Chaos-Based Image Encryption Enhanced by Deep Learning

Muhammad Hamza
Neptun Code: FV8ZPY

MSc Mathematics
Eötvös Loránd University

Supervisor: Dr. Lukács András

January 9, 2026

Outline

Introduction/ Motivation

- Secure image transmission is critical in modern digital communication
- Rapid growth of digital image transmission over open networks
- Traditional encryption schemes are not optimized for images

Introduction/ Motivation

- Secure image transmission is critical in modern digital communication
- Rapid growth of digital image transmission over open networks
- Traditional encryption schemes are not optimized for images
- Images have:
  - High redundancy
  - Strong pixel correlation
  - Large data size

Introduction/ Motivation

- Secure image transmission is critical in modern digital communication
- Rapid growth of digital image transmission over open networks
- Traditional encryption schemes are not optimized for images
- Images have:
  - High redundancy
  - Strong pixel correlation
  - Large data size
- Chaos theory provides:
  - Sensitivity to initial conditions
  - Pseudo-random behavior

Problem Statement

Objective

To design and implement a chaos-based image encryption system that:

- Scrambles pixel positions (permutation)
- Diffuses pixel values (confusion)
- Uses pseudo-random chaotic sequences
- Allows reversible decryption

Problem Statement

Objective

To design and implement a chaos-based image encryption system that:

- Scrambles pixel positions (permutation)
- Diffuses pixel values (confusion)
- Uses pseudo-random chaotic sequences
- Allows reversible decryption

Main Challenge

Ensuring strict reversibility under:

- Finite-precision arithmetic
- Floating-point overflow
- Numerical instability

Literature Review

- Zhou, Zhao, Wang (2022)
- Hybrid cryptosystem:
  - 4D hyper-chaotic Lorenz system
  - LSTM neural networks
- Deep learning enhances unpredictability of chaotic signals

Literature Review

- Zhou, Zhao, Wang (2022)
- Hybrid cryptosystem:
  - 4D hyper-chaotic Lorenz system
  - LSTM neural networks
- Deep learning enhances unpredictability of chaotic signals

Key idea adopted:

- Chaos + Deep Learning = Larger key space + stronger security

Literature Review

- Zhou, Zhao, Wang (2022)
- Hybrid cryptosystem:
  - 4D hyper-chaotic Lorenz system
  - LSTM neural networks
- Deep learning enhances unpredictability of chaotic signals

Key idea adopted:

- Chaos + Deep Learning = Larger key space + stronger security

References:

- S. Zhou, Z. Zhao, and X. Wang, Novel chaotic colour image cryptosystem with deep learning, Chaos, Solitons and Fractals, vol. 161, p. 112380, 2022.

Role of Chaotic Systems

- Chaotic systems exhibit:
  - Sensitivity to initial conditions
  - Ergodicity
  - Pseudo-random behavior

Role of Chaotic Systems

- Chaotic systems exhibit:
  - Sensitivity to initial conditions
  - Ergodicity
  - Pseudo-random behavior
- Small changes in initial parameters produce significantly different sequences
- Ideal for:
  - Pixel permutation
  - Diffusion control
  - Key generation

Two-Stage Encryption Scheme

Stage 1: Permutation

- Pixel positions are scrambled
- Controlled by chaotic sequences

Two-Stage Encryption Scheme

Stage 1: Permutation

- Pixel positions are scrambled
- Controlled by chaotic sequences

Stage 2: Diffusion

- XOR-based masking
- High sensitivity to plaintext changes

Image Encryption Results

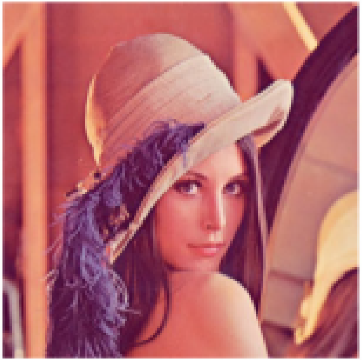

Figure: *

(a) Original Image

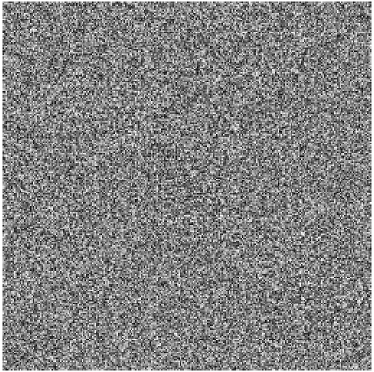

Figure: *

(b) Encrypted Image

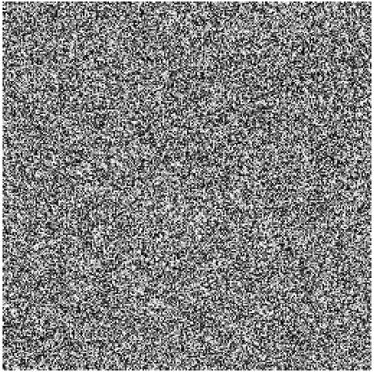

Figure: *

(c) Decrypted Image

Figure: Comparison of Original, Encrypted, and Decrypted Images

Histogram Analysis

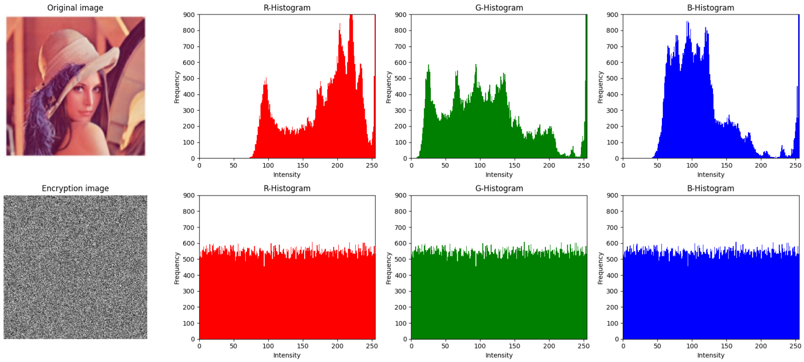

Figure: Histogram Comparison: Original vs Encrypted Image

Histogram Analysis

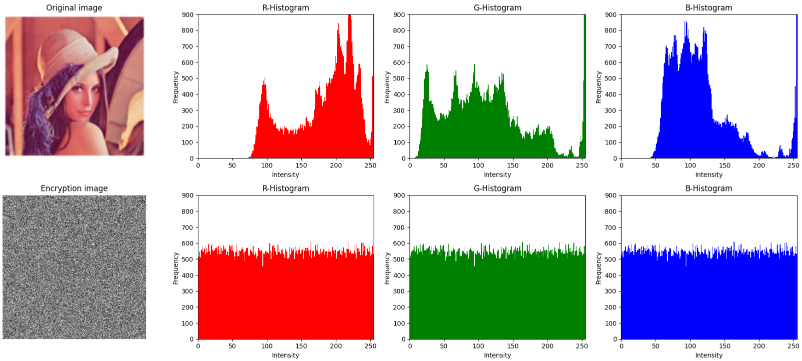

Figure: Histogram Comparison: Original vs Encrypted Image

- Uniform histogram after encryption
- Prevents statistical attacks

Pixel Correlation Analysis

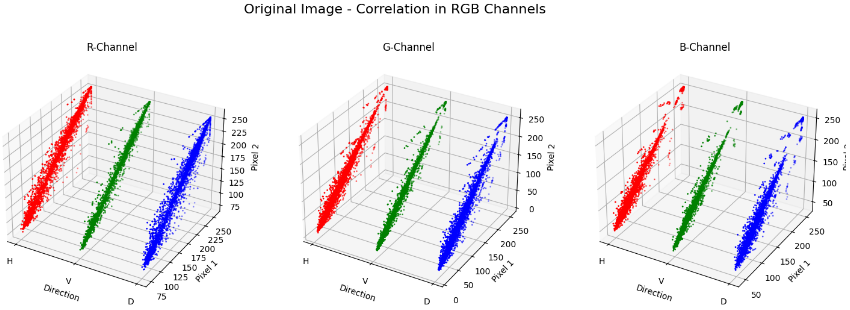

Figure: Pixel Correlation Before Encryption

Pixel Correlation Analysis

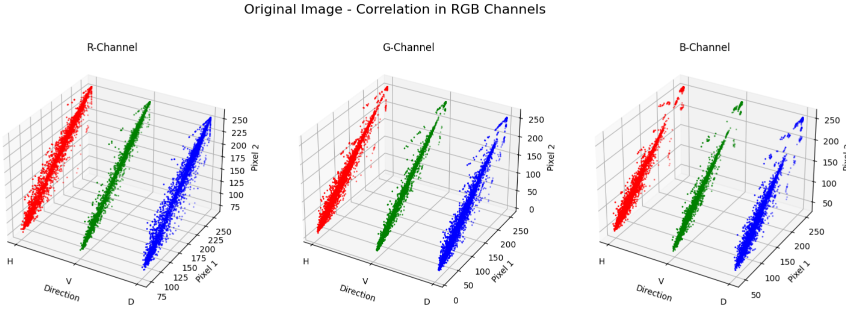

Figure: Pixel Correlation Before Encryption

- Original image: strong correlation

Pixel Correlation Analysis

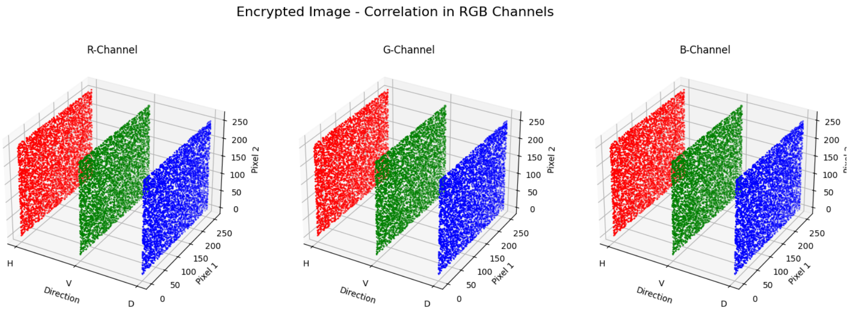

Figure: Pixel Correlation After Encryption

Pixel Correlation Analysis

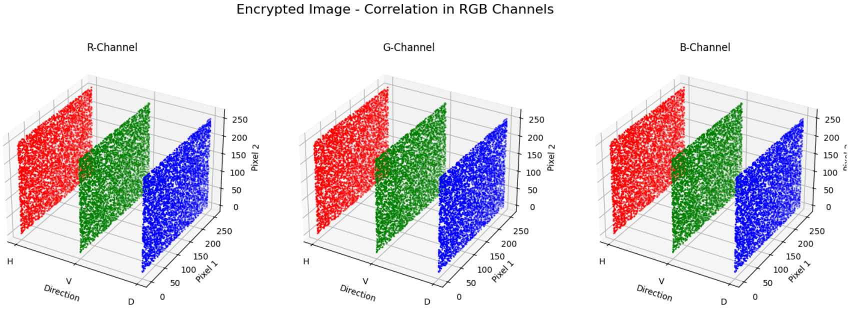

Figure: Pixel Correlation After Encryption

- Encrypted image: near-zero correlation

Security Metrics

- NPCR: High sensitivity to single-pixel changes
- UACI: Strong diffusion performance
- Entropy ≈ 8: Near-ideal randomness

Security Metrics

- NPCR: High sensitivity to single-pixel changes
- UACI: Strong diffusion performance
- Entropy ≈ 8: Near-ideal randomness

Conclusion

The encryption scheme satisfies major security requirements.

Observed Limitations

- Decryption is not perfectly lossless
- Floating-point precision issues
- Overflow in diffusion operations

Observed Limitations

- Decryption is not perfectly lossless
- Floating-point precision issues
- Overflow in diffusion operations

Key Insight

Cryptographic reversibility requires strict numerical control.

Plan for Next Semester

- Replace floating-point with integer arithmetic
- Strict inverse permutation and diffusion
- Improve numerical stability
- Extensive sensitivity and robustness testing

Plan for Next Semester

- Replace floating-point with integer arithmetic
- Strict inverse permutation and diffusion
- Improve numerical stability
- Extensive sensitivity and robustness testing

Goal

Perfect image reconstruction with strong encryption.

Conclusion

- Chaos-based encryption is highly effective
- LSTM improves randomness and key space
- Numerical rigor is critical for reversibility

Use of AI Tools in Code Development

- Python code for this project was developed with the assistance of AI tools:
  - **ChatGPT**
  - **Google Gemini**
- AI assistance was used for:
  - Writing initial Python code snippets
  - Structuring and formatting code
  - Suggesting improvements and debugging
- All final code was reviewed, modified, and verified

Thank You for Your Attention

Questions and Discussion

Muhammad Hamza
MSc Mathematics, ELTE