IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131132

AI-DRIVEN CHAOTIC SYSTEM FOR SECURE IMAGE ENCRYPTION AND DECRYPTION IN SIMULINK

Mrs.Manasa S[1], Amirtha B[2], Bhoomika P[3], Dhanushree C D[4], Divya Bai[5]

Assistant Professor, Electronics and communication Department, East West Institute of Technology, Bangalore, India[1]

Student, Electronics and communication Department, East West Institute of Technology, Bangalore, India[2]

Student, Electronics and communication Department, East West Institute of Technology, Bangalore, India[3]

Student, Electronics and communication Department, East West Institute of Technology, Bangalore, India[4]

Student, Electronics and communication Department, East West Institute of Technology, Bangalore, India[5]

Abstract: An efficient ANN-based chaotic system for image encryption and decryption, implemented in Simulink and MATLAB using the Xilinx System Generator (XSG) tool. A feed-forward neural network (FFNN) with one hidden layer and Tangent Sigmoid activation ensures high accuracy, validated through a low mean square error. The generated Verilog code from XSG is executed in Vivado for pixel distribution, enabling hardware-level optimization. Security tests, including histogram analysis, PSNR, and SSIM, demonstrate robust encryption performance. The system’s analysis and visualization, conducted within Simulink, MATLAB, and Vivado, confirm its effectiveness. This approach showcases ANN-based chaotic systems for secure and real-time image processing.

Keywords: Artificial Neural Networks (ANN), Chaotic Systems, Simulink, MATLAB.

I. INTRODUCTION

This project focuses on securing images using AI-driven techniques and chaotic systems for encryption and decryption, leveraging MATLAB's Simulink and Vivado tools. Chaotic systems generate unpredictable keys, ensuring highly secure encryption resistant to attacks. AI enhances the system by adding intelligence and adaptability.

Simulink enables efficient design, simulation, and testing of the encryption and decryption mechanisms, while Vivado facilitates seamless hardware synthesis and integration. The result is a robust system that protects sensitive images from unauthorized access.

II. METHODOLOGY

This diagram illustrates the methodology for a secure image encryption and decryption system using AI, chaotic systems, and tools like Simulink, Xilinx System Generator (XSG), and Vivado. The process begins with an input image undergoing pre-processing in MATLAB's Simulink to prepare it for encryption. Next, an artificial neural network (ANN)-based chaotic system is designed using XSG to generate secure and unpredictable encryption keys. The image is then encrypted and decrypted using ANNs to ensure security during transmission. Verilog code is generated using XSG and implemented in Vivado to optimize the encryption and decryption logic for pixel-level operations.

Finally, the decrypted image is interfaced with MATLAB for output, and the system's performance is evaluated using metrics such as histogram analysis, mean squared error (MSE), peak signal-to-noise ratio (PSNR), signal-to-noise ratio (SNR), and structural similarity index (SSIM). This comprehensive methodology ensures a robust and secure system for protecting sensitive images.

ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⪾ Peer-reviewed & Refereed journal ⪾ Vol. 13, Issue 11, November 2024
DOI: 10.17148/IJARCCE.2024.131132

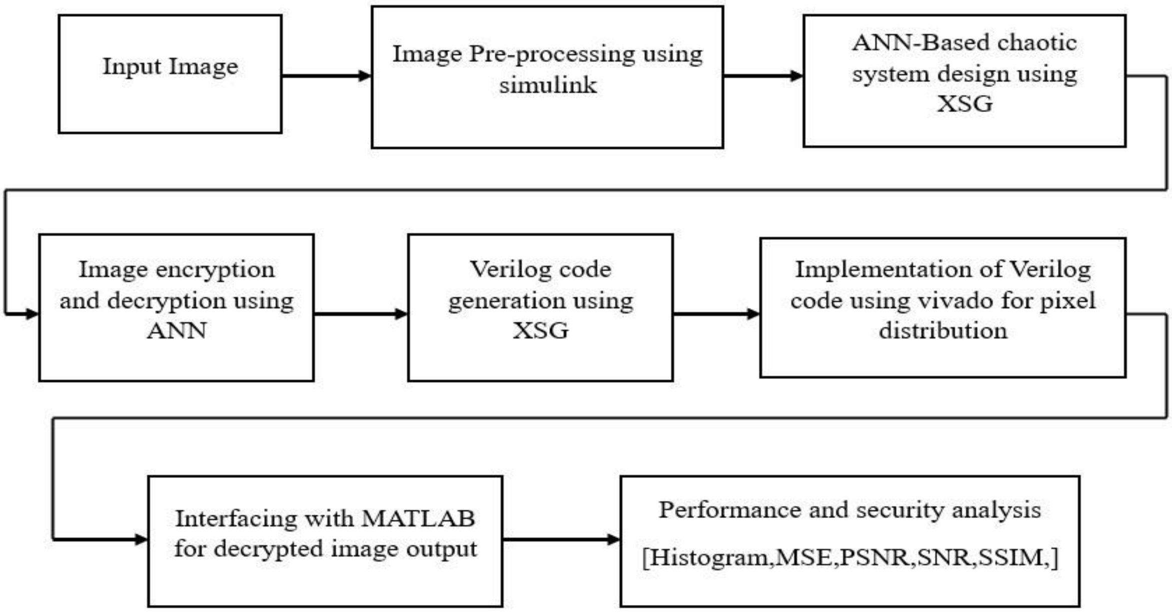

Figure1**:** Block diagram for Image Encryption and Decryption

III. IMPLEMENTATION

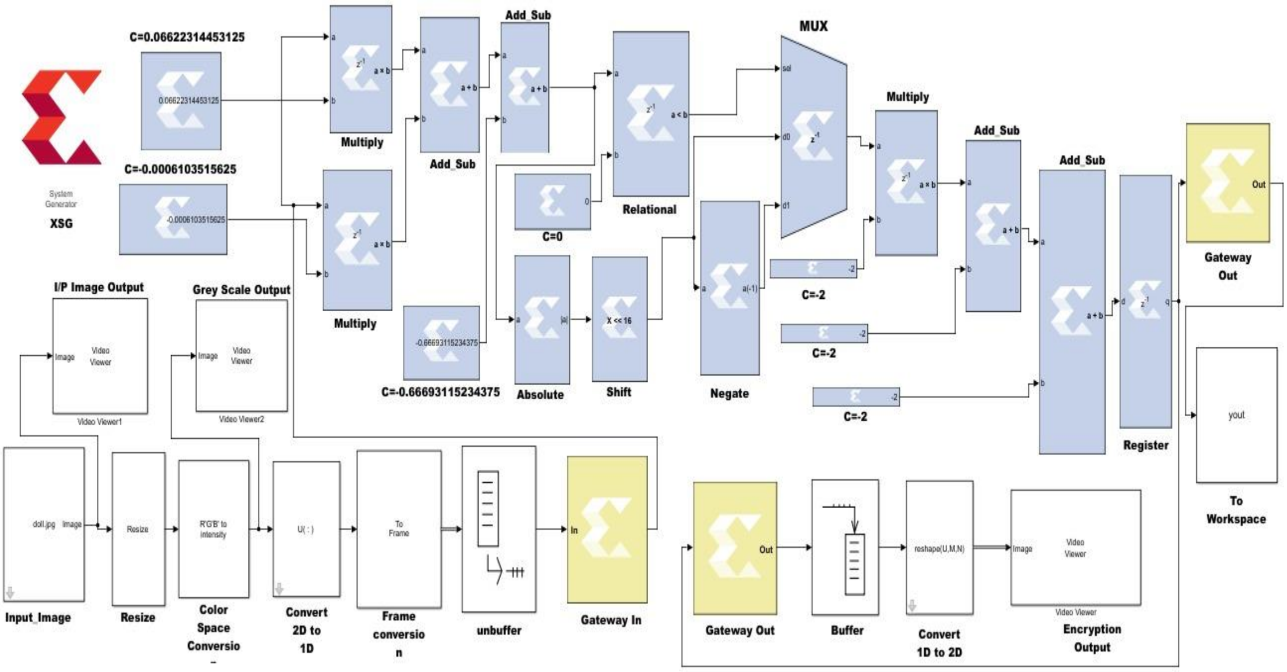

Figure 2**:** Block Diagram of Image Encryption System Using Xilinx System Generator (XSG) in Simulink

This diagram represents the implementation of an image encryption system using Xilinx System Generator (XSG) in MATLAB Simulink. The process begins with an input image, which is resized and converted from RGB to grayscale format. The 2D image is then flattened into a 1D vector for processing. Through a series of operations, including frame conversion and buffering, the data is passed through a gateway for further processing in the XSG environment.

ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024
DOI: 10.17148/IJARCCE.2024.131132

In the XSG section, chaotic systems are implemented using mathematical operations like multiplication, addition, subtraction, and shifting to generate encryption keys. These operations ensure high security by creating unpredictable outputs. The encrypted data is processed through multiple blocks for key integration and pixel manipulation, including relational comparisons, negations, and multiplexing (MUX). Finally, the encrypted image is reshaped back to its 2D form and displayed as the encryption output.

The system is designed to interact seamlessly with Simulink for pre-processing and visualization, while XSG handles the complex encryption logic. This implementation highlights an efficient integration of software tools and chaotic systems to achieve robust image encryption.

IV. RESULT

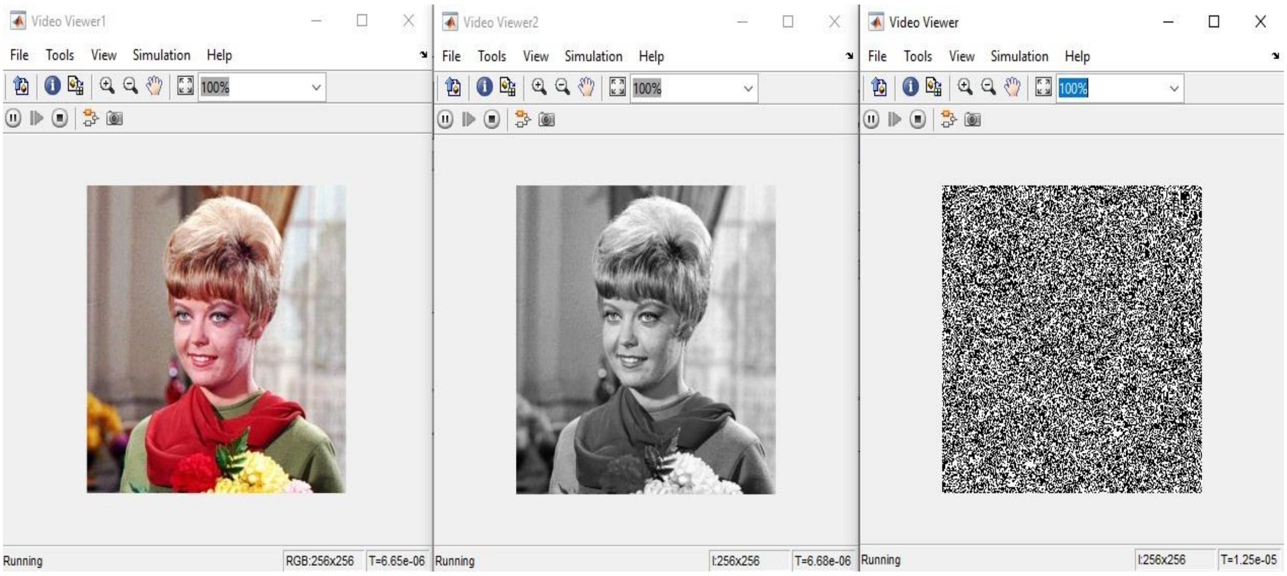

Figure 3: Original, Grayscale, and Encrypted Image Output

Figure 4: Image and its Histogram Analysis.

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131132

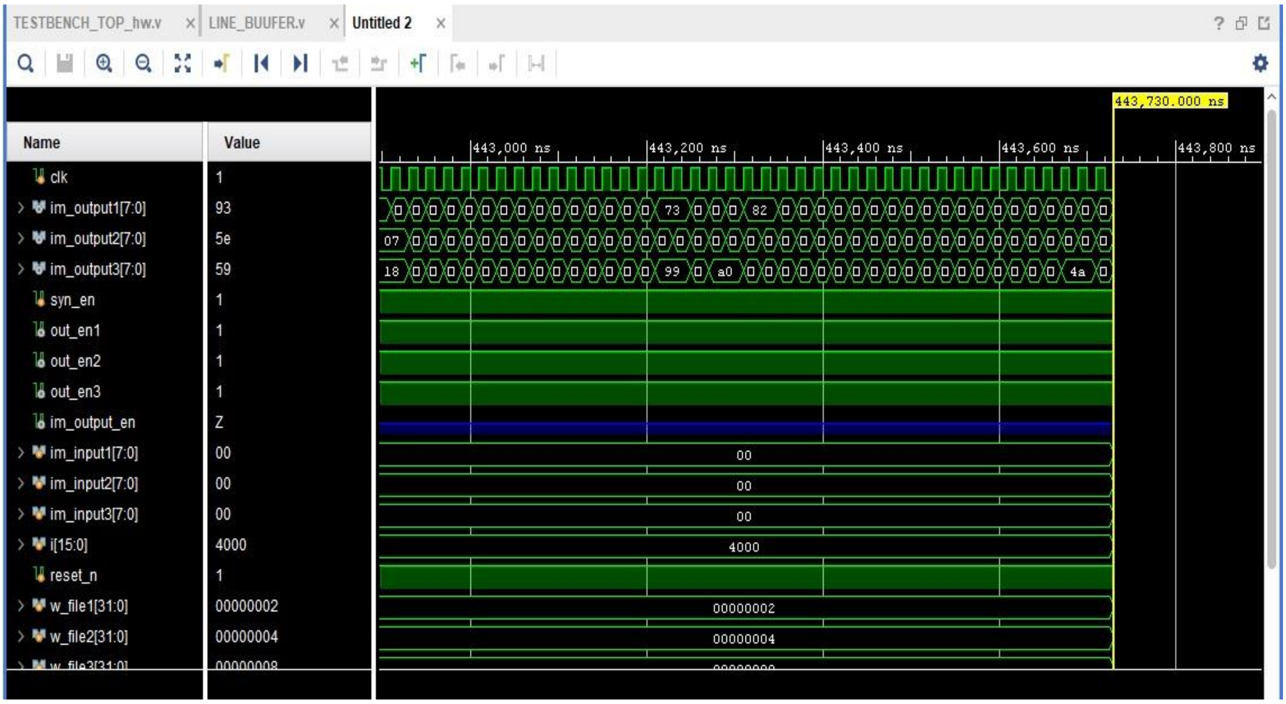

Figure 5: Signal Behavior During Encryption Process in Vivado

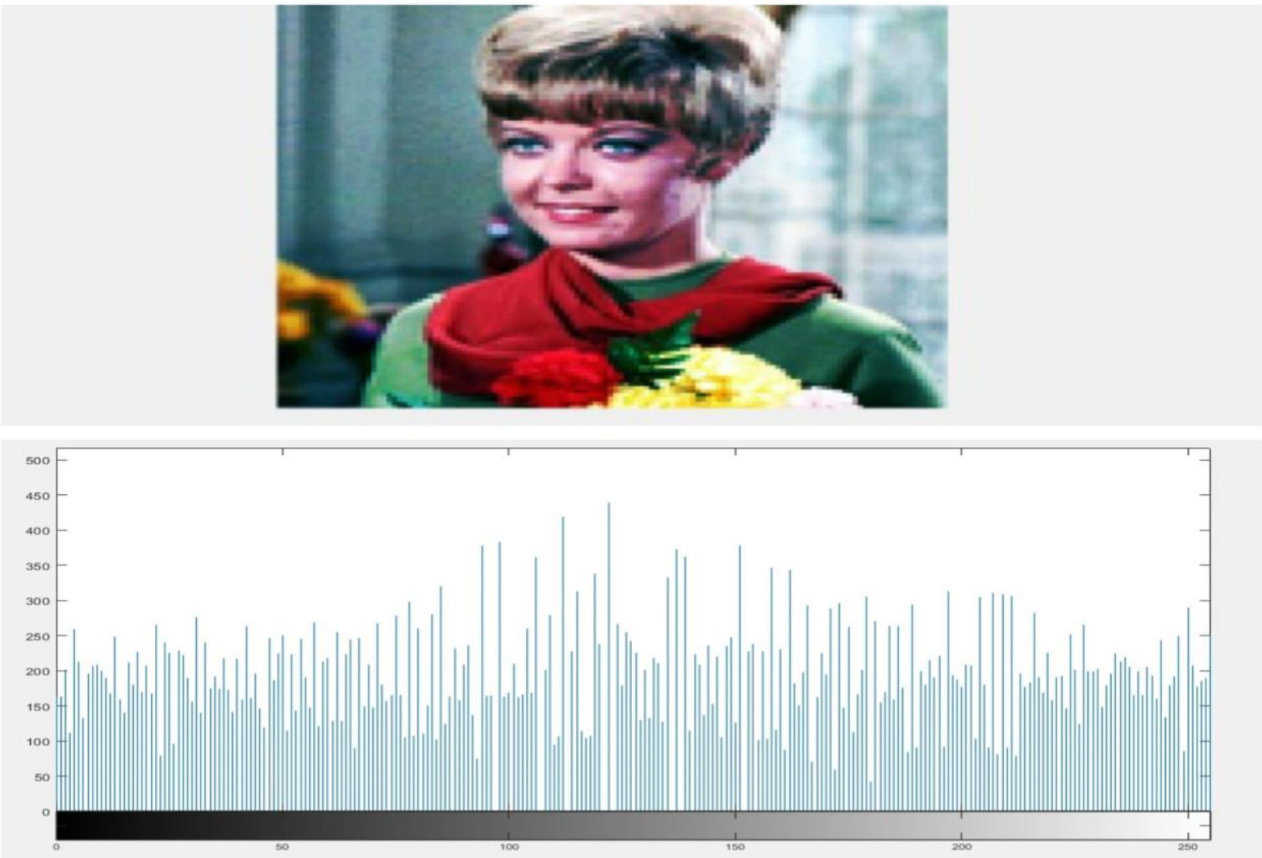

Figure 6: Filtered Image and Intensity Distribution

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 13, Issue 11, November 2024

DOI: 10.17148/IJARCCE.2024.131132


```
>> final_m_code
Mean Squared Error (MSE): 1.6422
Peak Signal-to-Noise Ratio (PSNR): 45.9365 dB
Signal-to-Noise Ratio (SNR): 41.5623 dB
Structural Similarity Index (SSIM): 0.9047
```

Figure 7**:** Image Quality Metrics Report

V. CONCLUSION

This project presents an efficient image encryption and decryption system using AI-driven techniques, chaotic systems, and tools like MATLAB's Simulink and Xilinx System Generator (XSG). Chaotic systems generate secure keys, while AI enhances adaptability and security. Simulink supports seamless design and simulation, ensuring efficient implementation of the system.

Performance metrics such as histogram analysis, MSE, PSNR, SNR, and SSIM validate the system's reliability in safeguarding image integrity. By integrating software-based methodologies, this system ensures high security and scalability, demonstrating its potential for protecting sensitive images in real-world applications.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to all those who have supported and guided me throughout the course of this project.

First, I would like to thank my project guide and faculty members for their valuable insights, continuous support, and encouragement. Their expertise and guidance were instrumental in the successful completion of this project.

I am also grateful to the technical staff and colleagues who helped with the hardware setup, troubleshooting, and system integration. Their collaborative efforts and suggestions were crucial in overcoming several challenges faced during the development of the project.

A special thanks to my family and friends for their unwavering support and motivation, which kept me focused and driven throughout this journey.

Lastly, I would like to acknowledge the resources and tools provided by the university and the online platforms, which played a significant role in enhancing my learning experience and ensuring the project's success.
This project would not have been possible without the contributions of all these individuals, and I am truly grateful for their support.

REFERENCES

[1]. "AI techniques for encrypt images based on the chaotic system implemented on field-programmable gate array**"** IAES International Journal of Artificial Intelligence (IJ-AI) Vol. 12, No. 1, March 2023

[2]. *"A Novel Design of an Image Encryption and Decryption Scheme Using Enhanced Cybersecurity Principles" 2023 International Conference on Emerging Research in Computational Science (ICERCS)*.

[3]. "A New Fast Color Image Encryption Scheme Using Chen Chaotic System" ©2017 IEEE SNPD 2017, June 26-28, 2017, Kanazawa, Japan.

[4]. "Improving for Chaotic Image Encryption Algorithm Based on Logistic Map" 0 ©2010 IEEE.

[5]. S. S. Hreshee, H. N. Abdullah, and A. K. Jawad, "A high security communication system based on chaotic scrambling and chaotic masking," *International Journal on Communications Antenna and Propagation (IRECAP)*, vol. 8, no. 3, p. 257, Jun. 2018, doi: 10.15866/irecap.v8i3.13541.

[6]. M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, p. 107484, Jun. 2020, doi: 10.1016/j.sigpro.2020.107484.

[7]. I. A. Taqi and S. M. Hameed, "A new color image encryption based on multi chaotic maps," *Iraqi Journal of Science*, vol. 59, no. 4B, pp. 2117–2127, Dec. 2018, doi: 10.24996/ijs.2018.59.4B.17.