NUMERICAL METHODS PROJECT MA-203

Numerical Analysis of Encryption/Decryption using Chaos Theory

Encryption can be loosely described as the conversion of a data type or information that needs to be relayed over a transmission channel to some format that will be unrecognizable to any outside person. Encryption is an essential topic of study because it enables us to transmit data or information safely and privately without interference or eavesdropping.

Problem Statement:

This project aims to successfully encrypt and decrypt an image signal using the method of Chaos Theory. A theoretical and mathematical model of the encryption technique will be developed, and the resulting system of equations will be solved numerically on a computer. The specific objectives are presented below:

1. Develop an encryption technique using chaotic equations with suitable assumptions.
2. Derive the governing equations of chaos theory using first principle methods.
3. Formulate the initial conditions with an efficient numerical method for computation purposes.
4. Efficient computation algorithm to perform encryption and retrieving the original data using decryption algorithm.
5. Developing computational time efficient method.

Methodology:

Steps involved in encryption and decryption:

1. Import the image and split it into two images.
2. Generate the chaotic sequences using a chaotic equation developed using numerical method.
3. Adding a security key provides a second layer of encryption to the image.
4. Using the same set of logic decrypting the encrypted image to the original image.

Mathematical equations:

The Lorenz system ODE's are,

$$\frac{dx}{dt} = \sigma(y - x) \qquad (1)$$

$$\frac{dy}{dt} = \text{x}(\rho - z) - y \qquad (2)$$

$$\frac{dz}{dt} = xz - \beta y \qquad (3)$$

In the real world, these equations relate the properties of a two-dimensional fluid layer uniformly warmed from below and cooled from above.

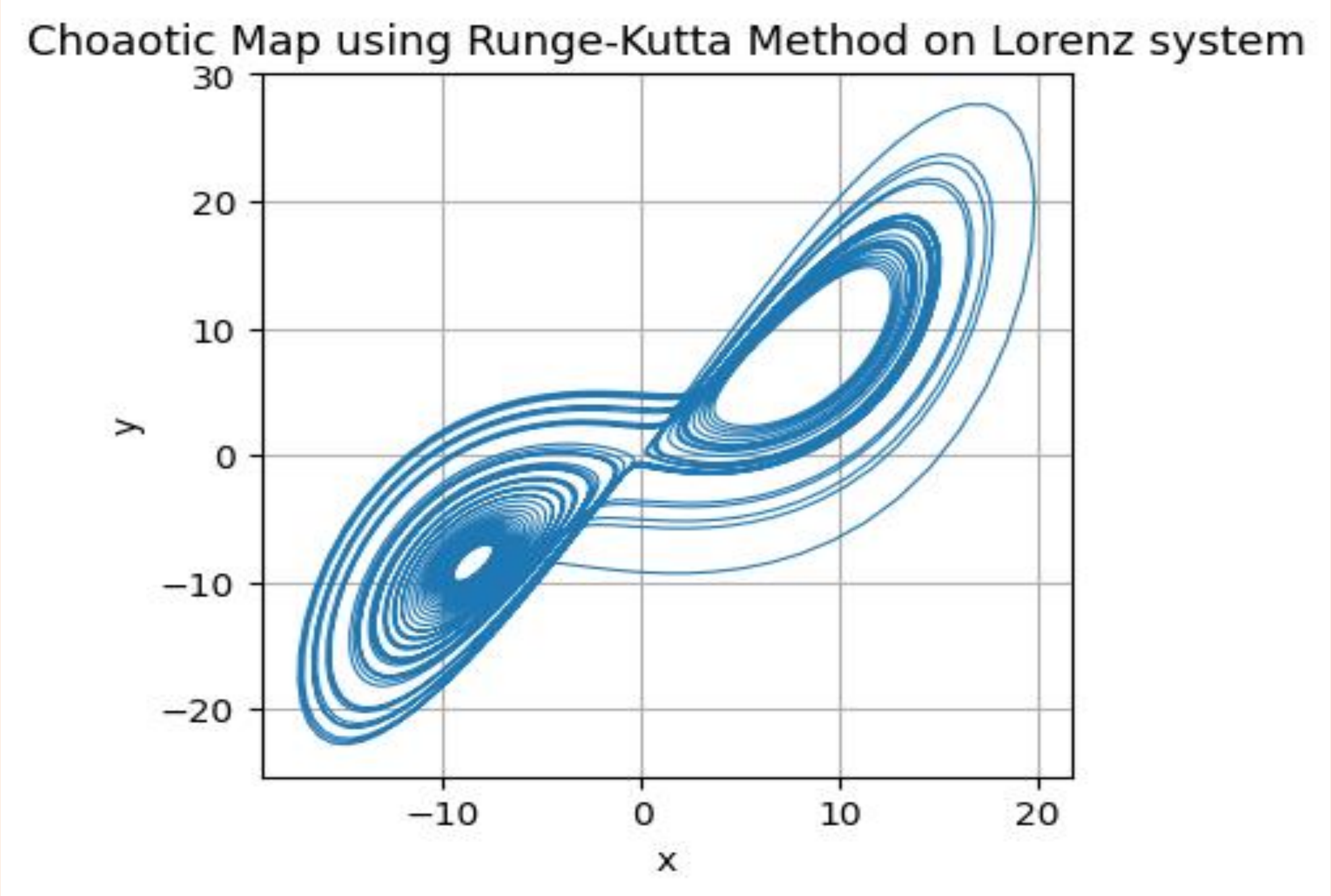
Here σ =10, ρ =28, β=8/3 are the constant system parameters

Numerical Method Used:

we have used Runge Kutta's fourth-order method to solve the equations. We have used this method because of its high accuracy compared to other numerical methods.

Runge Kutta's method is an iterative method, which includes the Euler method, for finding approximate solutions of nonlinear equations in each iteration.

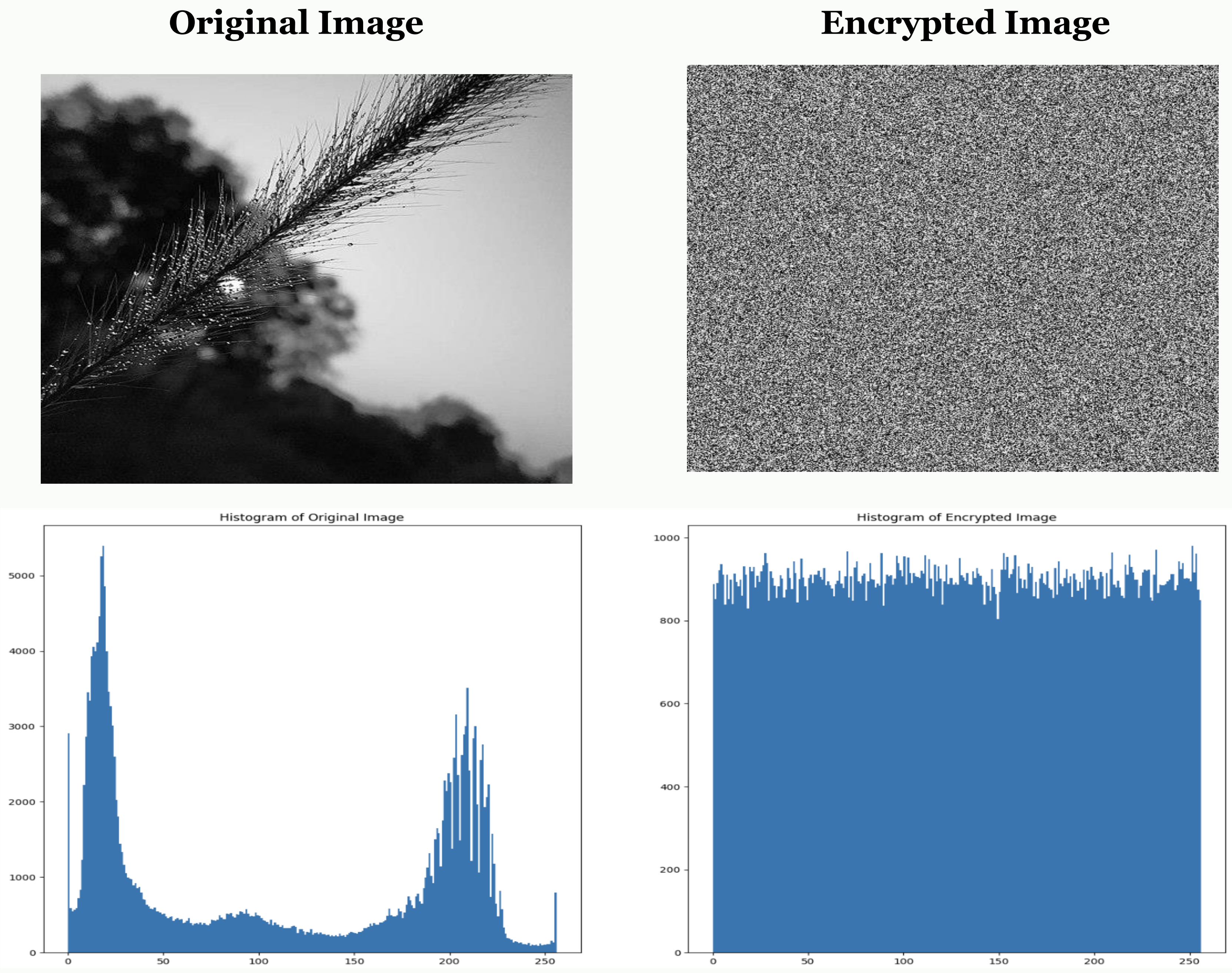
The numerical method is used here to develop the equations for the chaotic map which is used to develop the chaotic sequences to encrypt the original input image.



Group Members:

1. Aditya Kumar (22110015)
2. Archit Dhakar (22110031)
3. Aryan Sahu (22110031)

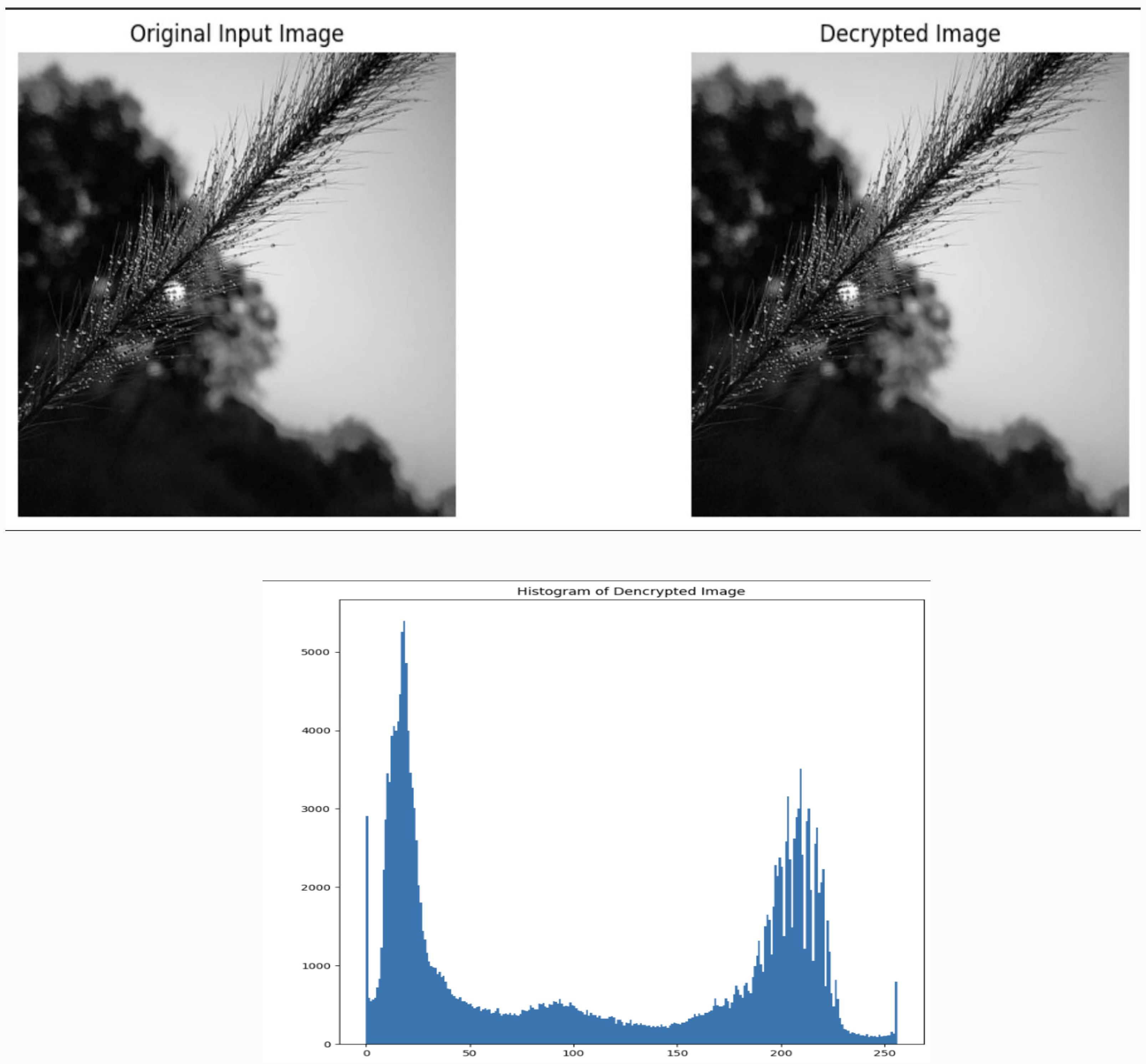
Results and Inferences:



Input image, encrypted image with histogram

Structural Similarity Index (SSIM): This parameter measures the pixel similarity between the input and decrypted images.

SSIR value for the original and decrypted image is 1.0, which indicates that our original and decrypted images are structurally similar.



Input image, decrypted image with histogram

Conclusion:

The encryption and decryption of images using chaotic functions derived from the Lorenz system and solved through Runge-Kutta's method provide a robust and secure approach to safeguarding sensitive image data. Using chaotic sequences as keys ensures high confidentiality, making it suitable for various applications, including secure image transmission and storage. However, managing and protecting the secret key for successful decryption and maintaining the system's security is essential.

References:

[1] Lorenz system of equations. Available online: Link

[2] DES encryptions method, Laissez Faire City Times, Vol 2, No. 28. Available: Link

[3] "Cryptography Introduction," GeeksforGeeks, 02-Nov-2018. [Online]. Available: Link

[4] "Chaos -- from Wolfram MathWorld," Wolfram MathWorld, 15-Mar-2006. [Online]. Available: Link