# Chaos-Based Image Encryption Enhanced by Deep Learning

Muhammad Hamza
Neptun code: FV8ZPY
Supervisor: Dr. Lukács András

MSc Mathematics, Institute of Mathematics, ELTE

June 4, 2026

Eötvös Loránd University (ELTE)

# Outline

- Motivation
- Literature Review
- Problem Statement
- Proposed Framework
- Chaotic System
- Results and Security Analysis
- Conclusion
- References

# Motivation

**Why does cryptography matter?**

- Cryptography protects private information during communication.

# Motivation

**Why does cryptography matter?**

- Cryptography protects private information during communication.
- It supports confidentiality, integrity, authentication, and trust.

# Motivation

**Why does cryptography matter?**

- Cryptography protects private information during communication.
- It supports confidentiality, integrity, authentication, and trust.
- It is widely used in email, VPNs, messaging apps, and secure digital services.

# Motivation

**Why does cryptography matter?**

- Cryptography protects private information during communication.
- It supports confidentiality, integrity, authentication, and trust.
- It is widely used in email, VPNs, messaging apps, and secure digital services.

**Image encryption** is important because digital images contain large amounts of visual information and are frequently shared across networks.

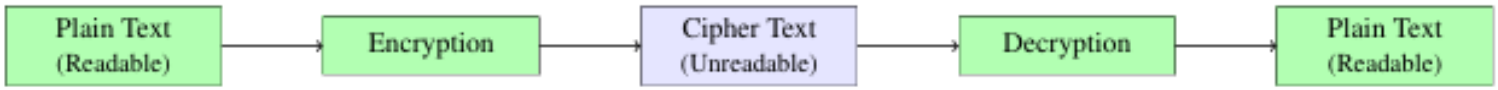



Figure: Cryptographic Process

# Literature Reviewed

**Main reference studied:**

- Zhou, Zhao, and Wang proposed a **chaotic colour image cryptosystem with deep learning**. (1)

# Literature Reviewed

**Main reference studied:**

- Zhou, Zhao, and Wang proposed a **chaotic colour image cryptosystem with deep learning**. (1)
- The method combines a **4D hyper-chaotic Lorenz system** with **LSTM neural networks**. (2)

# Literature Reviewed

**Main reference studied:**

- Zhou, Zhao, and Wang proposed a **chaotic colour image cryptosystem with deep learning**. (1)
- The method combines a **4D hyper-chaotic Lorenz system** with **LSTM neural networks**. (2)
- Chaotic systems provide deterministic but unpredictable sequences for secret key generation, pixel scrambling, and diffusion.

# Literature Reviewed

**Main reference studied:**

- Zhou, Zhao, and Wang proposed a **chaotic colour image cryptosystem with deep learning**. (1)
- The method combines a **4D hyper-chaotic Lorenz system** with **LSTM neural networks**. (2)
- Chaotic systems provide deterministic but unpredictable sequences for secret key generation, pixel scrambling, and diffusion.

**Central idea:** Use chaos for randomness and deep learning to enhance the unpredictability of the generated sequences.

# Problem Statement

This work investigates image encryption using pseudorandom matrices and sequence-based transformations implemented in Python.

# Problem Statement

This work investigates image encryption using pseudorandom matrices and sequence-based transformations implemented in Python.

- Pixel permutation hides spatial structure.

# Problem Statement

This work investigates image encryption using pseudorandom matrices and sequence-based transformations implemented in Python.

- Pixel permutation hides spatial structure.
- Channel diffusion and arithmetic masking change pixel values.

# Problem Statement

This work investigates image encryption using pseudorandom matrices and sequence-based transformations implemented in Python.

- Pixel permutation hides spatial structure.
- Channel diffusion and arithmetic masking change pixel values.
- The same pseudorandom data must be used during decryption.

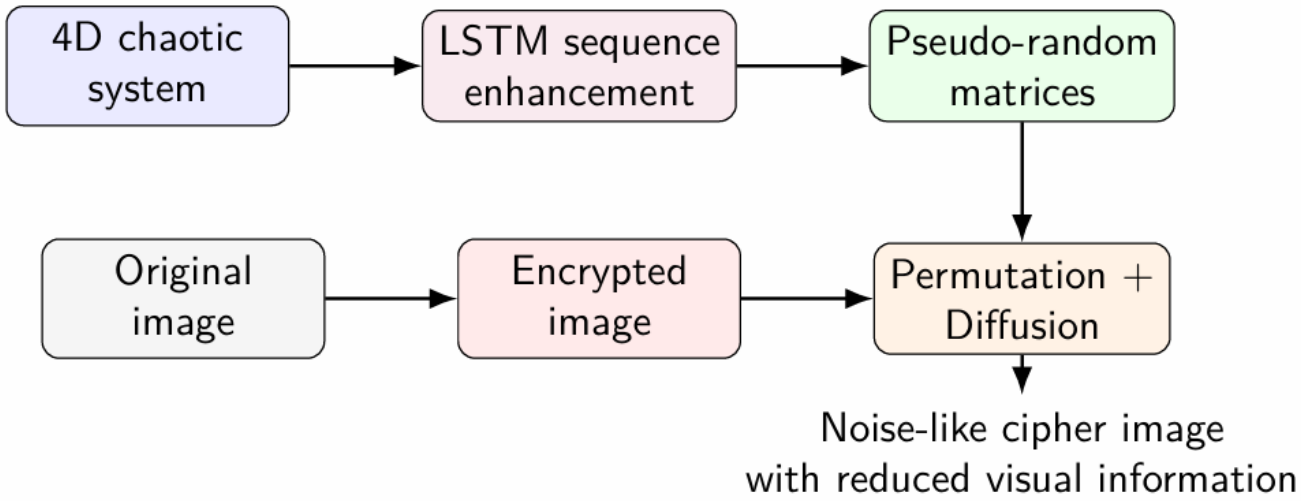
# Problem Statement

This work investigates image encryption using pseudorandom matrices and sequence-based transformations implemented in Python.

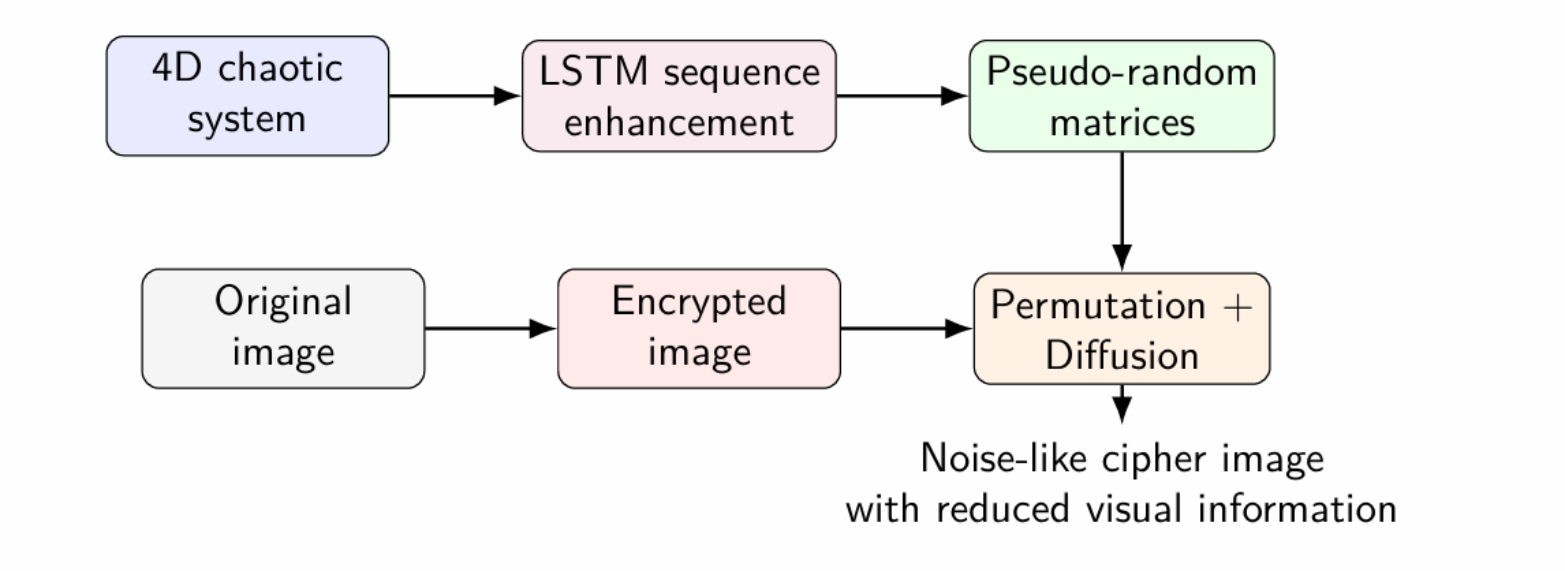
- Pixel permutation hides spatial structure.
- Channel diffusion and arithmetic masking change pixel values.
- The same pseudorandom data must be used during decryption.

**Key practical challenge:**
The encryption decryption pipeline must be strictly reversible despite finite precision arithmetic, data type bounds, overflow, and inversion order issues.

# Proposed Framework

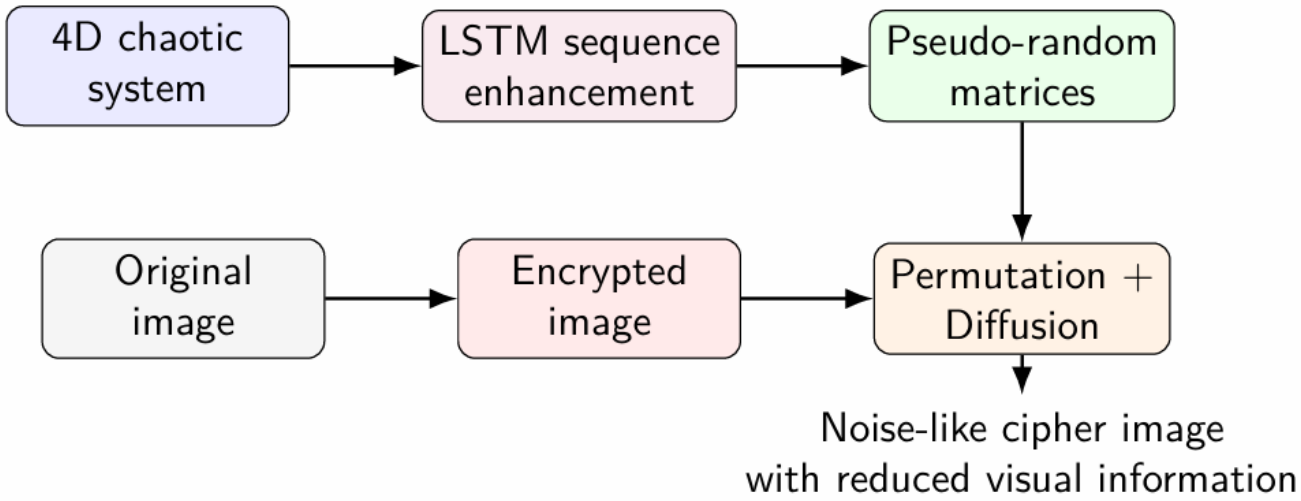


# Proposed Framework



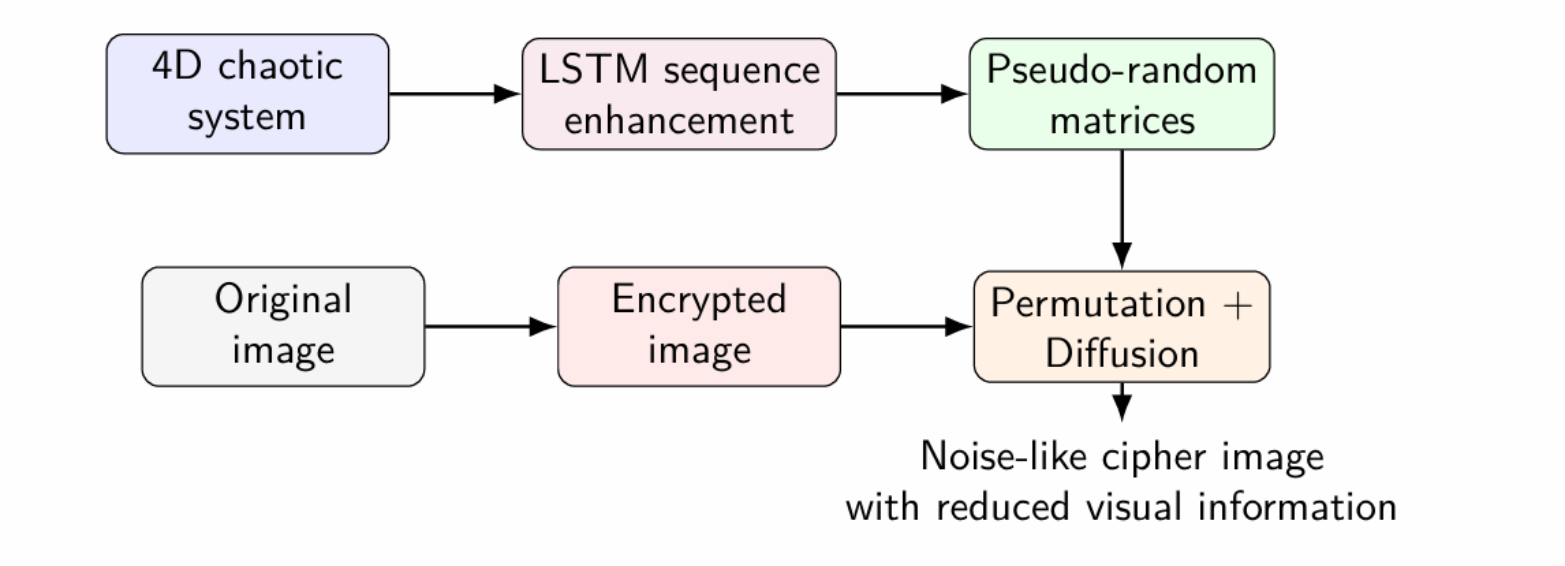

- Chaotic signals generate encryption sequences.

# Proposed Framework




- Chaotic signals generate encryption sequences.
- LSTM improves randomness and unpredictability.

# Proposed Framework




- Chaotic signals generate encryption sequences.
- LSTM improves randomness and unpredictability.
- Encryption uses scrambling and diffusion to hide image content.

# Chaotic System

The implementation uses a 4D chaotic system (3):

$$\begin{cases} x_1' = a(x_2 - x_1) + x_2 x_3 x_4, \\ x_2' = b(x_1 + x_2) - x_1 x_3 x_4, \\ x_3' = -cx_3 + x_1 x_2 x_4, \\ x_4' = -dx_4 + x_1 x_2 x_3. \end{cases}$$

# Chaotic System

The implementation uses a 4D chaotic system (3):

$$\begin{cases} x_1' = a(x_2 - x_1) + x_2 x_3 x_4, \\ x_2' = b(x_1 + x_2) - x_1 x_3 x_4, \\ x_3' = -c x_3 + x_1 x_2 x_4, \\ x_4' = -d x_4 + x_1 x_2 x_3. \end{cases}$$

- $a, b, c, d$ are system parameters.

# Chaotic System

The implementation uses a 4D chaotic system (3):

$$\begin{cases} x_1' = a(x_2 - x_1) + x_2 x_3 x_4, \\ x_2' = b(x_1 + x_2) - x_1 x_3 x_4, \\ x_3' = -cx_3 + x_1 x_2 x_4, \\ x_4' = -dx_4 + x_1 x_2 x_3. \end{cases}$$

- $a, b, c, d$ are system parameters.
- $x_1, x_2, x_3, x_4$ are state variables.

# Chaotic System

The implementation uses a 4D chaotic system (3):

$$\begin{cases} x_1' = a(x_2 - x_1) + x_2 x_3 x_4, \\ x_2' = b(x_1 + x_2) - x_1 x_3 x_4, \\ x_3' = -cx_3 + x_1 x_2 x_4, \\ x_4' = -dx_4 + x_1 x_2 x_3. \end{cases}$$

- $a, b, c, d$ are system parameters.
- $x_1, x_2, x_3, x_4$ are state variables.
- Chaotic trajectories are used to create random like sequences

# Chaotic System Projections

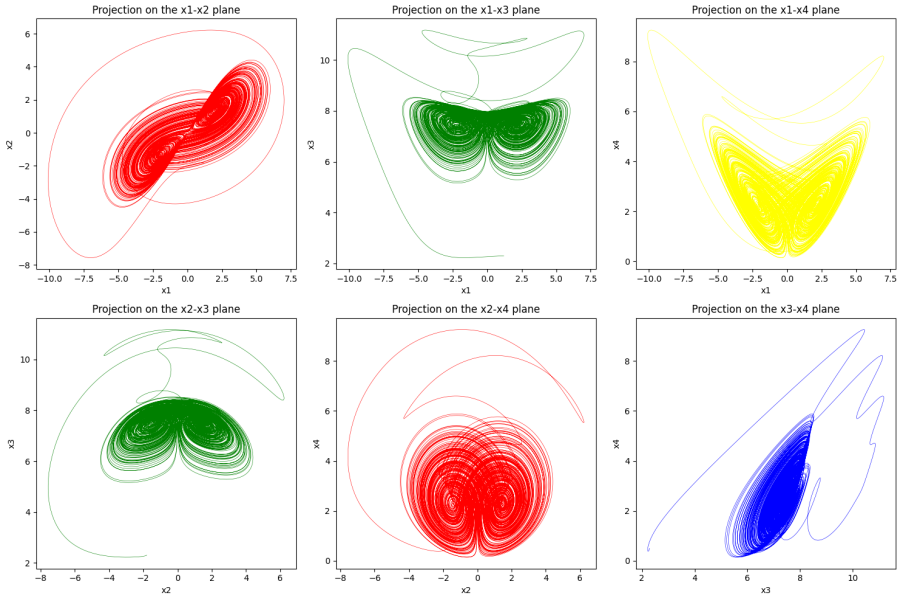



Figure: 2D-projection

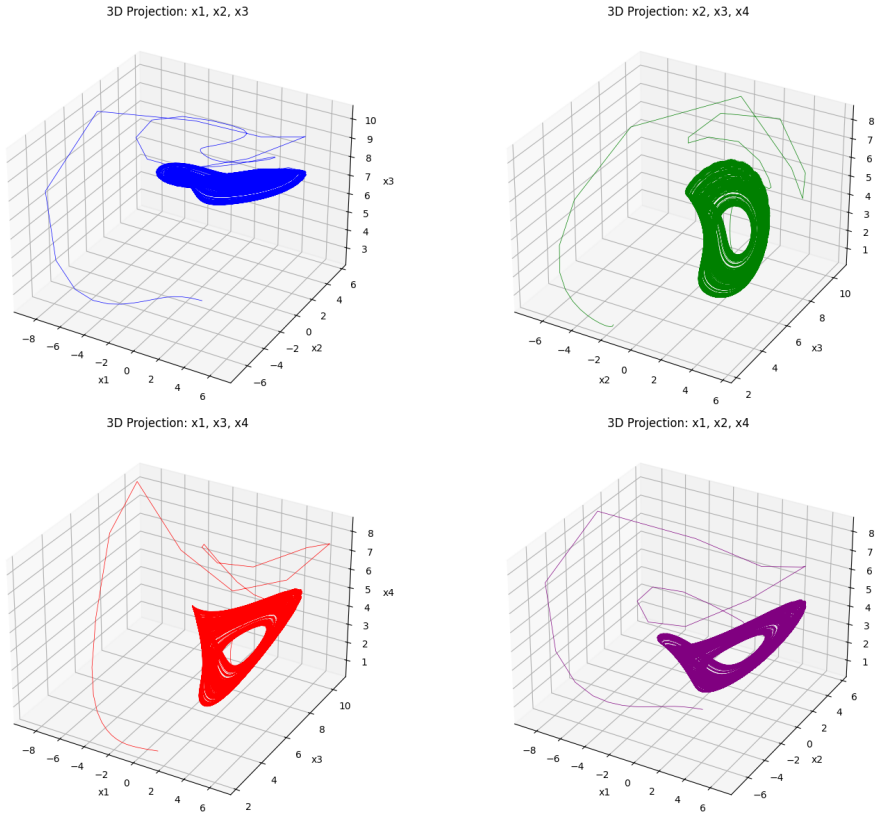



Figure: 3D-projection

- The projections show sensitive, non-periodic chaotic behavior suitable for pseudorandom sequence generation.

# LSTM-Enhanced Chaotic Signal Generation

- An LSTM model is trained on sequences from the chaotic system.
- Predicted sequences preserve chaotic properties.
- Deep learning adds additional unpredictability to the key-generation process.

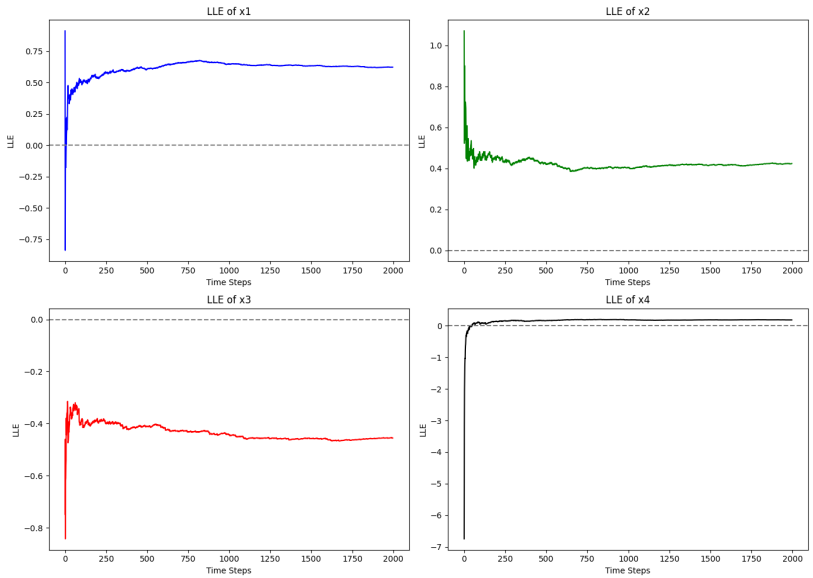



Figure: Largest Lyapunov exponent plots

**largest Lyapunov exponents:**

[0.880917, 0.918967, 1.349992, 0.914473]

All are positive, indicating chaotic behavior.

# Two-Stage Encryption

**Stage 1: Pixel scrambling / permutation**

Rearranges pixel positions so the spatial structure of the original image disappears.

# Two-Stage Encryption

**Stage 1: Pixel scrambling / permutation**
Rearranges pixel positions so the spatial structure of the original image disappears.

**Stage 2: Diffusion / masking**
Changes pixel values using chaotic pseudorandom matrices and sequence operations, so small plaintext changes produce large ciphertext changes.

# Two-Stage Encryption

**Stage 1: Pixel scrambling / permutation**
Rearranges pixel positions so the spatial structure of the original image disappears.

**Stage 2: Diffusion / masking**
Changes pixel values using chaotic pseudorandom matrices and sequence operations, so small plaintext changes produce large ciphertext changes.

- Encryption aims to produce a noise-like image.

# Two-Stage Encryption

**Stage 1: Pixel scrambling / permutation**
Rearranges pixel positions so the spatial structure of the original image disappears.

**Stage 2: Diffusion / masking**
Changes pixel values using chaotic pseudorandom matrices and sequence operations, so small plaintext changes produce large ciphertext changes.

- Encryption aims to produce a noise-like image.
- Decryption applies inverse operations using the same pseudorandom data.

# Two-Stage Encryption

**Stage 1: Pixel scrambling / permutation**
Rearranges pixel positions so the spatial structure of the original image disappears.

**Stage 2: Diffusion / masking**
Changes pixel values using chaotic pseudorandom matrices and sequence operations, so small plaintext changes produce large ciphertext changes.

- Encryption aims to produce a noise-like image.
- Decryption applies inverse operations using the same pseudorandom data.
- Strict reversibility is essential for lossless recovery.

# Results

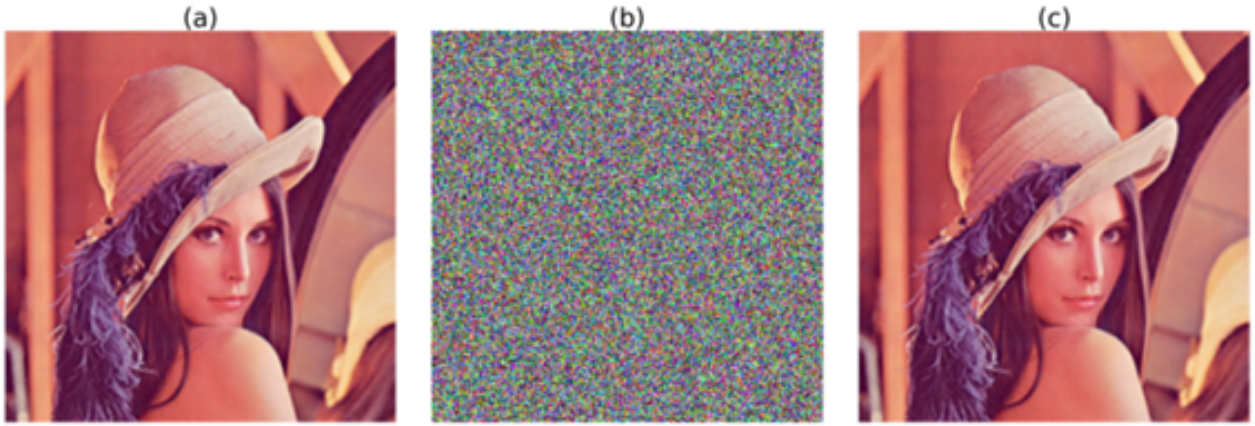



Figure: Original, encrypted, and decrypted images

- The encrypted image visually hides the original content.

# Results

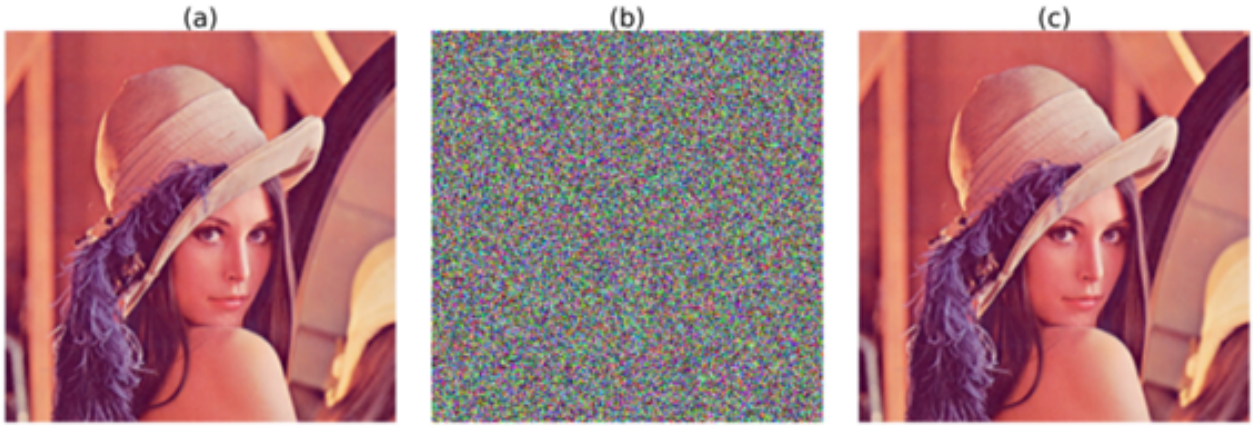



Figure: Original, encrypted, and decrypted images

- The encrypted image visually hides the original content.
- The decrypted image is close to the original, demonstrating the inverse pipeline.

# Results

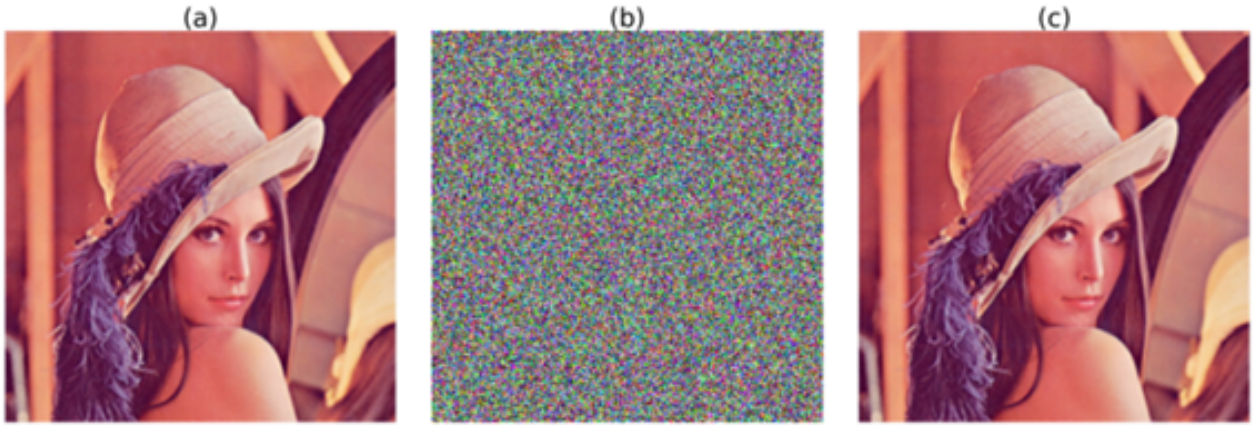



Figure: Original, encrypted, and decrypted images

- The encrypted image visually hides the original content.
- The decrypted image is close to the original, demonstrating the inverse pipeline.
- The report notes that exact lossless recovery requires careful numerical handling

# Correlation Analysis

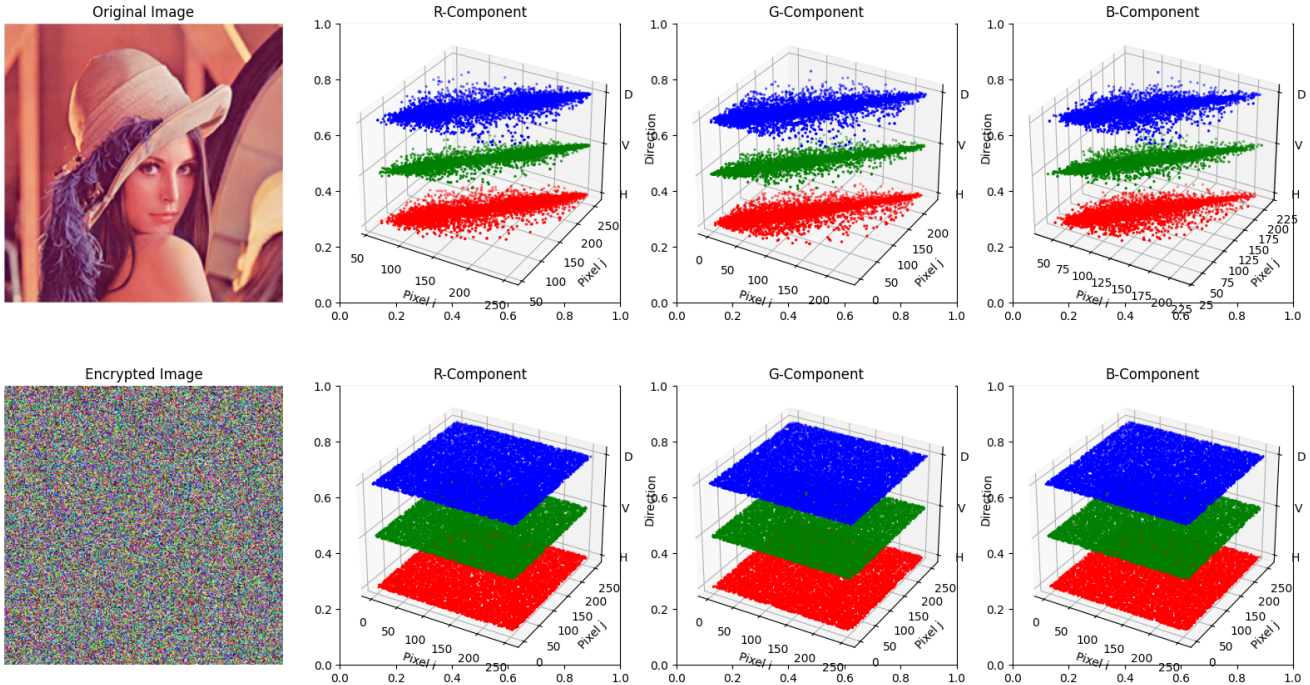



Figure: Correlation Analysis of Adjacent Pixels in Original and Encrypted Images

- Original images show visible correlation; encrypted images are much more uniform and independent.

# Histogram Analysis

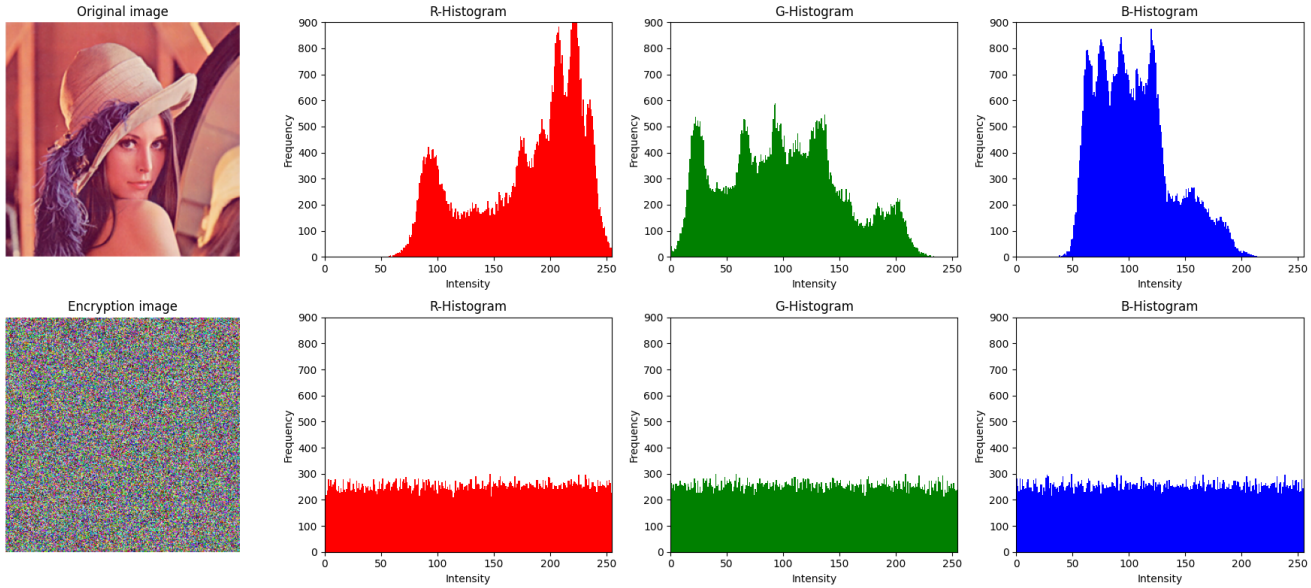



Figure: Histogram of original images and encrypted images

- The encrypted histogram is flatter and more evenly distributed, supporting resistance to statistical attacks.

# Security Indicators

- **Entropy close to 8**
  High randomness in encrypted image.

# Security Indicators

- **Entropy close to 8**
  High randomness in encrypted image.
- **Low pixel correlation**
  Adjacent pixels become statistically independent.

# Security Indicators

- **Entropy close to 8**
  High randomness in encrypted image.
- **Low pixel correlation**
  Adjacent pixels become statistically independent.
- **High NPCR**
  Strong sensitivity to small plaintext changes.

# Security Indicators

- **Entropy close to 8**
  High randomness in encrypted image.
- **Low pixel correlation**
  Adjacent pixels become statistically independent.
- **High NPCR**
  Strong sensitivity to small plaintext changes.
- **High UACI**
  Large average intensity change after tiny input changes.

# Security Indicators

- **Entropy close to 8**
  High randomness in encrypted image.
- **Low pixel correlation**
  Adjacent pixels become statistically independent.
- **High NPCR**
  Strong sensitivity to small plaintext changes.
- **High UACI**
  Large average intensity change after tiny input changes.
- **Key sensitivity**
  Wrong key prevents correct decryption.

# Security Indicators

- **Entropy close to 8**
  High randomness in encrypted image.
- **Low pixel correlation**
  Adjacent pixels become statistically independent.
- **High NPCR**
  Strong sensitivity to small plaintext changes.
- **High UACI**
  Large average intensity change after tiny input changes.
- **Key sensitivity**
  Wrong key prevents correct decryption.
- **Expanded key space**
  More resistance to brute-force attacks.

# Security Indicators

- **Entropy close to 8**
  High randomness in encrypted image.
- **Low pixel correlation**
  Adjacent pixels become statistically independent.
- **High NPCR**
  Strong sensitivity to small plaintext changes.
- **High UACI**
  Large average intensity change after tiny input changes.
- **Key sensitivity**
  Wrong key prevents correct decryption.
- **Expanded key space**
  More resistance to brute-force attacks.

Together, these indicators show that the chaotic LSTM method is designed to resist statistical, differential, and brute force attacks.

# Conslusion

- The project combines a 4D chaotic system and an LSTM network for color image encryption.

# Conslusion

- The project combines a 4D chaotic system and an LSTM network for color image encryption.
- LSTM-enhanced chaotic sequences improve unpredictability for pseudorandom matrix generation.

# Conslusion

- The project combines a 4D chaotic system and an LSTM network for color image encryption.
- LSTM-enhanced chaotic sequences improve unpredictability for pseudorandom matrix generation.
- Scrambling and diffusion effectively hide image content and reduce statistical structure.

# Conslusion

- The project combines a 4D chaotic system and an LSTM network for color image encryption.
- LSTM-enhanced chaotic sequences improve unpredictability for pseudorandom matrix generation.
- Scrambling and diffusion effectively hide image content and reduce statistical structure.
- Security analysis supports high randomness, low correlation, key sensitivity, and strong resistance to attacks.

# Conslusion

- The project combines a 4D chaotic system and an LSTM network for color image encryption.
- LSTM-enhanced chaotic sequences improve unpredictability for pseudorandom matrix generation.
- Scrambling and diffusion effectively hide image content and reduce statistical structure.
- Security analysis supports high randomness, low correlation, key sensitivity, and strong resistance to attacks.

**Future improvement:**
Strengthen exact reversibility by controlling data types, modular arithmetic, overflow behavior, and inverse-operation ordering.

# 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.

# References I


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

[2] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.

[3] Qi, G., Du, S., Chen, G., Chen, Z. (2005). On a four-dimensional chaotic system. Chaos, Solitons Fractals, 23(5), 1671-1682.

# Thank you for your attention

Eötvös Loránd University (ELTE)