Available online at www.garmian.edu.krd

Passer Journal of Basic and Applied Sci

Passer 8 (Issue 2) (2028) 979-986

Original Article

Polynomials and Steganography for Designing a Secure Cryptosystem

Zahra Eimad Sukban[1], Hassan Rashed Yassein[*1], Nibras Hadi Jawad[1]

[1]*Department of Mathematics College of Education University of Al-Qadisiyah Diwaniyah Iraq.*

Received 26 January 2026; revised 14 July 2026;
accepted 25 July 2026; available online 01 September 2026

DOI: 10.24271/psr.2026.572279.2572

ABSTRACT

This paper focuses on integrating two techniques: the first is encryption (which changes the form of data) using NinMat algebra with a mathematical structure, and the second is data hiding (which hides the existence of the data itself) inside random images with the addition of specific filters to change its location. This gives the proposed system a high level of security, which enhances privacy and confidence in sending information using it and securing it from various attacks that it is exposed to from unauthorized parties. Therefore, the goal of this system is to preserve information from various risks when it is intercepted in the transmission medium or when its sources are compromised in light of the rise of the digital society.

Keywords: Steganography, Lorenz system, Cryptosystem, Floyd-Steinberg Dithering filter.

1 Introduction

Researchers are working on designing and developing encryption systems due to their importance in protecting information from various threats. This requires building multi-layered security methods, which can be achieved by combining encryption and steganography, with each stage involving several steps. This makes it difficult for attackers to access the final encrypted text, as the final encrypted text has passed through numerous steps, each producing a new encrypted text. Steganography is an important technology in the field of information security, as it aims to hide the presence of confidential data within digital media such as images, making these media appear normal and not arouse suspicion.

Steganography dates back to ancient times when slaves would tattoo their fingernails with secret messages and wait for the hair to grow back before sending the slave with hidden messages [1]. During World War II, the Germans used microdot technology to reduce the size of written information, making it extremely difficult to detect [2]. In 1992, Kurak and McHugh argue that it's easy to inject hidden information into digital images [3]. In 2002, Christian proposed a model that combines information concealment with protection against eavesdropping [4]. In 2009, Channalli and Jadhav proposed scheme that combined encryption with anonymity to transfer larger amounts of data [5]. In 2014, Mazurczyk and Caviglione proposed a security framework to detect and prevent data hiding in smartphones [6]. In 2019, Liu et al. proposed a solution based on steganography in the video [7]. In 2022, Kaur et al. provided a comprehensive review summarizing recent developments in Image steganography techniques [8]. In 2024, Badhan and Malhi proposed a sophisticated system that combines encryption with steganography to create a double layer of security that is difficult to breach [9]. In 2025, Rebeen et al. introduced open-source firewalls provide in-depth security features for SD-WAN architectures [10]. Majid et al. proposed a system with increased complexity and time cost by combining encryption with steganography [11]. Dana et al. study comprehensively explores security challenges and advancements in fog-enabled Vehicular Ad Hoc Networks [12]. Nahla & Bashar proposed combining chaotic structures with biometric integrity as an innovative approach in those stressful conditions [13]. In 2026, Saja et al. It further explores other innovations in the security domain, such as autonomous security operation centers (ASOCs) and the potential impact of quantum [14]. Baranawal et al. using least significant bit substitution (LSB), field-switching methods or advanced neural network techniques to preserve the visual quality of the original image in secret messages [15].

* Corresponding author
E-mail address hassan.yaseen@qu.edu.iq
Peer-reviewed under the responsibility of the University of Garmian.

2 Floyd-Steinberg Dithering Filter

It is an algorithm for dithering frequency technology that demonstrates its brilliance in its exceptional ability to simulate color gradients using a limited number of colors while maintaining the illusion of depth and visual gradation. technique works by applying a filter to an image to distribute errors in a balanced way while quantizing the image's pixels. It searches for the closest available color to improve the difference between two color values (i.e., between the image's color values and the selected color value). The difference or error value is then distributed across the pixels adjacent to the pixel being modified. This technique relies on error distribution filters, using values such as x 7, where x is the actual pixel value

of the image, and weights of adjacent values: 3, 5, and 1, each value divided by their sum, which is 16. The resulting color density and blurring make it more difficult to detect the locations of pixels where data is hidden. This is the goal for achieving optimal results in steganography [16].

3 Lorenz System

The Lorenz system represents a cornerstone in understanding complex dynamical systems [17], as it emerged in 1963 as a mathematical model simulating convection phenomenon in the atmosphere. It is characterized by sensitivity to initial conditions, such that even a slight, almost negligible change at the beginning of the trajectory can lead to completely different and unexpected results. This chaotic behavior, governed by complex mathematical maps, gives the system an exceptional ability to generate sequences characterized by randomness and unpredictability. This system relies on variables x, y, z with the values of these variables being randomly selected from the interval [0,1] each time. In other words, each time the system is run, the starting values of the variables can be selected at random from this field. The modified Lorenz equation [18] as follows:

$$x = (\alpha - 1) * (y - x) \quad (1)$$
$$y = x * (\rho - z) - y \quad (2)$$
$$z = x * y - \beta * z + x \quad (3)$$

In this paper, the improved Lorenz system was used because it is more chaotic and more complex with and $\alpha = 10, \rho = 28, \beta = {}^{8}/_{3}$. The purpose of using Lorenz is to generate a random, chaotic map of the locations of values that will be selected from the image to hide data, making it more difficult to access or detect the locations of the modified pixels in the image and to know their correct order.

4 Proposed ℕ𝕄TR-Stego System

The proposed ℕ𝕄TR-Stego system relies on combining a new, highly secure algebraic encryption system with image hiding using a specific technique. The proposed system consists of four phases: cryptography, Steganography, text retrieval, and decryption, as follows:

4.1 Cryptography (ℕ𝕄TR Cryptosystem)

Define a new algebra over field F is said to be NinMat which denoted by ℕ𝕄 as below:

Assume a set

$$\mathbb{NM} = \left\{ \begin{bmatrix} a_0 & a_1 & a_2 \\ a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 \end{bmatrix} \middle| a_i \in F \, , for\ all\ i = 0, \dots, 8 \right\},$$

let $\mathcal{A}, \mathcal{B} \in \mathbb{NM}$ and $\delta \in F$ such that

$$\mathcal{A} = \begin{bmatrix} \eth_0 & \eth_1 & \eth_2 \\ \eth_3 & \eth_4 & \eth_5 \\ \eth_6 & \eth_7 & \eth_8 \end{bmatrix}, \mathcal{B} = \begin{bmatrix} \Im_0 & \Im_1 & \Im_2 \\ \Im_3 & \Im_4 & \Im_5 \\ \Im_6 & \Im_7 & \Im_8 \end{bmatrix}$$

then the addition$(+)$, scalar multiplication$(\circ)$ and multiplication $(*)$ define on ℕ𝕄 as follows:

$$\mathcal{A} + \mathcal{B} = \begin{bmatrix} \eth_0 + \Im_0 & \eth_1 + \Im_1 & \eth_2 + \Im_2 \\ \eth_3 + \Im_3 & \eth_4 + \Im_4 & \eth_5 + \Im_5 \\ \eth_6 + \Im_6 & \eth_7 + \Im_7 & \eth_8 + \Im_8 \end{bmatrix} \quad (4)$$

$$\delta \circ \mathcal{A} = \begin{bmatrix} \delta\eth_0 & \delta\eth_1 & \delta\eth_2 \\ \delta\eth_3 & \delta\eth_4 & \delta\eth_5 \\ \delta\eth_6 & \delta\eth_7 & \delta\eth_8 \end{bmatrix} \quad (5)$$

$$\mathcal{A} * \mathcal{B} = \begin{bmatrix} \eth_0 \cdot \Im_0 & \eth_1 \cdot \Im_1 & \eth_2 \cdot \Im_2 \\ \eth_3 \cdot \Im_3 & \eth_4 \cdot \Im_4 & \eth_5 \cdot \Im_5 \\ \eth_6 \cdot \Im_6 & \eth_7 \cdot \Im_7 & \eth_8 \cdot \Im_8 \end{bmatrix} \quad (6)$$

respectively.

Now, let's design the ℕ𝕄TR cryptosystem based on the ℕ𝕄 algebra with positive integers parameters N, q and p having $gcd(q, p) = 1$ and satisfy the equation $q > (6d + 1)p$ where d is the number of coefficients. Consider the truncated polynomial rings $\mathcal{F} \cong Z[x]/(x^N - 1)$, $\mathcal{F}_p \cong Z_p[x]/(x^N - 1)$ and $\mathcal{F}_q \cong Z_q[x] / (x^N - 1)$, and three ℕ𝕄 algebras:

$$\mathcal{H} = \left\{ \begin{bmatrix} f_0(x) & f_1(x) & f_2(x) \\ f_3(x) & f_4(x) & f_5(x) \\ f_6(x) & f_7(x) & f_8(x) \end{bmatrix} \middle| f_i(x) \subset \mathcal{F} \, , i = 0, \dots, 8 \right\},$$

$\mathcal{H}_p \ and \ \mathcal{H}_q$ which defined similar to $\mathcal{H}$ but $f_i(x)$ belong to $\mathcal{F}_p \ and \ \mathcal{F}_q$ respectively. Define the six subsets $\ell_{\mathcal{A}}, \ell_{\mathcal{B}}, \ell_{\mathcal{C}}, \ell_{\mathcal{S}}, \ell_{\mathcal{T}}, \ell_m \subset \mathcal{H}$ by the form:

$$\ell_{\mathcal{A}} = \left\{ \mathcal{A} \in \mathcal{H} \middle| \begin{matrix} \eth_i, i = 0, \dots, 8 \ has \ d_{\eth_i} coffecient \ equal \ 1 \, , d_{\eth_i} - 1 \\ coffecient \ equal \ -1, other \ wise \ equal \ 0 \end{matrix} \right\},$$

$$\ell_{\mathcal{B}} = \left\{ \mathcal{B} \in \mathcal{H} \middle| \begin{matrix} b_i, i = 0, \dots, 8 \ has \ d_{\Im_i} coffecient \ equal \ 1, d_{\Im_i} \ coffecient \\ equal \ -1, other \ wise \ equal \ 0 \end{matrix} \right\}$$

$$\ell_m = \left\{ m \in \mathcal{H} \middle| coffecient \ of \ m_i, i = 0, \dots, 8 \ \text{lies in interval} \ (\frac{-p}{2} \, , \frac{p}{2}] \right\}$$

$, \ell_{\mathcal{C}}, \ell_{\mathcal{S}} \ and \ \ell_{\mathcal{T}}$ which define similar to $\ell_{\mathcal{B}}$. The phases of ℕ𝕄TR are explained as follows:

I. Key generation

The recipient selects three polynomials $\mathcal{A}, \mathcal{B}$ and $\mathcal{C}$ from $\ell_{\mathcal{A}}, \ell_{\mathcal{B}}$ and $\ell_{\mathcal{C}}$ respectively, $\mathcal{A}$ must have inverse modulo p. After that calculate the public key $\mathcal{Z}$ by the formula:

$$\mathcal{Z} \cong \mathcal{A}_p^{-1} * (\mathcal{B} * \mathcal{C}) \ (mod\ q) \tag{7}$$

where $\mathcal{A}, \mathcal{B}$ and $\mathcal{C}$ are private keys.

II. Encryption

After the sender obtain public key $\mathcal{Z}$ from the recipient, The sender write the message m as the element in ℓ_m and select privet key $\mathcal{S}, \mathcal{T}$ from $\ell_{\mathcal{S}}, \ell_{\mathcal{T}}$ respectively. The ciphertext is calculated following:

$$\mathbb{E} \equiv p(\mathcal{Z} * \mathcal{S} + \mathcal{T}) + m \ (mod\ q) \tag{8}$$

with coefficient lies in the interval $(\frac{-q}{2}, \frac{q}{2}]$.

4.2 Steganography

The sender follows these steps on the encrypted message $\mathbb{E}$:

Step 1: Convert the ciphertext $\mathbb{E}$ from polynomials to binary using ASCII encoding.

Step 2: Select a BMP image (to ensure no data loss during compression).

Step 3: Apply a Floyd filter to the selected image to remove some noise, which helps adjust the image pixels in a way that matches their original colors. This ensures the adjustments are invisible to the naked eye and undetectable by statistical analysis tools.

Step 4: Select chaotic locations based on the Lorenz system.

Step 5: Combine the binary system from Step 1 with the image data using the least significant bit (LSB).

4.3 Retrieval

After the recipient receives an image containing hidden data, it takes the following steps:

Step 1: Locates the data hiding points after the sender shares the x, y, and z keys.

Step 2: Obtains a binary system using the least significant bit (LSB).

Step 3: Converts the binary system to polynomials using ASCII bits.

Step 4: Converts the polynomials to algebraic elements ϽM.

In step 4, the recipient receives a ciphertext $\mathbb{E}$.

4.4 Decryption

In order for the recipient to receive the explicit message, the following steps must be taken:

$$\mathcal{K} \equiv \mathcal{A} * \mathbb{E} \ \equiv \mathcal{A} * (p(\mathcal{Z} * \mathcal{S} + \mathcal{T}) + m) \ (mod\ q)$$
$$\equiv \mathcal{A} * (p\big((\mathcal{A}_p^{-1} * (\mathcal{B} * \mathcal{C})) * \mathcal{S} + \mathcal{T}\big) + m) \ (mod\ q)$$
$$\equiv p\big((\mathcal{B} * \mathcal{C}) * \mathcal{S} + \mathcal{A} * \mathcal{T}\big) + \mathcal{A} * m \ (mod\ q) \tag{9}$$

where the coefficient lie in the interval $(\frac{-q}{2}, \frac{q}{2}]$.

Now, transform $\mathcal{K}(mod\ q)$ to $(mod\ p)$ to obtain

$$У \equiv \mathcal{K}(mod\ p) \equiv p((\mathcal{B} * \mathcal{C}) * \mathcal{S} + \mathcal{A} * \mathcal{T}) + \mathcal{A} * m(mod\ p)$$
$$\equiv \mathcal{A} * m(mod\ p). \tag{10}$$

Therefore, $m \equiv \mathcal{A}_p^{-1} * У \ (mod\ p)$ with coefficient lies in interval $(\frac{-p}{2}, \frac{p}{2}]$.

5 Illustrative examples

I- Cryptography

Let $(N, p, q) = (9,3,59)$, $d_a = d_b = d_c = d_s = d_t = 4$.

1. Key generation

The recipient selects $\mathcal{A} = \begin{bmatrix} a_0(x) & a_1(x) & a_2(x) \\ a_3(x) & a_4(x) & a_5(x) \\ a_6(x) & a_7(x) & a_8(x) \end{bmatrix}$, with

$$a_0(x) = 1 + x - x^2 - x^5 - x^6 + x^7 + x^8, \ a_1(x) = x - x^2 + x^3 - x^4 + x^5 + x^6 - x^7,$$

$$a_2(x) = 1 + x - x^2 - x^4 + x^5 + x^7 - x^8, a_3(x) = 1 - x + x^2 - x^3 + x^6 - x^7 + x^8,$$

$$a_4(x) = 1 - x^2 + x^4 - x^5 + x^6 - x^7 + x^8 \ , a_5(x) = 1 + x^2 - x^3 - x^4 + x^5 + x^6 - x^7,$$

$$a_6(x) = -1 - x^2 - x^3 + x^4 + x^5 + x^7 + x^8, a_7(x) = 1 + x - x^2 + x^3 + x^5 - x^6 - x^7,$$

$$a_8(x) = x - x^2 - x^3 + x^5 + x^6 - x^7 + x^8 \ ,$$

where $\mathcal{A}$ has inverse with respect to the modulo 3.

$$a_0{}^{-1}(x) = 2x + 2x^2 + 2x^3 + x^4 + x^5 + x^7 + x^8, \ a_1{}^{-1}(x) = 2x^4 + x^6 + x^8,$$

$$a_2{}^{-1}(x) = x + 2x^2 + 2x^3 + 2x^4 + x^5 + 2x^8, a_3{}^{-1}(x) = 2 + x^2 + 2x^3 + 2x^4 + 2x^5 + x^6 + x^7 + x^8,$$

$$a_4{}^{-1}(x) = 2x^3 + 2x^4 + 2x^6 + 2x^7 + 2x^8, a_5{}^{-1}(x) = 2 + 2x + 2x^2 + 2x^3 + x^4 + x^5 + x^6 + 2x^8,$$

$$a_6{}^{-1}(x) = 1 + 2x + x^2 + 2x^3 + 2x^4 + 2x^6 + x^7 + 2x^8, \ a_7{}^{-1}(x) = 1 + x + 2x^3 + 2x^4 + x^5 + x^6 + 2x^8,$$

$$a_8{}^{-1}(x) = 1 + x + 2x^3 + x^4 + x^5 + 2x^7 + 2x^8,$$

after that the recipient select $\mathcal{B}$ and $\mathcal{C}$ such that:

$$b_0(x) = 1 - x^2 - x^3 + x^4 - x^5 + x^6 + x^7 - x^8, b_1(x) = x + x^2 - x^3 - x^4 + x^5 - x^6 + x^7 - x^8,$$

$$b_2(x) = 1 - x - x^2 + x^3 - x^4 - x^5 + x^7 + x^8, b_3(x) = 1 - x - x^2 - x^4 + x^5 - x^6 + x^7 + x^8,$$

$$b_4(x) = 1 - x - x^2 + x^3 + x^5 - x^6 - x^7 + x^8, b_5(x) = -1 + x - x^2 + x^3 - x^4 - x^5 + x^6 + x^7,$$

$$b_6(x) = 1 - x - x^2 + x^3 + x^4 - x^6 - x^7 + x^8, b_7(x) = -1 - x - x^2 + x^3 + x^5 - x^6 + x^7 - x^8,$$

$$b_8(x) = 1 - x - x^2 + x^3 - x^4 - x^5 + x^6 + x^8, c_0(x) = 1 - x + x^2 - x^4 - x^5 + x^6 + x^7 - x^8,$$

$$c_1(x) = -1 + x - x^3 + x^4 - x^5 - x^6 + x^7 + x^8, c_2(x) = 1 + x + x^2 - x^3 - x^4 - x^5 - x^6 + x^8,$$

$$c_3(x) = 1 + x^2 - x^3 + x^4 - x^5 - x^6 + x^7 - x^8, c_4(x) = x - x^2 - x^3 + x^4 - x^5 + x^6 - x^7 + x^8,$$

$$c_5(x) = -1 - x + x^2 - x^4 + x^5 + x^6 - x^7 + x^8, c_6(x) = -1 + x - x^2 + x^3 - x^4 - x^5 + x^6 + x^8,$$

$$c_7(x) = 1 + x - x^2 - x^3 + x^4 - x^5 + x^6 - x^7, c_8(x) = 1 - x - x^2 + x^3 + x^5 - x^6 - x^7 + x^8,$$

after that calculate $\mathcal{Z} \equiv \mathcal{A}^{-1} * \mathcal{B} * \mathcal{C} (mod\ 3)$, where

$$z_0(x) = x + 2x^4 + x^5 + 2x^8, z_1(x) = 2 + 2x + 2x^2 + x^3 + x^4 + x^5,$$

$$z_2(x) = 2 + 2x + x^4 + 2x^5 + x^6 + x^8, z_3(x) = 1 + 2x + 2x^3 + 2x^5 + x^7 + x^8,$$

$$z_4(x) = 1 + x^4 + x^5 + 2x^6 + 2x^7 + 2x^8, z_5(x) = x + 2x^2 + 2x^3 + 2x^4 + 2x^5 + x^6 + 2x^8,$$

$$z_6(x) = x + x^2 + x^3 + 2x^5 + x^6 + x^7 + 2x^8, z_7(x) = 1 + x + 2x^2 + x^3 + 2x^4 + 2x^5 + x^6 + 2x^8,$$

$$z_8(x) = 2x + 2x^2 + 2x^3 + 2x^4 + x^6 + 2x^7 + x^8.$$

2. Encryption

The sender writes the massage "Mathematics" and convert to the binary system by bit ASCIL-7 code for binary representations.

1001101 1100001 1110100 1101000 1100101 1101101 1100001 1110100 1101001 1100011 1110011

Therefore, convert the binary system to polynomial m where

$$m_0(x) = 1 + x^3 + x^4 + x^6 + x^7 + x^8, m_1(x) = x^4 + x^5 + x^6 + x^7, m_2(x) = 1 + x^3 + x^4 + x^6,$$

$$m_3(x) = x + x^2 + x^5 + x^7 + x^8, m_4(x) = 1 + x^2 + x^3 + x^5 + x^6 + x^7, m_5(x) = x^3 + x^4 + x^5 + x^6 + x^8,$$

$$m_6(x) = x^2 + x^3 + x^5 + x^8, m_7(x) = 1 + x + x^5 + x^6 + x^7 + x^8, m_8(x) = 1 + x^3 + x^4.$$

The sender selects $\mathcal{S}\ and\ \mathcal{T}$ such that:

$$s_0(x)Q = 1 + x + x^3 - x^4 - x^5 - x^6 + x^7 - x^8, s_1(x) = -1 - x + x^2 - x^4 - x^5 + x^6 + x^7 + x^8,$$

$$s_2(x) = 1 - x + x^2 + x^3 - x^4 + x^5 - x^7 - x^8, s_3(x) = 1 + x - x^2 - x^3 + x^5 - x^6 - x^7 + x^8,$$

$$s_4(x) = x - x^2 + x^3 - x^4 + x^5 + x^6 - x^7 - x^8, s_5(x) = 1 + x + x^2 - x^3 + x^4 - x^5 - x^6 - x^8,$$

$$s_6(x) = 1 + x + x^2 - x^3 - x^4 - x^5 + x^6 - x^7, s_7(x) = -1 + x^2 - x^3 - x^4 - x^5 + x^6 + x^7 + x^8,$$

$$s_8(x) = x - x^2 + x^3 - x^4 + x^5 - x^6 + x^7 - x^8, t_0(x) = 1 - x - x^2 + x^3 + x^5 - x^6 - x^7 + x^8,$$

$$t_1(x) = 1 + x + x^2 - x^3 - x^4 - x^5 + x^6 - x^7, t_2(x) = 1 + x - x^2 - x^3 + x^4 - x^5 - x^7 + x^8,$$

$$t_3(x) = -1 + x - x^2 + x^3 - x^4 - x^5 + x^6 + x^8, t_4(x) = 1 - x - x^2 + x^3 - x^4 - x^5 + x^7 + x^8,$$

$$t_5(x) = -1 + x^2 - x^3 - x^4 - x^5 + x^6 + x^7 + x^8, t_6(x) = 1 + x - x^2 - x^4 - x^5 + x^6 - x^7 + x^8,$$

$$t_7(x) = x - x^2 + x^3 + x^4 - x^5 - x^6 - x^7 + x^8, t_0(x) = 1 - x - x^2 + x^3 - x^4 + x^6 - x^7 + x^8,$$

respectively.

Compute $\mathbb{E} \equiv p(\mathcal{Z} * \mathcal{S} * \mathcal{T}) + m\ (mod\ 59)$,

$$e_0(x) = 59 + 50x + 9x^2 + 54x^3 + x^4 + 3x^5 + 4x^6 + 54x^7 + 10x^8,$$

$$e_1(x) = 6 + 6x^2 + 54x^4 + 42x^5 + 57x^6 + 4x^7 + 12x^8,$$

$$e_2(x) = 1 + 9x + 57x^3 + x^4 + 56x^5 + 4x^6 + 53x^7,$$

$$e_3(x) = 7x + 57x^2 + 56x^3 + 3x^4 + 54x^5 + 6x^6 + 51x^7 + 7x^8,$$

$$e_4(x) = 10 + x^2 + 7x^3 + 56x^4 + 57x^5 + 51x^6 + x^7,$$

$$e_5(x) = 50 + 53x + 50x^2 + 10x^3 + x^4 + 4x^5 + 16x^6 + 56x^7 + x^8,$$

$$e_6(x) = 3 + 56x + 57x^2 + 57x^3 + 53x^4 + 4x^5 + 56x^6 + 6x^7 + 7x^8,$$

$$e_7(x) = 54 + 13x + 9x^3 + 51x^5 + 57x^6 + x^7 + 57x^8,$$

$$e_8(x) = 4 + 50x + 3x^2 + 57x^3 + 4x^4 + 56x^7 + 6x^8,$$

II- Steganography

Convert $\mathbb{E}$ to binary system chain by ASCII,

0111011 0110010 0001001 0110110 0000001 0000011 0000100 0110110 0001010 0000110 0000000 0000110

0000000 0110110 0101010 0111001 0000100 00011000000001 0001001 0000000 0111001 0000001 0111000 0000100 0110101 0000000 0000000 0000111 0111001 0111000 0000011 0110110 0000110 0110011 00001110001010 0000000 0000001 0000111 0111000 0111001 0110011 0000001 00000000110010 0110101 0110010 0001010 0000001 0000100 0010000 0111000 00000010000011 0111000 0111001 0111001 0110101 0000100 0111000 0000110 00001110110110 0001101 0000000 0001001 0000000 0110011 0111001 0000001 01110010000100 0110010 0000011 0111001 0000100 0000000 0000000 0111000 0000110

with size $(63 * N) = (63 * 9) = 567$.

Select a BMP image (to ensure no data loss during compression)

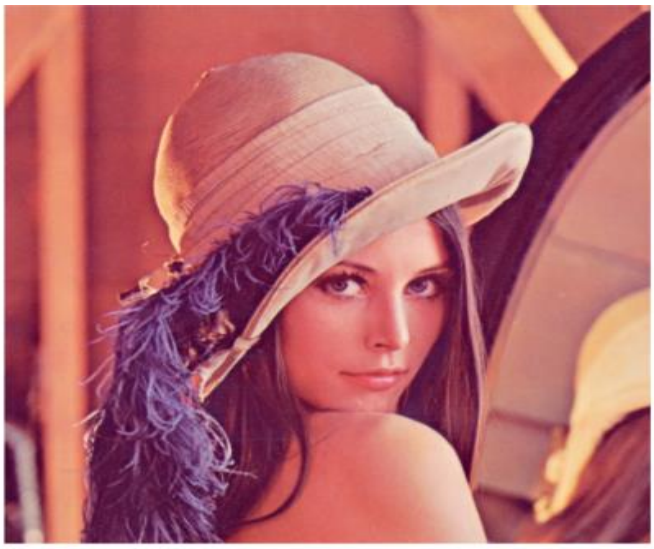

Figure 1: Original image.

We apply the Floyd filter to the image in Figure 1 to obtain the image in Figure 2.

Figure 2: Image after Floyd filter.

Select chaotic locations based on the Lorenz system and combine the binary system with the image data using the least significant bit (LSB).

Figure 3: Image after hiding.

III- Retrieval

After the recipient receives an image as shown in Figure 3, they proceed with the steps in section 5.3 to obtain the encrypted text $\mathbb{E}$.

IV- Decryption

The recipient compute $\mathcal{K} \equiv \mathcal{A} * \mathbb{E}\ (mod\ 59)$

$$k_0(x) = 17 + 38x + 50x^2 + 18x^3 + 48x^4 + 22x^6 + 4x^7 + 45x^8,$$

$$k_1(x) = 12 + 37x + 47x^2 + 19x^3 + 6x^4 + 15x^5 + 35x^6 + 10x^7,$$

$$k_2(x) = 2 + x + 21x^2 + 38x^3 + 5x^4 + 41x^5 + 15x^6 + 4x^7 + 54x^8,$$

$$k_3(x) = 44 + 26x + 32x^2 + 20x^3 + 37x^4 + 12x^5 + 2x^6 + 51x^7 + 17x^8,$$

$$k_4(x) = 16 + 44x + 8x^2 + 56x^3 + 13x^4 + 31x^5 + 7x^6 + 58x^7 + 9x^8,$$

$$k_5(x) = 47 + 36x + 3x^2 + 21x^3 + 48x^4 + 24x^5 + 43x^7 + 19x^8,$$

$$k_6(x) = 46 + 46x + 46x^2 + 13x^3 + 22x^4 + 3x^5 + 19x^6 + 2x^7 + 43x^8,$$

$$k_7(x) = 40 + 53x + 22x^2 + 2x^3 + 21x^4 + 38x^5 + 19x^6 + 58x^7 + 48x^8,$$

$$k_8(x) = 58 + 10x + 34x^2 + 9x^3 + 7x^4 + 16x^5 + 43x^6 + 51x^7 + 11x^8,$$

All the coefficient lies in the interval $(\frac{-59}{2}, \frac{59}{2}]$.

$$k_0(x) = 17 - 21x - 9x^2 + 18x^3 - 11x^4 + 22x^6 + 4x^7 - 14x^8,$$

$$k_1(x) = 12 - 22x - 12x^2 + 19x^3 + 6x^4 + 15x^5 - 24x^6 + 10x^7,$$

$$k_2(x) = 2 + x + 21x^2 - 21x^3 + 5x^4 - 18x^5 + 15x^6 + 4x^7 - 5x^8,$$

$$k_3(x) = -15 + 26x - 27x^2 + 20x^3 - 22x^4 + 12x^5 + 2x^6 - 8x^7 + 17x^8,$$

$$k_4(x) = 16 - 15x + 8x^2 - 3x^3 + 13x^4 - 28x^5 + 7x^6 - x^7 + 9x^8,$$

$$k_5(x) = -12 - 23x + 3x^2 + 21x^3 - 11x^4 + 24x^5 - 16x^7 + 19x^8,$$

$$k_6(x) = -13 - 13x - 13x^2 + 13x^3 + 22x^4 + 3x^5 + 19x^6 + 2x^7 - 16x^8,$$

$$k_7(x) = -19 - 6x + 22x^2 + 2x^3 + 21x^4 - 21x^5 + 19x^6 - x^7 - 11x^8,$$

$$k_8(x) = -1 + 10x - 25x^2 + 9x^3 + 7x^4 + 16x^5 - 16x^6 - 8x^7 + 11x^8,$$

Compute $\mathcal{N} \equiv \mathcal{K}(mod\ 3)$,

$$n_0(x) = 2 + x^4 + x^6 + x^7 + x^8, n_1(x) = 2x + x^3 + x^7, n_2(x) = 2 + x + 2x^4 + x^7 + x^8,$$

$$n_3(x) = 2x + 2x^3 + 2x^4 + 2x^6 + x^7 + 2x^8, n_4(x) = 1 + 2x^2 + x^4 + 2x^5 + x^6 + 2x^7,$$

$$n_5(x) = x + x^4 + 2x^7 + x^8, n_6(x) = 2 + 2x + 2x^2 + x^3 + x^4 + x^6 + 2x^7 + 2x^8,$$

$$n_7(x) = 2 + x^2 + 2x^3 + x^6 + 2x^7 + x^8, n_8(x) = 2 + x + 2x^2 + x^4 + x^5 + 2x^6 + x^7 + 2x^8,$$

In the final, calculate $m \equiv \mathcal{A}^{-1} * \mathcal{N}(mod\ 3)$

$$m_0(x) = 1 + x^3 + x^4 + x^6 + x^7 + x^8, m_1(x) = x^4 + x^5 + x^6 + x^7, m_2(x) = 1 + x^3 + x^4 + x^6,$$

$$m_3(x) = x + x^2 + x^5 + x^7 + x^8, m_4(x) = 1 + x^2 + x^3 + x^5 + x^6 + x^7,$$

$$m_5(x) = x^3 + x^4 + x^5 + x^6 + x^8, m_6(x) = x^2 + x^3 + x^5 + x^8, m_7(x) = 1 + x + x^5 + x^6 + x^7 + x^8,$$

$m_8(x) = 1 + x^4 + x^5$, where all coefficients of the last term lie in the interval $(\frac{-3}{2}, \frac{3}{2}] = (-1,1]$.

Convert the polynomial to binary after that obtain the original message text using ASCLL-7 code, hence the text is "Mathematics",

6 Analysis of results

This section presents the security level of the proposed system, which consists of several layers in terms of cryptography and steganography, as follows:

1- The security level of the Nitro encryption method, which involves one of two paths. The first path depends on the sample space of the $\mathcal{B}$ and $\mathcal{C}$ in the public key. Assuming that the size of the two sets $\ell_{\mathcal{B}}$ and $\ell_{\mathcal{C}}$ is smaller than $\ell_{\mathcal{A}}$ Therefore, the security size is as follows:

$$\left(\frac{N!}{(d_b!)^2(N-2d_b)!}\right)^9 \left(\frac{N!}{(d_c!)^2(N-2d_c)!}\right)^9 = \frac{(N!)^{18}}{((d_b!)^2(N-2d_b)!(d_c!)^2(N-2d_c)!)^{18}}.$$

The second path depends on the size for the keys $\mathcal{S}$ and $\mathcal{T}$ of ciphertext; therefore, the security size will be as follows:

$$\left(\frac{N!}{(d_s!)^2(N-2d_s)!}\right)^9 \left(\frac{N!}{d_t!(d_t-1)!(N-2d_t+1)!}\right)^9 = \frac{(N!)^{18}}{(d_t!)^{18}\left((N-2d_s)!d_t!(d_t-1)!(N-2d_t+1)!\right)^9}.$$

2- Hiding encrypted data, where the hiding mechanism relied on the following:

I- Applying the Floyd dithering filter to the image:

This type of filter was applied to the image to make the locations of the modified pixels difficult to detect. It distributes uniform noise (similar to random noise) throughout the image, making it challenging for statistical analysis to detect differences before and after modification (hiding). The modifications were naturally hidden within the image, making it difficult to distinguish between the modified and original pixels, as shown in Figures 4. Furthermore, the filter's flexibility in allowing any image shape and hiding at any pixel location provided the freedom to choose any pixel location for hiding.

with statistical measures of the difference between the two images are as follows:

MSE: 0.000342, PSNR: 82.790 dB, SSIM: 1.000000

MBCI (Mean number of variable bits per channel/pixel): 0.000342.

II- Selecting the modified bit within each pixel:

After representing the image and the encoded text in binary, the LSB principle was used (i.e., the last bit of each pixel was modified), which is called semi-transparent or pure hiding. This does not cause a noticeable change in the image due to the similarity that may occur between the encoded text bit and the image bit.

Figure 4: Image before and after hiding.

III- Selecting pixel locations in the modified image:

This proposal relies on a chaotic matrix of the modified locations, deviating from the usual sequential order. This is achieved using modified Lorenz equations, which yielded a reliable, unpredictable chaotic path based on the obtained measurements (According to Lyapunov's chaos criteria (0.83004, 0.0010723, and -13.4978), the system is sensitive to even the slightest change in the initial value). Thus, if a single bit is detected, the attacker cannot determine the location of the preceding bit or predict the location of the following bit. This type of system is able to resist statistical steganalysis due to its randomness. Using a Lorenz system leads to resistance to identifying the modified LSB in the image, which in turn resists histogram/chi-square tests. The high PSNR value obtained by the proposed system indicates the imperceptibility of detecting the locations of the modified pixels through visual attacks. Furthermore, the modified chaotic system adopted is sensitive to even the slightest change, which leads to resistance to analytical attacks.

It is noticeable that the larger the image used to hide the encrypted data, the more complex it becomes, in addition to increasing the amount of encrypted data that can be hidden or stored in the image.

7 Merits of the ℕMTR-Stego System

One of the most important advantages of this proposed system is its multi-stage approach, which results in a very high level of security and complexity, thus enhancing the method's efficiency. The original text cannot be directly accessed from the ciphertext because the system's first stage is encryption, achieved through the design of a multi-dimensional algebraic encryption system. This stage consists of key generation and encryption. The second stage is hiding, which involves using an image with a filter and implementing Lorenz. The third stage is retrieval, which aims to obtain the ciphertext through several steps, including identifying hiding locations and using the least significant bit. The fourth stage is decryption, which converts the ciphertext back into the original text. Another advantage of this system is its ability to encrypt multiple messages, whether from multiple sources or a single source, due to the multidimensional algebraic intent used in constructing the ℕMTR method.

Conclusions

This paper is based on the principle of double protection. While encryption serves as the first line of defense by altering the fundamental structure of the data to make it unintelligible, steganography comes as a security cover that conceals the existence of the data itself within images. The innovative combination of these two approaches raises the level of security to unprecedented levels, which is reflected in this work through the employment of NM cryptosystem and NinMat algebra algorithms to ensure superior content encryption. To enhance this system, the research relied on the Lorenz system with its high chaotic capabilities to generate unpredictable paths, combined with the LSB technique in the spatial domain to ensure precise data embedding within the cover. Additionally, Floyd–Steinberg Dithering was integrated to distribute color errors and improve the visual quality of the resulting image, reducing the likelihood of detection. This integration makes the proposed method an effective solution that surpasses traditional techniques in addressing contemporary hacking challenges in sensitive applications such as secure communications, intellectual property protection, and data transmission over untrusted channels.

References

[1] Silman, J. Steganography and Steganalysis: An Overview. *SIANS Institute*, (2001).
[2] Jamil, T. Steganography: The art of hiding information is plain sight. *IEEE Potentials* **18**, 1–12 (1999).
[3] Kurak C. & McHugh J. A cautionary note on image downgrading. *Proc. 8th IEEE Annu. Comput. Secur. Appl. Conf.*, 153–159 (1992).
[4] Cachin C. An Information-Theoretic Model for Steganography. *Inf. Comput.* **192**, 306–318 (2004).

[5] Channalli S. &Jadhav A. A Steganography: An Art of Hiding Date. *Int. J. Comput. Sci. Eng.* **1**, 141–137 (2009).
[6] Mazurczyk W. & Caviglione L. Steganography in modern smartphones and mitigation techniques. *IEEE Commun. Surv. Tutor.* **16**, 334–357 (2014).
[7] Liu Y., Liu S., Wang Y. & Zhao H., Video steganography: A review. *Neurocomputing* **335**, 238–250 (2019).
[8] Kaur C., Singh S., Kaur M. & Lee H. A Systematic Review of Image Steganography Approaches. *Arch. Comput. Methods Eng.* **29**, 4505–4528 (2022).
[9] Badhan A. & Malhi S. S. A Review on Hybrid Cryptosystem. *Proc. 9th Int. Conf. Internet Everything Microw. Embed. Commun. Netw.* 1–7 (2024).
[10] Rebeen R. H. A. & D. H. A. Comparative Analysis of Flexiwan, OPNSense, and pfSense Cybersecurity Mechanisms in MPLS / SD-WAN Architectures. *Passer J. Basic Appl. Sci.* **6**, 27–32 (2024).
[11] Majeed N. D., Al-Askery A. J., Hasan F. S. & Abood S. A survey on steganography and image encryption techniques. *Electr. Eng. Tech. J.* **2**, 11–24 (2025).
[12] Dana. K. H., Foad S. M. & Firas A. A. Enhanced Security Taxonomy for Fog-Enabled VANETs: A Comprehensive Survey on Attacks, Challenges, Applications and Architectures. *Passer J. Basic Appl. Sci.* **7**, 37–61 (2025).
[13] Nahla A. Bashar M. N. Enhancing Biometric Security with Dynamic Chaotic Systems: A Narrative Review. *Passer J. Basic Appl. Sci.* **7**, 257–268 (2025).
[14] Saja S. M., Hind I. M., Nuha S. M., Nigar M. S. & Hayder Q. F. Future Directions in Artificial Intelligence for Cybersecurity: Emerging Trends and Key Developments. *Passer J. Basic Appl. Sci.* **8**, 400–409 (2026)
[15] Baranawal N., Sakpal H., Manoj P., Kadam K. & Kumar M. Steganography Hider System, *Int. J. Sci. Res. Eng. Trends*, **12**, 1–6 (2026).
[16] Floyd R. W. & Steinberg L. An adaptive algorithm for spatial greyscale. *Proc. Soc. Inf. Disp.* **17**, 77–75 (1976).
[17] Mischaikow K. & Mrozek M. Chaos in The Lorenz Equation: A Computer-Assisted proof. *Bull. Am. Math. Soc.* **32**, 66–72 (1995).
[18] Jawad N. H. & Abdulhadi S. Efficient Brakerski-Fan- Vercauteren Algorithm Using Hybrid-Position-Residues Number System. *Int. J. Math. Comput. Sci.* **20**, 549–553 (2025).