SCHOOL OF COMPUTER ENGINEERING

KALINGA INSTITUTE OF INDUSTRIAL TECHNOLOGY

BHUBANESWAR, ODISHA - 751024

May 2024

A PROJECT REPORT
on

"IMAGE ENCRYPTION USING CHAOTIC MAPS"

Submitted to

KIIT Deemed to be University

In Partial Fulfillment of the Requirement for the Award of

BACHELOR'S DEGREE IN

COMPUTER SCIENCE AND ENGINEERING

BY

Abhirup Chowdhury	**2105347**
Ankita Ghosh	**2105355**
Bhramari Sarkar	**2105364**
Sattwik Sen	**2105403**
Soumya Kanti Datta	**21051262**

UNDER THE GUIDANCE OF

DR. CHITTARANJAN PRADHAN

KIIT Deemed to be University

School of Computer Engineering
Bhubaneswar, ODISHA 751024

CERTIFICATE

This is certify that the project entitled

"**IMAGE ENCRYPTION USING CHAOTIC MAPS**"

submitted by

Abhirup Chowdhury	2105347
Ankita Ghosh	2105355
Bhramari Sarkar	2105364
Sattwik Sen	2105403
Soumya Kanti Datta	21051262

is a record of bonafide work carried out by them, in the partial fulfillment of the requirement for the award of Degree of Bachelor of Engineering (Computer Science & Engineering) at KIIT Deemed to be university, Bhubaneswar. This work is done during the year 2023-2024, under our guidance.

Date:02/04/2024

(Chittaranjan Pradhan)
Project Guide

ACKNOWLEDGEMENTS

We are profoundly grateful to **DR. CHITTARANJAN PRADHAN** of **Affiliation** for his expert guidance and continuous encouragement throughout to see that this project has reached its target since its commencement to its completion.

Abhirup Chowdhury
Ankita Ghosh
Bhramari Sarkar
Sattwik Sen
Soumya Kanti Datta

ABSTRACT

The rapid advancement of information technology and the creation of public communication networks, which facilitate the widespread transmission of digital images, have made secure communication a crucial concern over the past 20 years. In this paper, image encryption was achieved using chaotic map functions . The suggested algorithm divides the image into blocks and encrypts them using XOR operation and chaotic windows, exhibiting proper performance based on the experimental results. Additionally, the generated encrypted images have homogeneous histograms and a sizable key space. This algorithm's sufficiently large-enough NPCR and UACI show that it is resistant to differential attacks, in addition to being appropriate for noisy communication networks and potentially being made use of in parallel processing

Keywords: Chaotic Logistic Mapping, Pixel Shuffling, Matrix Multiplication, Substitution-Permutation Network (XOR)

CONTENTS

List of Figures

Chapter 1

Introduction

Digital images are now frequently transmitted around the globe via transmission media, so protecting them from leaks has become crucial in recent years. To store and transfer digital images, a variety of applications such as military image databases, secure video conferencing, medical imaging systems, cable TV, online personal photo albums, etc. need a dependable, quick, and strong security system. The development of strong encryption techniques is a result of the requirements to meet the security needs of digital images. Many encryption algorithms have been proposed in the literature over the past ten years, each based on a different principle. Among them, chaos-based encryption methods are thought to be useful for real-world applications since they offer a good balance of computational power, speed, high security, complexity, and reasonable computational overheads. Certain features of digital images include bulk data capacity, strong correlation between neighboring pixels, redundancy of data, and less sensitivity than text data that is, a slight change in any pixel's attribute does not significantly impair the image's quality.
Consequently, because they demand a significant amount of processing power and time, traditional ciphers like IDEA, AES, DES, and RSA are not appropriate for real-time picture encryption. 2ith a high degree of security features but a slow processing speed would be of limited utility.

There are several numbers of chaos-based encryption algorithms has been developed in recent years. Among this, we have discussed two algorithms in this paper-

a) Image Encryption Using Chaotic Logistic Map
b) Image Encryption Using Chaotic Lorenz System

.

Chapter 2

Basic Concepts/ Literature Review

Chaotic dynamics are used in chaotic maps to jumble an image's pixels in order to encrypt its content. Some of the key concept used in this process are

1. Chaotic Maps :-

1.1 Logistic functions:-
The logistic map is a mathematical formula that, when repeated under specific circumstances, displays chaotic behavior. The recurrence relation defines it.

$$ƒ(x) = r\ x\ (1 - x)$$

The logistic equation has a maximum of ¼r at ½ and is parabolic, similar to the quadratic mapping with $f(0) = f(1) = 0$. The width of the parabola remains constant while the height is altered by changing the parameter. (This differs from the quadratic mapping, which moves up or down while maintaining its general shape.)

1.2 Lorenz System:-The meteorologist Edward Lorenz identified three ordinary differential equations in 1963 that show chaotic behavior; these equations are collectively referred to as the Lorenz system. The dynamics of a simplified atmospheric convection model are described by these equations. Because of its fascinating behavior, the Lorenz system has been extensively studied in the fields of chaos theory and nonlinear dynamics.

Usually, the equations are expressed as follows:

$$dx/dt = \sigma(y - x)$$
$$dy/dt = x(\rho - z) - y$$
$$dz/dt = xy - \beta z$$

where σ, ρ, and β are parameters and x, y, and z are the state variables that represent the system's variables.

2.Key Generation :- Encryption keys are generated as a stream of pseudo-random numbers using a chaotic logistic map. The key to both encrypting and decrypting the image is found in the logistic map's initial conditions (seed) and parameters.

3.Pixel Scrambling :- The image's pixel locations are subjected to the chaotic dynamics produced by the logistic map. The logistic map generates a chaotic sequence that modifies the position of each pixel. The process of scrambling ensures that the image's spatial information is distorted, making it challenging for unauthorized users to understand the content.

4.Substitution-Permutation Network (SPN): To produce confusion and diffusion, SPN is a cryptographic structure that combines substitution and permutation operations. The chaotic sequence produced by the logistic map in the context of image encryption using chaotic logistic maps can be used to establish the sequence in which the substitution and permutation operations are applied to the image pixels.

Chapter 3

Problem Statement / Requirement Specifications

Background: Private and sensitive information can be found in images. They are important for a number of uses, such as medical imaging, remote sensing, and military communication. It is essential to safeguard this data against unauthorized use and alteration.

Goal: Create a reliable image encryption system that protects the integrity and confidentiality of image data while it is being transmitted and stored. While preventing unwanted access, the system should enable safe access and encryption of the images for authorized users.

3.1 Project Planning

The project's goal is to secure communication and protect data by implementing image encryption using the Lorenz System and Logistic Function. The project's objectives center on algorithm implementation, testing, and performance evaluation. Its scope includes the encryption of multiple image formats.

The timeline is split down into phases for testing, research, development, and documentation. Progress is monitored through the use of milestones. Software, and people resources are all needed, and jobs are assigned according to skill level and availability. Throughout the course of the project, potential obstacles are addressed through the development of risk management strategies.

The development plan lists tasks like using specific programming languages and frameworks to implement algorithms and integrate them with image processing libraries. Unit, integration, and system testing are among the testing methods used, and criteria are set for assessing the efficacy of encryption.

3.2 Project Analysis

The project analysis focuses on using the Lorenz System and Logistic Function for image encryption, which provides a special method of boosting security. These chaotic systems offer strong protection against unwanted access by supplying the unpredictable nature required for encryption. To guarantee a successful implementation, though, obstacles like

possible performance problems and the requirement for effective key management must be overcome.

The project shows viability in spite of these obstacles by carefully allocating resources and planning. The encryption technique's adaptability makes it possible to encrypt different kinds of images, which increases its use in a range of situations. Moreover, the project stands out from conventional encryption techniques due to its inventive use of chaotic systems, which may provide better security.
Thorough testing and optimization are necessary to improve performance without sacrificing security in order to mitigate issues. To properly protect encrypted data, strong key management procedures must also be set up.

To sum up, the project has great potential to advance image encryption methods and provide increased security for the transmission and storage of visual data. The project has the potential to make a significant contribution to the field of cryptography research and applications with careful planning and diligent execution.

3.3 System Design

3.3.1 Design Constraints

- **Design Constraints for Logistic Map**

- The encryption scheme must provide a high level of security by employing complex chaotic maps and cryptographic techniques to generate keys and mask the image content to prevent unauthorized access to image data.

- The encryption and decryption algorithms should be highly sensible to the encryption key.

- Strong encryption and decryption algorithms should be able to tolerate transmission errors or noise without affecting the quality of the decrypted image.

- The encryption scheme should be adaptable to security threats and technological advancement without disrupting existing systems or compromising security.

- The encryption and decryption process must be optimized to minimize computational overhead, ensuring fast performance.

- It should scale efficiently to encrypt and decrypt images regardless of their dimensions, ensuring versatility and reliability.

- **Design Constraints for Lorenz System**

- The encryption algorithm must ensure a high level of security to protect sensitive image data from unauthorized access or tampering.
- Strong encryption should withstand a variety of assaults, such as known-plaintext, statistical, and brute-force attacks.

- The encryption procedure ought to be resilient to a range of assaults, such as known-plaintext, statistical, and brute-force attacks.

- The encryption and decryption procedures should be computationally efficient to save processing time and provide security while still being feasible for real-time or almost real-time systems.

- Images of different sizes and formats should be handled by the encryption method scalable to avoid appreciable performance reduction.

- In order to enable a smooth integration of the encryption technique into current systems and applications, it should be compatible with popular image formats and platforms.

3.3.2 System Architecture OR Block Diagram

Block Diagram for Logistic Map System

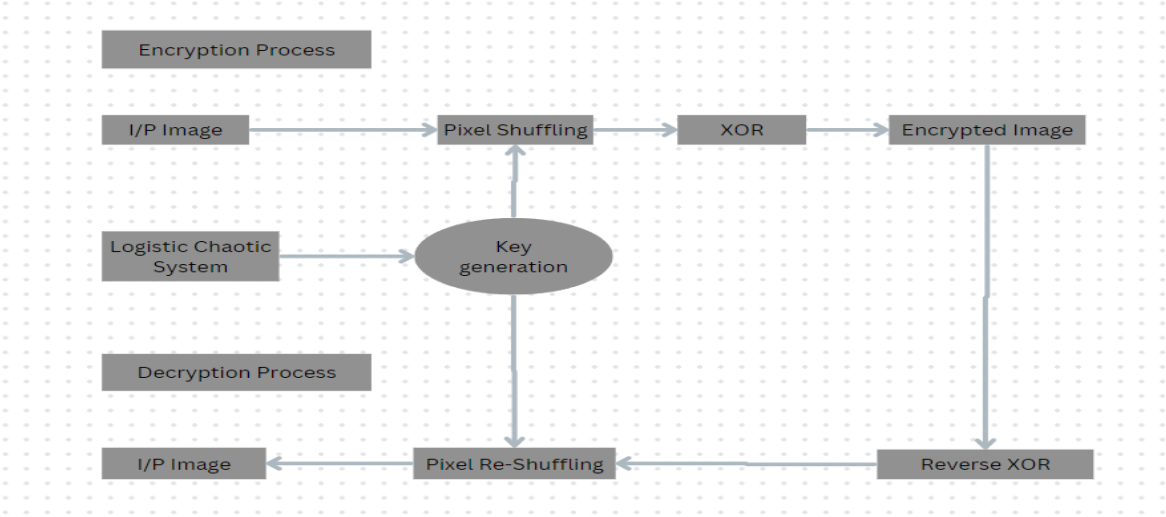
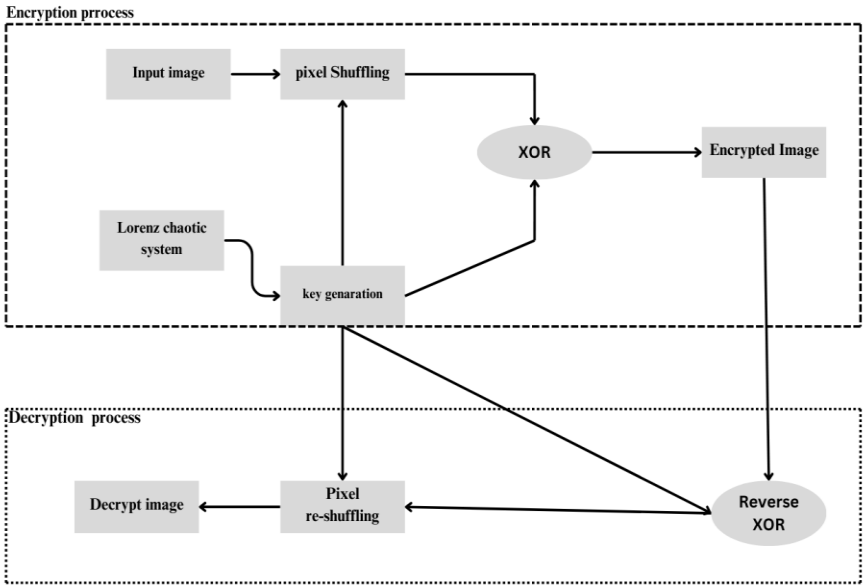


Fig:-1 Logistic Map

Block Diagram for Lorenz System



Lorenz system

Fig:-2

Chapter 4

Implementation

In this section, present the implementation done by you during the project development.

4.1 Methodology OR Proposal

- **Methodology for Logistic Map**

Image encryption using a logistic map involves using chaotic systems, specifically the logistic map, to generate pseudo-random numbers which are then used to scramble the pixels of an image.

Generation of Chaotic Sequence:

The logistic map generates a sequence of numbers that appears random but is deterministic. This sequence is obtained by iterating the logistic map equation over an initial value of (x0) and a chosen value of (r). The chaotic nature of this sequence makes it suitable for cryptographic purposes.

Key generation using Logistic Map:

Generate a secret key that includes parameters required for the logistic map equations. These parameters typically include the initial value(seed), the growth parameter(r), and the number of iterations(n) for generating pseudo-random numbers.

Initialize the logistic map with the seed value(x0) and the growth parameter(r). Iterate the logistic map equation for n iterations to generate a sequence of pseudo-random numbers. The logistic map equation is:

$$x_{n+1}=r*x_n*(1-x_n)$$

where:

- x_n is the current value of the logistic map
- x_{n+1} is the next value of logistic map
- r is the growth parameter.

Encryption Process using Logistic Map:

The encryption process involves using the chaotic sequence as a key to shuffle or permute the pixels of the image. This can be achieved through operations such as bitwise XOR, addition and subtraction between the pixel values and corresponding elements of the chaotic sequence.

The encryption process can be represented as:

$$C_i = P_i \text{ XOR } K_i$$

where:

- C_i is the encrypted pixel value.
- P_i is the original pixel value of the image
- K_i is the corresponding element of the chaotic sequence used as the encryption key.

Chaotic Behavior:-

The logistic map exhibits chaotic behavior when the growth rate parameter (r) is within certain ranges, typically (r\in(3.57,4]). In this range, the logistic map displays sensitive dependence on initial conditions , meaning small changes in the initial value(x0) can lead to significantly different trajectories of the chaotic sequence.

Decryption: To decrypt the image,the recipient needs the same secret key used for encryption. The decryption process involves reversing the encryption steps.

- **Methodology for Lorenz System**

Three ordinary differential equations (ODEs) that represent convection in the atmosphere in a simplified form are called the Lorenz system. For specific initial conditions and parameter values, it displays chaotic behavior, which means that even small changes in the initial state can have a significant impact on long-term results. This is a thorough mathematical justification:

$$dx/dt = \sigma(y - x)$$
$$dy/dt = x(\rho - z) - y$$
$$dz/dt = xy - \beta z$$

Where

- x, y, and z represent state variables, often interpreted as proportional to the rate of convection, horizontal temperature variation, and vertical temperature variation, respectively

- σ (sigma) is the Prandtl number, a dimensionless number representing the ratio of kinematic viscosity to thermal diffusivity.

- r is the Rayleigh number, another dimensionless number representing the ratio of buoyancy forces to viscous forces. It controls the intensity of convection.

- β (beta) is a dimensionless parameter representing the ratio of the container height to a characteristic horizontal length scale.

Physical Interpretation of Lorenz System:

- The first equation describes how the rate of convection (x) is influenced by the temperature difference between the horizontal layers (y - x). High σ (low thermal diffusivity) promotes a stronger influence of the temperature difference.

- The second equation represents the change in horizontal temperature variation (y). It includes three terms:

  - rx: The rate of convection (x) multiplied by r, which signifies the contribution of convection to the horizontal temperature variation. Higher r implies stronger convection and a larger impact.

  - y: A decay term for the horizontal temperature variation, representing heat loss to the surroundings.

  - xz: The interaction between the vertical temperature variation (z) and the rate of convection (x). This term captures the advection of heat by the convective flow.

- The third equation describes the change in vertical temperature variation (z). It is driven by the product of the horizontal and vertical temperature variations (xy), representing the transfer of heat between these layers. The term βz accounts for the dissipation of heat at the top and bottom boundaries.

Chaotic Behavior:-

The Lorenz system exhibits chaotic behavior when the Rayleigh number (r) exceeds a critical value (typically around 25.35 for $\sigma = 10$ and $\beta = 8/3$). In this chaotic

regime, even tiny differences in initial conditions lead to solutions that diverge exponentially over time. This means that small changes in the initial state of the system

can result in vastly different long-term outcomes, making accurate long-term predictions impossible.

Key Generation Using Lorenz System:-

As mentioned, the initial conditions for x, y, and z at a particular time (t0) are crucial for image encryption using the Lorenz system. These starting points are indicated as follows:

- x(t0)
- y(t0)
- z(t0)

The choice of these initial conditions significantly influences the generated chaotic sequence, which acts as the "encryption key."

Sensitivity to initial condition:-

The sensitivity of chaotic systems to initial conditions is one of their distinguishing features. This means that over time, significantly different chaotic sequences can result from even small changes in the initial values (x(t0), y(t0), and z(t0)). This can be stated mathematically as:

$$| \Delta x(t0) | \approx \exp(\lambda * t) | \Delta x(t0) |$$

Where:

- $\Delta x(t0)$ represents a small change in the initial value of x
- λ is a positive constant that characterizes the system's sensitivity (larger λ implies higher sensitivity)
- t is the time

This exponential dependence shows that even a minute change in the initial conditions can be amplified over time, resulting in a completely different chaotic sequence.

Limitation for secure Key generation

- **Guessing the initial condition:-** Due to the sensitivity of the Lorenz system, an attacker with some knowledge of the system and the encrypted image might be able to guess the initial conditions with sufficient effort. This could potentially lead to decrypting the image.

- **Limited key Space:-**The chaotic sequence generated by the Lorenz system, despite its seemingly random behavior, has a finite length determined by the chosen parameters and integration time. This translates to a finite number of possible keys, making the system vulnerable to brute-force attacks where an attacker tries all possible keys until they find the correct one.

Permutation and Combination: The chaotic sequence or bit stream is then used to manipulate the image data:

- **Permutation:** Randomly rearranging the order of pixels in the image.
- **Combination:** Replacing each pixel value with a new value based on the chaotic sequence (e.g., using XOR operation).

Decryption: Ideally, this involves reversing the encryption steps, requiring knowledge of the initial conditions and parameters used.

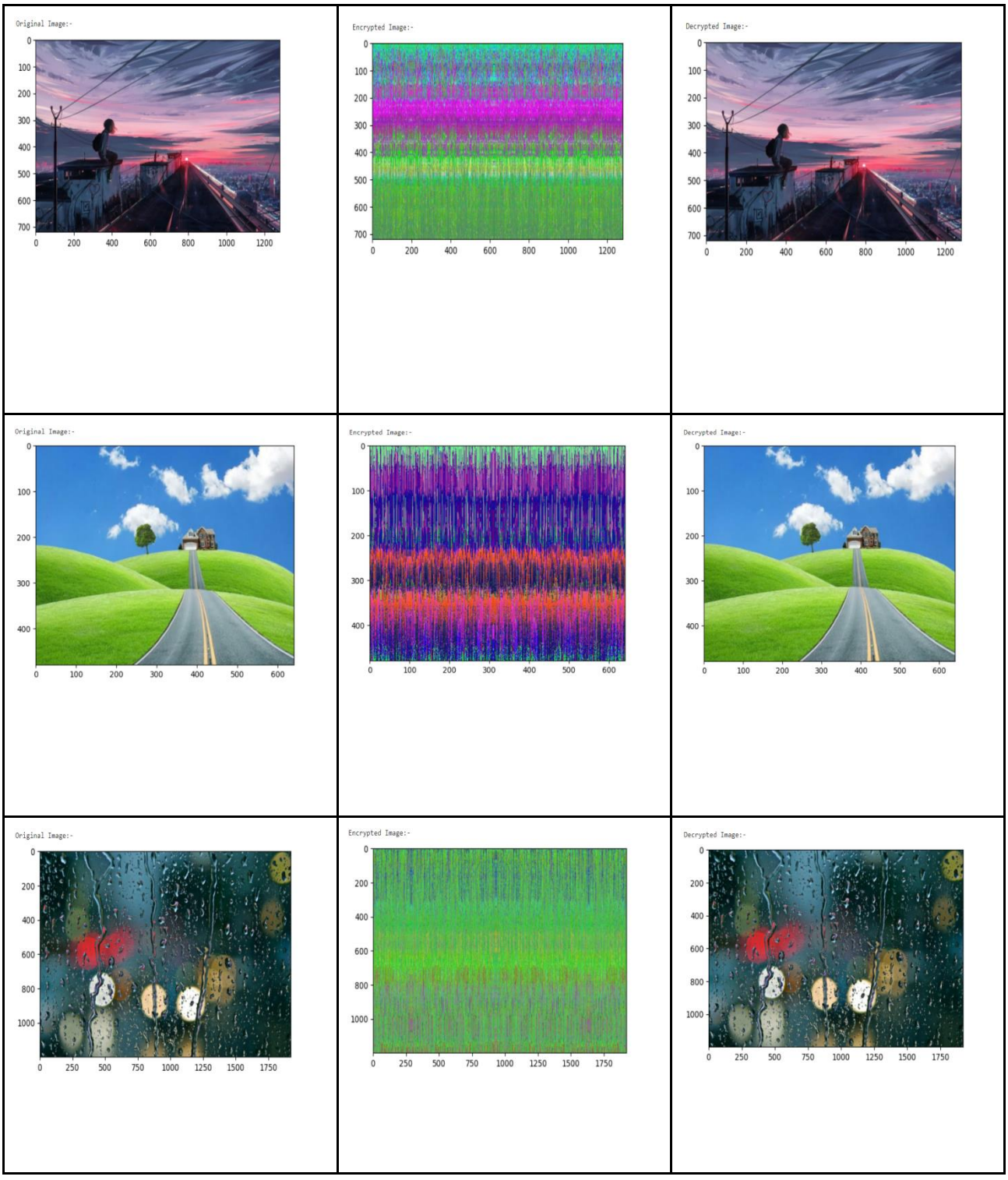
4.2 Testing OR Verification Plan

In this project of image encryption using chaotic maps, continuous testing has to be done to maintain the security of the image throughout the algorithm. This has been followed through these parameters.

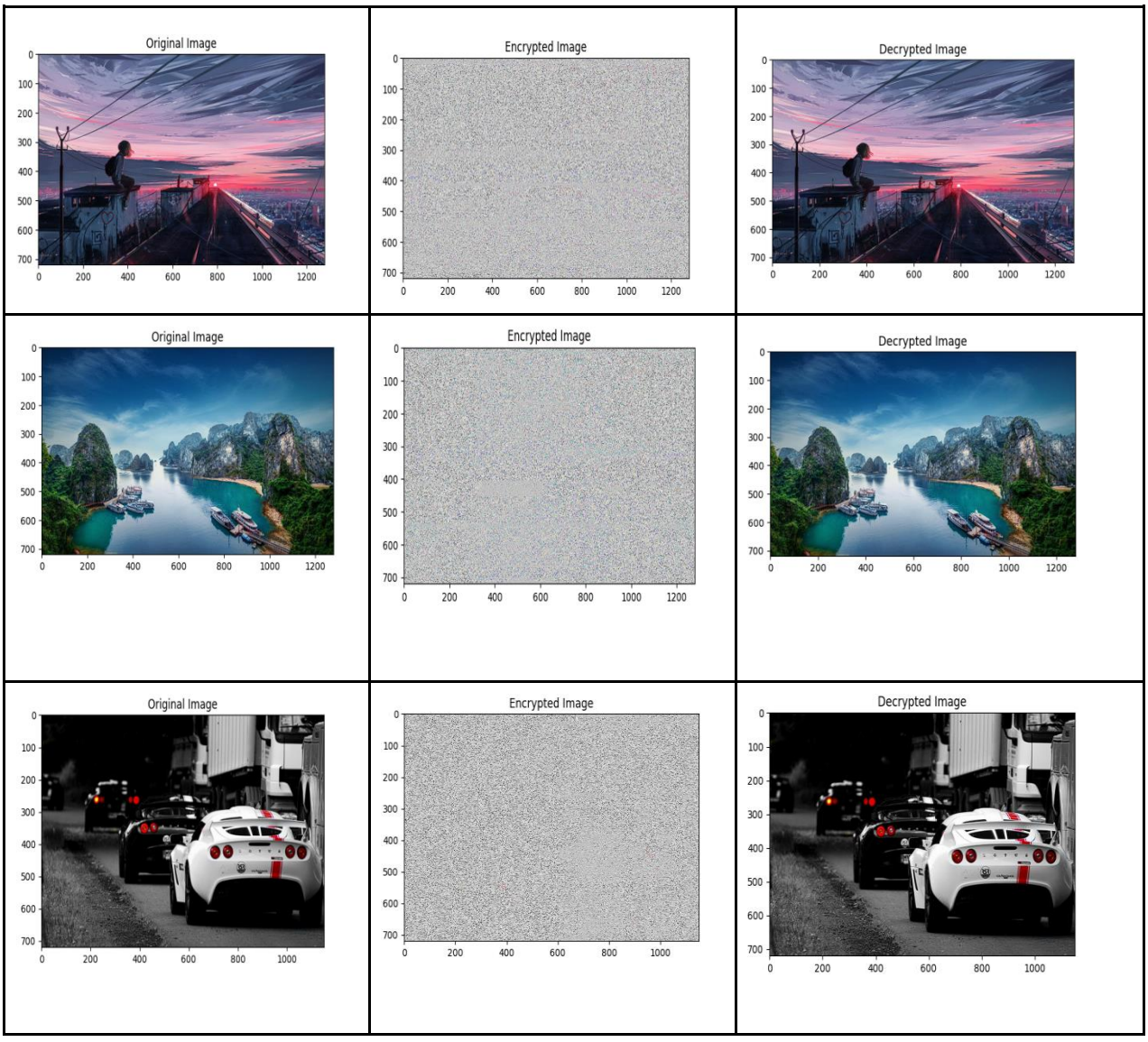
Test ID	Test Case Title	Test Condition	System Behavior	Expected Result
D01	Demo1.bmp Size : 1280*720	If the original image is encrypted and using decryption function ,the encrypted image is decrypted to get the original image	Entropy: Encrypted_img : 7.188 Decrypted_img: 7.558 MSE:103.283 PSN: 27.990 Correlation:0.127	Image Encrypted
T02	Demo2.bmp Size: 1280*720	If the original image is encrypted and using decryption function ,the encrypted image is decrypted to get the original image	Entropy: Encrypted_img : 6.885 Decrypted_img: 6.960 MSE:104.215 PSN: 27.951 Correlation:0.075	Image Encrypted
	Demo3.bmp Size: 1152*720 S	If the original image is encrypted and using decryption function ,the encrypted image is decrypted to get the original image	Entropy: Encrypted_img : 6.881 Decrypted_img: 7.330 MSE:105.513 PSN: 27.897 Correlation:0.061	Image Encrypted

Test ID	Test Case Title	Test Condition	System Behavior	Expected Result
T01	Trial1.bmp Size : 1280*720	If the original image is encrypted and using decryption function ,the encrypted image is decrypted to get the original image	Entropy: Encrypted_img : 7.892 Decrypted_img: 7.558 MSE:105.508 PSN: 56.900 Correlation:0.0009	Image Encrypted
T02	Trial2.bmp Size: 1280*720	If the original image is encrypted and using decryption function ,the encrypted image is decrypted to get the original image	Entropy: Encrypted_img : 7.827 Decrypted_img: 7.570 MSE:105.545 PSN: 57.294 Correlation:0.0003	Image Encrypted
T03	Trial3.bmp Size: 1152*720 S	If the original image is encrypted and using decryption function ,the encrypted image is decrypted to get the original image	Entropy: Encrypted_img : 7.999 Decrypted_img: 6.359 MSE:105.494 PSN: 54.649 Correlation:-0.0011	Image Encrypted

4.3.1 Result Analysis for Logistic Map



4.3.2 Result Analysis for Lorenz System



4.4 Quality Assurance(NPCR and UACI)

NPCR:-

NPCR (Normalized Pixel Change Rate) is a metric used commonly for evaluating the performance of image encryption algorithms. When the difference between two images is measured the one with the higher NPCR indicates better encryption. A higher NPCR implies that a small change in the plain text image results in a significant change in the cipher image. This sensitivity to changes helps ensure that the encrypted images are resistant to attacks attempting to recover the original image from the cipher text. Hence, when designing or evaluating image encryption algorithms,achieving a higher NPCR value is desirable.

UACI:-

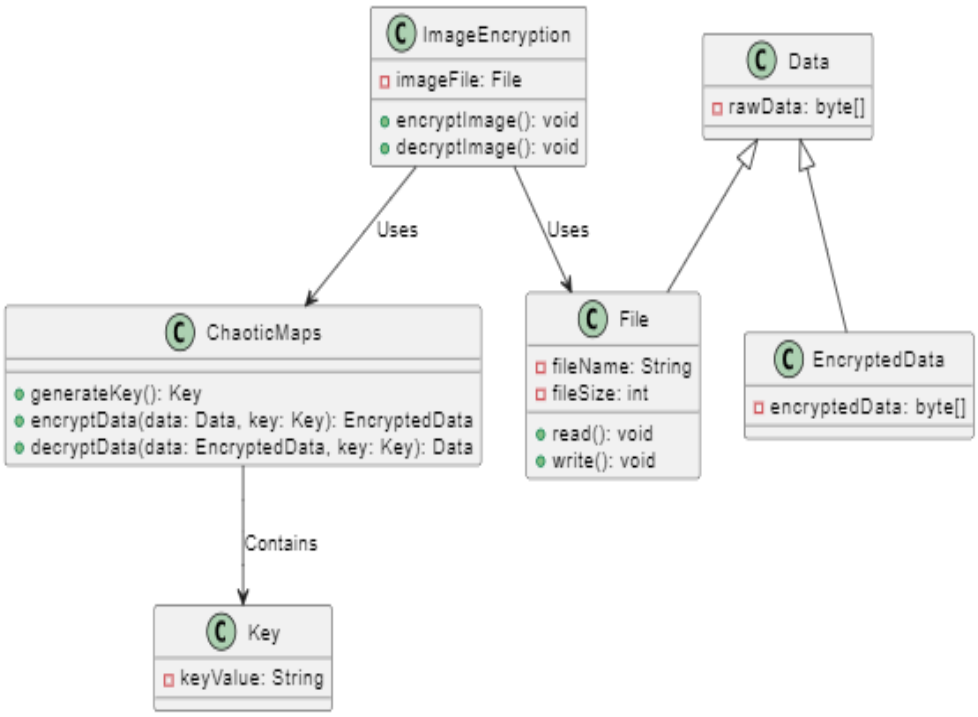
UACI (Unified Average Changing Intensity) is a metric used for evaluating the image encryption algorithms. Here when the average intensity change between the two encrypted images is being measured, the lower value UACI indicates better encryption. A lower UACI implies that a small change in the plain text image results in a significant change in the cipher image thereby enhancing the security of the encryption algorithms. Hence, when designing or evaluating image encryption algorithms,achieving a lower UACI value is desirable to ensure robustness against attacks .

Chapter 5

Standards Adopted

Githublink:->https://github.com/Soumya-Kanti-Datta/Image-Encryption-using-Chaotic-Maps/tree/main

5.1 Design Standards



5.2 Coding Standards

Pseudo Code for Logistic Function :-

```
Key Generation:
  keygen(x, r, size):
      key = []  // Initialize an empty list for the key
      for i in range(size):
          x = r * x * (1 - x)  // Logistic map function
          key.append(int((x * pow(10, 16)) % 256))  // Calculate key value and append to the list
      return key

Index Generation:
  indexgen(x, r, size):
      index = []  // Initialize an empty list for the index
      k = []      // Initialize an empty list for the chaotic map values
      for i in range(size):
          x = r * x * (1 - x)  // Logistic map function
          k.append(x)          // Store chaotic map value
          index.append(i)      // Store index value
      // Sort index based on chaotic map values in ascending order
      for i in range(size):
          for j in range(size):
              if k[i] > k[j]:
                  k[i], k[j] = k[j], k[i]     // Swap chaotic map values
                  index[i], index[j] = index[j], index[i]  // Swap corresponding index values
      return index

Encryption:
  encryption(img, index, key, height_of_image, width_of_image):
      encrypted_image = np.zeros_like(img)  // Initialize an array for encrypted image
      for i in range(height_of_image):
          for j in range(width_of_image):
              for z in range(3):  // Iterate over the 3 color channels
                  encrypted_image[i, j, z] = img[i, index[j], z] ^ key[z]  // XOR operation
      return encrypted_image

Decryption:
  decryption(encrypted_image, index, key, height_of_image, width_of_image):
      decrypted_image = np.zeros_like(encrypted_image)  // Initialize an array for decrypted image
      for i in range(height_of_image):
          for j in range(width_of_image):
              for z in range(3):  // Iterate over the 3 color channels
                  decrypted_image[i, index[j], z] = encrypted_image[i, j, z] ^ key[z]  // XOR operation
      return decrypted_image

Main:
  img = mpimg.imread("trial.bmp")
  key = keygen(0.000001, 3.14, height_of_image * width_of_image)
  index = indexgen(0.1, 3.69, width_of_image)
  encrypted_image = encryption(img, index, key, height_of_image, width_of_image)
  decrypted_image = decryption(encrypted_image, index, key, height_of_image, width_of_image)
  // Display original image, encrypted image, and decrypted image
```

Pseudo code for Lorenz System:-

```
// putfunction ImageEncryptionDecryptionUsingLorenzSystem(image_file_path):
    // Initialize variables
    read original image from image_file_path
    height = height of original image
    width = width of original image

    // Generate chaotic key sequences using Lorenz equations
    xkey, ykey, zkey = LorenzKey(0.01, 0.02, 0.05, height * width)

    // Initialize encrypted image array
    initialize encrypted_image with zeros of shape [height, width, 4] (RGBA format)

    // Shuffling Rows
    for each row in original image:
        shuffle row indices based on chaotic xkey sequence

    // Shuffling Columns
    for each column in original image:
        shuffle column indices based on chaotic ykey sequence

    // Convert the original image to RGBA format
    concatenate original image with alpha channel filled with 255

    // Encrypting the image
    l = 0
    for each pixel in original image:
        generate encryption key zk from chaotic zkey sequence
        perform XOR encryption of pixel with zk
        update encrypted_image with the encrypted pixel value
        increment l

    // Display the encrypted image
    display encrypted_image

    // Initialize decrypted image array
    initialize decrypted_image with zeros of shape [height, width, 4] (RGBA format)

    // Decrypting the image
    l = 0
    for each pixel in encrypted_image:
        generate decryption key zk from chaotic zkey sequence
        perform XOR decryption of pixel with zk
        update decrypted_image with the decrypted pixel value
        increment l

    // Reverse Column Shuffling
    for each row in decrypted_image:
        unshuffle column indices based on chaotic ykey sequence

    // Reverse Row Shuffling
    for each column in decrypted_image:
        unshuffle row indices based on chaotic xkey sequence

    // Display the decrypted image
    display decrypted_image
 your code here
```

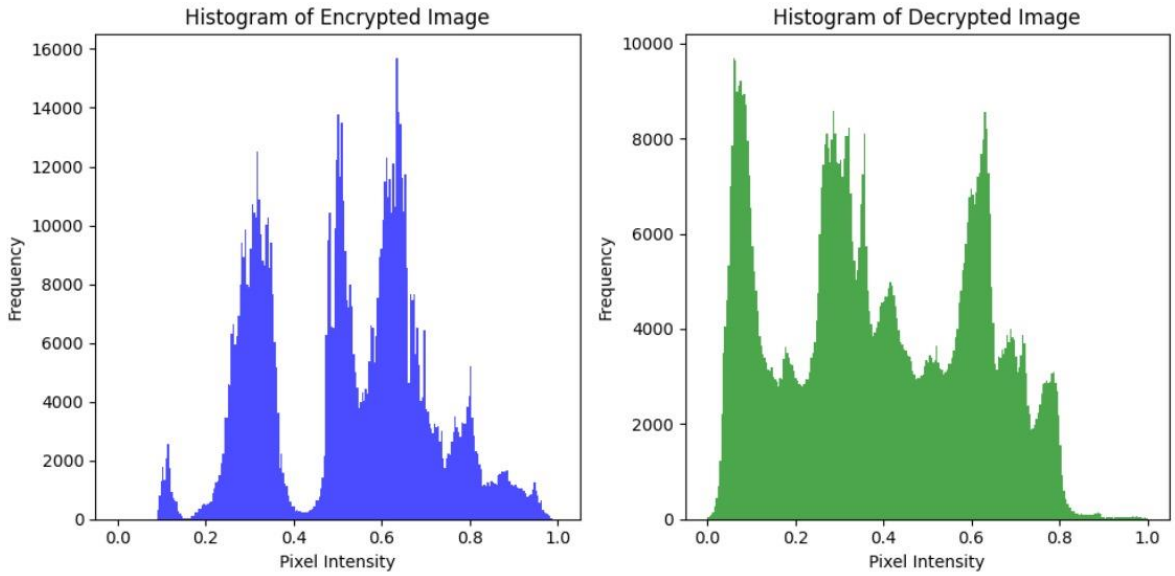
5.3 Testing Standards

Method used to verify the effectiveness of the encryption method:

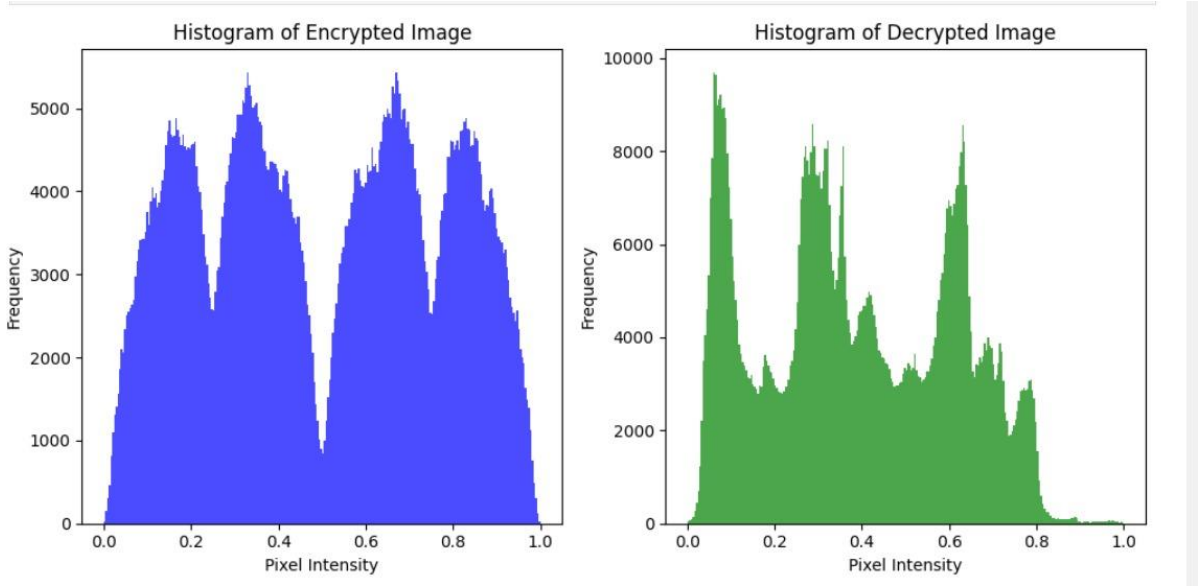
1.HISTOGRAM ANALYSIS: It is one of the straightforward approaches to demonstrate the quality of image encryption.It demonstrate the gray level intensity and the statistical information of an image as well as distribution of the pixel intensity values,in addition to providing information about the plain image to be used in histogram attack.It is to visualize and graphically analyze the pixel frequencies in

the image for each pixel or intensity between 1 and 255.It plots the number of pixels for each tonal value.

FOR LOGISTIC SYSTEM



FOR LORENZ SYSTEM



2.ENTROPY ANALYSIS: It assesses the randomness and unpredictability introduced by chaotic systems during encryption. It defines how much info or unpredictable present in an image. Chaotic maps generate key sequences used for pixel scrambling and diffusion.Value of right entropy is 8

which signifies image is more secure.By analyzing the entropy of these sequences,we evaluate the encryption's robustness against attacks.A uniformly distributed chaotic sequence enhances security,preventing inference of patterns from the cipher text.

3.CORRELATION COEFFICIENT: It assesses the statistical dependence between pixel values in the original image and the encrypted image.A low correlation coefficient indicates that the encryption process effectively breaks any linear relationship between pixels,enhancing security.Chaotic maps introduce randomness, making it challenging to predict pixel transformations.Researchers analyze the correlation to validate the robustness of chaotic-based encryption algorithms,ensuring that ciphertexts inhibit minimal correlation with the plain text.

4.PEAK SIGNAL TO NOISE RATIO: It is a widely used metric to evaluate the quality of an encrypted image compared to its original image. Its purpose is to measure the reconstruction fidelity between the original and encrypted images. It is expressed in decibels(dB).A higher PSNR value indicates better image quality. It indicates encrypted image closely resembles the original. It helps validate the robustness of encryption methods against attacks.

Chapter 6

Conclusion and Future Scope

6.1 Conclusion

In conclusion, for image encryption by employing chaotic systems such as the logistic map and Lorenz system , it offers a promising avenue for securing sensitive visual data. These systems exhibit chaotic behavior, allowing the creation of pseudo random sequences that are extremely responsive to initial conditions. The security of encrypted images can be significantly enhanced by utilizing the inherent unpredictability and complexity of chaotic dynamics by providing protection against unauthorized access and ensuring confidentiality during the transmission and storage of image data.

Moreover, incorporating chaotic maps into image encryption algorithms adds a level of intricacy that strengthens defense against cryptographic attacks.The non-linear and deterministic nature of chaotic systems makes it complicated for decrypting the image for unauthorized entities, thereby elevating the computational burden needed to compromise the encryption scheme.

Yet, it’s vital to recognize the hurdles linked to deploying chaotic map-based encryption systems, such as selecting parameters, managing synchronization, and dealing with computational demands.For realizing the full potential of chaotic map-based image encryption, addressing these challenges through rigorous analysis, optimization techniques, and cryptographic enhancements is very crucial.

In summary, harnessing chaotic maps like the logistic map and Lorenz system shows great potential for enhancing image encryption security. With ongoing research and development, these approaches have the capacity to substantially bolster the safeguarding of sensitive visual data across diverse fields such as healthcare, military operations and multimedia communication.

6.2 Future Scope:

The future scope of image encryption using logistic maps and the Lorenz system of chaotic maps holds considerable promise across various domains.

- **Enhanced Security Measure:** Further research can delve into enhancing encryption methods by exploring innovative chaotic maps or integrating several chaotic systems to bolster security measures. This entails exploring the potential of employing higher dimensional chaotic systems for encryption purposes.

- **Optimization and Efficiency:** Future endeavors should focus on improving encryption algorithms to minimize the computational burden without compromising security. This entails researching innovative approaches for selecting parameters, synchronizing systems, and managing keys to make the encryption process more efficient.

- **Real World Applications:** The demand for secure image communication and storage is increasing in various industries like healthcare, finance and multimedia. Future efforts can center on creating practical uses of chaotic map-based encryption that cater to the specific needs of these sectors by tailoring encryption techniques to provide robust security for images while aligning with industry standards and requirements.

- **Integration with Blockchain and IoT:** With evolving technologies of blockchain and IoT, there is potential for integrating chaotic map-based encryption into these systems to ensure secure and decentralized image data storage and communication.

- **Adaptation to Emerging Technologies:** With the emerging quantum computing advance, there’s a need to adapt chaotic map-based encryption to ensure resilience against quantum attacks, by developing quantum-resistant encryption algorithms based on chaotic systems.

Reference:-

Research paper links for image encryption using Logistic chaotic maps:-

https://ieeexplore.ieee.org/document/6754860/

https://www.sciencedirect.com/science/article/pii/S0030402622004843

https://www.researchgate.net/publication/280314246_Image_encryption_using_chaotic_maps

https://en.wikipedia.org/wiki/Chaotic_cryptology

Research paper links for image encryption using Lorenz chaotic maps:-

https://researchgate.net/publication/319275465_Image_encryption_algorithm_based_on_Lorenz_chaotic_map_with_dynamic_secret_keys

https://link.springer.com/article/10.1007/s11042-021-10695-5

https://ieeexplore.ieee.org/document/7861097

https://www.sciencedirect.com/science/article/pii/S0030402622004934

YouTube links used for reference of writing the algorithms:-

https://youtu.be/3UwD0KJr7_g?si=pT0TsbybNIgha2nK

https://youtu.be/5lMd2DW1XHA?si=UdaIKBf9T94BhSzY

.

INDIVIDUAL CONTRIBUTION REPORT:

IMAGE ENCRYPTION USING CHAOTIC MAPS

ABHIRUP CHOWDHURY
2105347

Abstract: The project explores the effectiveness of implementing chaotic systems like the logistic map and lorenz system for digital image encryption. We have demonstrated their ability to create unpredictable sequences by analyzing their dynamic properties. Through thorough experimental analysis, we can confirm the capacity of chaotic maps to enhance the security of image encryption.

Individual contribution and findings: For the image encryption using Chaotic maps, I have contributed to the code implementation part of Logistic Map, including the key generation, encryption algorithm and debugging of the code . I ensured that it met the project's requirements and contributed to the overall success of the Image Encryption Using Chaotic Maps.

Individual contribution to project report preparation: I have made meaningful contributions to the project's report to the coding standards, testing standards, conclusion and future scope. It was my responsibility to review the project statement and requirement specifications and my involvement further extends to the result analysis of Logistic System.

Full Signature of Supervisor:

…….

Full signature of the student

Abhirup Chowdhury

……..

INDIVIDUAL CONTRIBUTION REPORT:

IMAGE ENCRYPTION USING CHAOTIC MAPS

ANKITA GHOSH
2105355

Abstract: The project explores the effectiveness of implementing chaotic systems like the logistic map and Lorenz system for digital image encryption. We have demonstrated their ability to create unpredictable sequences by analyzing their dynamic properties. Through thorough experimental analysis, we can confirm the capacity of chaotic maps to enhance the security of image encryption.

Individual contribution and findings: For the image encryption using Chaotic maps, I have contributed to the code implementation part of Logistic Map, including the key generation, encryption algorithm. Through the meticulous attention to detail and through testing the code , I ensured that it met the project's requirements and contributed to the overall success of the Image Encryption Using Chaotic Maps.

Individual contribution to project report preparation: I have made meaningful contributions to the project's report to the testing standards consisting of various parameters like Histogram, Entropy, PSNR and correlation and design the block diagram of image encryption using logistic maps. It was my responsibility to review the project statement and requirement specifications and my involvement further extends to the result analysis of Logistic System.

Full Signature of Supervisor: Full signature of the student

Ankita Ghosh

……. ……..

INDIVIDUAL CONTRIBUTION REPORT:

IMAGE ENCRYPTION USING CHAOTIC MAPS

BHRAMARI SARKAR
2105364

Abstract: The project explores the effectiveness of implementing chaotic systems like the logistic map and Lorenz system for digital image encryption. We have demonstrated their ability to create unpredictable sequences by analyzing their dynamic properties. Through thorough experimental analysis, we can confirm the capacity of chaotic maps to enhance the security of image encryption.

Individual contribution and findings: For the image encryption using Chaotic maps,I have contributed to the code implementation part of Logistic Map, including the key generation , chaotic sequence generation and encryption algorithm. Through the meticulous attention to detail and through testing the code , I ensured that it met the project's requirements and contributed to the overall success of the Image Encryption Using Chaotic Maps.

Individual contribution to project report preparation: I have made meaningful contributions to the project's report to the methodological framework concerning the implementation of chaotic map techniques within the logistic map for the image encryption. My involvement extends to the continuous evaluation of quality assurance metrics, including the assessment of NPCR(Normalized Pixel Change Rate) and Unified Average Changing Intensity(UACI).I have formulated the concluding remarks and clarified avenues for the future exploration.

Full Signature of Supervisor:

…….

Full signature of the student

Bhramari Sarkar

……..

INDIVIDUAL CONTRIBUTION REPORT:

IMAGE ENCRYPTION USING CHAOTIC MAPS

SATTWIK SEN
2105403

Abstract: The project explores the effectiveness of implementing chaotic systems like the logistic map and lorenz system for digital image encryption. We have demonstrated their ability to create unpredictable sequences by analyzing their dynamic properties. Through thorough experimental analysis, we can confirm the capacity of chaotic maps to enhance the security of image encryption.

Individual contribution and findings: For the image encryption using Chaotic maps, I have contributed to the code implementation basically in the debugging part of Lorenz System, including the key generation, chaotic sequence generation and encryption and decryption algorithm. Through continuous testing of the code I made sure that the Image Encryption using Lorenz System met all the criteria of the project.

Individual contribution to project report preparation:

I have made meaningful contributions to the project's report to the abstract, introduction, project planning,design and methodology and block diagram of Lorenz system. It was my responsibility to review the project statement and requirement specifications and my involvement further extends to the result analysis of Lorenz System.

Full Signature of Supervisor: Full signature of the student

Sattwik Sen

……. ……..

INDIVIDUAL CONTRIBUTION REPORT:

IMAGE ENCRYPTION USING CHAOTIC MAPS

SOUMYA KANTI DATTA
21051262

Abstract: The project explores the effectiveness of implementing chaotic systems like the logistic map and Lorenz system for digital image encryption. We have demonstrated their ability to create unpredictable sequences by analyzing their dynamic properties. Through thorough experimental analysis, we can confirm the capacity of chaotic maps to enhance the security of image encryption.

Individual contribution and findings: For the image encryption using Chaotic maps,I have contributed to the code implementation part of Lorenz System, including the key generation, chaotic sequence generation and encryption and decryption algorithm. Through continuous testing of the code I made sure that the Image Encryption using Lorenz System met all the criteria of the project.

Individual contribution to project report preparation: I have made meaningful contributions to the project's report to the Testing OR Verification Plan of the image encryption and decryption. It was my responsibility to review the project statement and requirement specifications and my involvement further extends to the result analysis of Lorenz System.

Full Signature of Supervisor:

…….

Full signature of the student

Soumya Kanti Datta

……..

IMAGE ENCRYPTION USING CHAOTIC MAPS

ORIGINALITY REPORT

23%	13%	16%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.coursehero.com Internet Source	4%
2	Submitted to Banaras Hindu University Student Paper	2%
3	Ying Kai Hung, Yan Pei, Jianqiang Li. "Chapter 23 Single-to-Multi Music Track Composition Using Interactive Chaotic Evolution", Springer Science and Business Media LLC, 2024 Publication	1%
4	www.researchgate.net Internet Source	1%
5	www.mdpi.com Internet Source	1%
6	Shishir Kumar Shandilya, Agni Datta, Atulya K. Nagar. "A Nature-Inspired Approach to Cryptology", Springer Science and Business Media LLC, 2023 Publication	1%
7	Majid Khan, Tariq Shah. "A Literature Review on Image Encryption Techniques", 3D	1%

Research, 2014
Publication

8	Parisa Gholizadeh Pashakolaee, Hadi Shahriar Shahhoseini, Morteza Mollajafari. "Hyper-chaotic Feeded GA (HFGA): a reversible optimization technique for robust and sensitive image encryption", Multimedia Tools and Applications, 2017 Publication	1 %
9	N.K. Pareek, Vinod Patidar, K.K. Sud. "Image encryption using chaotic logistic map", Image and Vision Computing, 2006 Publication	1 %
10	Hossein Movafegh Ghadirli, Ali Nodehi, Rasul Enayatifar. "An overview of encryption algorithms in color images", Signal Processing, 2019 Publication	1 %
11	link.springer.com Internet Source	1 %
12	"Handbook of Multimedia Information Security: Techniques and Applications", Springer Science and Business Media LLC, 2019 Publication	1 %
13	Rui Wang, Guozheng Yang, Xuehu Yan, Shengyang Luo, Qiang Han. "Secret image	1 %

sharing in the encrypted domain", Journal of Visual Communication and Image Representation, 2023
Publication

14	Submitted to KIIT University Student Paper	1 %
15	Sen Zhang, Tao Jia. "Numerical investigation of the information complexity in Lorenz system based on Shannon entropy", Fluid Dynamics Research, 2022 Publication	1 %
16	Axelle Amon, Marc Lefranc. "1 Introduction to dynamical systems", Walter de Gruyter GmbH, 2023 Publication	<1 %
17	Un Sook Choi, Sung Jin Cho, Jin Gyoung Kim, Sung Won Kang, Han Doo Kim, Seok Tae Kim. "Color Image Encryption Based on PC-MLCA and 3-D Chaotic Cat Map", 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), 2019 Publication	<1 %
18	J. Tangkeh, J Gryzagoridis. "Optimizing the performance of the domestic wall mounted space comfort heater", 2017 International Conference on the Domestic Use of Energy (DUE), 2017 Publication	<1 %

19	Sathish Gunasekaran, Manish Kumar. "Secure data communication using DNA computing adaptable to wireless sensor network", Elsevier BV, 2022 Publication	<1 %
20	Liling Zhao, Xiaoao Duanmu, Quansen Sun. "A Prior-Knowledge-Based Generative Adversarial Network for Unsupervised Satellite Cloud Image Restoration", Remote Sensing, 2023 Publication	<1 %
21	Yue Wu. "Image encryption using the two-dimensional logistic chaotic map", Journal of Electronic Imaging, 2012 Publication	<1 %
22	www.worldleadershipacademy.live Internet Source	<1 %
23	Submitted to University of Bedfordshire Student Paper	<1 %
24	Submitted to Florida State University Student Paper	<1 %
25	Submitted to National Institute of Technology Warangal Student Paper	<1 %
26	deepai.org Internet Source	<1 %

27	arxiv.org Internet Source	<1 %
28	Submitted to University of Strathclyde Student Paper	<1 %
29	eurchembull.com Internet Source	<1 %
30	www.atmosp.physics.utoronto.ca Internet Source	<1 %
31	Naskar, Prabir Kr., and Atal Chaudhuri. "A robust image encryption technique using dual chaotic map", International Journal of Electronic Security and Digital Forensics, 2015. Publication	<1 %
32	online.journals.tubitak.gov.tr Internet Source	<1 %
33	repository.iiitd.edu.in Internet Source	<1 %

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	On		