Eötvös Loránd University

Chaos-Based Image Encryption Enhanced by Deep Learning

Project Report

Submitted by	Muhammad Hamza
Neptun code	FV8ZPY
Course title	Directed Studies 1
Supervisors name	Dr. Lukács András
MSc Mathematics, Institute of Mathematics, ELTE	

1. 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.

2. 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) [1]. The authors propose a hybrid cryptosystem that integrates a 4D hyperchaotic Lorenz system with Long Short-Term Memory (LSTM) neural networks [2].

3. Main Ideas and Technical Contributions

3.1. LSTM-Enhanced Chaotic Signal Generation

The authors 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.

3.2. Two-Stage Encryption Architecture

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

3.3. Expanded Key Space

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

3.4. Security Validation

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

3.5. Implementation Results and Observations

The scheme was implemented and tested using numerical simulations. Encrypted images exhibit noise-like characteristics, and statistical evaluations confirm robustness and consistency with published results.

4. Plan for Next Semester

Future work will be guided towards making the image encryption scheme proposed more reversible and numerically stable. The processing of chaos sequences is performed with the help of a LSTM model to increase the efficiency of encryption and flexibility. In particular, the encryption and decryption operations will be performed using more accurate integer data types in order to avoid the information loss in overflow and rounding. The integers that are used to store the pseudorandom sequences and matrices are supposed to be created and stored in the representation of integers as opposed to the floating-point numbers to ensure a perfect invertibility. In addition, both encryption and decryption pipeline will be re-architectured to do permutation and diffusion steps in reverse order. Further testing including quantitative indicators of the pixel-wise error, correlation coefficients, and important sensitivity analysis will be conducted in order to test the robustness and safety of the improved algorithm. These enhancements are aimed at producing the perfect replica of the initial picture and simultaneously with a strong encryption rate performance.

References

[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.