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

ORIGINAL ARTICLE OPEN ACCESS

Color Image Encryption Using Elliptic Curve Cryptography and Chaotic Maps

Joel Kinganga [a], Nathanaél Kasoro [a], Issa Ramadhani [a], and Alain Musesa [a]

[a] University of Kinshasa, Kinshasa, Democratic Republic of the Congo

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

ARTICLE INFO
Received: Aug. 11, 2025
Revised: Nov. 22, 2025
Accepted: Nov. 30, 2025
Published: Dec. 30, 2025

ABSTRACT: ***Background:*** *The regular use of connected devices on the internet by users of social media generates a large quantity of multimedia data every second, and the data concerned may be of a variable nature, such as text data, color images, video, and audio. We can confirm that online security is becoming an area that is increasingly being explored by researchers around the world to guarantee and ensure the authenticity and confidentiality of exchanged data.* ***Objective:*** *The goal of this article is to introduce a new dynamic cryptosystem for encrypting color images, using elliptic curves and chaotic functions.* ***Methods:*** *This new system serves to generate the coefficients of the curve, create the encryption keys, and create the prime number of the curve. The new system utilizes the length of the encryption keys, which encompasses all points on the curve and relates to the discrete logarithm problem of elliptic curves, thereby justifying the difficulty in uncovering hidden information.* ***Results:*** *The results were obtained with the assistance of several analyses, including histogram analysis, correlation coefficient analysis, differential attack analysis, and key space analysis. The results obtained confirm the robustness and reliability of the proposed cryptographic system.* ***Conclusions:*** *By combining the two systems (elliptic curves and chaotic functions), we obtain a new hybrid system capable of operating with reduced encryption key lengths and random values, which makes our new system sensitive to initial conditions.*

KEYWORDS: *Encryption; Images; Decryption; Elliptic curves; Chaotic function*

INTRODUCTION

For a long time, people have sought ways to share secret information with their loved ones confidentially. They have always aimed to ensure the confidentiality and integrity of the data exchanged [1], [2]. Recently, cryptography has emerged as a vital science that guarantees the confidentiality of messages, attracting significant interest from researchers to facilitate secure data exchange and prevent unauthorized access to or understanding of this information, even when transmitted through unsecured channels [3], [4]. Nowadays, color images are increasingly common in data exchanges, largely due to the prevalence of high-speed internet. This data is often vulnerable to attacks, making it essential to ensure authentication and confidentiality when transmitting such important and sensitive information over public networks. To this day, research is ongoing in the pursuit of robust and quickly implementable cryptographic systems to ensure the confidentiality of exchanged data, especially since color images are currently the most commonly used type of multimedia data in communications. The need for continued research arises because several cryptographic systems have been compromised due to issues like execution time or the length of public or private keys used for encryption, highlighting the necessity for strong and resilient systems. One widely used technique for encrypting multimedia data, particularly images, involves hybrid cryptographic systems that ensure both confidentiality and integrity. This approach utilizes block encryption of pixels combined with chaotic functions to produce pseudo-random values for the encryption of image blocks. Additionally, it employs elliptic curves, which provide shorter key sizes linked to discrete logarithm problems for image encryption. To encrypt and decrypt information, researchers have recently developed algorithms such as those described in [5], [6]. In [7], the authors propose an image encryption algorithm that works in

an industrial Internet of Things environment. With this algorithm, multiple images can be encrypted using a combination of matrices and values generated by a chaotic map and a cyclic construction. The matrices are used to permute the positions of the pixels in the images. A new method of data encryption using the steganography technique was proposed in [8]. The authors conceal an image as secret data in a video used as a cover file. They use a sinusoidal chaotic map that is sensitive to changes in initial values and non-periodic to enhance image security. Moreover, other researchers, as in [9]–[11], have developed hybrid cryptographic systems combining chaos theory, elliptic curves, and symmetric cryptographic systems for encrypting color images. In [12], [13], the authors have extended their research into the encryption of medical images by proposing new methods using pixels to form the points of the elliptic curve. To avoid using large prime numbers, researchers in [14] use elliptic curves with binary extension, which reduces the computational load for image encryption. The piecewise linear chaotic function is used to generate pseudo-random numbers to mask the original image, and the substitution box (S-Box) is then applied to rearrange the pixels of the already masked image. Then, in [15], the authors proposed a chaotic image encryption system that increases the computation speed of chaotic sequence generation. They use the addition operator and points from the elliptic curve to generate a chaotic sequence. A new image encryption method using isomorphic elliptic curves was proposed in [16]. In this method, the authors take advantage of the key size to convert simple images to a point on the curve, using the Klobiz method for encryption. In [17]–[20], researchers conducted several other studies on color image encryption using chaotic functions and elliptic curves. Today, researchers increasingly prefer elliptic curves because they represent data as points on a curve. Similarly, chaotic functions are in high demand for their ability to generate a large number of random values. Our motivation for developing a hybrid system primarily stems from the challenge of discrete logarithms in elliptic curves. Starting from a specific point on the curve, known as the generator, we can easily derive all other points on that curve. Thus, if information is transformed into points on a curve, it can be readily retrieved. Additionally, the random and unpredictable nature of chaotic functions allows us to create multiple equations by varying the coefficients A, B, and P. This results in dynamic equations, meaning the information can be encrypted using several different equations rather than just one.

Our contribution is the implementation of a dynamic hybrid encryption system combining elliptic curves and chaotic functions (sine and logistic functions). The data are transformed into points on the curve and encrypted with equations whose coefficients (A, B, and P) of the curve vary due to the unpredictable nature of chaotic functions. Besides the introduction and conclusion, the present work is organized as follows: The second section discusses the tools and methods used, specifically focusing on the basic notions of elliptic curves as they apply to cryptography and the developed chaotic system. With chaotic functions, we have chosen the sine and logistic functions. The third section focuses on the encryption and decryption of the proposed system. Finally, the results and analysis are presented in the fourth section.

MATERIALS AND METHODS

To establish a data encryption system, several tools are necessary. In our article, we utilized both the MATLAB and Python languages to code our algorithm. These languages also enabled us to create various diagrams, such as the bifurcation diagram, histograms, and images, as well as to obtain the results we present here.

Chaotic Systems

It's important to note that a system is considered chaotic when it is both unpredictable and deterministic, meaning it is sensitive to initial conditions. Two initial conditions that are infinitely close can result in vastly different outcomes. Chaotic systems are deterministic, producing the same values when the same functions are applied. These chaotic systems have numerous applications in cryptography because they make predictions extremely difficult. Chaotic functions are very sensitive to initial conditions [21]. Despite their deterministic nature, they do not allow the evolution of the curve's trajectory to be predicted in advance. Considering two or more initial conditions that are close together at the outset, curves on the plane overlap and then gradually dissociate to generate different values. Our proposed system is based on chaotic functions. We used two chaotic functions, namely the logistic function and the sine function. These two functions were chosen to randomly generate the values to be used to diffuse our image and the coefficients A and B of the elliptical curve to make our equation dynamic.

The Logistic Function

In (1), for a critical value of r, let's take $r_c = 3.56996$. The function X_n no longer displays an orderly structure but rather one in the form of an infinite cycle. And each time the initial value X_0 changes, the function becomes different. This function is generally the most widely used in cryptography.

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

As we can read in [22], [23], the parameter r is a positive value between 1 and 4, and the value of X_n is between 0 and 1. Chaotic behavior occurs when r is equal to the value 3.6. Figure 1 shows the bifurcation diagram of the logistic function with the quantity X_n as a function of parameter r.

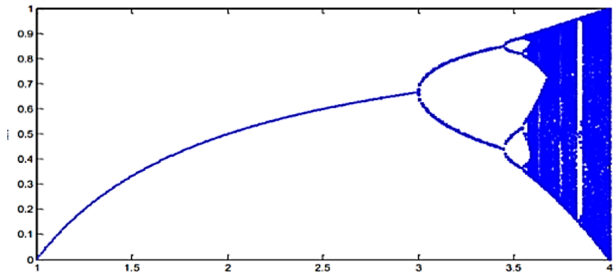

Figure 1. Bifurcation diagram of the logistic map

Therefore, for $r < r_c$, regardless of the initial value X_0 in the interval $[0, 1]$, the function converges to a finite structure. However, for values of $r > r_c$, our system becomes chaotic. To generate random values with our logistic function, we consider the parameter $r > 3.56996$. For the value of $r = 3.6$. Here are some generated values: [0.2596 0.7110 0.7601 0.6745 0.8121 0.5644 0.9094 0.3047 0.7836 0.6272 0.8649 0.4321 0.9077 0.3099 0.7911 0.6114 0.8789 0.3938 0.8830 0.3820 0.8733 0.4094 0.8944 0.3494]. The random aspect of this function is clearly visible in Figure 2.

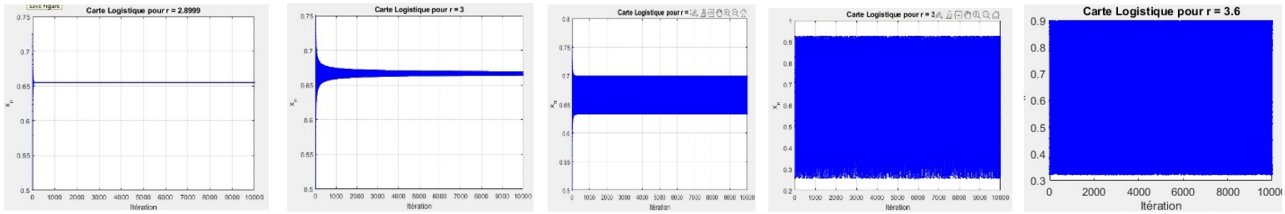

Figure 2. The evolution of the randomness of the chaotic function for r= 2, 2.9, 3, 3.6

The Part of Linear Chaotic Function (Tent Map)

This suite is mostly demanded because of its easy implementation, its simple representation, and its beneficial dynamic behavior, as shown in (2) and read in [24].

$$X_n = \left\{ \begin{matrix} r\frac{X_n}{2}, siX_n < 0.5 \\ r\frac{1-X_n}{2}, siX_n \geq 0.5 \end{matrix} \right\} \tag{2}$$

where: $X_n \in (0,1) \quad n \in N, X_0$ is the initial value. The control parameter r takes values in the range $(0, 0.5)$. The part of the linear chaotic sequence has good confusion, as explained in [25], and can generate a good random sequence required by cryptographic systems.

Sine Function

Equation (3) gives the shape of the sine function:

$$X_{n+1} = r * \sin(\pi X_n) \tag{3}$$

When y takes on a value of 1, i.e., $r = 1$, chaotic behavior begins. This behavior is identical to that of the logistic function described in [26]. This function is quadratic around the value $x = 0.5$. Its periodic window is wider than that of the logistic map, as explained in [27]. For the sine function, the function becomes chaotic from Y=1. Some values are: [0.2589 0.7265 0.7573 0.6906 0.8260 0.5198 0.9981 0.0061 0.0191 0.0599 0.1872 0.8409 0.4949 0.9247 0.2577 0.7076]. The random nature of the sine function is clearly visible in Figure 3.

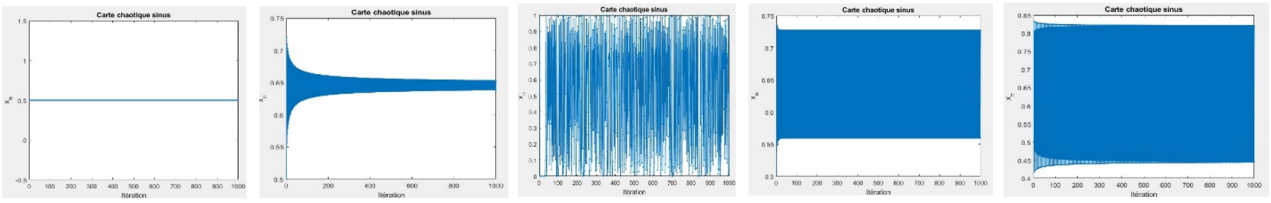

Figure 3. The evolution of the randomness of the sine function for r=0.5,0.8,0.9,1.0

Elliptical Curves

Two early authors, Klobiz and Miler, used the notion of elliptic curves in cryptography. The challenge lies in solving the discrete logarithm problem within the curve's point group. As we can see in [1], [28]–[30], an elliptic curve must verify the form of Weierstrass equation (4):

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{4}$$

If we assume that, $y = \frac{x}{z}$, and $y = \frac{y}{z}$, as described in [31], we have a homogeneous equation, and the curve becomes like (5).

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5}$$

Law of Composition

Let E be a real elliptic curve, and let Q and P be two points on the curve. We derive the law of composition:

$+ : ExE \to E : (P, Q) \to P + Q$ on the set E according to the following rules:

1. If $Q = O$, then $P + Q = P$, i.e., the point at infinity O acts as the neutral element for the $+$ operation defined on E.
2. If P and Q do not have the same abscissa, then the line D passing through P and Q intersects the curve E at a third point R. $P + Q = -R$.
3. If $Q = -P$, then necessarily $P + Q = P + (-P) = O$ (given the first point). After this, $P - P = O$ it noted directly.
4. If $P = Q$, then the line D tangent to E at P intersects the curve at a third point R, so $P + P = 2P = -R$.

Graphically, this can be explained in Figures 4 and 5.

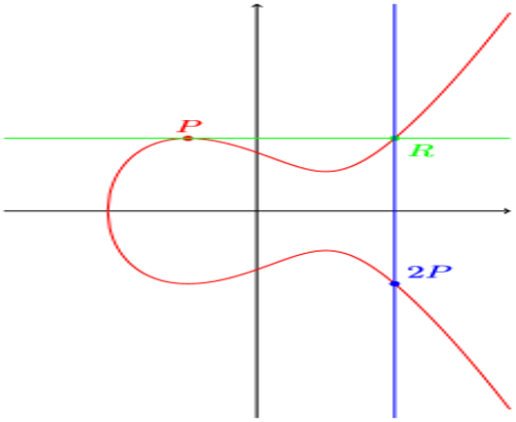

Figure 4. Calculation of $P + Q$

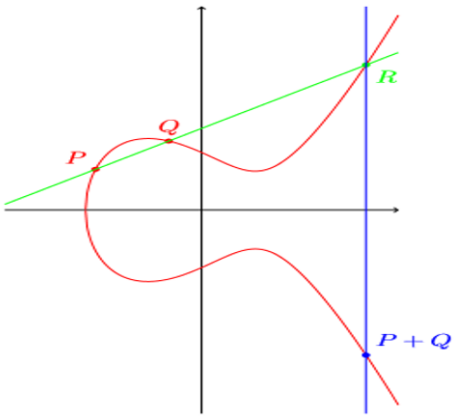

Figure 5. Calculation of $2P$

An elliptic curve is a set of solutions that satisfy (6):

$$Y^2 = X^3 + AX + B \tag{6}$$

These equations are called Weierstrass equations, named after a mathematician who studied them in the 19th century. Equations (7) and (8) are two examples of these equations, and Figure 6 shows their graphs.

$$E_1 : Y^2 = X^3 - 3X + 3 \tag{7}$$

$$E_2 : Y^2 = X^3 - 6X + 5 \tag{8}$$

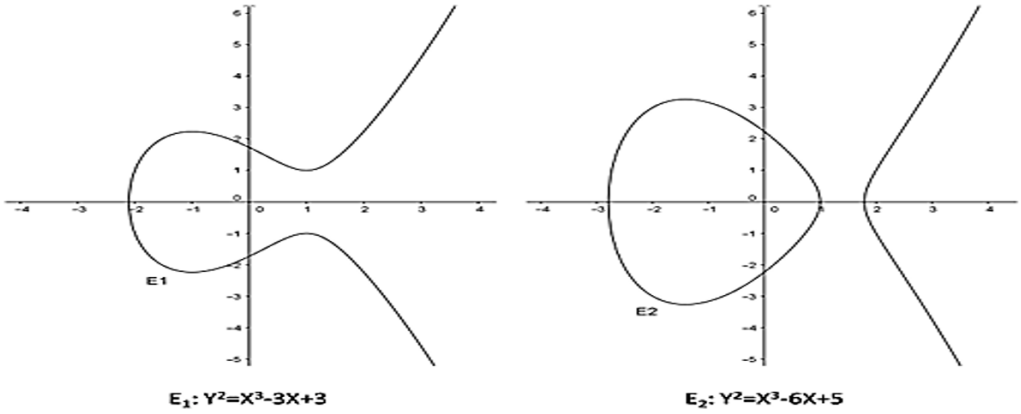

Figure 6. Graph of examples of Weierstrass equations (7) and (8)

Elliptic curves possess a fascinating property: it is possible to randomly select two points on an elliptic curve, add them together, and derive a third point. This form of addition is not the conventional kind; rather, it is associative, commutative, and includes a neutral element. The process combines two points on the curve in a way that resembles traditional addition. To accurately explain this addition law on elliptic curves, we use geometric concepts. Let E be an elliptic curve and P and Q two points on the curve, as we can see in Figure 7. First, let's draw line L, a line that passes through points P and Q.L intersects curve E at P, Q, and R. By projecting point R onto the X-axis, in other words, by multiplying its Y-coordinate by the value -1, we obtain a new point called R'. This point is called the sum of points P and Q. If we denote the addition law by $\oplus$, we write: P$\oplus Q = R$.

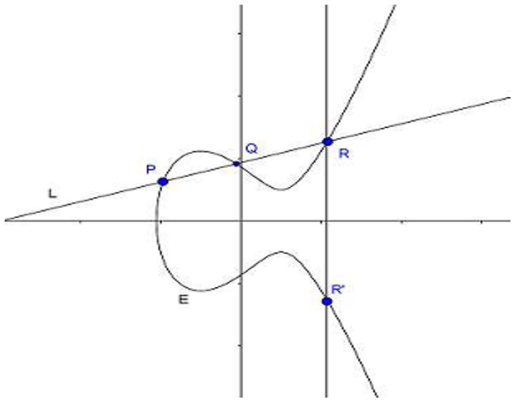

Figure 7. The addition law for elliptic curves

Let's add point P to itself. How line L, which connects points P and Q, behave if point Q slides along the curve and becomes very close to P. In this case, line L becomes tangent to E at P, as shown in Figure 8.

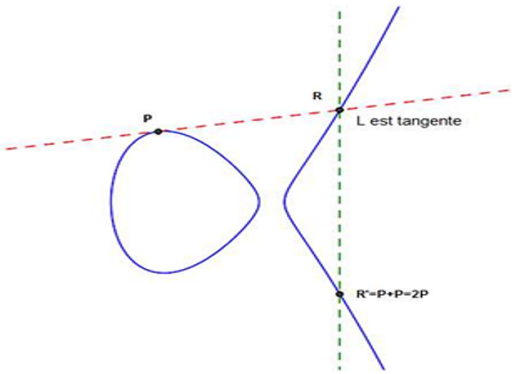

Figure 8. The addition of a curve to itself

If we consider line L as tangent to E at P, we see that L intersects E at P and also at R, another point on the curve. Therefore, line L always intersects curve E at three points, but point P is counted twice. Now let's consider point P and its symmetrical point, $P' = (a, -b)$ on the X-axis, where P is defined as $P = (a, b)$. L crosses point P, and P' is the vertical straight line $x = a$, and L intersects E at two points, point P and P', as shown in Figure 9.

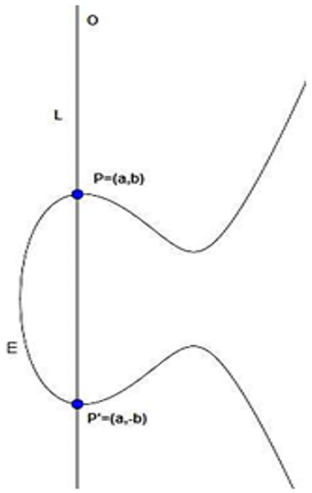

Figure 9. The addition of point p and its symmetrical point

Let's create a point O that lies at infinity, even though it does not exist in our plane. Let's say that $P \oplus Q = O$. Another problem arises: finding how to add our point at infinity, O, and another ordinary point, such as P. Since the point at infinity lies on the vertical lines and this line intersects E on the right at points P and P', to add them, we simply project P' onto the X-axis, which always takes us to P. Therefore, $P \oplus O = P$. The O functions as the origin, and since P lies on the X-axis, we can add P to O and P' on the right. To perform the addition, we simply project P' onto the X-axis, which always brings us back to P. Therefore, $P \oplus O = P$. O functions like 0, in addition to elliptic curves. In the set of solutions to equation E of the elliptic curve, we must add an extra point O, where A and B must satisfy equation (9):

$$4A^3 + 27B^2 \neq 0 \tag{9}$$

This quantity is called the discriminant of E. This quantity is different from 0, meaning that the polynomial must not have repeated roots. If we consider E as an elliptic curve, then the addition law on the curve E has the following property:

Let P be a point on the curve E;

1. Inverse: $\forall P \in E, P + (-P) = O$
2. Identity: $\forall P \in E, (P + O) = (O + P)$

3. Association: $\forall P, Q$ and $R \in E, (P + Q) + R = P + (Q + R)$
4. Commutativity: $\forall P, Q \in E, (P + Q) = (Q + P)$

Therefore, we can say that the addition law on elliptic curves forms an abelian group. Its algorithm is as follows:

Let E be an elliptic curve and P_1 and P_2 two points on the curve.

1. If $P_1 = 0$ also $P_1 + P_2 = P_2$
2. Otherwise, If $P_2 = 0$ also $P_1 + P_2 = P_1$
3. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$
4. If $x_1 = x_2$ and $y_1 = -y_2$ then $P_1 + P_2 = O$
5. Otherwise, calculate λ using the formula:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \\ \frac{3x^2 + a}{2y_1} \end{cases} \tag{10}$$

$$x_3 = \lambda^2 - x_1 - x_2 \tag{11}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \tag{12}$$

Then

$$(x_3, y_3) = P_1 + P_2 \tag{13}$$

Elliptic Curves Over Finite Fields

The theory of elliptic curves is applicable in cryptography under the sole condition that only elliptic curves whose points have coordinates in a finite field F_p are considered. This elliptic curve over the finite field is defined simply by the equation:

$$E : Y^2 = X^3 + AX + B \text{ Avec A and B} \in F_p \; 4A^3 + 27B^2 \neq 0 \tag{14}$$

Encryption Decryption Image Process

In this section, we explain the processes of encrypting and decrypting images. In Figure 10, we present our process diagram for encrypting color images with elliptic curves by applying the following steps:

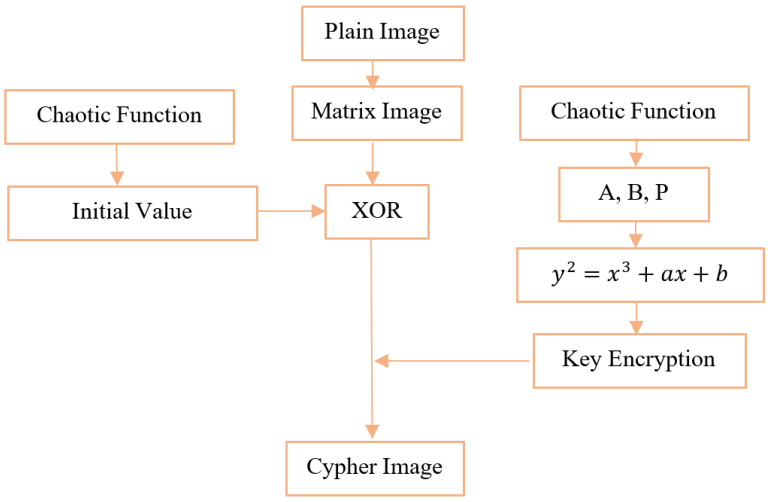

Figure 10. Image encryption steps using elliptic curves

Step 1: For the Sender and Receiver

- Agree on an equation of the form $Y^2 = X^3 + AX + B$ and a prime number p between the sender and the receiver.
- Find the points on the curve and choose the generator $G = (x, y)$.

- Choose a n_A and n_B such as $n_A, n_B < p-1$, and calculate $P_A = n_A * G$ and $P_B = n_B * G$
- Calculate the public key K.

Step 2: For the Sender - Load the image and display the image matrix.
- Convert each pixel of the image to hexadecimal form $(h_1\ h_2)_{16}$ then to decimal $(d_1\ d_2)_{10}$
- Calculate the quantities (c_1, c_2) using formulas 14 and 15 below and B(1,1) as follows:

$c_1 = d_1 + x + y \bmod p$
$c_2 = d_2 + c_1 \bmod p$
$B(1,1) = \bmod(c_1, 16) * 16 + \bmod(c_2, 16)$ and send B(1,1)

Step 3: For the receiver - Convert the encrypted pixel values to hexadecimal and decimal and find (d_1 and d_2) using formulas (15) and (16) below:

$c_1 = x_1 * 16 + x_1$
$c_2 = x_1 * 16 + x_2$

$$d_1 = (c_1 - x - y) \bmod p \tag{15}$$

$$d_2 = (c_2 - c_1) \bmod p \tag{16}$$

- Find the original image using the formula: $E(1,1) = d_1 * 16 + d_2$ Suppose that two people want to exchange an image and decide to use the following elliptic curve: $E : y^2 = x^3 + x + 3\,(\text{mod}31)$. The parameters used by these two people are: $\{A, B, G, p\} = \{1, 3, (1, 6), 31\}$. Some points generated with the curve are as follows: ([1, 6], [1, 25], [3, 8], [3, 23], [4, 3], [4, 28], [5, 3], [5, 28], [6, 15], [6, 16], [9, 11], [9, 20], [12, 10], [12, 21], [14, 8], [14, 23], [15, 13])

Let's take the image Dog as an example. The sender wants to send this image to receiver B. The steps below must be taken into account for the exchange of this image.

Step 1: Key creation by the sender and receiver

Sender

1. Select n_A as a private key: $n_A = 15 \in [1, 30]$
2. With the chosen number, calculate the public key $P_A = n_A * G = 15(1.6) = (30.30)$

Receiver

1. Select n_B as a private Key: $n_B = 21 \in [1, 30]$
2. With the chosen number, calculate the public key $P_B = n_B * G = 21(1.6) = (4.3)$

The points $P_A = (30, 30)$ and $P_B = (4, 3)$ are considered to be the public keys that the sender and receiver exchange.

Step 2: Encryption process used by the sender to send the image

1. In Table 1, we find the pixels of the dog image. Each pixel of the image must be converted to hexadecimal, having the form $(h_1, h_2)_{16}$

Table 1. Pixels in the dog image in decimal

A	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**...**
1	192	198	200	198	194	194	193	...
2	194	197	198	198	198	197	199	...
3	202	205	206	205	204	203	200	...
4	199	198	197	194	192	191	188	...
5	191	194	192	189	188	187	187	...
6	192	201	200	189	185	191	185	...
...	...	...	...	...	...	...	...	

The first value A(1,1)=192 in our table converted to $(C4)_{16}$

2. Convert the hexadecimal value found in 1 to decimal with the form (d1, d2)$_{10}$ $(C4)_{16} = (C, 4)_{16}$ = having the form (d1, d2)$_{10}$ $= (12, 4)_{10}$

3. The secret key for the sender calculated as follows: $K = n_A * P_B = 15(4, 3) = (3, 8)$. Multiplying a value between 1 and p-1, for example $S = 19; (x, y) = S(K) = S(3, 8) = 19(3, 8) = (24, 26)$

4. The calculation of c_1 as follows: $c_1 = d_1 + x + y \bmod p = (12 + 24 + 26) \bmod 31 = 10$

5. The calculation of c_2: $c_2 = d_2 + c_1 \bmod p = (4 + 10) \bmod 31 = 14$

 DOI: https://doi.org/10.23851/mjs.v36i4.1728

6. The encrypted value for this pixel calculated using the formula below: B(1,1)=mod$(c_1, 16) *$ 16+mod$(c_2, 16)$ = mod(10,16)*16+mod(14,16)=174

These steps are repeated for all pixels in the image to be encrypted to find the values shown in Table 2.

Table 2. Pixels in the encrypted dog image

B	1	2	3	4
1	174	188	197	...
2	185	174	198	...
3	203	173	188	...
4	...	...	...	...

Step 3. Decryption

To decrypt the information, the receiver converts each pixel of the encrypted image into hexadecimal with the form $(h_1, h_2)_{16}$ separating these values with a comma to obtain $(h_1, h_2)_{16}$ then converting it from hexadecimal to decimal $(x_1, x_2)_{10}$. By performing the various calculations below, to obtain (d_1, d_2).

$$c_1 = x_1 * 16 + x_1$$
$$c_2 = x_1 * 16 + x_2$$
$$d_1 = (c_1 - x - y) \bmod p$$
$$d_2 = (c_2 - c_1) \bmod p$$

The formula below can be executed by the transmitter to recover the original image:

$$E(1,1) = d_1 * 16 + d_2$$

RESULTS AND DISCUSSION

Data transmitted over unsecured channels is vulnerable to attackers who aim to discover what is being exchanged. Security analysis assesses whether a cryptosystem can withstand such attacks. An effective cryptographic system is one that is resilient against all forms of hacking attempts. This section discusses a security analysis using selected images. Among the analyses covered are frequency histogram analysis, key space evaluation, entropy, correlation analysis, and more. We have selected four images to test our system: three color images and one black-and-white image, specifically of Lena, a baboon, fruits, and a cameraman.

Security Analysis

Attacking our proposed system and retrieving the hidden information is practically impossible because the receiver and sender must first agree on an equation for the curve, where the coefficients and prime number are derived from a randomly generated chaotic function. Next, they must agree on generator $G(x, y)$, which represents a point on the curve. Finally, the number chosen by both individuals exchanging information must be less than P, which remains secret. This means that our system is more secure against attacks.

Key Space Analysis

To access hidden information, attackers aim to uncover the key used for encryption. If the key space is sufficiently large, the encryption method becomes more robust, rendering brute force attack methods employed by hackers ineffective [32]. To generate keys with our proposed system, we used elliptic curves and chaotic functions. Three parameters were used (a_1, b_1, p_1), each parameter having at least 16 bits, for a total of $2^{(48)}$. Two parameters were also used to obtain the key space with the logistic map, namely (x_0, r), and the values generated were used with XOR to confuse the original image. For a logistic function, the key space is $2^{(53)}$. In total, we have $2^{(101)}$ possible combinations. Our proposed system is dynamic; the parametersa,b,p of the equation change each time we want

to encrypt the data. The data is not encrypted with the same equation. This also means that the encryption key space is dynamic. As a result, our system is resistant to all forms of attack (differential attack, brute force attack, known text attack) from malicious individuals.

Key Sensitivity Analysis

For an effective encryption system, the encryption key must be sensitive to initial conditions [32]. The keys produced by our proposed system are dynamic because they are generated by a chaotic function that responds to initial conditions. As the coefficients of the curve equation vary, the generating point of the curve also shifts, resulting in different keys for the transmitter and receiver. This dynamism makes the keys challenging to recover.

Histogram Analysis

In this analysis, it is crucial for researchers to confirm that the encrypted image is statistically distinct from the original image, as outlined in [33], [34]. The histogram of an image's frequencies illustrates the distribution of its pixels. A notable difference between the encrypted and original images should be evident, demonstrating a consistent and uniform distribution. Figures 11 and 12 display the histograms for both the original and encrypted images.

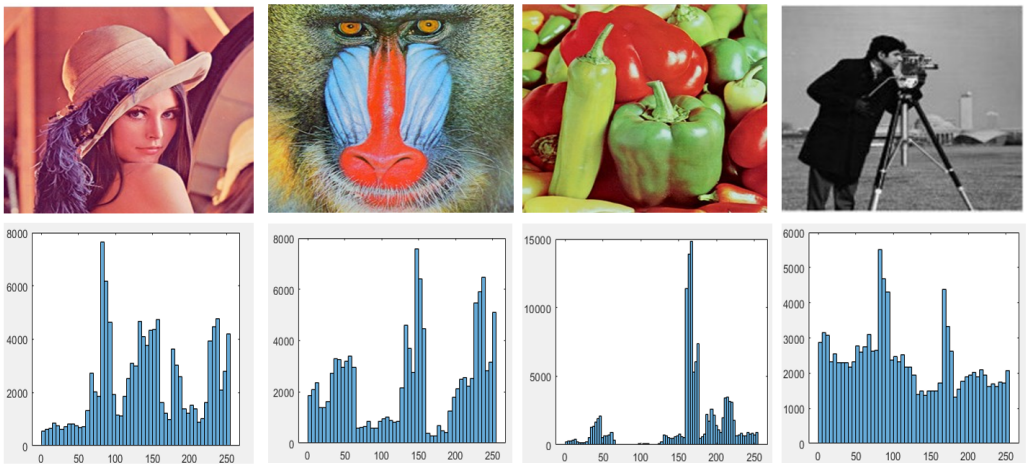

Figure 11. Clear images and their histograms for Lena, Baboon, Fruits, and Cameramen

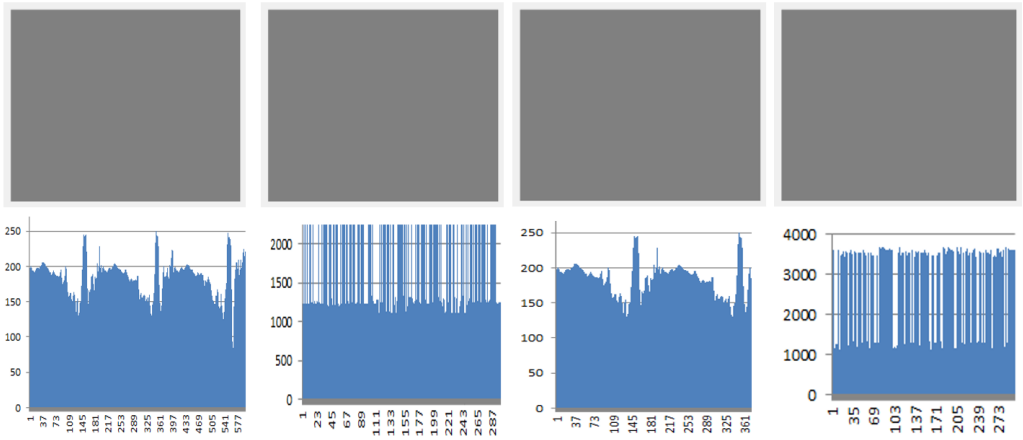

Figure 12. The encrypted images and their histograms for Lena, Baboon, Fruits, and Cameramen

Correlation Analysis

As explained by the authors in [30], [35], one of the statistical methods used to assess the quality of encryption, to quantify the strength of the linear relationship, the link and the trends that exist between two variables is correlation analysis. This is represented by a correlation coefficient with a value between 0 and 1. The closer this value is to 1 or -1, the stronger and more linear the relationship is; the closer it is to 0, the weaker and more non-linear the relationship is [32], (17) represents this coefficient:

$$r = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - x)^2}\sqrt{\sum_{i=1}^{n}(y_i - y)^2}} \tag{17}$$

This formula is applied to determine the values in Table 3. In (17), r is the correlation coefficient, the number of observations is represented by n, and the values of two variables, the encrypted image and the original image, are represented by X_i and Y_i for our four images in Figure 11.

Table 3. The correlation coefficients between the clear image and the encrypted image

No.	Images	Coefficient
1	Lena	-0.06
2	Baboon	-0.05
3	Fruit	0.5
4	Cameramen	0.6

With the results found in Table 3, we can say there is no significant relationship between the pixels of the image encrypted with our proposed encryption system based on elliptic curves and chaotic functions. For the same image encrypted with ECC associated with chaotic functions, as shown by the correlation coefficient r, after encryption, there is no significant relationship between the two.

Information Entropy

The entropy of a color image is a measure of the diversity of pixels in the image as well as its complexity, as explained in [14], [36]. This metric is used in image processing to analyze the amount of information and texture in the image. According to Shannon, entropy is calculated using (18).

$$H = -\sum P_i \log_2(P_i) \tag{18}$$

where P_i is the probability of a given gray level.

The entropy of a satisfactory encryption system must not exceed the value 8; it must be around 8. So then, as mentioned in Table 4, the entropy of our chosen images is all close to the value 8. This means that our proposed system is resistant to attacks from malicious individuals

Table 4. Clear and Encrypted image entropy

No.	Image	Entropy clear image	Encrypted image entropy
1	Lena	6.4723	7.9010
2	Baboon	6.7024	7.8882
3	Fruits	6.4909	7.7987
4	Cameraman	7.1034	7.9012

Analysis of Differential Attacks

Two important measures are used to assess the resistance of an encryption algorithm to differential attacks: the normalized pixel change rate (NPCR) and the unified average change intensity (UACI). Equations (19)-(21) of NPCR and UACI [37] are used to quantify the sensitivity of an encryption

algorithm to changes in plaintext.

$$D(i,j) = \begin{cases} 0, I_1(i,j) = I_2(i,j) \\ 1, I_1(i,j) \neq I_2(i,j) \end{cases} \tag{19}$$

$$NPCR = \frac{\sum_{i=1}^{l} \sum_{j=1}^{b} D(i,j)}{l \times b} \times 100\% \tag{20}$$

$$UACI = \frac{\sum_{i=1}^{l} \sum_{j=1}^{b} \mathrm{I}_1(i,j) - I_2(i,j)\mathrm{I}}{l \times b \times 255} = 100\% \tag{21}$$

The weaker UACI values and higher NPCR values indicate a more secure algorithm against differential attacks, as they suggest that small changes to the plaintext image result in larger changes to the encrypted image. These values can be calculated using (19)-(21). Table 5 presents the values of NPCR and UACI found by applying these formulas and proves the algorithm's resistance to attack.

Table 5. UACI and NPSR values for the selected images

No.	The Image	UACI	NPCR (%)
1	Lena	34.3700	100
2	Baboon	33.0025	99.8
3	Fruits	32.3025	100
4	Cameraman	31.3725	99.9

Additional analyses can be conducted on the original and encrypted images using mean square error (MSE) and peak signal-to-noise ratio (PSNR), as referenced in [38]. MSE is a quantitative metric that measures the average squared difference between the pixels of the original and encrypted images; a low MSE indicates that the two images are nearly identical. In contrast, PSNR assesses the uniformity of the image, with a low value signifying a significant difference between the original and encrypted images. An effective encryption system should exhibit a high MSE value and a low PSNR value. Equations (22)-(25) can be used to compute these metrics.

$$MSE_{PE} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (p_{ij} - e_{ij})^2 \tag{22}$$

$$MSE_{PD} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (p_{ij} - d_{ij})^2 \tag{23}$$

$$PSNR_{PE} = 20 \log_{10} \frac{\max(P)}{\sqrt{MSE_{PE}}} \tag{24}$$

$$PSNR_{PD} = 20 \log_{10} \frac{\max(P)}{\sqrt{MSE_{PD}}} \tag{25}$$

where p represents the original image and the encrypted image E and D, the decrypted image. The quantities M, N, and Max (P) show the width, height, and values of the image. In Table 6, we find the respective values of MSE and PSNR. The PSNR parameter values show the level of image degradation compared to the original image due to high MSE values. This highlights the significant difference between the original and encrypted images.

Table 6. MSE and PSNR values for the selected images

No.	The Image	MSE	PSNR
1	Lena	2304	0.02
2	Baboon	6400	0.00
3	Fruits	2504	0.03
4	Cameraman	2400	0.02

Limitations and Vulnerability of the Proposed System

Due to their key lengths, cryptographic systems based on elliptic curves offer high security and have gained popularity among researchers in recent years. The combination of chaotic functions and elliptic curves adds complexity to our system, making it less susceptible to attacks. Our proposed system is capable of encrypting not only color images but also black-and-white images. Among the selected images shown in Figure 11, we have the cameraman image, which is in black and white. While our system can also encrypt large images, the process is relatively slow, as it requires time to convert each pixel of the image into a point on the curve for encryption.

Research [7]–[11], [16], [20] contains cryptographic systems proposed by authors in the past. This section conducts a comparative study between these systems and ours, as outlined in Table 7. The system proposed by the authors in [11] seems to be cumbersome in the sense that there are several permutations coming from the S-Box created by the elliptic curve and the chaotic map, as well as difficulty in exchanging encryption keys between the sender and the receiver. The S-boxes that generate the encryption keys in [16] are static, predictable, lack random characteristics, and are insensitive to initial conditions.

Table 7. Comparison of the proposed system with existing systems

Ref.	Entropy	NPCR	UACI
Proposed scheme	7.9010	100.0	34.37
Ref. [11]	7.9985	99.96	33.98
Ref. [16]	7.9498	99.66	33.71
Ref. [20]	7.9975	99.61	33.50

In contrast, our proposed system uses chaotic functions that generate random values. They are dynamic, unpredictable, and sensitive to initial conditions. It is simple and has fewer permutations due to the absence of the S-Box, but it is also dynamic. None of the methods proposed by [11], [16], [20] use a dynamic curve equation; they all use a static equation. Malicious individuals can access the information once they know the equation. Table 7 presents a comparative analysis between our proposed system and other recent encryption schemes by researchers. The points below outline the comparison of the Lena image between our system and those of other researchers.

The results of the differential attack analysis (UACI and NPCR) in Table 7 show that our proposed cryptosystem is resistant to attacks and also excels among existing algorithms in terms of [11], [20]. The entropy value of our proposed system is also close to 8, as is that of other researchers in [7], [11], [20]. This proves that our system has good values. Observing the correlation coefficient of the proposed schemes and ours shows that our cryptosystem is resistant to statistical attacks because its value is close to zero, like that of the others. Our system differs from others in that it is dynamic and allows the values of the elliptic curve coefficients to be generated randomly using two chaotic functions and the value of the prime number p. During encryption, the data is not encrypted with a static equation but rather a dynamic one. Not only should the curve equation be dynamic, but the generator and all keys should also be dynamic.

CONCLUSION

In this article, we introduced a new dynamic encryption system for color images that utilizes elliptic curves along with two chaotic functions: the sine function and the logistic function. Unlike other researchers, our system does not rely on the same equation; instead, the values of the coefficients A and B of the Weierstrass equation are variable and generated by the chaotic function. To create confusion with the original image, we apply the XOR operation between the random values produced by the chaotic function, which correspond to the total number of pixels in the original image, and the original image itself. The results from our analyses demonstrate the high level of security and robustness of our system. It is capable of withstanding brute force attacks, differential attacks, and other threats from malicious actors. Our system provides enhanced security compared to other recently proposed systems that rely solely on a static Weierstrass equation, thanks to its dynamic equation. However, our proposed system cannot encrypt large images with a small prime number or

small images with a large prime number, as the number of points on the curve is dependent on the prime number p. The choice of this prime number must align with the size of the image. Although encrypting large images with a large prime number can be time-consuming, this duration becomes manageable if the prime number is appropriately selected. Additionally, the new system we propose can be adapted for the encryption of black and white images, videos, and audio, which is the focus of our future research.

SUPPLEMENTARY MATERIAL

No supplementary material is provided for this study.

AUTHOR CONTRIBUTIONS

Joel Kinganga: Design and methodology. Nathanaél Kasoro: Investigation. Issa Ramadhani: Software. Alain Musesa: Writing, reviewing, and editing.

FUNDING

This research received no external funding.

DATA AVAILABILITY STATEMENT

None.

ACKNOWLEDGMENTS

We would like to express our gratitude to the English-speaking team for correcting grammatical styles, as well as to the mathematicians from the department of mathematics and computer science at the university of Kinshasa for their explanations of elliptic curves.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

DECLARATION OF GENERATIVE AI USE

The authors declare that no generative Al or Al-assisted technologies were used in the preparation of this manuscript.

REFERENCES

[1] K. A. Sattar, T. Haider, U. Hayat, and M. D. Bustamante, "An efficient and secure cryptographic algorithm using elliptic curves and max-plus algebra-based wavelet transform," *Applied Sciences*, vol. 13, no. 14, Art no. 8385, 2023, doi: 10.3390/app13148385.

[2] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color image encryption through chaos and KAA map," *IEEE Access*, vol. 11, pp. 11 541–11 554, 2023, doi: 10.1109/access.2023.3242311.

[3] A. T. Heru, Faisal, and S. R. Manalu, "File encryption and decryption application using elliptic curve Diffie-Hellman algorithm and chaotic map function," *Procedia Computer Science*, vol. 245, pp. 39–48, 2024, doi: 10.1016/j.procs.2024.10.227.

[4] K. E. Kinani, F. Amounas, S. Bendaoud, M. Azrour, and M. Badiy, "New image crypto-compression scheme based on Ecc and chaos theory for high-speed and reliable transmission of medical images in the IOMT," *Cybernetics and Information Technologies*, vol. 24, no. 4, pp. 108–125, 2024, doi: 10.2478/cait-2024-0038.

[5] J. Kinganga, N. Kasoro, and A. Musesa, "Dynamics data encryption based on chaotic functions and elliptic curves: Application to text data," *Al-Mustansiriyah Journal of Science*, vol. 36, no. 1, pp. 56–68, 2025, doi: 10.23851/mjs.v36i1.1616.

[6] M. M. Trung, L. P. Do, D. T. Tuan, N. V. Tanh, and N. Q. Tri, "Design a cryptosystem using elliptic curves cryptography and Vigenère symmetry key," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, Art no. 1734, 2023, doi: 10.11591/ijece.v13i2.pp1734-1743.

[7] M. Alawida, "A novel image encryption algorithm based on cyclic chaotic map in industrial IoT environments," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 8, pp. 10 530–10 541, 2024, doi: 10.1109/tii.2024.3395631.

[8] M. M. Naji, A. T. Abdulsada, and S. M. Wadi, "Video steganography based on sine chaotic map and the RSA technique," *MINAR International Journal of Applied Sciences and Technology*, vol. 6, no. 3, pp. 115–132, 2024, doi: 10.47832/2717-8234.20.11.

[9] R. Flores-Carapia, V. M. Silva-García, and M. A. Cardona-López, "A dynamic hybrid cryptosystem using chaos and Diffie-Hellman protocol: An image encryption application," *Applied Sciences*, vol. 13, no. 12, Art no. 7168, 2023, doi: 10.3390/app13127168.

[10] 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.

[11] T. Qayyum, T. Shah, A. Y. Hummdi, A. Aljaedi, and Z. Bassfar, "An innovative feasible approach for multi-media security using both chaotic and elliptic curve structures," *IEEE Access*, vol. 12, pp. 10 411–10 427, 2024, doi: 10.1109/access.2024.3354170.

[12] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, "Medical image encryption: A comprehensive review," *Computers*, vol. 12, no. 8, Art no. 160, 2023, doi: 10.3390/computers12080160.

[13] A. S. Alali, R. Ali, M. K. Jamil, J. Ali, and Gulraiz, "Secure medical image encryption with hyperelliptic curve based S-boxes," *Scientific Reports*, vol. 15, no. 1, Art no. 18179, 2025, doi: 10.1038/s41598-025-02102-y.

[14] S. S. Jamal, Z. Bassfar, O. Lahlou, A. Aljaedi, and M. M. Hazzazi, "Image encryption based on elliptic curve points and linear fractional transformation," *IEEE Access*, vol. 12, pp. 53 335–53 347, 2024, doi: 10.1109/access.2024.3385677.

[15] A. M. Abbas, A. A. Alharbi, and S. Ibrahim, "A novel parallelizable chaotic image encryption scheme based on elliptic curves," *IEEE Access*, vol. 9, pp. 54 978–54 991, 2021, doi: 10.1109/access.2021.3068931.

[16] I. Khalid, S. S. Jamal, T. Shah, D. Shah, and M. M. Hazzazi, "A novel scheme of image encryption based on elliptic curves isomorphism and substitution boxes," *IEEE Access*, vol. 9, pp. 77 798–77 810, 2021, doi: 10.1109/access.2021.3083151.

[17] M. Ramzan, T. Shah, M. M. Hazzazi, A. Aljaedi, and A. R. Alharbi, "Construction of S-Boxes using different maps over elliptic curves for image encryption," *IEEE Access*, vol. 9, pp. 157 106–157 123, 2021, doi: 10.1109/access.2021.3128177.

[18] P. Parida, C. Pradhan, X.-Z. Gao, D. S. Roy, and R. K. Barik, "Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps," *IEEE Access*, vol. 9, pp. 76 191–76 204, 2021, doi: 10.1109/access.2021.3072075.

[19] A. S. Alali, R. Ali, M. K. Jamil, J. Ali, and Gulraiz, "Dynamic S-Box construction using Mordell elliptic curves over Galois field and its applications in image encryption," *Mathematics*, vol. 12, no. 4, Art no. 587, 2024, doi: 10.3390/math12040587.

[20] K. M. Hosny, Y. M. Elnabawy, A. M. Elshewey, S. M. Alhammad, D. S. Khafaga, and R. Salama, "New method of colour image encryption using triple chaotic maps," *IET Image Processing*, vol. 18, no. 12, pp. 3262–3276, 2024, doi: 10.1049/ipr2.13171.

[21] A. Tiwari, P. Diwan, T. D. Diwan, M. Miroslav, and S. P. Samal, "A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication," *Scientific Reports*, vol. 15, no. 1, Art no. 14151, 2025, doi: 10.1038/s41598-025-95995-8.

[22] 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, Art no. 106006, 2024, doi: 10.1088/1402-4896/ad75c5.

[23] M. Jiang and H. Yang, "Image encryption using a new hybrid chaotic map and spiral transformation," *Entropy*, vol. 25, no. 11, Art no. 1516, 2023, doi: 10.3390/e25111516.

[24] 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, Art no. 31, 2020, doi: 10.3390/mi12010031.

[25] 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.

[26] 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.

[27] 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.

[28] 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, Art no. 107564, Sep. 2021, doi: 10.1016/j.asoc.2021.107564.

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

[30] 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, Art no. 87, 2024, doi: 10.1007/s10462-024-10719-0.

[31] S. Kanwal, S. Inam, S. Al-Otaibi, J. Akbar, N. Siddiqui, and M. Ashiq, "An efficient image encryption algorithm using 3D-cyclic chebyshev map and elliptic curve," *Scientific Reports*, vol. 14, no. 1, Art no. 29626, 2024, doi: 10.1038/s41598-024-77955-w.

[32] M. J. Obaid and N. F. H. Al Saffar, "Asymmetric image encryption based on singular cubic curve with chaotic map," *Iraqi Journal of Science*, vol. 65, no. 5, pp. 2605–2618, 2024, doi: 10.24996/ijs.2024.65.5.21.

[33] B. Long, Z. Chen, T. Liu, X. Wu, C. He, and L. Wang, "A novel medical image encryption scheme based on deep learning feature encoding and decoding," *IEEE Access*, vol. 12, pp. 38 382–38 398, 2024, doi: 10.1109/access.2024.3371888.

[34] K. Lata and L. R. Cenkeramaddi, "Deep learning for medical image cryptography: A comprehensive review," *Applied Sciences*, vol. 13, no. 14, Art no. 8295, 2023, doi: 10.3390/app13148295.

[35] 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, Art no. 1264, 2023, doi: 10.3390/diagnostics13071264.

[36] 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, 2023, doi: 10.1109/access.2022.3230096.

[37] M. H. S. Hasan and M. H. S. H. Ahmed, "Digital image encryption based on elliptic curve cryptography," in *2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, IEEE, May 2024, pp. 20–25, doi: 10.1109/mi–sta61267.2024.10599647.

[38] Y. Lahraoui, S. Lazaar, Y. Amal, and A. Nitaj, "A novel ECC-based method for secure image encryption," *Algorithms*, vol. 18, no. 8, Art no. 514, 2025, doi: 10.3390/a18080514.