Eötvös Loránd University

Chaos-Based Image Encryption Enhanced by Deep Learning

Project Report

Submitted by	Muhammad Hamza
Neptun code	FV8ZPY
Course title	Directed Studies 2
Supervisors name	Dr. Lukács András
MSc Mathematics, Institute of Mathematics, ELTE	

1. Introduction

Cryptography is the science and practice of keeping secure communication. It refers to the methods used to keep private information sent between two parties out of the hands of the public or third parties [1].

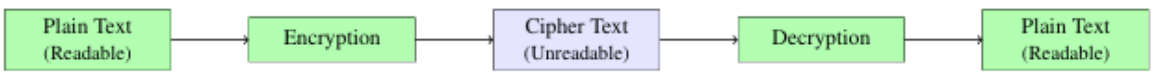

Figure 1: Cryptographic process

The same key, known as the Secret Key, is utilized for both encryption and decryption in symmetric-key cryptography. Both the sender and the receiver must have this key before any secure communication can occur. It is highly efficient for encrypting large

datasets. Asymmetric key cryptography, commonly referred to as public-key cryptography, is a cryptographic method that employs two keys that are theoretically connected but different.

2. Applications of Cryptography

Cryptography also plays a crucial role in secure communication apps, such as email, virtual private networks (VPNs), and messaging apps, securing and protecting against unauthorized access. Furthermore, cryptography techniques are essential in postquantum cryptography, which protects data against future quantum threats, especially relevant for IoT systems and secure communication channels. Overall, cryptography techniques are the backbone of modern digital security structures, ensuring trust, accountability, security, confidentiality, and integrity across different applications.

3. Literature Reviewed

The primary work studied is the paper by Zhou, Zhao, and Wang entitled *Novel Chaotic Colour Image Cryptosystem with Deep Learning*, published in *Chaos, Solitons and Fractals* (2022) [2]. The authors propose a hybrid cryptosystem that integrates a 4D hyperchaotic Lorenz system with Long Short-Term Memory (LSTM) neural networks [3]. Digital images are frequently used as information carriers in networks because they are straightforward to use and contain a large amount of information [4]. Chaos theory was developed in the 1960s by the American scientist Edward Lorenz [5]. Chaotic systems play a crucial role in the encryption of images in contemporary cryptographic algorithms. It is used to generate sequences that exhibit randomness and unpredictability, yet are deterministic. Additionally, these sequences are utilized to construct the secret key for image encryption, encrypt the image pixels, modify the pixel values (diffusion), and scramble the image pixels (scrambling) [6] [7].

4. Problem Statement

This project talks about the problem of encryption of digital images using pseudorandom matrices and sequence-based transformations using Python (Google Colab). The specified technique uses the pixel permuting strategy, channel diffusion and arithmetic masking process of the original image to conceal the graphic pattern and to protect the message. The encryption keys are pseudorandom matrices and sequences which are initialised with external data files to control the scrambling and diffusion process. Decryption stage is

intended to reverse these processes using the same pseudorandom data to retrieve the original image. Among the primary challenges that have been taken into consideration in this work is the necessity to ensure that the encryption-decryption pipeline is always strictly reversible, in case finite-precision arithmetic and data type bounds are also present together with the correct order of invoking the inverse operations.

According to this Python implementation, it can be concluded that the provided encryption scheme is efficient in visually cloaking the content of the initial image as the result of its encryption has a noise-like nature and has no shape. This process of decryption is not however a complete re-creation of the original image meaning that the system of encryption-decryption is not purely lossless. The difference identifies some practical limitations due to overflow in the data type and floating-point representation of pseudorandom matrices, and insignificant flaws in the inversion of permutation and diffusion steps. Thus, it can be seen that on the one hand, the project is successful in demonstrating the principles of image scrambling and encryption, and on the other, it shows the importance of rigorous numerical manipulation and strictly invertible operations to the structure of a powerful image encryption algorithm. The outcomes infer the notion that more enhancement is required to restore the original image to its full extent.

5. Main Ideas and Technical Contributions

5.1. LSTM-Enhanced Chaotic Signal Generation

This train an LSTM network on sequences generated by a hyper-chaotic Lorenz system to produce new chaotic signals. These retain chaotic behavior while introducing additional unpredictability.

5.2. Two-Stage Encryption Architecture

The encryption process includes pixel scrambling followed by diffusion using cascaded XOR operations, ensuring strong sensitivity to plaintext changes.

5.3. Expanded Key Space

The integration of chaotic initial conditions with deep learning parameters significantly enlarges the key space beyond brute-force feasibility.

5.4. Security Validation

High NPCR and UACI values, near-zero pixel correlation, and entropy values close to 8 confirm strong security properties.

5.5. Implementation Results and Observations

Four-Dimensional Chaotic System

Guoyuan Qi et al. [8] proposed a four-dimensional chaotic system, described by the following equations.

$$\begin{cases} x_1' = a(x_2 - x_1) + x_2x_3x_4, \\ x_2' = b(x_1 + x_2) - x_1x_3x_4, \\ x_3' = -cx_3 + x_1x_2x_4, \\ x_4' = -dx_4 + x_1x_2x_3. \end{cases}$$

Here, a, b, c, d are system parameters that control the dynamics of the system, while x_1, x_2, x_3, x_4 are state variables. These equations, implemented in Python programming, generate the 3D and 2D projections of this chaotic system. Figures show the three-dimensional and two-dimensional projections of our chaotic system.

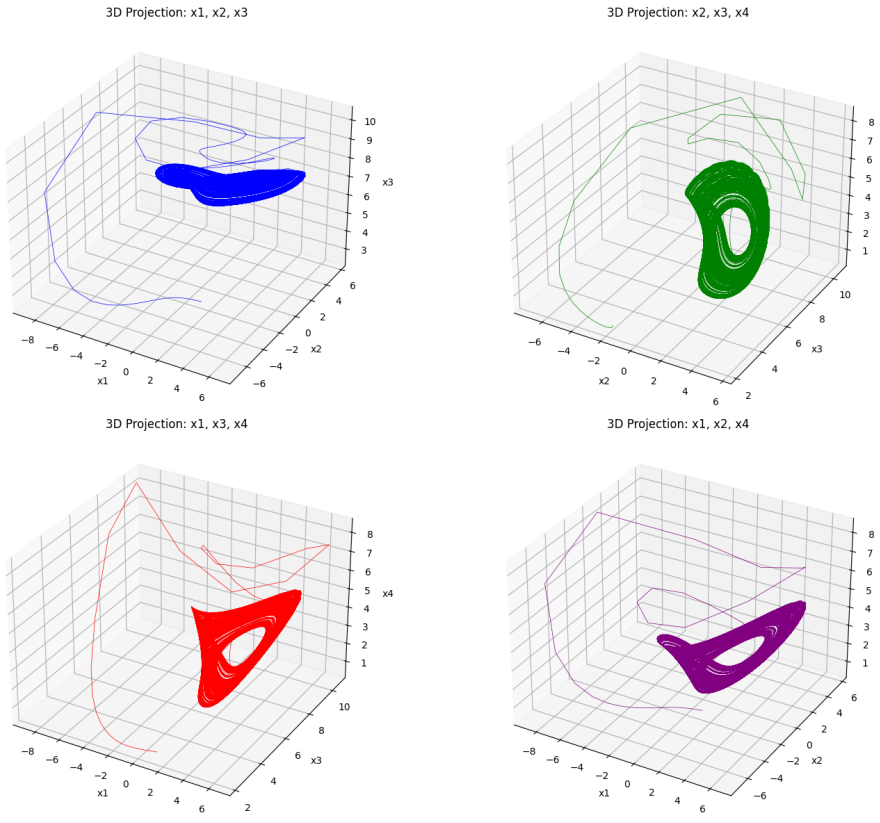

Figure 2: Three dimensional projection of the 4D chaotic system

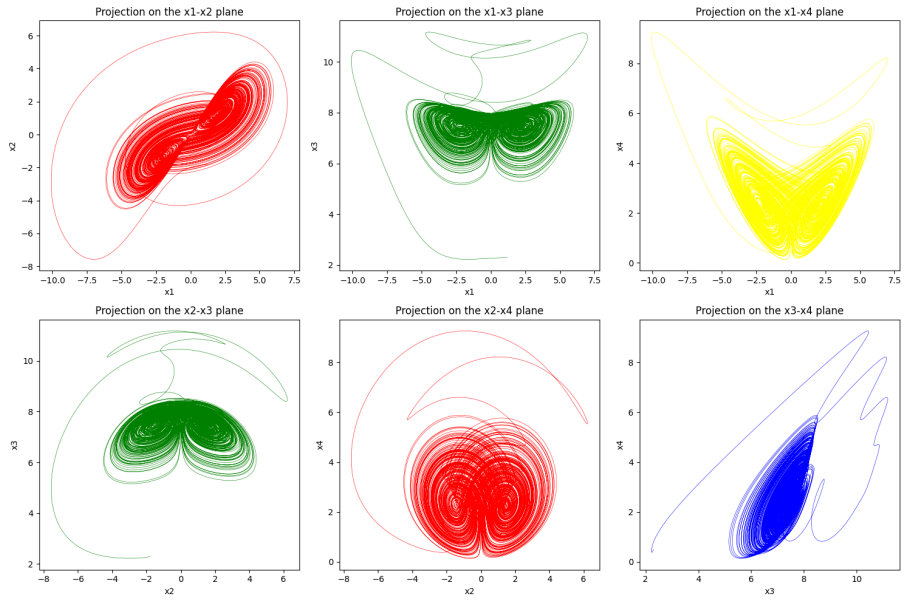

Figure 3: Two dimensional projection of the 4D chaotic system

Largest Lyapunov Exponent

Mathematically, Largest Lyapunov Exponent is defined as:

$$\lambda_1 = \frac{1}{t_N - t_0} \sum_{i=1}^{N} \log_2 \frac{D'(t_i)}{D(t_{i-1})}.$$

where N is total number of steps, $t_N - t_0$ is the difference of time, and $D(t_i)$ is the distance between phase space reconstruction at time t_i and its neighborhood.

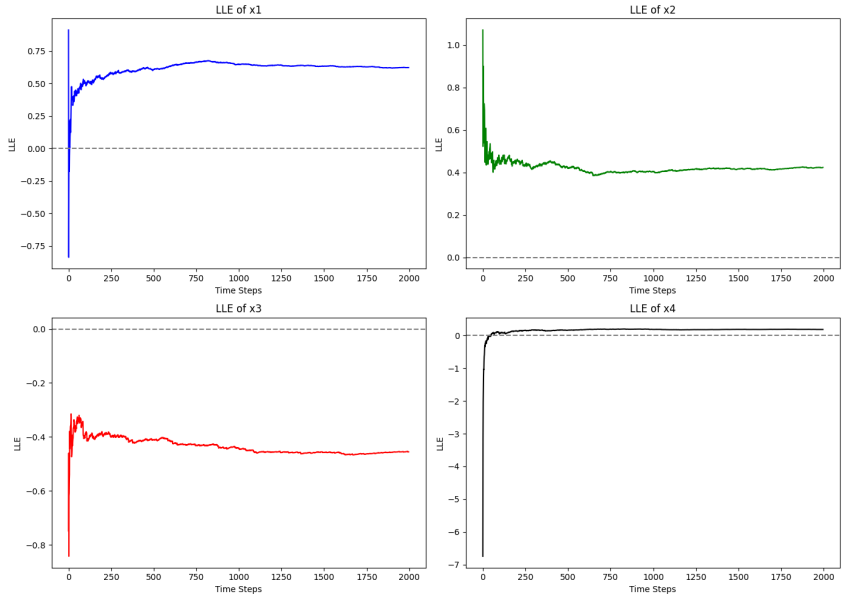

Figure 4: Loss function and root mean square error (RMSE) for each of the four variables.

To test whether the predicted sequences x_i, y_i, z_i, w_i generated by the LSTM model fulfilled the chaotic properties. We will use the method to calculate the largest Lyapunov exponent. As shown in above Figure, the curve remains above y=0. This shows that the predicted sequences retain the chaotic nature of the original system. The final stabilized values of the largest Lyapunov exponent are [0.880917, 0.918967, 1.349992, 0.914473], and all of these are positive.

Proposed Images Encryption and Decryption

In order to improve the security and randomness of the proposed image encryption algorithm, the LSTM deep learning algorithm and a four-dimensional chaotic algorithm have been used. The generated sequences by the four-dimensional chaos algorithm are further improved by the LSTM algorithm to create random matrices for the encryption process. This technique successfully scrambles the pixels of the image using two steps of permutation and then diffusion. In other words, this algorithm effectively scrambles the image pixel locations and changes the pixel value.

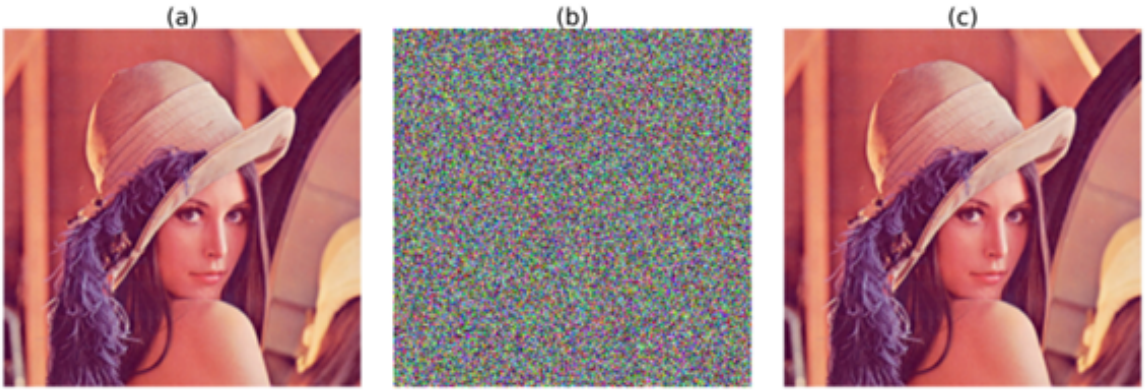

Figure 5: (a) Original (b) Encrypted (c) Decrypted image

Security Analysis

The security analysis of the suggested image encryption technique is performed using some statistical and cryptanalytic methods. It is evident from the results that the encrypted image has very high entropy, pixel independence, and even distribution of pixel values in the histogram. This means that the proposed method ensures very high randomness and is resistant to any kind of statistical attacks. The result of differential attack on this system has shown that even slight change in the input plain text will generate different cipher text, which proves the high security and sensitivity of the algorithm. Furthermore, the results of key sensitivity analysis have shown that the system is highly sensitive to

the secret keys used in encryption.
The following formula determines this correlation coefficient:

$$r = \frac{\mathrm{Cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{1}$$

where

$$\mathrm{Cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{2}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{3}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{4}$$

Here, N is the total number of pixels chosen from the image, and x, y are two adjacent pixels in the horizontal, vertical, and diagonal directions.

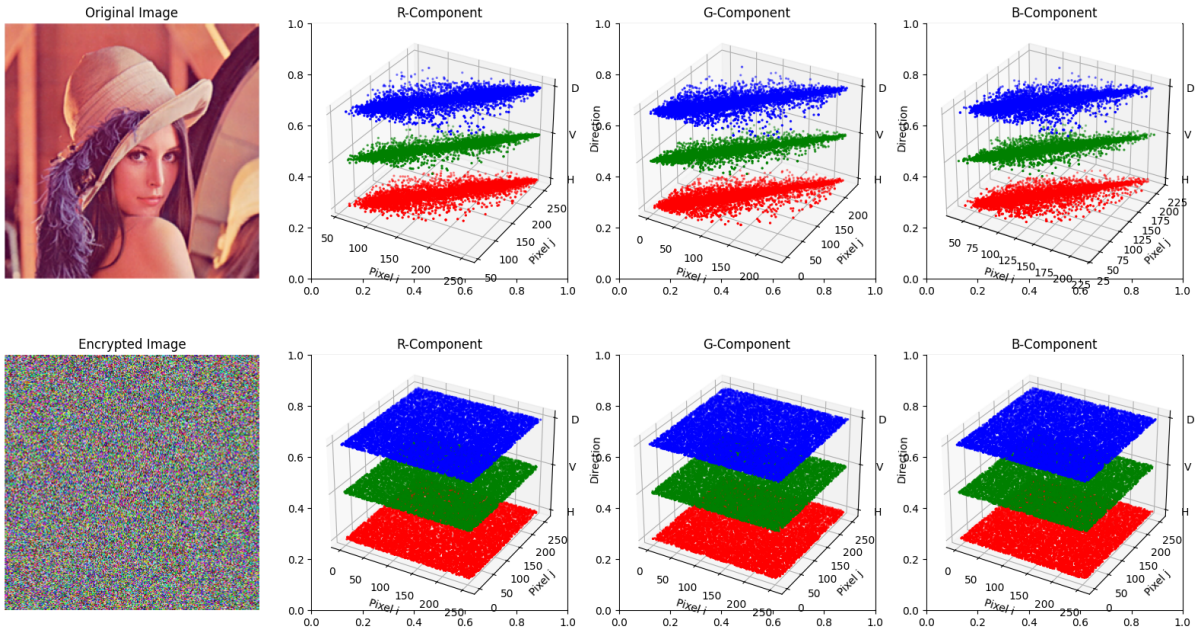

Figure 6: Correlation Analysis of Adjacent Pixels in Original and Encrypted Images.

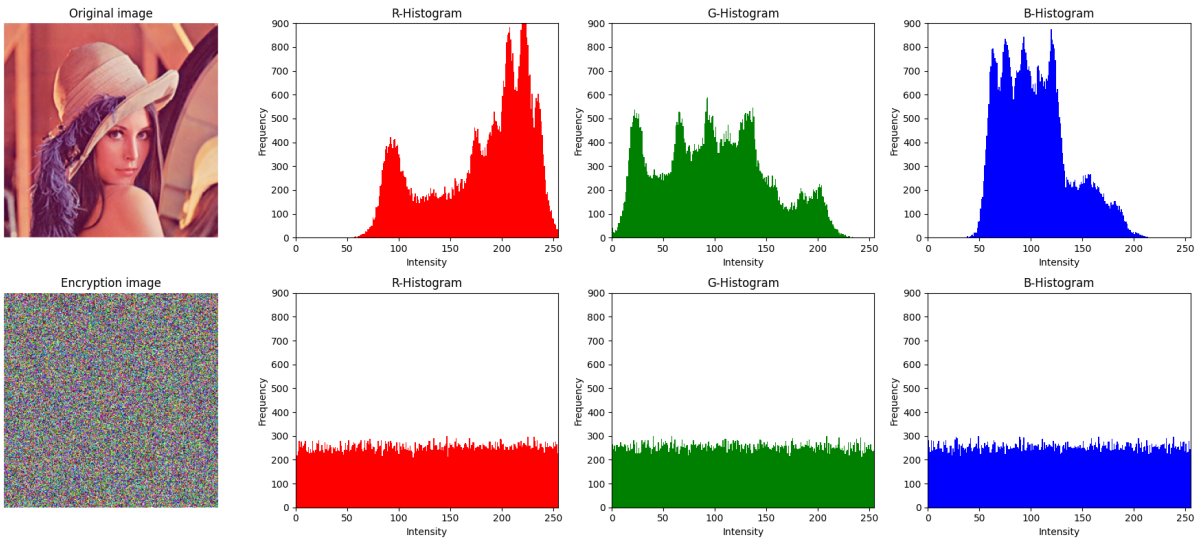

Figure 7: Histogram of original images and encrypted image. a histogram of original image; b histogram of encrypted image

6. Conclusion

The proposed research presents a secure and efficient method for encrypting color images based on the combination of a four-dimensional chaotic system with an LSTM deep neural network model. The LSTM neural network enhances the unpredictability of the chaotic sequence used to create pseudo-random matrices for the scrambling and diffusion operations involved in the encryption process. The results of security analysis include high levels of entropy, low values of correlation between the pixels, strong NPACR and UACI indices, key sensitivity, and a huge size of the key space, thus exhibiting strong resistance against various attacks.

Link of Google Colab

https://colab.research.google.com/drive/1IbGO9H6t95QqgnFJzq9HTKyY70QKFq-q?usp=sharing

References

[1] Stallings, W. (2006). Cryptography and network security, 4/E. Pearson Education India.

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

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

[4] Chen, L. P., Yin, H., Yuan, L. G., Lopes, A. M., Machado, J. T., & Wu, R. C.(2020). A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations. Frontiers of Information Technology & Electronic Engineering, 21(6), 866-879.

[5] Lorenz, E. N. (2017). Deterministic Nonperiodic Flow 1. In Universality in Chaos, 2nd edition (pp. 367-378). Routledge.

[6] Zheng, J., & Hu, H. (2022). A highly secure stream cipher based on analog-digital hybrid chaotic system. Information Sciences, 587, 226-246.

[7] Tong, X., Liu, X., Liu, J., Zhang, M., & Wang, Z. (2021). A novel lightweight block encryption algorithm based on combined chaotic S-box. International Journal of Bifurcation and Chaos, 31(10), 2150152

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