2023 IEEE Devices for Integrated Circuit (DevIC) | 979-8-3503-4726-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/DevIC57758.2023.10135027

Proceedings of

5th International Conference

on

2023 Devices for Integrated Circuit (DevIC)

7-8 April, 2023, Kalyani, Nadia, India

Organized by

IEEE KGEC Student Branch Chapter

In association with

Department of ECE, Kalyani Government Engineering College

Edited by

Dr. Angsuman Sarkar
Dr. Sandip Nandi

Kalyani Government Engineering College

2023 Devices for Integrated Circuit (DevIC)

Part Number: CFP23K13-ART

ISBN: 979-8-3503-4726-5

2023 IEEE Devices for Integrated Circuit (DevIC) | 979-8-3503-4726-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/DevIC57758.2023.10135010

Table of Contents

2023 IEEE Devices for Integrated Circuit (DevIC) | 979-8-3503-4726-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/DevIC57758.2023.10134922

2023 IEEE Devices for Integrated Circuit (DevIC), 7-8 April, 2023, Kalyani, India

One Dimensional Chaotic map Implementation in FPGA board for Image Encryption

Pradipta Sarkar
Department of Electronics and Communication Engineering
Dr. B. C. Roy Engineering College
Durgapur, India
pradipta.sarkar@bcrec.ac.in

Anup Kumar Das
Department of Electronics and Communication Engineering
Dr. B. C. Roy Engineering College
Durgapur, India
anup.das@bcrec.ac.in

Aloke Saha
Department of Electronics and Communication Engineering
Dr. B. C. Roy Engineering College
Durgapur, India
aloke.saha@bcrec.ac.in

***Abstract*— Internet information transport has always been accompanied by significant security concerns. After and during the epidemic, it has been noticed that as digital transactions increase, so do instances of intrusion and hacking. Consequently, the demand for safe transactions increases. This study proposes a cryptographic method for image encryption and decryption based on chaotic and associated algorithms. In this article one dimensional logistic chaotic map has been implemented in FPGA board for image encryption and addition, we conduct several performance analyses and methods, such as Histogram Analysis, Entropy Analysis, to evaluate the quality of the encryption and confirm that the specified standard has been fulfilled.**

Keywords— chaos, FPGA, encryption, decryption.

I. INTRODUCTION

There are many engineering and scientific applications for chaotic phenomena, including nonlinear control, secure data communication, and image encryption [1]. It is generally agreed upon in the academic literature that microcontrollers, discrete electrical components, and an FPGA board can be used to build chaos-based systems [2]. Rapid prototyping of chaotic phenomena has gained popularity thanks to the implementation of chaotic systems in field-programmable gate arrays (FPGA) [3]. To quickly prototype new hardware, many researchers are turning to FPGAs for use in chaos systems, memresistors, and other non-clonable physical functions [4]. In this paper, one dimensional chaotic image encryption and decryption of colour image has been implemented in hardware environment i.e. using FPGA board. Encryption is a technique for hiding the sensitive information for the purposes of storing and transmitting it in a format that only the intended recipients can understand and process in secure environment [6]. Banking transactions, defence security information, and medical image diagnostics are just a few examples of the kinds of confidential data that can be protected using encryption, which is both effective and secure even when stored and transmitted over unsecured channels. There are a few cryptographic apps [7-8] in the literature that make use of chaos theory, but most of them are built in Matlab or on microcontrollers. A method of encrypting data using quadratic and cubic maps on the bit plane is detailed in [9]. In reference [10], we find a lossy method of picture compression and encryption using singular value decomposition, discrete wavelet transform, and Huffman coding.

The two-dimensional Sine-Henon adaptation model is described in [11]. (2D-SHAM). Colorful DNA coding and time chaos are shown graphically in [12]. To improve the safety of the encrypted image, the hash function SHA-256 modifies the structure parameters and initial conditions, while the nonlinear coupled algorithm map-based coupled map lattice creates the secret key sequences [13]. The paper [14] details the implementation of a real-time image cryptosystem using two ATMEGA 32 microcontrollers. Image encryption makes use of a hyperchaotic scheme, as described in [15]. The novel colour based image encryption is describes in [16]. Since no prior work describes using FPGA to implement chaotic cryptosystems in colour images, we present the implementation method of chaos-based cryptosystems in FPGA here, specifically the one dimensional logistic map in a chaotic regime. The structure of the section that follows is as follows: The second section explains the algorithm of one-dimensional logistic map using FPGA. In Section III, a block diagram and explanation of the proposed FPGA-based encryption are presented. The results of simulation experiments and cryptanalysis techniques such as histogram, entropy analysis, etc. are described in Section IV. Section V describes the concluding remarks.

II. PROPOSED ALGORITHMS

A. Process flow description:

The one-dimensional logistic chaotic map has been implemented in the FPGA Xilinx BASYS-3 board for image encryption and decryption purpose. The equation of the one dimensional chaotic maps is given by

$$x_{i+1} = r * x_i * (1 - x_i) \quad (1)$$

Where r is the parameter value. The chaotic regimen of the equation (1) when the r is in between 3 to 3.99. In the proposed scheme r is choosen as 3.89.

The FPGA Basys -3 board is equipped with the necessary components; it has 450 MHz of internal clock frequency, an analog-to-digital converter (ADC), 33,280 logic cells distributed across 5200 slices of memory, 5 clock control tiles, 90 DSP slices, and 1800 Kbit of fast block ram. At first a colour image has been separated into R-channel, G- channel and B-channel matrix by MATLAB software and the pixel values of three channels has been saved into the memory. One dimensional chaotic map also implemented in Matlab software to encrypt the pixel values of three channels. Next the 128 by 128 colour pixel values of R-channel logical operation (EX-OR) with the 128 by 128 chaotic sequence of the initial values of (xi=0.5, r=3.89) and saved into the memory location. The same process repeated for G-channel and B-Channel Pixel values and the chaotic sequence of the

979-8-3503-4726-5/23/$31.00 ©2023 IEEE