Analog Integrated Circuits and Signal Processing (2025) 123:57
https://doi.org/10.1007/s10470-025-02401-4

Two dimensional chaotic scheme for image encryption in FPGA

Pradipta Sarkar[1] · Anup Kumar Das[1] · Aloke Saha[1] · Mrinal Kanti Mandal[2]

Received: 19 July 2024 / Revised: 21 March 2025 / Accepted: 2 April 2025

Abstract
Transmitting data via the Internet has always posed significant security threats. Before and after the epidemic, there have been reports of an increase in hacking and infiltration cases in proportion to the number of digital transactions. As a result, there is a greater need for secure financial transactions. This field of study suggests using chaotic sequences, complex keys, and bit shuffling in encryption algorithms as a secure method for encrypting and decrypting images in a software and hardware environment. In order to ensure that the encryption meets the requirements, this article employs a variety of approaches and performance evaluations, such as histogram analysis, correlation, NPCR, UACI, the NIST test, MAE, and entropy analysis. This article describes how to use an FPGA board with a novel chaotic map that is two-dimensional and initialised using complex bit and key shuffling to encrypt colour images for security enhancement.

Keywords Chaos · Key · FPGA · Encryption · Decryption

1 Introduction

With the increasing significance of digital data in various domains, the need for secure communication and storage techniques has become paramount. Encryption plays a crucial role in ensuring the confidentiality and integrity of sensitive information, including digital images. Chaos-based encryption methods have emerged as a promising approach due to their inherent complexity and unpredictability [1–3]. Chaos refers to deterministic, nonlinear dynamical systems characterised by a sensitive dependence on initial conditions. Chaotic systems exhibit complex behaviour, including irregular fluctuations and aperiodic dynamics [4–6]. In this comprehensive overview, we delve into the fundamentals, techniques, challenges, and recent advancements in chaos-based image encryption [7–10]. Examples of chaotic systems commonly utilised in encryption include logistic maps, Henon maps, Lorenz systems, and coupled map lattices [11–13]. Chaos-based encryption harnesses the unpredictability and complexity of chaotic systems to generate cryptographic keys and perform encryption operations. The encryption process typically involves key generation, image transformation, encryption, and decryption stages [14, 15]. Chaotic sequences generated by chaotic systems serve as encryption keys, allowing image data to be scrambled to achieve confidentiality [16–18]. Block chain based image encryption techniques are also an important topic [19, 20]. Neural network-based image encryption has been very significant in recent research [20, 21]. Vehicle to vehicle and vehicle to ground communication and digital image encryption scheme has been described in the article [33, 34]. The Henon map, a two-dimensional chaotic system, offers enhanced complexity compared to one-dimensional maps [22]. Henon map-based encryption techniques involve iterating the Henon map equations to generate chaotic sequences. The encryption process enhances its security by using these sequences for pixel permutation and diffusion operations.

FPGA (Field-Programmable Gate Array)-based image encryption stands at the forefront of modern cryptographic techniques, offering unparalleled speed, flexibility, and security in protecting digital images from unauthorised access [23, 24]. This cutting-edge technology harnesses the reconfigurable nature of FPGAs to implement complex encryption algorithms directly into hardware, enabling real-time encryption and decryption of images with high efficiency [25, 26].

At the heart of FPGA-based image encryption lies the FPGA itself—a semiconductor device consisting of

✉ Anup Kumar Das
anupkumardgp@gmail.com

1 Department of Electronics and Communication Engineering, Dr. B. C. Roy Engineering College, Durgapur, India

2 Department of Physics, NIT Durgapur, Durgapur, India

Published online: 28 April 2025