# COLLEGE OF ENGINEERING AND MANAGEMENT, KOLAGHAT

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

# Title: Image Encryption based on Logistic Function

Under the supervision of

***Dr. Chinmay Maiti***

Presented by

**Kasturi Chatterjee (10700121042)**

**Nisha Masanta (10701621020)**

**Abir Datta (10700121121)**

# Content

1. Introduction
2. Image Encryption Algorithm
3. Experimental Result
4. Verify The Results
5. Real-Life Applications
6. Scope for Future Work
7. Conclusion
8. References

# Abstract

With the exponential growth of digital communication and data exchange, ensuring the confidentiality of image data has become increasingly critical. This project presents a robust image encryption method based on the **logistic map**, a simple yet powerful chaotic function known for its sensitivity to initial conditions and unpredictability. The proposed technique leverages the chaotic behavior of the logistic function to generate pseudo-random sequences, which are then used to scramble pixel positions and alter intensity values in grayscale images.

The encryption process enhances image security by significantly reducing pixel correlation and increasing entropy, making it resistant to statistical and brute-force attacks. Evaluation metrics  to validate the effectiveness of the algorithm. This method offers advantages such as simplicity, high speed, and low computational overhead, making it suitable for real-time and resource-constrained environments.

Overall, this project demonstrates the potential of chaotic systems, particularly the logistic map, as a lightweight and efficient tool for secure image encryption in modern digital applications.

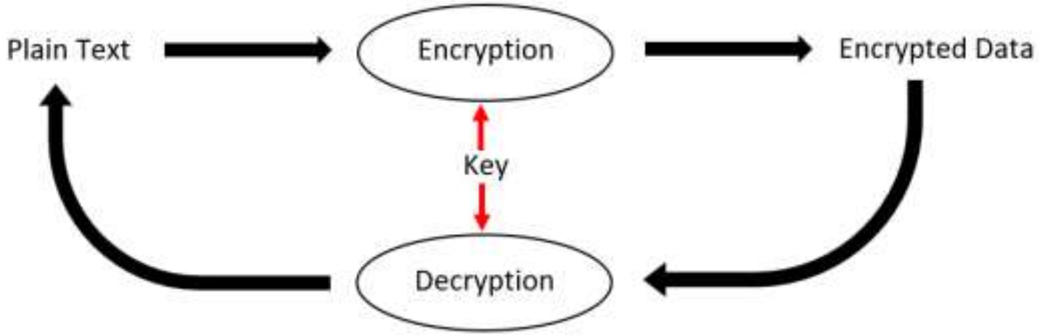
# Introduction

**What is Image Encryption?**

Image encryption is the process of converting an image into an unrecognizable format to protect its content from unauthorized access. This ensures data security during transmission or storage. These processes protect sensitive information from unauthorized access, tampering, and misuse, making them indispensable in various domains.

**Importance of Image Encryption :**

- **Data Privacy**: Protects sensitive visual information, such as medical images or personal photos.
- **Prevents Unauthorized Access**: Safeguards images from interception or misuse during communication.
- **Secure Storage**: Ensures images stored in cloud or local storage are inaccessible without decryption.
- **Supports Digital Forensics**: Enhances the security of image evidence in investigations.



## Objectives of the Project

- To develop a robust image encryption algorithm using chaotic maps.
- To ensure high levels of security, randomness, and resistance against cryptographic attacks.
- To evaluate the performace of the encryption method through standard metrics.

## Areas of Application

- **Secure Image Transmission**: Protect images during transmission over public or private networks.
- **Data Storage Security**:Ensure secure storage of sensitive visual data, such as medical images or government records.
- **Real-Time Systems**:Apply encryption for real-time systems like video surveillance or live streaming.
- **Digital Rights Management**: Protect copyrighted images and media from unauthorized usage.

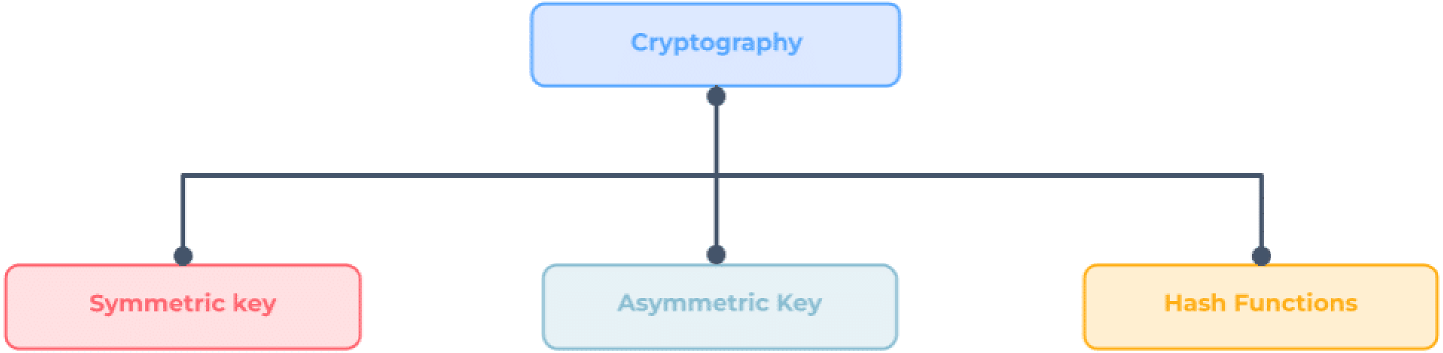
# Cryptography

**Cryptography** is the science and art of securing communication by converting information into a form that is unintelligible to unauthorized parties.

**Key Concepts in Cryptography:**

- **Confidentiality**: Ensures that information is accessible only to those authorized to access it.
- **Integrity**: Protects information from being altered without detection.
- **Authentication**: Verifies the identity of users and the origin of the information.
- **Non-repudiation**: Prevents the denial of actions or messages by the parties involved.

**Types of Cryptography :**


Cryptography

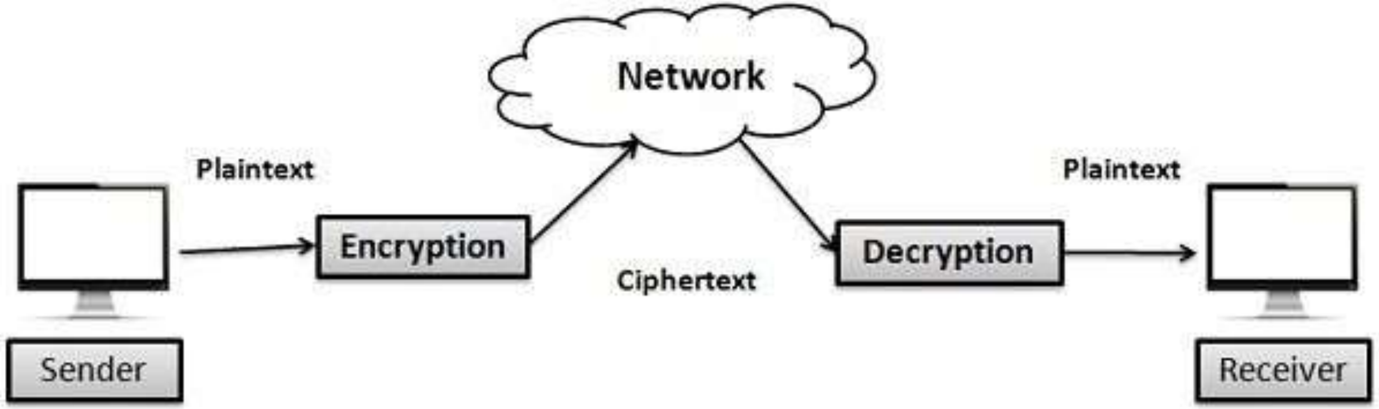
Symmetric key

Asymmetric Key

Hash Functions

# Image Encryption Algorithm

- **Image Encryption** is the process of converting plaintext (readable data) into ciphertext (unreadable data) using an algorithm and a key, to protect the information from unauthorized access. It is a fundamental technique in cryptography to ensure data confidentiality.
- **Image decryption** refers to the process of converting an encrypted image (ciphertext) back to its original form (plaintext) using a decryption algorithm and the corresponding decryption key. This process ensures that only authorized users can access the original image.



# Image Encryption using Logistic Map

**Logistic Map**

The **logistic map** is a mathematical equation that shows how a system can behave **chaotically**, meaning small changes in starting values cause big differences in results. The **logistic map** is a simple nonlinear chaotic function defined as:

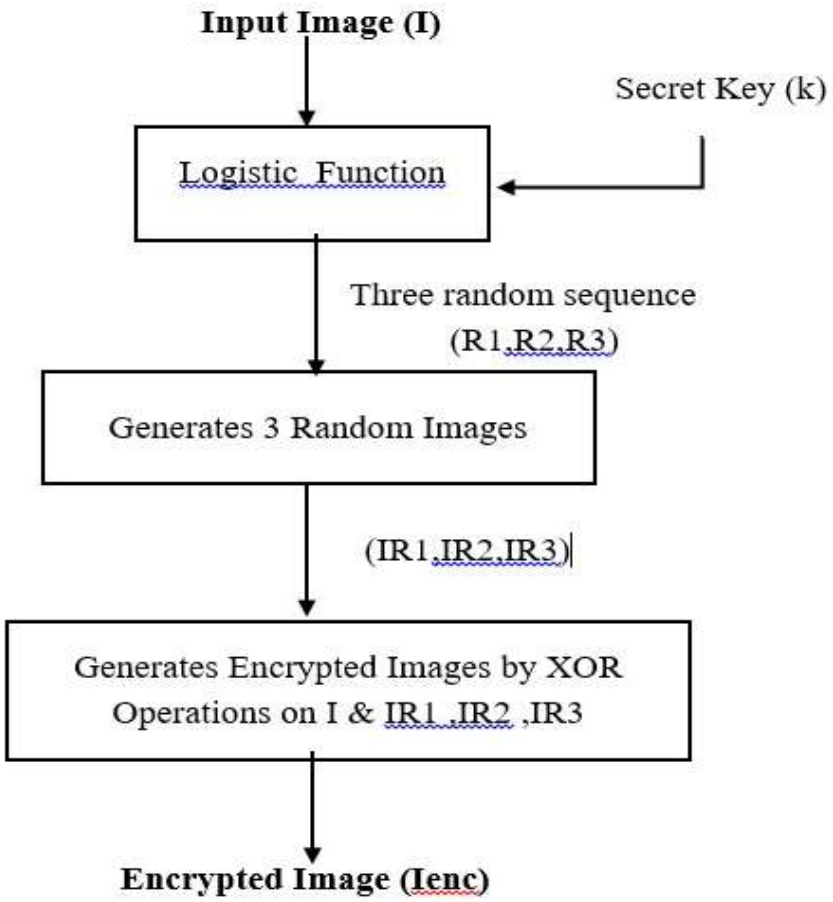
$$\boxed{x_{n+1} = rx_n(1 - x_n)}$$

- Xn is a number between 0 and 1, representing the state of the system at iteration n,
- Xn+1 is the next value in the sequence,
- r : control parameter (typically 3.57 < r ≤ 4.0 for chaotic behavior).

**Why Logistic Map?**

- Simple to implement.
- High sensitivity to initial conditions.
- Generates **chaotic sequences** suitable for encryption.
- Lightweight and fast for image processing.

# Workflow of the Project



**Input Image (I)**

Secret Key (k)

Logistic Function

Three random sequence (R1,R2,R3)

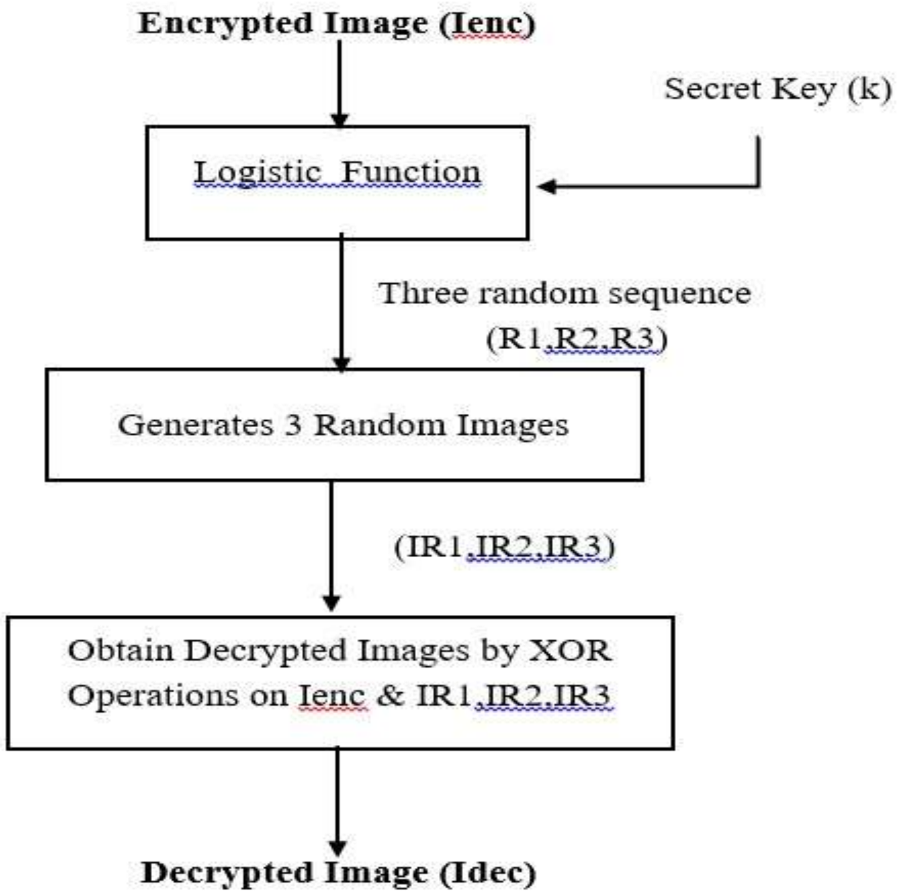
Generates 3 Random Images

(IR1,IR2,IR3)

Generates Encrypted Images by XOR Operations on I & IR1 ,IR2 ,IR3

**Encrypted Image (Ienc)**

**Block diagram of Image Encryption**



**Encrypted Image (Ienc)**

Secret Key (k)

Logistic Function

Three random sequence (R1,R2,R3)

Generates 3 Random Images

(IR1,IR2,IR3)

Obtain Decrypted Images by XOR Operations on Ienc & IR1,IR2,IR3

**Decrypted Image (Idec)**

**Block diagram of Image Decryption**

# Methodology

**Steps**:

**Encryption Process**

1. Input grayscale image
2. Initialize parameters (x0, r)
3. Generate chaotic sequence
4. Convert image to pixel matrix
5. Perform pixel-wise XOR with chaotic sequence
6. Output encrypted image

**Decryption Process**

1. Decryption is the reverse process.
2. Requires the same key parameters:
    - Initial value x0
    - Control parameter r
3. XOR operation is reversible.
4. Output decrypted image.

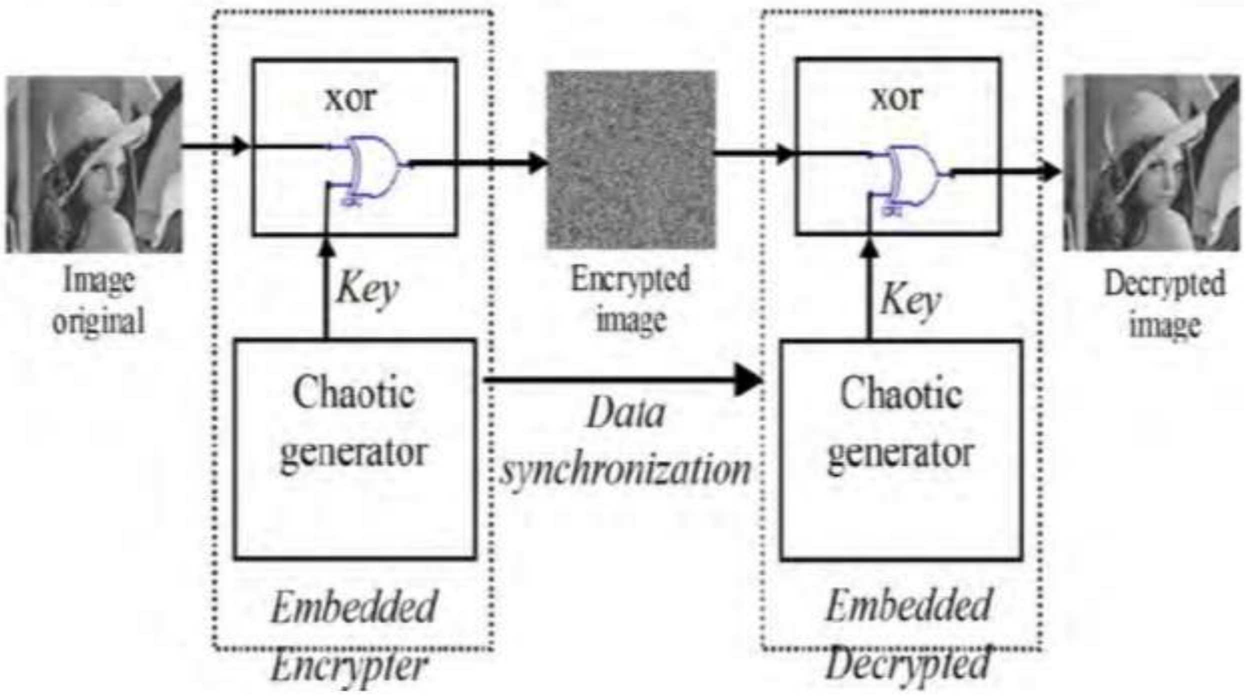


**Figure- Working of Image Encryption using Logistic Map**

# Security Evaluation Metrics

To assess the effectiveness of the encryption, key statistical metrics are used. These include entropy, correlation coefficient, NPCR, UACI, and scatter plots. Together, they evaluate the randomness, sensitivity, and security strength of the encrypted image. These are -

- **Histogram**: Shows pixel intensity distribution, encrypted images have a uniform histogram.
- **Entropy**: Measures pixel randomness. Ideal value ≈ 8 indicates high uncertainty and strong encryption.
- **Correlation Coefficient**: Assesses similarity between adjacent pixels (horizontal, vertical, diagonal).
- **NPCR (Number of Pixel Change Rate)**: Evaluates how much the image changes when a single pixel is altered.
  A value > 99% shows strong sensitivity to input changes.
- **UACI (Unified Average Changing Intensity)**: Measures average intensity variation between two encrypted images.
  Ideal ≈ 33%, signifying effective diffusion.
- **Scatter Diagram**: Visualizes pixel-to-pixel correlation. Encrypted images exhibit random scatter,confirming low statistical predictability.

# Experimental Results

- **Original Grayscale Image :**

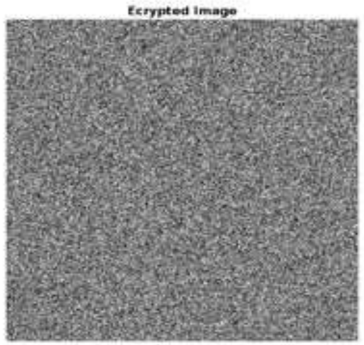
Baboon
(a)

Boat
(b)

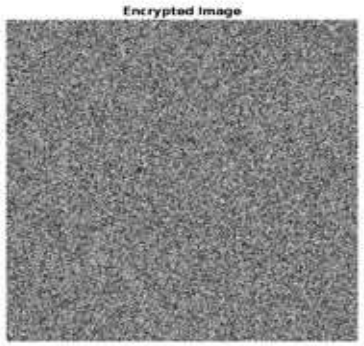
Lena
(c)

Peppers
(d)

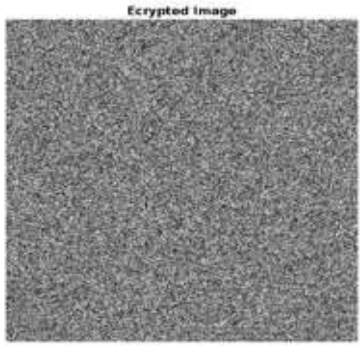
- **Encrypted Image: Output after applying logistic map-based encryption, appears noisy and random :**



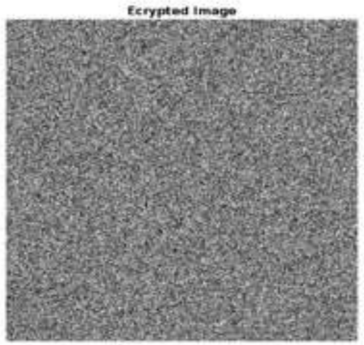
Baboon
(a)



Boat
(b)

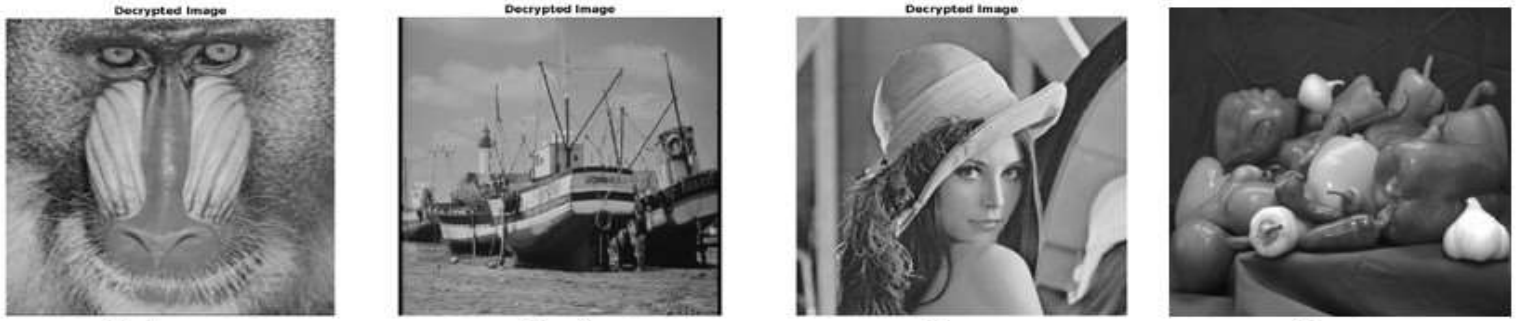


Lena
(c)



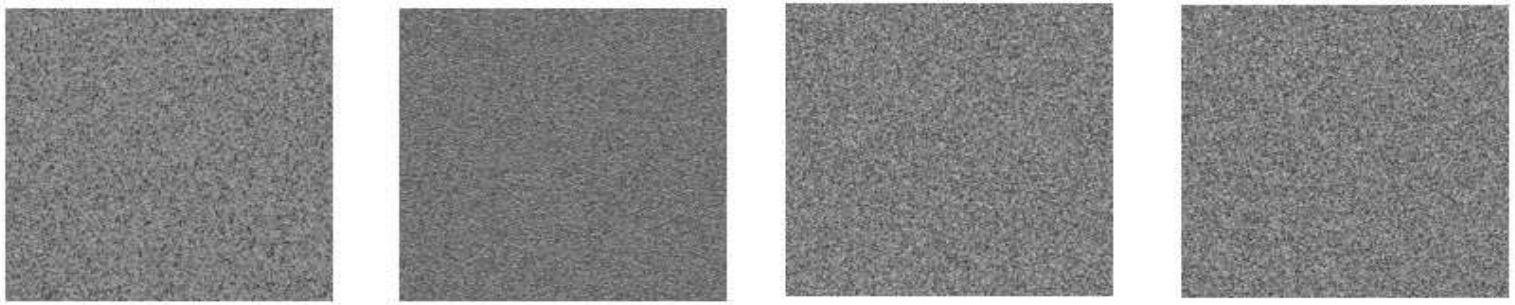
Peppers
(d)

- **Decrypted Image Using Original Key :**



Baboon (a) Boat (b) Lena (c) Peppers (d)

- **Decrypted Image Using Fake Key :**



Baboon (a) Boat (b) Lena (c) Peppers (d)

The comparison clearly shows that only the correct key can successfully decrypt the image, while a fake key results in meaningless output—highlighting the algorithm's high **key sensitivity** and **security strength**.

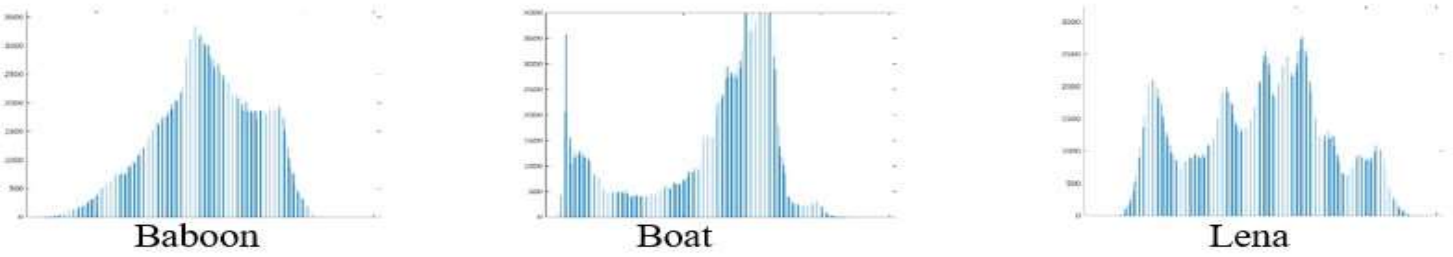
# Verify The Results

**Histogram Analysis** :

Below figure illustrates the histogram comparison between the original and encrypted images:

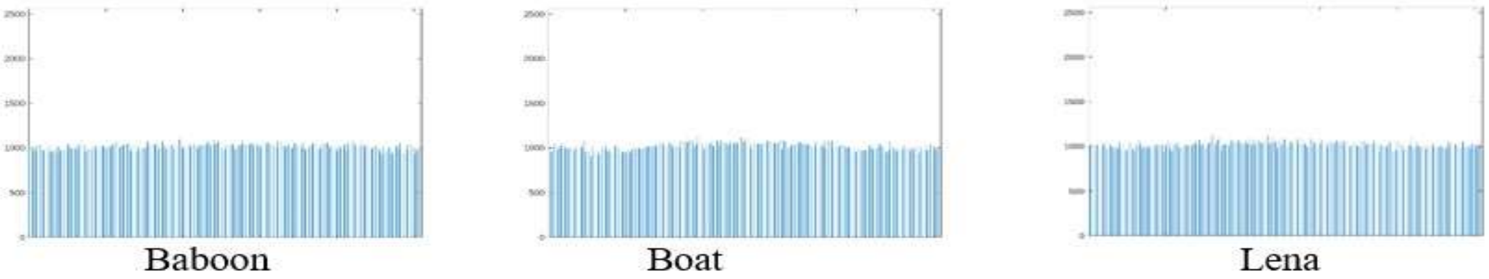
**(a) Original Image Histogram**: Displays a non-uniform distribution, with visible peaks corresponding to pixel intensity patterns—revealing statistical structure.

**(b) Encrypted Image Histogram**: Shows a nearly uniform distribution, indicating that pixel values are well-randomized. This uniformity confirms that the encryption effectively conceals visual and statistical information from potential attackers.



Baboon Boat Lena

a) Original Image



Baboon Boat Lena

b) Encrypted Image

## Entropy Analysis :

The table presents the entropy values of original and encrypted grayscale images. Entropy measures the **randomness or uncertainty** in pixel intensity values—higher values indicate stronger encryption.

(a) **Original Images** (Lena, Baboon, Boat, Peppers) show entropy values ranging from **6.99 to 7.44**, reflecting some inherent pixel correlation and structure.

(b) **Encrypted Images** consistently achieve entropy values close to **8.0**, which is ideal for 8-bit grayscale images. This indicates that the encrypted images are highly randomized and **resistant to statistical attacks**.

| Image | Grayscale | |
|---|---|---|
| | Original | Encrypted |
| Lena | 7.445455 | 7.999144 |
| Baboon | 7.164027 | 7.998842 |
| Boat | 7.072747 | 7.999069 |
| Peppers | 6.991022 | 7.999156 |

Table - Entropy Analysis between Original Images and Encrypted Images

The significant increase in entropy confirms the effectiveness of the logistic map-based encryption in producing secure and unpredictable image outputs.

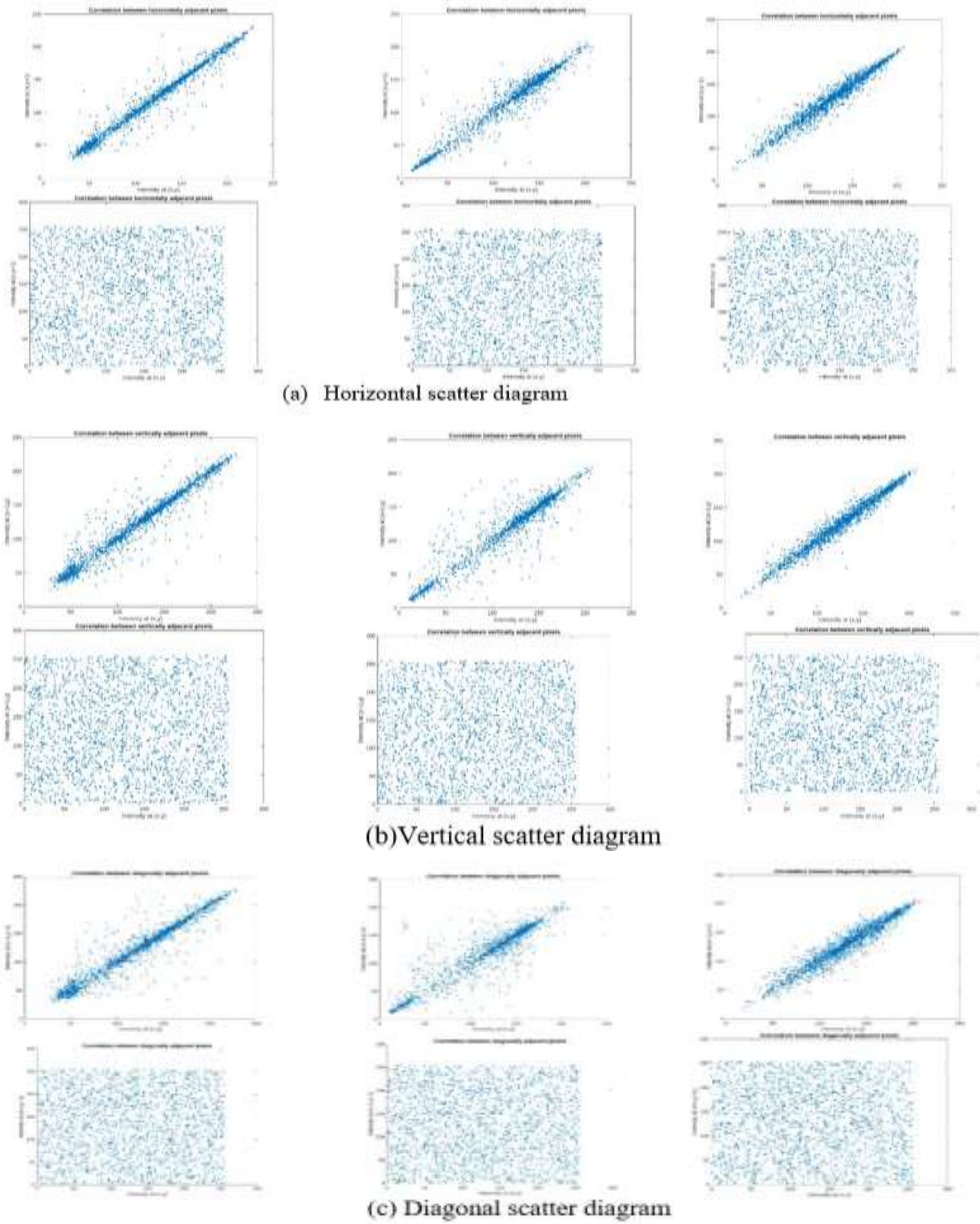
## Correlation Coefficients :

This table presents the **correlation coefficients** of grayscale images measured in three directions: **horizontal, vertical, and diagonal**, before and after encryption.

| Images | | Grayscale | | |
|---|---|---|---|---|
| | | Horizontal | Vertical | Diagonal |
| Lena | Org img : | 0.972341 | 0.985764 | 0.959466 |
| | Enc img : | 0.000687 | 0.000048 | -0.001998 |
| Baboon | Org img : | 0.980266 | 0.974441 | 0.957612 |
| | Enc img : | 0.001949 | 0.001836 | 0.002059 |
| Boat | Org img : | 0.964536 | 0.977619 | 0.943539 |
| | Enc img : | -0.003610 | -0.000400 | -0.000748 |
| Peppers | Org img : | 0.991654 | 0.992074 | 0.984778 |
| | Enc img : | -0.000568 | 0.002352 | 0.000171 |

Table - Correlation Coefficients calculated in horizontal, vertical, and diagonal directions for both the original and encrypted grayscale images

The correlation coefficients drop from high (≈0.94–0.99) in original images to near zero or negative in encrypted images, confirming that the encryption effectively removes pixel dependencies and ensures statistical security.



(a) Horizontal scatter diagram

(b)Vertical scatter diagram

(c) Diagonal scatter diagram

Lena Boat Baboon

## Scatter Diagram Analysis :

The scatter diagrams illustrate the relationship between adjacent pixel values in horizontal, vertical, and diagonal directions for three grayscale images: **Lena**, **Boat**, and **Baboon**.

**(a) Horizontal Scatter Diagram**

**(b) Vertical Scatter Diagram**

**(c) Diagonal Scatter Diagram**

In all three directions, the **original images** show clustered points along the diagonal line, indicating **high correlation** between adjacent pixels. After encryption, the scatter points become **randomly distributed**, confirming that pixel relationships are destroyed and the encrypted images exhibit **strong randomness and security**.

These scatter plots visually confirm that the encrypted images are **statistically decorrelated**, ensuring that the encryption provides **robust protection** against statistical and visual analysis attacks.

## Number of Pixel Change Rate (NCPR) measure (%) for key sensitivity analysis :

Table shows the **Number of Pixel Change Rate (NPCR)** values for different grayscale images under two test conditions:

- **Case 1**: Encryption with a slight change in the original image.
- **Case 2**: Encryption with a slight change in the secret key.

| Test Condition | Case 1 | Case 2 |
|---|---|---|
| Image | NPCR | NPCR |
| Lena | 99.5819 | 97.5044 |
| Baboon | 99.5819 | 97.5044 |
| Boat | 99.5819 | 97.5044 |
| Peppers | 99.5819 | 97.5044 |

**NCPR measurements**

In **Case 1**, all images (Lena, Baboon, Boat, Peppers) exhibit a **high NPCR of 99.5819%**, indicating that even a minor change in the image results in significant pixel changes in the encrypted output, confirming strong **sensitivity to plaintext**.

In **Case 2**, the NPCR drops to **97.5044%**, still indicating good **key sensitivity**—a small change in the encryption key causes substantial changes in the ciphertext.

These results confirm the encryption method's robustness against **differential attacks** and demonstrate its ability to ensure **strong diffusion**.

**Unified Average Changing Intensity (UACI) measure (%) for key sensitivity analysis :**

This table presents the **Unified Average Changing Intensity (UACI)** values (in %) under two test conditions:

- **Case 1**: Slight change in the input image.
- **Case 2**: Slight change in the encryption key.

| Test Condition | Case 1 | Case 2 |
|---|---|---|
| Image | UACI | UACI |
| Lena | 28.3505 | 30.9509 |
| Baboon | 26.7738 | 30.7008 |
| Boat | 28.5810 | 30.8960 |
| Peppers | 31.5972 | 31.4413 |

**UACI measurements**

UACI evaluates the average intensity difference between two encrypted images.

- In **Case 1**, UACI values range from **26.77% to 31.59%**, showing good **diffusion** when the input image is slightly altered.
- In **Case 2**, UACI values range from **30.70% to 31.44%**, indicating **strong key sensitivity**—even a minor change in the key significantly affects the encryption output.

These values, being close to the ideal (~33%), confirm the encryption algorithm's **robustness and resistance** to differential and key-based attacks.

# Advantages And Limitations Of Image Encryption Using Logistic Function

## Advantages

- High security using chaotic logistic map
- Fast and lightweight encryption
- Strong key sensitivity
- Effective image confidentiality
- Resistant to statistical attacks
- Scalable to various image sizes
- No visual patterns in encrypted output
- Suitable for real-world secure image applications

## Limitations

- Limited key space (basic logistic map)
- Highly sensitive to initial parameters
- Designed mainly for grayscale images
- No built-in compression support
- Not an industry-standard algorithm
- Possible numerical instability
- Lacks authentication and integrity checks

# Real-Life Applications

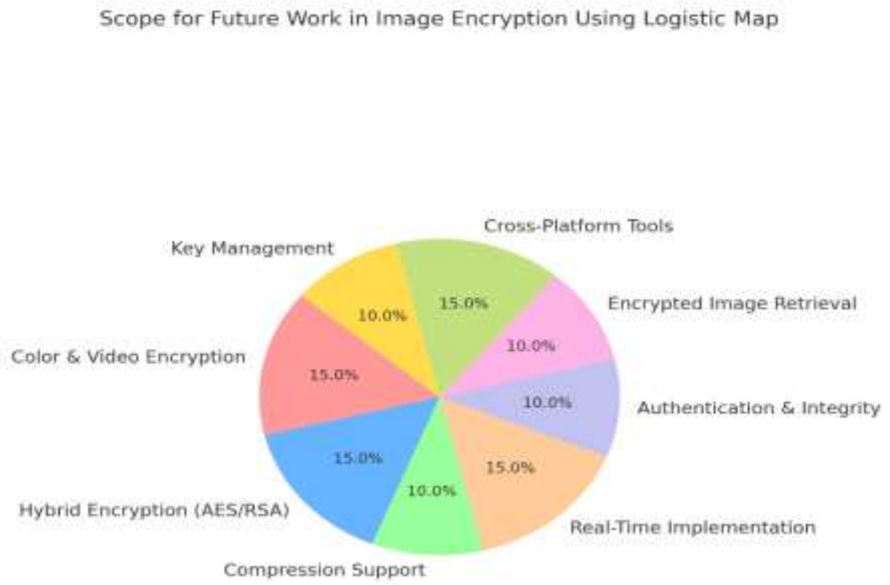
With the rise of digital media, securing image data is crucial. **Logistic map-based encryption** offers a lightweight and effective solution for protecting visual information. Its ability to generate highly random and unpredictable encrypted images makes it suitable for a wide range of **real-life applications**, including -

- **Secure Image Transmission** – Ensuring safe communication in military, medical, and confidential government operations.
- **Medical Imaging Protection** – Safeguarding patient records and diagnostic images (e.g., X-rays, MRIs).
- **Cloud Storage Security** – Encrypting personal or sensitive images before uploading to cloud platforms.
- **Surveillance Systems** – Preventing unauthorized access to CCTV and security camera footage.
- **Satellite and Remote Sensing** – Protecting satellite imagery used in defense, weather, and geospatial analysis.
- **Biometric Data Protection** – Encrypting facial, fingerprint, and retinal images in identity verification systems.
- **Social Media and Messaging Apps** – Securing shared images from interception or misuse during transmission.

# Scope for Future Work

While the current implementation of logistic map-based image encryption demonstrates strong security and performance, there is significant potential for further enhancement. Future developments can focus on expanding functionality, improving efficiency, and increasing adaptability to meet the evolving demands of modern digital security systems.

- Extend to color and video encryption
- Integrate Use Arnold Cat Map for better pixel scrambling.
- Combine with AES/RSA for hybrid security
- Include authentication and integrity checks
- Develop encrypted image retrieval methods
- Implement real-time encryption with hardware support
- Build a cross-platform user tool or app



Scope for Future Work in Image Encryption Using Logistic Map

# Conclusion

- **Logistic map-based image encryption** provides an efficient, secure, and chaos-driven approach to protecting digital images against unauthorized access and analysis.
- It ensures **high sensitivity to initial conditions and keys**, making brute-force and differential attacks nearly impossible.
- The algorithm demonstrates **excellent statistical properties**, including low correlation, high entropy, and strong NPCR/UACI values—proving its robustness.
- Its **simplicity and low computational cost** make it ideal for **embedded systems, IoT devices, and real-time security applications**.
- Overall, the method offers a **promising alternative** to traditional encryption systems for image-specific security needs in both academic and industrial domains.

# REFERENCES

## Books

**“Cryptography and Network Security”** by William Stallings

**“Chaos and Fractals: New Frontiers of Science”** by Heinz-Otto Peitgen et al.

## Research Papers / Journals

**Kanso, A., & Smaoui, N. (2009).** “Logistic chaotic maps for binary numbers generations”

**Guan, Z., Huang, F., & Guan, W. (2005).** “Chaos-based image encryption algorithm

## Websites

**ResearchGate** – https://www.researchgate.net

**IEEE Xplore Digital Library** – https://ieeexplore.ieee.org

# Thank You