Chaotic based Grain 128-bit stream cipher for image encryption

Meghana S Ramesh[a], Dr. Shivaputra[b]*

[a]M. Tech Student, Bengaluru-560056, India

[b]Assistant Professor, Bengaluru-560056, India

ABSTRACT: Secure transmission and storage of data are most important for a successful communication system. Cryptography protects the information so that the intruder cannot have access to the data of interest. There are various algorithms implemented to transform the information to be transmitted into cipher form so that it does not have any traces of its original form and can be protected from trespasser. Chaotic based Grain 128-bit is a stream cipher made up of a linear and a non-linear feedback shift registers, which is fed by a chaotic logistic map and a Boolean non-linear filter, which is fed by both LFSR and NLFSR. Key is generated using Chaotic based Grain 128-bit stream cipher and is used in the application for image encryption. The generation of the key is implemented on Xilinx ISE xc7a100t-3csg324 using Verilog code is also discussed. Analysis of the work is done by plotting a histogram of input, encrypted, and decrypted images.

Keywords: Cryptography, Linear feedback shift register (LFSR), Non-linear feedback shift register (NLFSR), Cipher, Encryption, and decryption.

1. Introduction

Different forms of contents such as text, audio, image, video, etc are transmitted from one point to another in various ways. To have successful communication, the information at the receiver end should not be corrupted. This is achieved by providing security to the data to be transmitted. One of the popular methods is to convert the original data into cipher form so that the trespasser cannot have access to it. Cryptography deals with protecting the data using codes so that the data can be accessed only by the intended users.

Stream and block ciphers are the two types of ciphers used in a symmetric key cryptographic system. The key generation using stream ciphers in software is much faster than in block cipher. Stream ciphers are also resistive against various statistical attacks and are made up of LFSRs and NLFSRs. The properties of the sequence generated using LFSRs coincide with that of truly random sequences [1]. Global Positioning System (GPS) uses sequences generated by LFSRs. L2 frequency band Civil Moderate signal also uses sequences generated by LFSRs as the sequences generated by LFSRs have properties similar to pseudo random sequence. But, the order of the sequence is less comparatively and hence the cycle repeats after certain number of bits. Thus, they result in poor correlation properties [2]. The non-linearity increases the randomness properties in the sequence generated, thus increasing the security of transmission of information through the unprotected medium. The encryption process in stream cipher is bit by bit XOR operation between key stream and the input stream of bits.

The security of the cryptographic system depends upon the strength of the key generated using cryptographic algorithm. Hence, the strength of the key decides the strength of the security system. More random the key generated, more secure the system. Hence, the random number generator is the basic and important block in a cryptographic system. Lots of research are going on regarding design of an efficient random number generators. It is a challenge to generate a true pseudorandom sequence having desired statistical properties necessary for cryptographic systems [3]

Satellite applications require binary sequences having good correlation properties. They also require sequences having suitable linear complexity [4]. A survey on chaotic encryption algorithms of the speech signal and cryptographic requirements is discussed in [5]. Cryptographic applications require random binary sequences having large linear complexity properties. In [6], random binary number is generated using matrix recurrence relation which is defined over Z4. The sequence generated has larger linear complexity properties. Water Marked Image Encryption Using Logistic Map

Innovative Design, Analysis and Development Practices in Aerospace and Automotive Engineering pp 481–491

Analysis and Design of an Optical Biosensor Using Mathematical Modeling

G. Sowmya Padukone, H. Uma Devi, Shivaputra & Meenakshi L. Rathod

Conference paper | First Online: 27 September 2020

Part of the Lecture Notes in Mechanical Engineering book series (LNME)

Abstract

Photonics is a branch of science which deals with creation, perception, and arrangement of light in a suitable form. The waves are electromagnetic waves (EM waves) where electric and magnetic waves are perpendicular to each other. These sensors are used to detect diseases like cancer, forensic analysis, pattern, parental recognition, pattern recognition, etc. But, photonic biosensors are first designed so as to get the optical-designed simulation pattern using MEEP and opti-FDTD algorithms. The patterns are

2021 | OriginalPaper | Chapter

Modified E-Shaped Resonator-Based Microstrip Dual-Mode Bandpass Filter

Authors: Shobha I. Hugar, Vaishali Mungurwadi, J. S. Baligar

Published in: International Conference on Communication, Computing and Electronics Systems

Publisher: Springer Singapore

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 171 (2020) 2067–2072

Procedia Computer Science

www.elsevier.com/locate/procedia

Third International Conference on Computing and Network Communications (CoCoNet'19)

Novel Approach For Center Frequency And Bandwidth Tuning In Multimode Resonator Based Microstrip Dual-Mode Bandpass Filter

Shobha I Hugar[a], Vaishali Mungurwadi[b], J S Baligar[c]

[a]*Sapthagiri College of Engineering,Bangalore57,India*

[b]*Sarvajanik College Of Engineering,Surat,India*

[c]*Dr Ambedkar Institute f Technology,Bangalor,India*

Abstract

This paper demonstrates a novel approach for both center frequency and bandwidth tuning in dual mode Bandpass filter. The proposed filter is configured from a half wavelength multimode resonator structure. The Ultra-wide bandpass response of multimode resonator is extracted using an inter-digital feed structure which provides good input/output coupling. By deploying stepped admittance structure perturbation element in to the symmetrical plane of multimode resonator, dual-mode response is achieved with three upper stop band transmission zeros(TZs). The coupling between two degenerative mode frequencies is controlled by admittance ratio Y of stepped admittance structure. Changing admittance ratio(Y) of stepped admittance structure, results in change in even mode resonance frequency and location of three upper stop band transmission zeros while keeping odd mode frequency fixed. Proposed filter has size of 14mm*30mm.

Keywords: Multi-mode resonator(MMR); Ultra-wideband(UWB);Transmission Zeros(TZ).

1.Introduction

Modern wireless communication system needs compact, high frequency selective, wide stopband tunable bandpass filters. In literature many tunable filters have been reported using dual mode resonators[1]-[12].Tuning is achieved in 3 ways i) Fixed center frequency and tunable bandwidth ii) Fixed bandwidth and tunable center frequency iii)

10.1016/j.procs.2020.04.222

Proceeding of Fifth International Conference on Microelectronics, Computing and Communication Systems pp 383–400

An Insight into the Existing Reversible Arithmetic and Logic Unit Designs

S. Girija & B. G. Sangeetha

Conference paper | First Online: 10 September 2021

Part of the Lecture Notes in Electrical Engineering book series (LNEE,volume 748)

Abstract

International Technology Roadmap for Semiconductors-ITRS2.0 predicts an end to traditional scaling and shrinking of chips by 2028. The future depends on the alternative technology to fill the gap and perform better than the existing technology. There are numerous technologies emerging, one among them being the reversible logic is fast gaining the importance due to the quantum technology for minimal dissipation of energy whose operation is reversible in nature. Arithmetic and logic operations are the core of any processing system and its importance is found in all

Proceedings of the International Conference on Computational Intelligence and Sustainable Technologies pp 349–360

Optimized 64-bit Reversible BCD Adder for Low-power Applications and Its Comparative Study

K. N. Hemalatha, S. Girija & B. G. Sangeetha

Conference paper | First Online: 12 February 2022

Part of the Algorithms for Intelligent Systems book series (AIS)

Abstract

Reversible logic has emerged its importance in the framework of recent technology as such optical computing and quantum computation. Reversible logic does not loose bits of information during computation. In the proposed work, a class of new design for reversible 4-bit and 64-bit BCD adder circuits is designed. Design of 64-bit BCD adder is first of its kind when related with the present reversible BCD adder in the literature. Proposed design uses 11 constant inputs, 22 garbage outputs, and the quantum cost are 72. Quantum cost of the

DOI: 10.1109/RTEICT49044.2020.9315649 • Corpus ID: 231616715

An Efficient High-Speed Lifting Based 1D/2D-DWT VLSI Architecture Using CDF-5/3 Wavelet Transform For Image Processing Applications

M. Sushmitha, S. Chetan, Sayantam Sarkar • Published 12 November 2020 • Computer Science •
2020 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)

There are various Discrete Wavelet Transform architectures that are designed to fulfil certain requirements and criteria's. The convolution method which is an old traditional method which requires more multipliers, hardware resources and huge memory storage which is not apt to yield high speed and efficient image processing, signal processing application designs when compared to lifting method. In this paper, we have proposed an architecture for lifting scheme based CDF-5/3 2D-DWT, which… Expand

Energy Efficient Greedy Scheduling of Tasks for DVFS Enabled Heterogeneous Multicore Processors

Publisher: IEEE

K Siddesha ; G V Jayaramaiah All Authors

Abstract: Nowadays the demand for high performance computing systems like servers, increasing since these systems, process many real-time applications with the help of heterogeneou... **View more**

Metadata

Abstract:

Nowadays the demand for high performance computing systems like servers, increasing since these systems, process many real-time applications with the help of heterogeneous processors. However, in multicore systems power consumption is always a concern. In most of the processor based systems dynamic voltage and frequency scaling is a common method adopted to save energy. In processing many heterogeneous tasks, it is appropriate to propose a combined energy efficient scheduling using DVFS. In this article, we introduce a task scheduling model along with DVFS method for high performance computing system. The proposed greedy scheduler assigns the tasks to the suitable processor core based on their energy profile and probability value of the incoming task. The simulation results show that the proposed scheduling

Expert Clouds and Applications pp 647–663

Smart Driving Assistance Using Arduino and Proteus Design Tool

N. Shwetha, L. Niranjan, V. Chidanandan & N. Sangeetha

Conference paper | First Online: 16 July 2021

Part of the Lecture Notes in Networks and Systems book series (LNNS,volume 209)

Abstract

In the modern era, the automobile trading has enhanced a lot by adding more safety features to protect the driver and vehicle on the road. Majorly, the accident occurs due to the fault in the system or ignorance of the driver. This paper demonstrates the digital framework, wherein the sensors are connected to the centralized system through the CAN bus with the main controller for leveraging proper alert information to the driver. The primary goal of the proposed system is to make the driver more comfortable to drive by providing the real-time data like status of the traffic signal, vehicle headlight

Advance System for Driving Assistance Using Arduino and Proteus Design Tool

Publisher: IEEE

N Shwetha ; L Niranjan ; V Chidanandan ; N Sangeetha All Authors

Abstract: In the recent years, the automobile industry has improved a lot for modifying and adding more advanced features to make more protective safe environment for the drive and... **View more**

Metadata

Abstract:

In the recent years, the automobile industry has improved a lot for modifying and adding more advanced features to make more protective safe environment for the drive and the vehicle on the road which inter reduces road accidents. As the major cause of road accidents are due to the fault in the system or ignorance of the driver. This paper presents the digital framework, which works as a control system along with some sensors connected to the centralized microcontroller for proper alert information to the driver. The main idea is to make the driver more comfortable by providing digital driver warning and control system in Realtime with the help of CAN protocol which is incorporated with the controller. The major advantage of this system is to provide the user with relevant information like status of traffic light ahead of the vehicle, leakage of

International Conference on Information Processing

ICInPro 2021: **Data Science and Computational Intelligence** pp 258–272

Real Conversation with Human-Machine 24/7 COVID-19 Chatbot Based on Knowledge Graph Contextual Search

Tanuja Patgar, Ripal Patel & S. Girija

Conference paper | First Online: 01 January 2022

Part of the Communications in Computer and Information Science book series (CCIS,volume 1483)

Abstract

The outbreak of the COVID-19 pandemic has changed the whole world scenario and made researchers innovate on the corona virus. Researchers are working on information that includes symptoms, Infection spreading, preventive measures, health and travel advisories, and help lines for further assistance. During this pandemic scenario, the health assistant Chatbot is a very useful conversation tool for COVID-19, which provides preliminary medical advice and preventive measure suggestions. The paper proposes an Artificial Intelligence-based Re-Co Chatbot to

International Conference on Computer Networks and Inventive Communication Technologies

ICCNCT 2019: **Second International Conference on Computer Networks and Communication Technologies** pp 152–161

A Novel Security Scheme of Temporal-Key Based Encryption Policy in Sensor Applications

M. N. Premakumar ✉ & S. Ramesh

Conference paper | First Online: 22 January 2020

Part of the Lecture Notes on Data Engineering and Communications Technologies book series (LNDECT,volume 44)

Abstract

The contribution of Wireless Sensor Network (WSN) towards commercial sensing application is tremendously progressing day-by-day. However, it is still shrouded by security problems owing to less practical applicability of existing research solutions as well as inherent nature of resource constrained nodes. Key management in encryption technique is one of the most frequently exercised techniques; however, it lacks the robustness against various

Designing of Reconfigurable Compact Bandpass Microstrip Filter

Publisher: IEEE

C.S. Kavitha Devi ; H. Umadevi ; Jambunath S. Baligar All Authors

Abstract:A Reconfigurable Bandpass Microstrip Filter is designed and simulated to Reconfigured Compact Bandpass Microstrip (RCBM) Filter to minimize the size of the filter and to ... **View more**

Metadata

Abstract:

A Reconfigurable Bandpass Microstrip Filter is designed and simulated to Reconfigured Compact Bandpass Microstrip (RCBM) Filter to minimize the size of the filter and to enhance its bandwidth (BW). The achieved BW is 1.44GHz with minimum amount of insertion loss of -0.5dB and compactness of 1/3 rd size reduction in the filter compared to its original filter size, by this methodology.

Published in: 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)

Date of Conference: 12-14 June 2019 **INSPEC Accession Number:** 18971557

ASIC Implementation of Rabbit Stream Cipher Encryption for Data

Publisher: IEEE

Prathima N. ; Chetan S. ; Syed M. Rehman All Authors

Abstract: Over a network to secure information and to remain confidential cryptography plays a very important role in today's life. Cryptography is an method of converting informat... **View more**

Metadata

Abstract:

Over a network to secure information and to remain confidential cryptography plays a very important role in today's life. Cryptography is an method of converting information to a non-understandable form and then being able to convert it to the understandable form by the recipient. High level of security can be used for computing small power using lightweight stream ciphers. The new pipelined approach is proposed for Stream encryption means each letter one by one followed by the changing the encryption key after each letter. Here the work presents the design, simulation, and synthesis. Further the design is developed using cadence EDA physical design tools for optimizations on constraints like area, delay and low power consumption. Validation of data transmission in secure form (i.e., audio, image and text) using rabbit stream cipher algorithm is [illegible] implementation [illegible] using [illegible]

Emerging Research in Computing, Information, Communication and Applications pp 533–540

Dual-Mode Wide Band Microstrip Bandpass Filter with Tunable Bandwidth and Controlled Center Frequency for C-Band Applications

Shobha I. Hugar, Vaishali Mungurwadi & J. S. Baligar

Conference paper | First Online: 11 September 2019

Part of the Advances in Intelligent Systems and Computing book series (AISC,volume 906)

Abstract

This paper presents a unique approach for designing dual-mode wide band BPF with tunable bandwidth and controlled center frequency for C-band (4–8 GHz) applications. The proposed filter is designed using radial stub-loaded dual-mode $\lambda_g/2$ resonator to get wide passband. The dual-mode behavior of the resonator, i.e., odd- and even-mode resonance frequencies are realized by inserting a radial stub at the center of the resonator and further the size of filter is reduced by folding the resonator. A modified

Access provided by:
Dr. Ambedkar Institute of Technology

Sign Out

Dual Band Microstrip BPF with Controlled Wide and Narrow Pass Bands

Publisher: IEEE

Shobha I Hugar ; Vaishali Mungurwadi ; J S Baligar **All Authors**

Abstract

Document Sections

Authors

Figures

References

Citations

Keywords

Abstract: The proposed work demonstrates reconfiguration of wideband response of multimode resonator to dual band BPF with wide and narrow passbands. The proposed filter comprises ... **View more**

Metadata

Abstract:
The proposed work demonstrates reconfiguration of wideband response of multimode resonator to dual band BPF with wide and narrow passbands. The proposed filter comprises of half wave SIR based multimode resonator, with Bowtie radial stub integrated into its symmetrical plane. To attain dual band characteristics from wideband response a new transmission zero is created in wide passband which splits it into wide and narrow passbands. A new transmission zero is procured by Bowtie radial stub. The wide and narrow passbands are centered at 5.5 GHz and 12.5 GHz respectively. To procure flat pass band response, a high impedance Interdigital feed structure is used at input and output. Due to this feed structure, the insertion loss S_{21} is at almost 0dB line in first passband. Further by varying the radial angle θr of Bowtie stub, both passbands are controlled by manipulating the location of new transmission

Emerging Research in Electronics, Computer Science and Technology pp 1107–1118

Optimal Resource Allocation and Binding in High-Level Synthesis Using Nature-Inspired Computation

K. C. Shilpa, C. LakshmiNarayana & Manoj Kumar Singh

Conference paper | First Online: 24 April 2019

Part of the Lecture Notes in Electrical Engineering book series (LNEE,volume 545)

Abstract

Allocation of resource and binding it to functional unit at high-level synthesis an optimal problem to minimize the area and performance in terms of resource sharing and binding is presented in this paper. The paper presents the comparative analysis of nature-inspired computation techniques for resource allocation and binding: 1. Evolutionary-based computation: genetic algorithm. 2. Swarm intelligence-based computation: particle swarm optimization. The comparative analysis of the results shows genetic algorithm surpasses particle swarm

Face Recognition Based on Windowing Technique Using DCT, Average Covariance and Artificial Neural Network

Publisher: IEEE

A. Divya ; K.B. Raja ; K.R. Venugopal All Authors

Abstract: The field of Face Recognition (FR) is still a thought-provoking problem, while in recent advances of Artificial Neural Networks (ANN) has shown improved performance in FR... **View more**

Metadata

Abstract:
The field of Face Recognition (FR) is still a thought-provoking problem, while in recent advances of Artificial Neural Networks (ANN) has shown improved performance in FR rate. In this paper, we propose face recognition based on windowing technique using Discrete Cosine Transform (DCT), average covariance and ANN. The novel concept of windowing technique is used to divide each image to 4x4,8X8 and 16X16 size of windows. The DCT is applied on each window to obtain DCT co-efficients. The covariance matrix is computed on each DCT coefficient matrix and average value of each block is also computed to obtain final feature value. The computation of an average covariance reduces the original size of face image by around 97% i.e., the number of co-efficients in the final feature set is only around 3% of the original

Proceedings of the International Conference on Intelligent Systems and Signal Processing pp 25–33

Automatic Fire Detection Using Combination of Color Cue and Flame Flicker

Ripal Patel, Kashyap Mandaliya, Pushkar Shelar, Rushi Savani & Chirag I. Patel

Conference paper | First Online: 19 January 2018

Part of the Advances in Intelligent Systems and Computing book series (AISC,volume 671)

Abstract

This paper presents the novel algorithm for automatic fire detection from still images and video sequences. Proposed technique has been using the color cue and flame flicker for detecting fire. This paper proposes a combination of two algorithms to detect fire from video clips. Firstly, the algorithm defines the method to detect fire in static images which can be called as color feature technique. Secondly, the algorithm defines to detect the fire in video sequences, which can be called as flicker

Linearity enhancement of 0.5µm E/D pHEMT class E power amplifier for PCS applications

Publisher: IEEE

P. Shanthi ; J. S. Baligar All Authors

Abstract: This paper presents a monolithic power amplifier (PA) using 0.5µm enhancement pseudomorphic high-electron mobility transistor (E/D pHEMT) technology with builtin linearizer... **View more**

▸ Metadata

Abstract:

This paper presents a monolithic power amplifier (PA) using 0.5µm enhancement pseudomorphic high-electron mobility transistor (E/D pHEMT) technology with builtin linearizer circuit. Integrated series diode and pHEMT switch linearizer with classE PA is designed. Two tone analysis and Envelope analysis are done to find the IMD3 and ACPR for the circuit with CDMA IS-95 modulated source. As the modulation becomes complex for the future transmission standards, distortion measurement replaces two tone signals with modulated signal (NB-CDMA). The simulated results for a diode and transistor linearizer circuit with two stage class E PA has improvement in IMD3 reduction to 5dBc and 14dBc. The AM-AM simulation for linearizer with diode and transistor appears linear for an input power of 4dBm and 14dBm respectively. ACPR improvement of these circuits is 12dBc and 20dBc respectively.

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 167 – 175

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

Natural Computation for Optimal Scheduling with ILP Modeling in High Level Synthesis

Shilpa K. C[a], LakshmiNarayana.C[b,*]

[a,b] *BMSCE, Department of Electrical Engineering Science, Visvesvaraya Technological University, Bangalore, 560019, India.*

Abstract

The concept of the natural computation for optimal scheduling in high level synthesis, for resource constraint and time constraint scheduling problem in automated integrated circuit synthesis using Integer Linear Programming (ILP) modeling is presented in this paper. This paper compares three natural computations paradigms: (i) evolution optimizer technique genetic algorithm, (ii) evolutionary programming, and (iii) swarm intelligence based particle swarm optimization. Experimental results indicate that evolution based Genetic Algorithm search is more powerful search compared to Evolutionary Programming and Particle Swam Optimization.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

Keywords: High Level Synthesis ; Data Flow Graph; Evolutionary Programming ; Genetic Algorithm ; Particle Swarm Optimization ; Very Large Scale Integration ; Integer Linear Programming

1. Introduction

Very Large Scale Integration (VLSI) circuits built with hundreds and thousands of transistors on a single chip, the design complexity of the chip increases in terms of number of gates, transistors and functionality.

* Corresponding author. Tel.: + 91-974-3300352.
E-mail address: shilpa.kc2@gmail.com

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.02.008