SecureVision: Advanced Image Encryption Using Chaos Theory

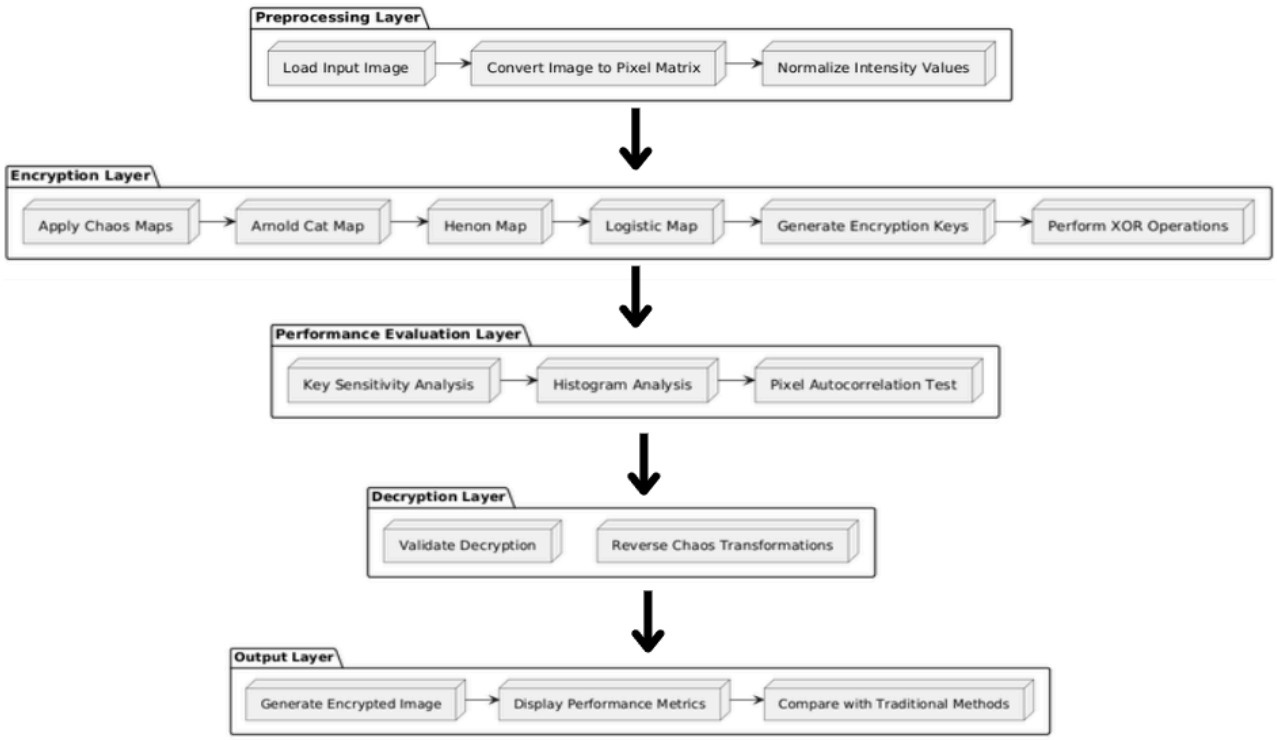
Members:

1. Aviral Srivastava 22BAI1187
2. Ishan Jain 22BCE5073
3. Garv Bhaskar 22BAI1371

1. Introduction

In the digital era, ensuring image security is a top priority. Traditional encryption methods like AES and RSA struggle with large image data, leading to inefficiencies in processing time and security. SecureVision presents an innovative approach using chaos-based encryption, leveraging chaotic system properties such as high sensitivity to initial conditions, ergodicity, and pseudo-random behavior. This project implements and compares chaos maps, including Arnold Cat Map, Henon Map, and Logistic Chaos Map, to deliver a high-security, computationally efficient image encryption system.

2. Architecture



The SecureVision encryption framework follows a structured methodology:

1. **Preprocessing:**
    - Convert images into pixel matrix representation.
    - Normalize intensity values for uniform processing.
2. **Chaos-Based Encryption:**
    - Apply chaos maps to shuffle and transform the pixel matrix.
    - Generate dynamic encryption keys using chaos functions.
    - Enhance security through XOR operations with chaotic sequences.
3. **Performance Evaluation:**
    - **Key Sensitivity Analysis:** Examining the impact of slight key variations on decryption.
    - **Histogram Analysis:** Ensuring uniform pixel distribution in encrypted images.
    - **Adjacent Pixel Autocorrelation:** Measuring randomness and breaking pixel redundancy.
4. **Decryption Process:**
    - Reverse chaos transformations.
    - Validate decrypted images against original inputs.

3. Literature Review

3.1 The Need for Advanced Image Encryption

With the rapid expansion of digital communication and the increasing reliance on image data across various fields such as medical imaging, satellite communications, and secure document storage, ensuring image security has become paramount. Traditional encryption algorithms like AES and RSA, while effective for text-based encryption, struggle with the unique characteristics of images due to their high redundancy, large file sizes, and the need for real-time processing. As a result, there is an urgent need for encryption methods that are computationally efficient while maintaining a high level of security.

Chaos-based cryptographic techniques have emerged as a powerful alternative due to their inherent non-linearity, sensitivity to initial conditions, and pseudo-random properties. Unlike conventional encryption techniques, chaotic systems can offer high-security encryption with reduced computational complexity, making them suitable for real-time image protection. These methods exhibit strong resistance to statistical and brute-force attacks, making them a viable alternative to conventional encryption mechanisms.

3.2 Previous Work in Chaos-Based Image Encryption

The application of chaotic systems in cryptography has been extensively explored in recent years. Several studies have highlighted the efficiency of different chaotic maps for encryption:

- Arnold Cat Map: Known for its ability to scramble pixel positions without modifying intensity values, thereby maintaining the image structure but disrupting its visual representation.

- Henon Map: Utilizes a two-dimensional chaotic sequence to introduce non-linearity in both row and column transformations, enhancing encryption robustness.

- Logistic Map: Features strong key sensitivity and dynamic intensity randomization, offering an additional layer of security against brute-force attacks.

While these approaches have shown promise, many implementations suffer from limitations such as periodicity in Arnold Cat transformations, increased computational overhead in Henon maps, and key dependency issues in Logistic-based encryption. Moreover, previous research has focused on the individual application of these chaos maps, often overlooking their potential when combined. Several research efforts have aimed to optimize encryption techniques, yet a fully optimized, hybrid chaos-based encryption framework remains an area of active exploration.

3.3 How Our Project Enhances Chaos-Based Encryption

Our project, SecureVision, builds upon existing research by integrating multiple chaotic maps in a hybrid encryption framework. By combining Arnold Cat, Henon, and Logistic Maps, we aim to achieve the following improvements:

- Increased Security Complexity: The use of multiple chaos maps ensures a layered encryption approach that is more resilient to attacks than single-map encryption.

- Optimized Computational Efficiency: By strategically applying these chaos maps, our approach minimizes redundant calculations and optimizes performance for large image encryption.

- Comprehensive Performance Evaluation: Unlike many existing studies that focus solely on encryption, we implement a detailed analysis of key sensitivity, histogram uniformity, and adjacent pixel correlation to assess encryption strength.

- Dynamic Key Mixing Mechanism: We introduce a novel key-mixing technique that enhances unpredictability and strengthens security against brute-force and differential attacks.

Our research contributes to the field by demonstrating the effectiveness of a hybrid chaotic encryption system, addressing the weaknesses of individual chaos maps while improving encryption robustness and computational efficiency. By evaluating multiple chaotic models and

combining their advantages, SecureVision provides a more secure, adaptable, and computationally efficient encryption framework.

4. Expected Outcomes

- Development of a robust chaos-based encryption solution that enhances security for image data.
- Implementation of multiple chaos maps in a hybrid encryption framework to maximize security and efficiency. Comprehensive performance evaluation through histogram analysis, adjacent pixel correlation, and key sensitivity tests.
- Creation of a scalable and computationally efficient encryption model suitable for real-world applications, including secure communications and digital media protection.
- Contribution to the field of image cryptography by demonstrating the advantages of a multi-chaos encryption approach over traditional single-chaos methods.

5. Conclusion

SecureVision aims to revolutionize digital image security by integrating chaos theory into encryption. By leveraging the strengths of Arnold Cat, Henon, and Logistic maps, our hybrid encryption framework enhances security, reduces computational complexity, and improves resilience against attacks. Through a comparative analysis of various chaos maps and an in-depth evaluation of encryption performance, our project will establish a more effective approach for high-performance, secure image encryption. The expected contributions of SecureVision will not only provide a scalable encryption model but also open avenues for further research in chaos-based cryptography and its applications in digital security.

References

1. X. Wang, Y. Zhang, and X. Bao, "A new chaotic image encryption algorithm based on permutation-diffusion structure," *IEEE Transactions on Multimedia*, vol. 21, no. 4, pp. 1101-1114, 2019.

2. Y. Wang, K. W. Wong, and X. Liao, "A novel chaotic image encryption scheme based on Arnold cat map and Henon map," *Optics & Lasers in Engineering*, vol. 96, pp. 75-85, 2017.

3. H. Liu and X. Liu, "Cryptanalysis and enhancement of an image encryption scheme using multiple chaotic maps," *Signal Processing*, vol. 175, pp. 107652, 2020.

4. Z. Hua, Y. Zhou, and H. Huang, "Efficient image encryption using chaotic maps and permutation-diffusion architecture," *Nonlinear Dynamics*, vol. 90, no. 2, pp. 961-975, 2017.