$$
$$2313.791870056828, 4628.926273798651, 1.0345500893763292e + 16,$$
$$2.0699240183612068e + 16, 4.141496371984788e + 16, 8.286290727107306e + 16,$$
$$1.6579180046761302e + 17, 3.3171562533249824e + 17, 6.636954045940614e + 17,$$
$$1.3279193273990157e + 18, 2.6568961120928517e + 18, 5.315907980856567e + 18,$$
$$1.0636049159887876e + 19, ...]$$

Figure 3 shows the fork diagram of the logistical sinusoidal tent.

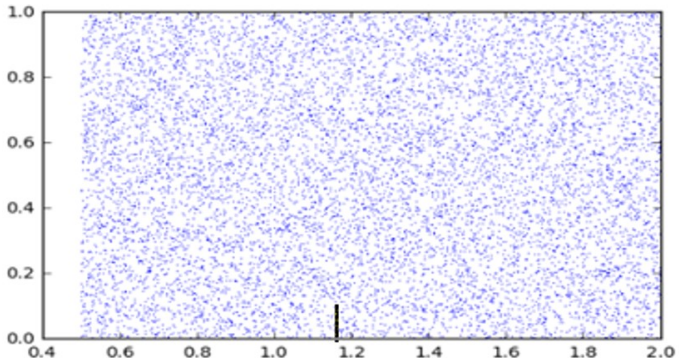

Figure 3. Logistic Sine Tent fork diagram

2 Proposed Algorithm

Step 1: Choose an equation of the form $y^2 = x^3 + ax + b$, and check whether this is a Weiestrass equation, then use the chaotic sequence to randomly generate the coefficients a and b of the curve.

Step 2: Choose a prime number P from the chaotic sequence.
Step 3: Generate the points of the curve and choose a group generator.
Step 4: For each character to be enciphered, find its hexadecimal ASCII, then find its decimal equivalent, separating it by a comma in the middle.
Step 5: Use the chaotic sequence to generate 2 keys for the sender and receiver. To create confusion, generate a number of dots identical to the size of the message to be encrypted. The values generated must be integers and reduced modulo P. These values must be multiplied by the point generator.
Step 6: Use the chaotic sequence to randomly generate a list of values corresponding to the number of characters to be encrypted.
Step 7: Make these values Integers, reduce them modulo P, multiply them with the point generator, and add them to the key found.
Step 8: Concatenate the two points, the point found by converting the character to be enciphered and the point found by the chaotic sequence for confusion. $P1$ and $P2$.
Step 9: Encrypt the two points from step 7 using the key found in step 5 and send it to the recipient.
Step 10: On reception, the receiver receives 3 points on the curve, 2 of which are for the encrypted message and one for the confusion. The sender and receiver must agree on the position of 2 of the 3 points that will constitute the encrypted message.

RESULTS AND DISCUSSION

Histogram Analysis

Figures 4 and 5 illustrate the frequency distribution of characters in the original text compared to the encrypted text using both the elliptic curve and RSA encryption systems. The analysis highlights significant alterations in the frequency patterns, demonstrating the effectiveness of our proposed cryptographic method in disrupting recognizable text structures.

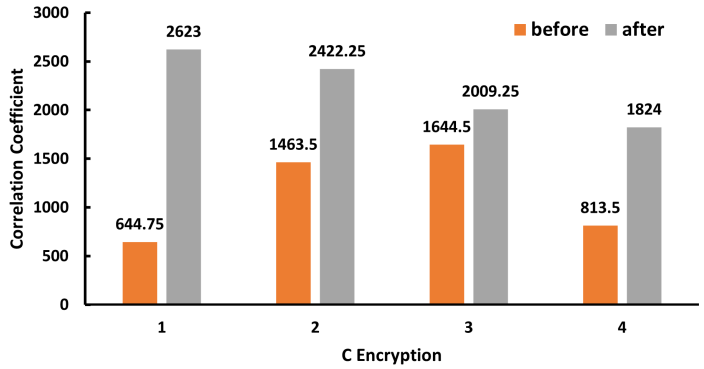

Figure 4. Original text and cipher text graph

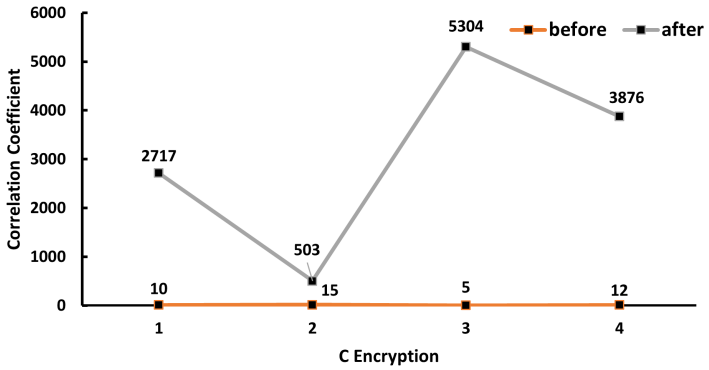

Figure 5. Graph of original text and cipher text

Using histogram analysis, a visual inspection reveals clear differences in the frequency patterns between the original text and the encrypted texts produced by the RSA and ECC cryptosystems. As

shown in Figure 6, the histogram of text encrypted with RSA, as studied in [1], differs significantly from the histogram of the same text encrypted with ECC, demonstrating the distinct behaviors of these cryptographic approaches.

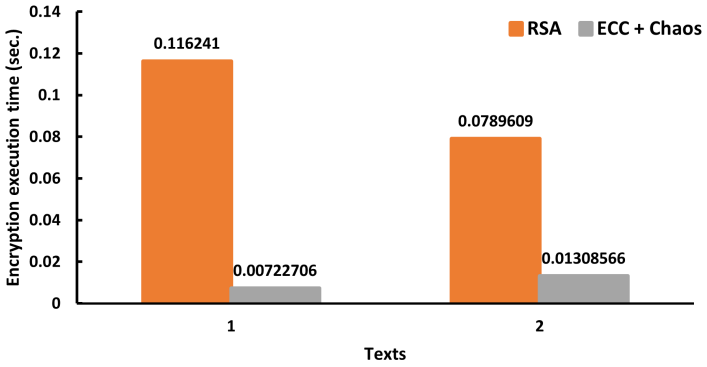

Figure 6. Cipher text graph

Correlation Analysis

Correlation analysis is a statistical method for measuring the strength of the linear relationship between two variables. It helps identify links, trends, and patterns between datasets. The correlation coefficient, a value ranging from -1 to 1, indicates the intensity and direction of this relationship. A coefficient closer to 1 or -1 signifies a stronger, more linear relationship, while a value near 0 indicates a weaker, non-linear relationship. The Pearson correlation formula, as shown in Equation 7, is used to calculate this coefficient [28].

$$r = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - x)^2}\sqrt{\sum_{i=1}^{n}(y_i - y)^2}} \tag{20}$$

The application of this formula is shown in Tables 1, 2, and 3 with ECC and RSA. Where r is Pearson's correlation coefficient, n is the number of observations, x_i and y_{i} are the values of the two variables for the i-th observation, $\bar{x}$ and $\bar{y}$ are the means of the two variables.

Table 1. Calculating the correlation coefficient of a text before and after Encryption with ECC

X before encryption	x after encryption	y before encryption	y after encryption	C before encryption	C after encryption	Xi-average X	Yi-average Y	(Xi-average X)(Yi-average y)	(Xi-average X)(Xi-average X)	(Yi-average Y)(XY-average y)
501.5	1926	788	3321	644.75	2623	-496.813	403.375	-200401.7	246822.7	162711.4
1170	1258	1758	3587	1463.5	2422.25	321.9375	202.625	65232.586	103643.8	41056.89
1893	1734	1396	2285	1644.5	2009.25	502.9375	-210.38	-105805.5	252946.1	44257.64
690.5	1737	936.5	1912	813.5	1824	-328.063	-395.63	129789.73	107625	156519.1
Average x and y				1141.56	2219.63			-111184.9	711037.5	404545.1
							Racine		843.2304	636.0386
							Coeff R		-83865.44	

Table 2. Calculating the correlation coefficient of a text before and after encryption with RSA

C before encryption	C after encryption	Xi-average X	Yi-average Y	(Xi-average X) (Xi-average y)	(Xi-average X) (Xi-average X)	(Yi-average Y) (Yi-average y)
10	2717	-0.5	-383	191.5	0.25	146689
15	503	4.5	-2597	-11686.5	20.25	6744409
5	5304	-5.5	2204	-12122	30.25	4857616
12	3876	1.5	776	1164	2.25	602176
10.5	3100			-22453	53	12350890
			Racine		7.280109889	3514.383
			Coeff R		-10838908.96	

Table 3. Calculating the correlation coefficient of a cipher text with RSA and ECC

Cipher ECC	Ciphert RSA	Xi-average X	Yi-average Y	(Xi-average X) (Xi-average y)	(Xi-average X) (Xi-average X)	(Yi-average Y) (Yi-average y)
2623	2717	403.5	-383	-154541	162812.25	146689
2422	503	202.5	-2597	-525893	41006.25	6744409
2009	5304	-211	2204	-463942	44310.25	4857616
1824	3876	-396	776	-306908	156420.25	602176
2220	3100			-1451283	404549	12350890
			Racine		636.0416653	3514.383
			Coeff R		-8018916.089	

The correlation analysis between texts before and after encryption, as shown in Tables 1, 2 and 3, indicates no discernible relationship when using either the RSA or ECC cryptographic systems. Furthermore, for the same text encrypted with RSA and ECC, there is no significant correlation between the resulting encrypted outputs, underscoring the distinct encryption behaviors of the two systems.

Cipher Time Analysis

Cipher time refers to the duration required to transform plain text into cipher text. This process involves the application of an encryption key and method. As detailed in [29] and illustrated in Table 4, cipher time is influenced by multiple factors, including processor speed, algorithm complexity, programming language efficiency, and the length of the text being encrypted. Our analysis demonstrates that the proposed system exhibits superior performance, with faster encryption times compared to RSA, highlighting its efficiency.

Table 4. Execution time of each algorithm for each text

Texts	Number of characters	Encryption execution time	
		RSA	ECC + Chaos
JOEL	4 Caract	0.116241	0.00722706
UNIKIN	6 Caract	0.0789609	0.01308566

The execution time of each algorithm varies depending on the text. The elliptic curve combined with chaotic sequences requires significantly less execution time, recording 0.00722706 seconds for ECC and chaos, compared to 0.116241 seconds for the RSA algorithm. For other texts, as detailed in the accompanying table, similar trends are observed. Figure 7 graphically illustrates the execution time before and after encryption, highlighting the efficiency of our proposed method.

Sensitivity to Changing Initial Conditions

A robust cryptosystem must exhibit sensitivity to initial conditions, a critical feature for ensuring data security against attacks. To evaluate the system's performance, we encrypted text using varying initial conditions. Tables 4 and 5 present the execution times of each algorithm before and after modifying initial conditions, along with key sensitivity analyses.

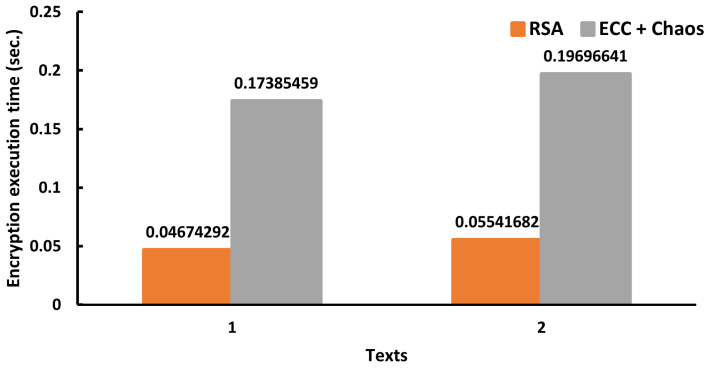

Figure 7. Run time before and after encryption Graph

Table 5. Execution time of each algorithm before modification of initial conditions

Texts	Number of characters	Encryption execution time	
		RSA	ECC + Chaos
JOEL	4 Caract	0.116241	0.00722706
UNIKIN	6 Caract	0.0789609	0.01308566

Key Sensitivity Analysis

For the initial condition, we changed the keys using the proposed chaotic sequence. The results are shown in Table 6.

Table 6. Execution time of each algorithm after changing the initial conditions

Texts	Number of characters	Second	
		RSA	ECC + Chaos
JOEL	4 Caract	0.04674292	0.17385459
UNIKIN	6 Caract	0.05541682	0.19696641

Similar to simple text encryption times, the execution times for the elliptic curve and chaotic sequence encryption remain consistently lower than those for RSA, both before and after modifying

initial conditions. This consistency underscores the reliability of our proposed system. The system's sensitivity to initial conditions is evident-altering parameters such as the encryption key results in changes in execution time and output. Figure 8 illustrates the variations in execution time when initial parameters are modified, demonstrating the system's adaptability and robustness.

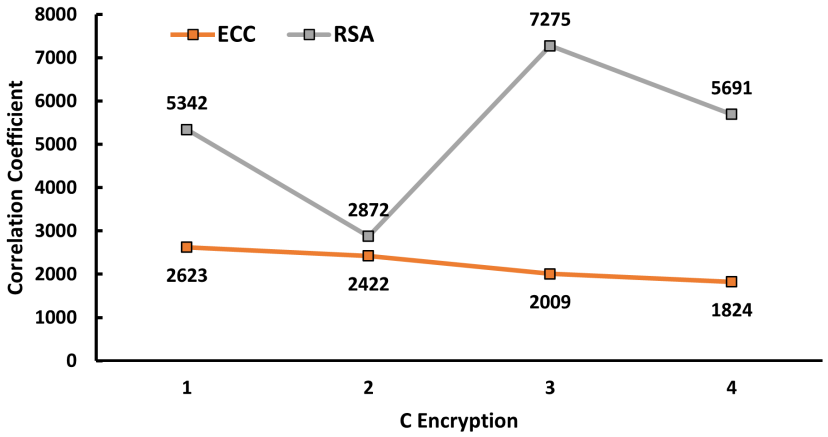

Figure 8. Run time graph

A comparative study was carried out to prove the effectiveness of our proposed algorithm and the algorithm proposed by other authors such as Ziadoon W. Salman, Hind Ibrahim Mohammed *et. al.*, in [12], entitled "SMS Security by Elliptic Curve and Chaotic Encryption Algorithms". Table 7 explains the difference between the two proposed algorithms.

Table 7. Comparative table of two algorithms

	Algorithm 1 (Our Algorithm)	**Algorithm 2 (Algorithm proposed by [16])**
Key length	The short keys generated by the elliptic curve of the form: $E = y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$	The short keys generated by the elliptic curve of the form: $E = y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
Run time	Our algorithm takes less time, as a multiplication operation of the curve points is used. $E = y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ $Key_1 = N_1 * (N_2 * G(x, y))$ $Key_2 = N_2 * (N_1 * G(x, y))$ $Key_1 = Key_2$	The algorithm proposed in [16] is slow because it uses two operators, addition and multiplication, to find the public or private keys. $A_1 = A^*(C + A)$ $A_2 = a^*A$ $B_1 = B^*(C + B)$ $B_2 = (b^*B)$
Key exchange	Our algorithm does not propose any key exchange between the sender and the receiver.	[16] proposed a key exchange, which is remarkable in steps 10 to 12 of Algorithm 2 and steps 2 and 3 of Algorithm 1.

After studying and comparing the two algorithms, we have concluded that although both employ elliptic curve–based encryption with short key sizes, our proposed algorithm is more efficient. Its efficiency stems largely from its foundation on the discrete logarithm problem on elliptic curves. Regarding execution time, our algorithm is faster because it only requires a multiplication operator to compute the private or public keys for encryption, as shown in Table 7. In contrast, [16] use both addition and multiplication, which causes their procedure to take longer than expected. Moreover, our algorithm does not involve key exchange; instead, the sender and receiver independently generate their keys after agreeing in advance on the curve equation and the generator of the curve points. On the other hand, the algorithm proposed in [16] involves key exchange between the sender and receiver, as illustrated in Algorithm 2, steps 2 and 3.

In this study, we used data encryption based on the Elliptic curve. At the end of our study, a comparative study with the RSA cryptographic system was carried out, as shown in the example.

Table 8. Text encryption table with ECC and Chaos

	J	**O**	**E**	**L**
$PU_{R1} = dU_{R1} * G(x_g, y_g)$	(490,204)	(490,204)	(490,204)	(490,204)
$PU_{R2} = dU_{R2} * G(x_g, y_g)$	(513,1372)	(1849,2511)	(3296,2595)	(891,1669)
$C_1 = PU_{R1} + K^*G(x_g, y_g)$	(8,3641)	(8,3641)	(8,3641)	(8,3641)
$C_2 = PU_{R2} + K^*G(x_g, y_g)$	(3843,3000)	(2507,3533)	(3460,928)	(3465,3459)
$C_3 = PU_{\nu 1} + K^*G(x_g, y_g)$	(3460,928)	(190,1)	(1672,729)	(3109,3014)
Points sent per character	(8,3641), (3843,3000), (3460,928)	(8,3641), (2507,3533), (190,1)	(8,3641), (3460,928), (1672,729)	(8,3641), (3465,3459), (3109,3014)

We want to experiment with our proposed system by encrypting the name JOEL. To do this, we use the equation of the curve, the equation of the curve of the form $y^2 = x^3 + 324x + 1287$, and a finite field F_{3851}. The prime number chosen is P=3851. The sender and receiver have each chosen the key using the proposed chaotic function, 1194 and 1759. This curve generates a total of 3927 points, and we have chosen the point (920, 2170) as the generator. The two people agreed on the point (3347, 1242) as the encryption key. To create confusion with the encrypted characters, we generated 4 random values (5, 50, 95, 185) using our chaotic sequence. After multiplying these values with the point generator and adding them to the key, we found the following points: [(3460, 928); (190, 1); (1672, 729); (3109, 3014)]. Table 8 shows the points found for each character of the cipher word. For the word JOEL, as a whole, the following points are sent: [(8,3641); (3843,3000); (3460,928); (8,3641); (2507,3533); (190,1); (8,3641); (3460,928); (1672,729); (8,3641); (3465,3459); (3109,3014)]. Character J is enciphered by the points [(8, 3641); (3843,3000); (3460,928)], and so on. We can see that for each encrypted character, 3 dots are sent to the sender. Of these 3 dots, one is considered confusion. The sender and receiver must agree on the position of the confusion point to be removed, which can be at the beginning, middle, or end of the set of points sent for each character.

Vulnerabilities and Limitations of the Proposed Method

Cryptography based on elliptic curves is a highly complex system that has been used by many researchers over the last few years, as it provides short key sizes that ensure good security. These systems are not vulnerable to attack. Our proposed cryptosystem is not vulnerable to attack as it is the fusion of elliptic curves and chaotic functions that make it more complex. Our proposed cryptosystem also has limitations in that it can only encrypt text data, not images or videos. And it's slow in terms of execution

Security Analysis

With cryptos stems bases on elliptic curves, chosen text attacks, known text attacks, are practically impossible because first the sender and receiver must agree on the equation of the curve E, to be used which must be of the form $y^2 = x^3 + ax + b$ on a finite field F_p. Also, a generator of the points of the curve $G(x, y)$. The sender and receiver must each choose a number less than P to make the private key with the generator of the points.

CONCLUSION

In this article, we have proposed a new text encryption method based on chaotic functions and elliptic curve cryptography. By merging three chaotic functions-the logistic function, the sine function, and the piecewise linear chaotic function-and integrating them with elliptic curves, we have developed a hybrid system capable of generating large random values for encryption and decryption keys. These chaotic functions also produce random coefficients for elliptic curve equations and generate confusion points to enhance security. The comprehensive analyses presented in this paper demonstrate the robustness of our proposed system. The fusion of chaotic functions makes the system highly sensitive to initial conditions, enhancing its resistance to cryptographic attacks. In future work, we plan to extend our algorithm to encrypt black-and-white and color images, further validating its versatility and robustness.

SUPPLEMENTARY MATERIAL

None.

AUTHOR CONTRIBUTIONS

Joel Kinganga: Design and methodology; Nathanael Kasoro: Research and data collection; Alain Musesa: Writing, reviewing, and editing.

FUNDING

None.

DATA AVAILABILITY STATEMENT

Data is available in the article.

ACKNOWLEDGMENTS

We are very grateful to mathematics and cryptography in the department of mathematics and computer science at the University of Kinshasa.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

REFERENCES

[1] J. Kinganga, N. Kasoro, R. Mabela, K. Kyamakya, and E. K. Kazadi, "HRS-3K: A hybrid encryption system based on matrix computation and RSA with disordered alphabet in $\mathbb{Z}/44\mathbb{Z}$," in *2021 International Conference on Cyber Security and Internet of Things (ICSIoT)*, IEEE, Dec. 2021, pp. 15–21. doi: 10.1109/icsiot55070.2021.00012.

[2] P. Kuppuswamy, S. Q. Y. A. K. Al-Maliki, R. John, M. Haseebuddin, and A. A. S. Meeran, "A hybrid encryption system for communication and financial transactions using RSA and a novel symmetric key algorithm," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 1148–1158, 2023. doi: 10.11591/eei.v12i2.4967.

[3] I. Khalid, T. Shah, S. M. Eldin, D. Shah, M. Asif, and I. Saddique, "An integrated image encryption scheme based on elliptic curve," *IEEE Access*, vol. 11, pp. 5483–5501, Dec. 2023. doi: 10.1109/access.2022.3230096.

[4] N.-R. Zhou, L.-L. Hu, Z.-W. Huang, M.-M. Wang, and G.-S. Luo, "Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm," *Expert Systems with Applications*, vol. 238, p. 122 052, Mar. 2024. doi: 10.1016/j.eswa.2023.122052.

[5] X. Zhang and J. Tian, "Multiple-image encryption algorithm based on genetic central dogma," *Physica Scripta*, vol. 97, no. 5, p. 055 213, 2022. doi: 10.1088/1402-4896/ac66a1.

[6] M. Habek, Y. Genc, N. Aytas, A. Akkoc, E. Afacan, and E. Yazgan, "Digital image encryption using elliptic curve cryptography: A review," in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, IEEE, Jun. 2022, pp. 1–8. doi: 10.1109/hora55278.2022.9800074.

[7] D. S. Laiphrakpam, R. Thingbaijam, K. M. Singh, and M. Al Awida, "Encrypting multiple images with an enhanced chaotic map," *IEEE Access*, vol. 10, pp. 87 844–87 859, Aug. 2022. doi: 10.1109/access.2022.3199738.

[8] M. Ahmad, S. Agarwal, A. Alkhayyat, A. Alhudhaif, F. Alenezi, A. H. Zahid, and N. O. Aljehane, "An image encryption algorithm based on new generalized fusion fractal structure," *Information Sciences*, vol. 592, pp. 1–20, May 2022. doi: 10.1016/j.ins.2022.01.042.

[9] S. Patel, B. K. P, and R. K. M, "Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique," *Multimedia Tools and Applications*, vol. 79, no. 43–44, pp. 31 739–31 757, 2020. doi: 10.1007/s11042-020-09551-9.

[10] S. R. M. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, pp. 774–781, 2020. doi: 10.11591/ijeecs.v18.i2.pp774-781.

[11] S. N. F. M. A. Antony and M. F. A. Bahari, "Implementation of elliptic curves in the polynomial blom key pre-distribution scheme for wireless sensor networks and distributed ledger technology," *Journal of Sensor and Actuator Networks*, vol. 12, no. 1, p. 15, 2023. doi: 10.3390/jsan12010015.

[12] M. Deshmukh and A. S. Rawat, "Lightweight symmetric key encryption for text using XOR operation and permutation matrix," *International Journal of Information Technology*, vol. 15, no. 7, pp. 3555–3562, 2023. doi: 10.1007/s41870-023-01407-3.

[13] M. R. Kumar, R. Mani, P. Revathi, S. Sabarinathan, and V. Govindan, "A robust and fast symmetric text encryption algorithm based on Fermat's two squares theorem," in *2023 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI)*, IEEE, Apr. 2023, pp. 1–5. doi: 10.1109/raeeucci57140.2023.10134472.

[14] T. Ivanova, B. Stoyanov, and D. Dobrev, "Secure text encryption based on Clifford attractors," in *2023 31st National Conference with International Participation (TELECOM)*, IEEE, Nov. 2023, pp. 1–4. doi: 10.1109/telecom59629.2023.10409685.

[15] Z. Abukari, E. Y. Baagyere, and M. M. Iddrisu, "A new text encryption scheme suitable for combating sniffing attacks in IoT applications via non-supersingular elliptic curves over binary extension fields," *Earthline Journal of Mathematical Sciences*, vol. 13, no. 2, pp. 451–472, 2023. doi: 10.34198/ejms.13223.451472.

[16] Z. W. Salman, H. I. Mohammed, and A. M. Enad, "SMS security by elliptic curve and chaotic encryption algorithms," *Al-Mustansiriyah Journal of Science*, vol. 34, no. 3, pp. 56–63, 2023. doi: 10.23851/mjs.v34i3.1318.

[17] A. Abdelli, W. El Hadj Youssef, L. Khriji, and M. Machhout, "Enhanced lightweight encryption algorithm based on chaotic systems," *Physica Scripta*, vol. 99, no. 10, p. 106 006, 2024. doi: 10.1088/1402-4896/ad75c5.

[18] J. Akbar, N. Siddiqui, S. Kanwal, and S. Inam, "A secure transmission of digital images using multiple chaotic maps and elliptic curve," *International Journal of Research Publication and Reviews*, vol. 5, no. 6, pp. 473–481, 2024. doi: 10.55248/gengpi.5.0624.1412.

[19] J. Liu, Z. Liang, Y. Luo, L. Cao, S. Zhang, Y. Wang, and S. Yang, "A hardware pseudo-random number generator using stochastic computing and logistic map," *Micromachines*, vol. 12, no. 1, p. 31, 2021. doi: 10.3390/mi12010031.

[20] S. Adhikari and S. Karforma, "A novel audio encryption method using Henon–Tent chaotic pseudo random number sequence," *International Journal of Information Technology*, vol. 13, no. 4, pp. 1463–1471, 2021. doi: 10.1007/s41870-021-00714-x.

[21] Q.-W. Zeng, Z.-Y. Wen, J.-F. Fu, and N.-R. Zhou, "Quantum watermark algorithm based on maximum pixel difference and tent map," *International Journal of Theoretical Physics*, vol. 60, no. 9, pp. 3306–3333, 2021. doi: 10.1007/s10773-021-04909-7.

[22] P. Kiran and B. D. Parameshachari, "Logistic sine map (LSM) based partial image encryption," in *2021 National Computing Colleges Conference (NCCC)*, IEEE, Mar. 2021, pp. 1–6. doi: 10.1109/nccc49330.2021.9428854.

[23] B. Khokhar, S. Dahiya, and K. S. Parmar, "Load frequency control of a microgrid employing a 2D Sine Logistic map based chaotic sine cosine algorithm," *Applied Soft Computing*, vol. 109, p. 107 564, Sep. 2021. doi: 10.1016/j.asoc.2021.107564.

[24] S. L. Nita and M. I. Mihailescu, "Elliptic curve-based query authentication protocol for IoT devices aided by blockchain," *Sensors*, vol. 23, no. 3, p. 1371, 2023. doi: 10.3390/s23031371.

[25] S. Kumar and D. Sharma, "A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm," *Artificial Intelligence Review*, vol. 57, no. 4, p. 87, 2024. doi: 10.1007/s10462-024-10719-0.

[26] A. O. David and O. Sulaimon, "Text encryption with improved elliptic curve cryptography," *Journal of Advances in Mathematics and Computer Science*, vol. 38, no. 3, pp. 32–41, 2023. doi: 10.9734/jamcs/2023/v38i31749.

[27] K. E. Abdullah and N. H. M. Ali, "A secure enhancement for encoding/decoding data using elliptic curve cryptography," *Iraqi Journal of Science*, vol. 59, no. 1A, pp. 189–198, 2018. doi: 10.24996/ijs.2018.59.1a.20.

[28] D. Uzun Ozsahin, E. Precious Onakpojeruo, B. Bartholomew Duwa, A. G. Usman, S. Isah Abba, and B. Uzun, "COVID-19 prediction using black-box based Pearson correlation approach," *Diagnostics*, vol. 13, no. 7, p. 1264, 2023. doi: 10.3390/diagnostics13071264.

[29] D. Vamsi and P. R. CH, "Hybrid image encryption using elliptic curve cryptography, Hadamard transform and hill cipher," *Webology*, vol. 19, no. 1, pp. 2357–2378, 2022. doi: 10.14704/web/v19i1/web19160.