ISSN: 2321-7782 (Online)
Volume 3, Issue 7, July 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

FPGA Based Reconfigurable Logic Blocks to Obtain Robust and Secured Images

Sunil B. Hebbale[1]
Professor
Dept. of CSE
KLE College of Engg. &Technology
Chikodi, Dist. Belagavi, Karnataka, India.

Ashwini V. Gavali[2]
Professor
Dept. of CSE
KLE College of Engg. &Technology
Chikodi, Dist. Belagavi, Karnataka, India.

Abstract: ***The purpose of the system is to (i) implement a reconfigurable FPGA based computing architecture with design objectives such as high performance, specialization and adaptability. FPGA can offer both the flexibility of computer software and ability to construct custom high performance computing circuits. (ii) Deploy number systems based cryptography schemes for secure sharing of internet and intranet resources without global protocol redeployment or architectural support. Natural numbers which are available in infinite volume are used to encrypt the given message. The Gaussian Farey fractions are used to encode the key number for access control matrix. The techniques proposed can help in increasing the accuracy and completeness of Internet topology discovery and leverage existing protocol and hardware features.***

Keywords: FPGA, ASIC, SNR, VRC, EHW, HDL, VLSI, VHSIC, CRT

I. INTRODUCTION

In the recent Internet architecture the support for securing the shared Internet resources is very limited. The shared Internet resources include medical scanned images, satellite images, scanned specimen signatures etc. Hence, nonlinear image processing with good flexibility and adaptability is highly desirable in many applications such as image transformation, correction of distortion effects, noise removal and histogram equalization.

As a result of limited support for both securing and identifying this shared Internet resources, the resource exhaustion does occur due to inefficiently scaling system, selfish resource consumption and malicious attack. Malicious users deviate arbitrarily from prescribed protocols expressly to exhaust shared resources. Typical examples of malicious behavior include mounting a distributed denial of service attack and saturating a link such that it is unusable. Basic services of information security include verification, preserving data integrity, providing non repudiation and ensuring secrecy. Similarly, integrity threat includes interception of data, modification of message, replay of message, masquerading and repudiation. In this context, cryptography can be used to provide confidentiality using encryption methods and can also provide data integrity, authentication and non-repudiation.

Calculations involved in image processing algorithms are real challenge in front of system designers today. Traditionally three methods are followed for designing a system. 1. ASIC (Application Specific Integrated Circuit) 2. Using microcontroller 3. FPGA (Field Programmable Gate Array). ASIC systems are most efficient one, but once it is made for any particular purpose, its functionality cannot be changed. Microcontroller based system gives flexibility in the functionality change but its speed of operation is much lower than ASIC systems. The third option is FPGA. FPGA systems can work with speed comparable to ASIC and with much more flexibility. Once a FPGA system is configured it acts as ASIC system. This limits to perform various types of applications with the speed of FPGA. This problem can be solved by configuring FPGA again and again. In this way we increase flexibility of FPGA. It makes use of existing algorithms and tries to make system more flexible.

The purpose of the system is to (i) implement a reconfigurable FPGA based computing architecture with design objectives such as high performance, specialization and adaptability. FPGA can offer both the flexibility of computer software and ability to construct custom high performance computing circuits. (ii) deploy number systems based cryptography schemes for secure sharing of internet and intranet resources without global protocol redeployment or architectural support. Natural numbers which are available in infinite volume are used to encrypt the given message. The Gaussian Farey fractions are used to encode the key number for access control matrix. The three distinct notions of security models namely co-operative, selfish and malicious users will be considered in this work. The techniques proposed can help in increasing the accuracy and completeness of Internet topology discovery and leverage existing protocol and hardware features.

Reconfigurable devices offer both the flexibility of computer software and the ability to design custom high performance computing circuits. The high performance image filters on FPGA will reduce evolution time.

II. WHY FPGA?

Typical non-linear image processing applications include the correction of non-linear distortion introduced by components, communication channels and compensation for non-linearity in input output devices. Slow SNR variations can typically arise due to changing noise characteristics from parameters such as weather, distance or input power.

Similarly, lack of synchronization in capturing a moving image with a static camera or vice versa can result in rapid SNR variation effects. Traditional adaptive filter works in a rectangular window whose size varies during filter operation depending on certain conditions. The optimal size of the window is crucial and influences the computation and memory requirements. However, this optimal size selection is highly application specific and its convergence from an initial value requires experimentation with various sizes of standard filters.

Similarly in the development of schemes for securing shared resources, recent development in deterministic polynomial time algorithm that determines whether a given number is a prime or composite number in public key cryptography, has thrown greatest challenge to explore the cryptographic algorithms using natural numbers.

III. WHAT IS FPGA?

Application specific hardware implementation offers much greater speed than a software implementation. With advances in the VLSI (Very Large Scale Integrated) technology hardware implementation has become an attractive alternative. Implementing complex computation tasks on hardware and by exploiting parallelism and pipelining in algorithms yield significant reduction in execution times.

There are two types of technologies available for hardware design. Full custom hardware design also called as Application Specific Integrated Circuits (ASIC) and semi custom hardware device, which are programmable devices like Digital signal processors (DSPs) and Field Programmable Gate Arrays (FPGA's).

Full custom ASIC design offers highest performance, but the complexity and the cost associated with the design is very high. The ASIC design cannot be changed and the design time is also very high. ASIC designs are used in high volume commercial applications.

Field Programmable Gate Arrays are reconfigurable devices. Hardware design techniques such as parallelism and pipelining techniques can be developed on a FPGA, which is not possible in dedicated DSP designs. Implementing image processing algorithms on reconfigurable hardware minimizes the time-to-market cost, enables rapid prototyping of complex algorithms and simplifies debugging and verification. Therefore, FPGAs are an ideal choice for implementation of real time image processing algorithms.

FPGAs have traditionally been configured by hardware engineers using a Hardware Design Language (HDL). The two principal languages used are Verilog HDL (Verilog) and Very High Speed Integrated Circuits (VHSIC) HDL (VHDL) which allows designers to design at various levels of abstraction.

The growth in both the capacity and application space of FPGAs has two main security implications. Firstly, today's FPGA designs represent a significant development investment which needs to be protected. Secondly, FPGAs are increasingly being used in applications that require security properties that are either not available today, or that are yet to be adequately investigated. Both have brought recent attention to the security attributes of FPGAs in the military, automotive, consumer industries, and also the research community, each with its own requirements and security perspectives.

IV. OBJECTIVE

This system introduces image processing using reconfigurable FPGAs and how it can be applied effectively for real world image processing applications. By exploring a large design search space, the system can adapt to changes in task environment through its ability to reconfigure its own structure online and autonomously. In this system, minimally sufficient resources are dynamically allocated based on noise levels at specific time instant. The architecture for image enhancement can compensate uniformly for both slow and rapid SNR (Signal to Noise Ratio) changes. The filter specifies small spatial masks and captures the essence of the full filter functions in the spatial domain.

In the context of development of polynomial time algorithm to determine whether the given number is a prime or not and the Shannon's principles of Confusion and Diffusion, the system is to build an Encryption and Decryption process using natural numbers. This is done by generating a group from any general natural number and then shows how this group can be used with Claude Shannon's principles for generation of a simple (yet as secure, as the one that is generated with the help of larger primes) encryption and decryption process.

The first step will be to analyze thoroughly the input–output specification for the Virtual Reconfigurable Circuits (VRC). The Virtual Reconfigurable Circuit architecture is designed for implementing real-world applications on evolvable hardware (EHW) in common FPGAs. The FPGA technologies offer basic digital blocks with flexible interconnections to achieve high speed digital hardware realization. The FPGA consists of a system of logic blocks, such as look up tables, gates, or flip-flops and some amount of memory. The image will be transferred to FPGA board which will perform the required filtering/processing using small spatial masks and captures the essence of the full filter function in the spatial domain. With Evolvable Hardware (EHW) it introduces a new approach to automatic design of image filters for a type of noise. The approach employs evolvable hardware at simplified functional level and produces circuits that outperform conventional designs. The entire EHW design can be realized using Hardware Descriptive Language (HDL). The image enhancement architecture will be compactly designed by exploiting the inherent parallelism. The designed module has the advantage that it is possible to execute image processing algorithms many times faster than that could be achieved if implemented using conventional processors.

A method to encode a Key in Hierarchical Single Key-Lock (SKL) mechanism based on Chinese Remainder Theorem (CRT) using natural numbers is proposed. Here key number is encoded using CRT. The tribes of Gaussian or Rational Farey Fractions with Natural numbers are used to encode the key number. The advantages of this encoding are, it is not required to decode the key to determine the access rights and it is also not required to derive the key number for already existing files. This method increases the security level of the system by encoding the key using arbitrary Farey Fraction with Natural numbers.

V. CONCLUSION

So far, it has been observed that current evolutionary techniques have practical limitation when applied for complex real world problems. Also the research spaces can become vast for large circuits and a greater deal of research needs to be directed at scalability. Hence, by using FPGA, one can still evolve circuits with limited interactions and so can be used by traditional designers as building blocks for larger circuits.

Initial research involved evolving circuits at a very high primitive gate level and results obtained using this approach showed that evolved circuits were less useful for more demanding commercial applications. Hence, to overcome this problem a function-level evolution is proposed in this work.

It has been proposed that the high robust and secured images can be obtained using FPGA based reconfigurable procedure by enhancing the image and reducing noise in the image. The image enhancement architecture will be compactly designed by exploiting inherent parallelism. The proposed system has the advantage that it is possible to execute image processing algorithms many times faster than that could be achieved using conventional processors. Noise affects the perceptual quality of the image. Therefore filtering is an essential part of any image processing system which is done using FPGA.

References

1. Anil K Jain, "Advanced Digital Image Processing", PHI India, 1995.
2. Boping Shi, Jingsong He, A Novel Edge detection technique with Orientation based similarity and Immunological Principles, IEEE Computer Society's Third International Conference on NaturalComputation, 2007.
3. Karel Slany and Lukas Sekanina, : Fitness Landscape Analysis and Image Filter Evolution Using Functional Level CGP", EuroGP 2007, pp 311-320.
4. Jim Torresen, Jorgen W Bakke and Lukas Sekanina, "Efficient Image Filtering and Information Reduction in Reconfigurable Logic", Proceedings of Norchip Conference 2004, pp 63-66.
5. Zdenek Vasicek and Lukas Sekanina, " An evolvable hardware system in Xilinx Virtex II Pro FPGA", International Journal on Innovative Computing and Applications, Vol 1, No 1, 2007,pp 63-73.
6. Giridhar Akula," Configurable logic blocks used to obtain secured images" PhD thesis, JNTUA, 2009.
7. Aniket Burkule & P. B. Borule " Use of Reconfigurable FPGA for Image Processing " ijarcsse., Vol 3, No. 1, Jan-2013, pp 432-436
8. Jinu Elizabeth & Ajay Daniel Peter, "FPGA Based Secure Biomedical Image Transmission" International Journal on Computer Applications Vol 69, No. 6, 2013,pp 39-43.

AUTHOR(S) PROFILE

Sunil B. Hebbale, received the M. Tech. degree in Computer Science & Engg. from VTU Belagavi in 2001 and B.E. degree in Computer Science & Engg. From Gulbarga University, Kalaburgi in 1998. He is having 15 yrs experience in teaching & is now with KLE College of Engg. &Technology, Chikodi, Dist. Belagavi, Karnataka, India.

Ashwini V. Gavali, received the M. Tech. degree in Computer Science & Engg. from Shivaji University, Kolhapur in 2008 and B.E. degree in Computer Science & Engg. from WCE, Sangli in 2000. She is having more than 10 yrs experience in teaching & is now with KLE College of Engg. &Technology, Chikodi, Dist. Belagavi, Karnataka, India.

