Secure and Efficient Image Encryption with Compression and Metadata Embedding

Digital data growth and the need for secure transmission have led to the development of robust image encryption methods. This project introduces a system that encrypts images using a dual-stage approach combining spatial shuffling with chaotic encryption.

The encrypted image is further compressed losslessly and enhanced by embedding metadata via steganography. The system also benefits from an extra encryption layer using AES S-Box substitution and a strengthened hashing stage that employs a superior algorithm compared to standard SHA-256.

Designed for diverse environments such as Google Colab and Jupyter Notebook, every aspect including performance and advanced security is thoroughly analyzed in the following sections.

Background and Motivation

Limitations of Traditional Methods

Single-method approaches are prone to attacks that exploit statistical patterns or repetitive structures.

Dual-Stage Encryption

Merging Arnold Cat Map and Logistic Map to form a layered security scheme.

Additional Security Features

Lossless compression, metadata embedding, enhanced hashing algorithm, and AES S-Box substitution to counter differential cryptanalysis.

Traditional image encryption methods typically rely on a single technique for pixel rearrangement or pixel value transformation. The motivation behind this project is to create a more robust system by combining complementary encryption techniques and adding multiple security layers for comprehensive protection.

Project Objectives

1 Dual-Stage Encryption

Develop a mechanism combining spatial shuffling via the Arnold Cat Map with chaotic encryption via the Logistic Map.

2 Enhanced Security

Incorporate AES S-Box substitution for extra nonlinear transformation and employ an improved hash algorithm with better collision resistance than SHA-256.

3 Optimization

Compress encrypted image data losslessly and embed critical metadata securely using steganography.

4 Deployment and Analysis

Enable cross-platform deployment and conduct thorough performance and security analyses using quality metrics and key sensitivity tests.

Methodology

Image Upload & Preprocessing

Ensures proper resizing and padding to yield a square image.

Multi-Layer Encryption

Shuffles pixel positions using Arnold Cat Map, transforms pixel values with Logistic Map, and applies AES S-Box substitution.

Compression & Hashing

Compresses encrypted data using a robust lossless algorithm and calculates a secure hash using an enhanced algorithm.

Metadata Embedding

Embeds encryption parameters and metadata into the encrypted image using least significant bits.

The system follows a clear series of stages that work together to provide robust security while maintaining efficiency. Decompression and decryption are performed in reverse order to precisely recover the original image, and the entire process is evaluated through quality metrics and performance timings.

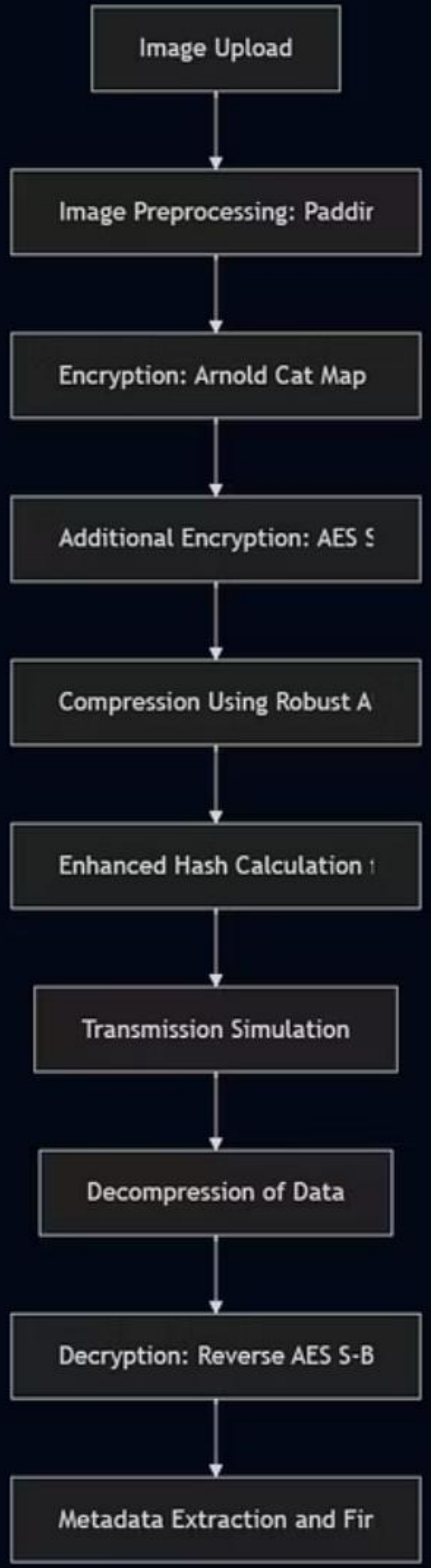


Image Upload

Image Preprocessing: Paddir

Encryption: Arnold Cat Map

Additional Encryption: AES S

Compression Using Robust A

Enhanced Hash Calculation

Transmission Simulation

Decompression of Data

Decryption: Reverse AES S-B

Metadata Extraction and Fir

Mathematical Foundations and Proofs

Arnold Cat Map Reversibility

Transformation matrix features a unit determinant guaranteeing an inverse transformation exists.

Logistic Map Chaos

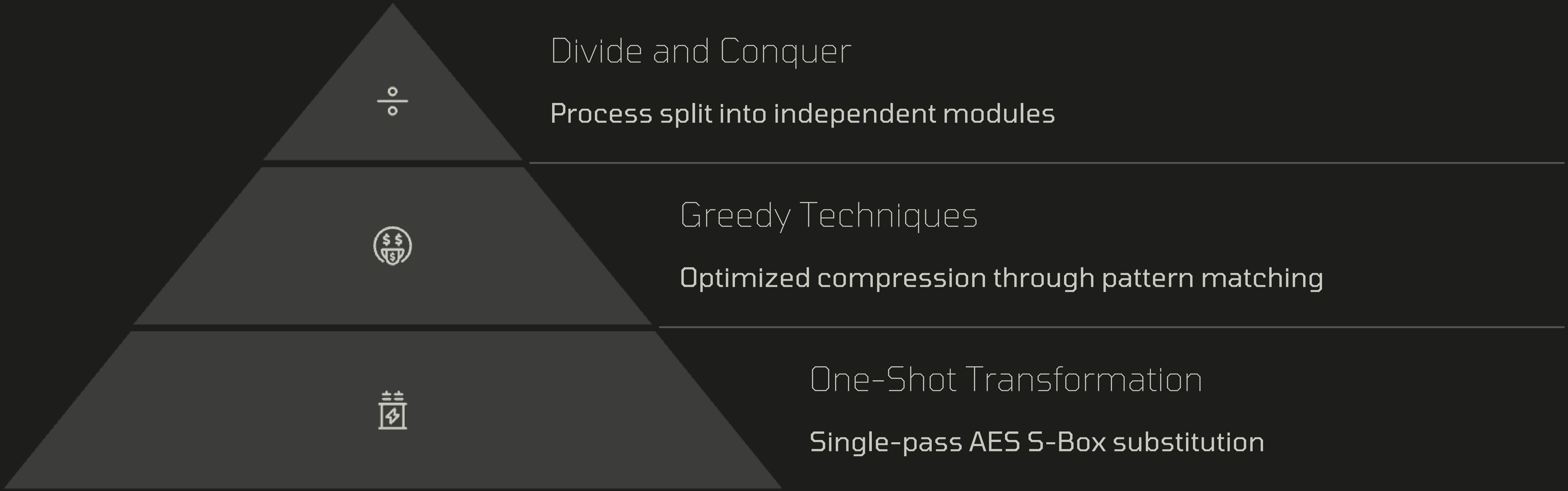
Nonlinear recurrence relation exhibits highly chaotic behavior within a specified parameter range.

XOR Operation Properties

Symmetric operation that is self-inverting, making it ideally suited for reversible encryption.

The mathematical foundations of this encryption system ensure both security and reversibility. The Arnold Cat Map provides deterministic pixel shuffling that can be precisely reversed, while the Logistic Map's sensitivity to initial conditions ensures robust encryption through chaotic behavior.

Algorithmic Paradigms and Approaches



Divide and Conquer

Process split into independent modules

Greedy Techniques

Optimized compression through pattern matching

One-Shot Transformation

Single-pass AES S-Box substitution

The system design leverages several classic algorithmic techniques. Divide and Conquer isolates tasks into distinct modules for better modularity and error isolation. Greedy Techniques optimize compression by finding the longest matching patterns in the data stream. The One-Shot Transformation ensures each byte is substituted without iterative refinement, providing extra confusion and security.

System Architecture and Flowcharts

Input Processing

Image upload, validation, and preprocessing

Encryption Pipeline

Arnold Cat Map shuffling, Logistic Map encryption, AES S-Box substitution

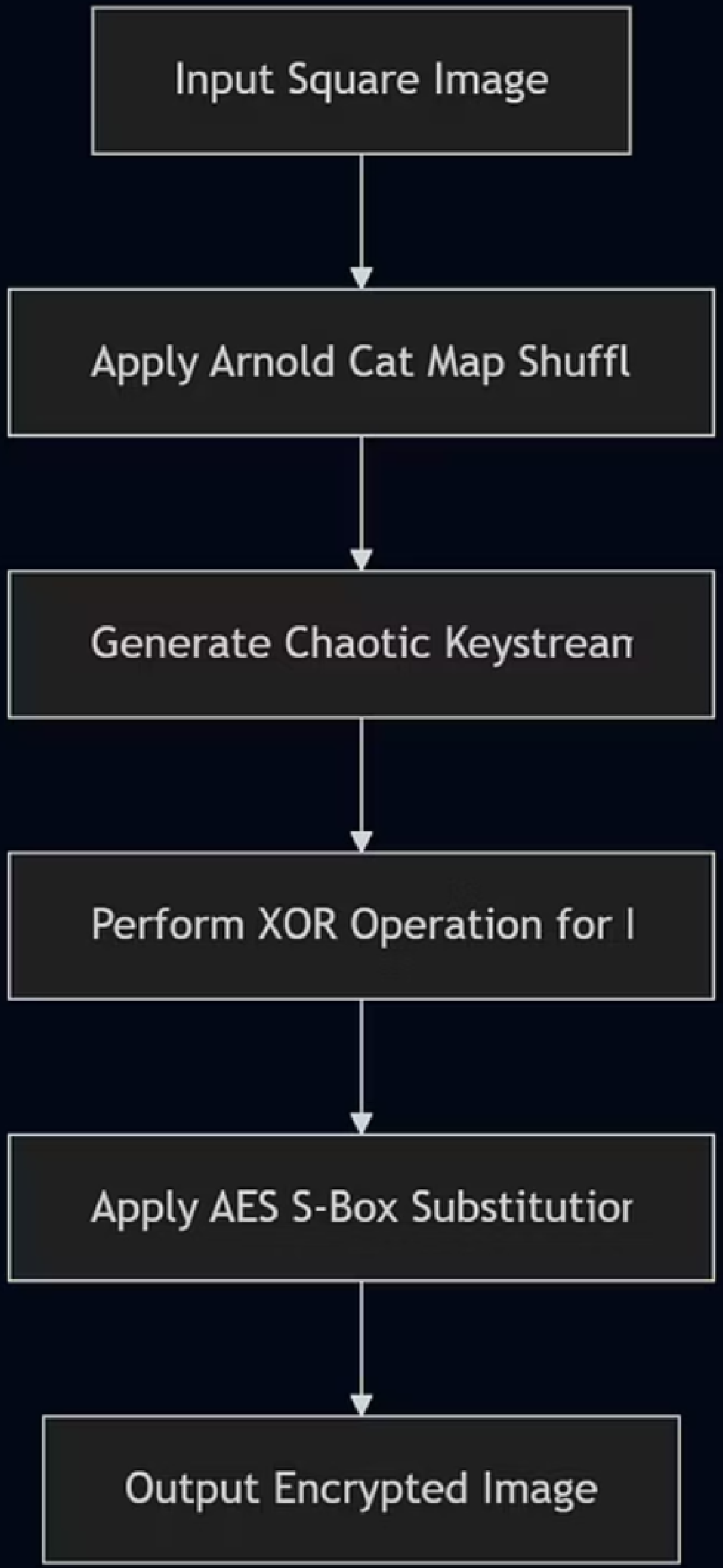
Data Processing

Compression, hashing, and metadata embedding

Decryption Pipeline

Metadata extraction, decompression, inverse operations

The system architecture follows a logical flow from input to output, with clear separation between encryption and decryption processes. Each module handles a specific task, allowing for efficient processing and easy maintenance. The encryption module now incorporates an extra layer for enhanced security.



Input Square Image

Apply Arnold Cat Map Shuffl

Generate Chaotic Keystrean

Perform XOR Operation for I

Apply AES S-Box Substitutior

Output Encrypted Image

Implementation Details

Image Preprocessing

Accepts multiple input forms such as raw bytes or image file paths. Standardizes color mode and ensures square dimensions through resizing or padding. Outputs processed image with original dimension information.

Encryption Routine

Shuffles input image using Arnold Cat Map. Applies chaotic keystream via Logistic Map using XOR operation. Adds AES S-Box substitution layer in a one-shot manner for enhanced security.

Decryption Routine

Reverses encryption steps: inverse AES S-Box lookup, XOR with same keystream, inverse Arnold Cat Map, and padding removal to restore original dimensions.

The implementation is designed for flexibility and robustness. The encrypted image is converted into a byte stream and compressed with a lossless algorithm. An enhanced hash is computed to verify data integrity, while encryption parameters and critical metadata are embedded into the least significant bits of the encrypted image.

Performance and Security Analysis

4

Performance Metrics

Timing for encryption, compression, decompression, and decryption

3

Quality Metrics

MSE, PSNR, SSIM between original and recovered images

2

Security Layers

Dual encryption plus AES S-Box and enhanced hashing

Security is fortified by a layered encryption approach that reduces vulnerability to single-method attacks. The Logistic Map provides chaotic sensitivity, ensuring that even minuscule key changes lead to unusable outputs. Enhanced data integrity verification and secure metadata embedding further strengthen the system.

Key sensitivity tests confirm that slight alterations in the key lead to markedly different and degraded decryption results, demonstrating the system's robustness against brute-force attacks.

Conclusion

This project presents a comprehensive image encryption system that integrates multiple security layers. The system combines spatial shuffling via the Arnold Cat Map with chaotic encryption via the Logistic Map and adds an AES S-Box substitution layer for extra security.

Image data is compressed lossless-ly and its integrity is verified using an enhanced hash algorithm superior to SHA-256. Metadata embedding via steganography ensures that decryption parameters are securely bundled with the image.

Algorithmic techniques such as divide and conquer, greedy methods, and one-shot substitution achieve an effective balance between performance and robust security. Extensive analyses indicate that the system is well suited both for academic research and practical applications in secure image transmission.