

# Chaotic Image Encryption Scheme Implemented in FPGA for Security Enhance

Publisher: **IEEE** [Cite This](#) [PDF](#)

Pradipta Sarkar ; Anup Kumar Das ; Alope Saha [All Authors](#)



Get Published in the  
*IEEE Open Journal  
of Circuits and  
Systems*

[Learn More](#)

- Abstract**
- Document Sections
- I. Introduction
- II. Proposed Method
- III. Result Analysis
- IV. Conclusion
- Authors
- Figures
- References
- Keywords

**Abstract:**  
The internet has always faced significant security challenges when it comes to transferring information. Throughout and following the recent outbreak, it has become evident that as digital transactions surge, so do incidents of hacking and breaches. This highlights the growing need for secure transaction methods. In response, this paper introduces a novel cryptographic approach for image encryption and decryption, utilizing chaotic algorithms. To ensure the robustness of the encryption, we perform a series of rigorous performance evaluations, including Histogram, Entropy, NPCR, UACI Analyses. This study showcases the implementation of a one-dimensional reduce Henon chaotic map on an FPGA board, enhancing both the encryption and integrity of images.

**Published in:** 2024 IEEE International Conference of Electron Devices Society Kolkata Chapter (EDKCON)

**Date of Conference:** 30 November 2024 - 01 December 2024 **DOI:** 10.1109/EDKCON62339.2024.10870838

**Date Added to IEEE Xplore:** 13 February 2025

**Publisher:** IEEE

**ISBN Information:**

**Conference Location:** Kolkata, India

**More Like This**

[Hardware synthesis of artificial neural networks using field programmable gate arrays and fixed-point numbers](#)  
2006 IEEE Region 5 Conference  
Published: 2006

[Field Programmable Gate Array Hardware Accelerator of Prime Implicants Generation for Single Output Boolean Functions Minimization](#)  
2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA)  
Published: 2019

[Feedback](#)

**2024 IEEE International  
Conference of Electron Devices  
Society Kolkata Chapter  
(EDKCON 2024)**

**Kolkata, India  
30 November - 1 December 2024**



**IEEE Catalog Number: CFP24P61-POD  
ISBN: 979-8-3503-7465-0**

	<i>Poulomi Ghosh, Sudip Ghosh and Hafizur Rahaman</i>	
23	<b>Investigation of FinFET with multi-channel structures on device characteristics</b>	111-116
	<i>Archana Singh, Manish Verma and Dhandapani Vaithyanathan</i>	
24	<b>DC Analysis of T shape gate, L shape gate, Y shape gate, Field-plate gate AlGaN/GaN based HEMT</b>	117-120
	<i>Lakhmikanta Mishra, G. N. Dash and Manasa Ranjan Jena</i>	
25	<b>Chaotic Image encryption scheme implemented in FPGA for security enhance</b>	121-125
	<i>Pradipta Sarkar, Anup Kumar Das and Alope Saha</i>	
26	<b>A Novel ASK Reversible Gate and Its Implementation in Ripple Carry Adder Design</b>	126-131
	<i>Aruru Sai Kumar, Pokala Santhosh, Neelima Nimmagadda, Barama Veda Harshitha, D Suvarna Aishwarya Lakshmi and Katkam Shashi Vardhan</i>	
27	<b>Securing the Future of Communication with Quantum Cryptography</b>	132-137
	<i>Parna Kundu, Sudipta Banerjee, Mousam Chatterjee, Himadri Sekhar Das, Aritra Bhowmik and Heranmoy Maity</i>	
28	<b>Classifying the Tongue Contours for Assistive Devices</b>	138-142
	<i>Dasari Lakshmi Prasanna, Suman Lata Tripathi and Inung Wijayanto</i>	
29	<b>Performance of HfO<sub>2</sub> on High Electron Mobility Transistor Compatible for Microwave Applications</b>	143-147
	<i>Swati Dhondiram Jadhav and Aboo Bakar Khan</i>	
30	<b>Enhancing Biosensing Sensitivity through Simulation-Based Study of N<sup>+</sup> Pocket Doped Vertical NC-TFET</b>	148-153
	<i>Raj Kumar, Girdhar Gopal, Rajendra Mitharwal and Tarun Varma</i>	
31	<b>Novel Sign-Magnitude Binary to Balanced-Ternary Encoder on Basys3 Artix7 FPGA</b>	154-157
	<i>Ashishit Anurag Daniel Tigga, Nishit Bayen, Suman Gorai, Pradipta Sarkar, Anup Das and Alope Saha</i>	
32	<b>Application of Machine Learning Approaches for Power Estimation of Digital VLSI Circuits at Register Transfer Level</b>	158-161
	<i>Chinmay Parmar and Manish I. Patel</i>	
33	<b>Improved Deepmaxoutmodel for Disease Prediction in Healthcare IoT Cloud System</b>	162-167
	<i>Preetha Pandu and A Packialatha</i>	
34	<b>An IoT-based Hardware System for Road Accident Detection and Notification using CNN-LSTM Algorithm</b>	168-173
	<i>Tanusree Chatterjee, Shibasish Dalui, Sanjib Roy, Rituraj Debnath and Avijit Mondal</i>	
35	<b>Design and FPGA Implementation of an Efficient Squarer Circuit Using Reversible Logic</b>	174-178
	<i>Mihir Lal Saha, Debjit Roy, Agnik Maity, Antarik Sinha, Mili Sarkar and Amitava Ghosh</i>	
36	<b>Unveiling Mental Stress: Examining the Impact on College Students' Well-being Using Machine Learning Based Solutions</b>	179-184

# Chaotic Image encryption scheme implemented in FPGA for security enhance

Pradipta Sarkar  
Department of ECE

Dr. B. C. Roy Engineering College  
Durgapur, India  
pradipta.sarkar@bcrec.ac.in

Anup Kumar Das  
Department of ECE

Dr. B. C. Roy Engineering College  
Durgapur, India  
anup.das@bcrec.ac.in

Aloke Saha  
Department of ECE

Dr. B. C. Roy Engineering College  
Durgapur, India  
aloke.saha@bcrec.ac.in

**Abstract**— The internet has always faced significant security challenges when it comes to transferring information. Throughout and following the recent outbreak, it has become evident that as digital transactions surge, so do incidents of hacking and breaches. This highlights the growing need for secure transaction methods. In response, this paper introduces a novel cryptographic approach for image encryption and decryption, utilizing chaotic algorithms. To ensure the robustness of the encryption, we perform a series of rigorous performance evaluations, including Histogram, Entropy, NPCR, UACI Analyses. This study showcases the implementation of a one-dimensional reduce Henon chaotic map on an FPGA board, enhancing both the encryption and integrity of images.

**Keywords**— chaos, encryption, FPGA, security.

## I. INTRODUCTION

Chaotic events have a broad spectrum of engineering and scientific uses, such as secure data transmission, nonlinear control, and image encryption [1]. Researchers largely agree that chaos-based systems can be built using FPGA boards, discrete electronic components, and microcontrollers [2]. The advent of field-programmable gate arrays (FPGAs) has accelerated the prototyping of chaotic phenomena, making it more accessible [3]. Many scholars are now employing FPGAs to quickly prototype new hardware for chaotic systems, memristors, and various non-clonable type of functions [4].

This study introduces a one dimensional reduce Henon chaotic map with bit shuffling of image in encryption and decryption system implemented on an FPGA board in a hardware environment. Encryption serves as a robust method for concealing sensitive information, such as banking transactions, defense security data, and various image of medical diagnostics. It continues to be both potent and safe, even as information is kept or conveyed through perilous pathways. Although some cryptography applications leverage chaos theory [5-6], most are based on Matlab or microcontrollers. For instance, [7] details a method for bit-plane data encryption using quadratic and cubic maps, and discusses a lossy technique for encrypting and compressing images via discrete wavelet transform, singular value decomposition, and Huffman coding.

The Sine-Transform-Based Chaotic System with FPGA is described in [8]. An artistic fusion of time chaos and colorful DNA coding is presented in [9]. Secret key sequences

generated by a nonlinear coupled map lattice algorithm and the SHA-256 hash function adjust structural parameters and initial conditions to enhance image encryption security [10]. Reference [11] elaborates on microcontroller based real-time image cryptosystem, while [12] discusses hyperchaotic techniques for image encryption. A novel color-based image encryption method is detailed in [13-15]. The memristors based chaotic cryptography has been discussed in the articles [16-17]. This paper is distinctive in presenting the use of FPGA for constructing chaos-based cryptosystems, specifically utilizing a one-dimensional reduce Henon map for color image encryption, an approach previously undocumented. The paper has been written in the following steps: In section II the methodology of the chaotic map implementation in hardware with colour image. In third section result analysis has been done and section IV conclusion has been made.

## II. PROPOSED METHOD

The FPGA Xilinx BASYS-3 platform has been outfitted with a one-dimensional reduce Henon chaotic map to facilitate image encryption and decryption technique. The equation for the one dimensional reduce Henon chaotic map is as follows:

$$x_{i+1} = (1 - ax_i^2) \quad (1)$$

The FPGA Xilinx BASYS-3 platform has been equipped with a one dimensional reduce Henon chaotic map for image encryption and decryption process. The chaotic map equation operates within its chaotic regime when the parameter  $a=1.4$ . and the initial value in between -1 and 1.

The FPGA Basys-3 board includes all necessary components: an analog to digital converter, a 450 MHz internal clock, 33,280 logic cells distributed among 5,200 memory slices, Five enchanting clock control tiles, ninety dynamic DSP slices, and a dazzling 1,800 Kbits of rapid block RAM. Initially, MATLAB software divides a color image into its R-channel, G-channel, and B-channel matrices. The pixel values from these channels are stored in memory, and the software applies a one-dimensional reduce Henon chaotic map to encrypt the pixel data.

For the encryption process, a chaotic sequence of 128 by 128, starting with ( $x_i = 0.5$ ) and ( $a = 1.4$ ), is applied to the R-channel pixel values using an EX-OR logical operation, then stored in memory. The identical process is enacted once more for the pixel values of the G-channel and B-channel,