AN AREA AND POWER EFFICIENT ON CHIP COMMUNICATION ARCHITECTURES FOR IMAGE ENCRYPTION AND DECRYPTION

Y.Amar Babu[1], G.M.V.Prasad[2]

[1]Dept. of ECE, L.B.R. College of Engineering, Mylavaram, India
[2]Principal, B.V.C. Institute of Technology and Science, Batlapalem, India

Abstract

The design of new electronic systems is getting more complex as more functionality is integrated into these systems. To design complex system, a predictable design flow is needed. A soft processor based System-on-Chip (SoC) is often mentioned as the hardware platform to be used in modern electronics systems for fast prototyping on FPGA. In this paper, a novel area and power efficient on chip communication architectures has been proposed for image encryption and decryption using single soft processor(Micro Blaze). Proposed System On Chip explores On chip Communication architectures features to efficiently implement the application. The SoC offers scalability and guarantees on the timing behavior when communicating data between various processing and storage elements. Proposed SoC has been implemented on Spartan6 FPGA and evaluated at 83.33MHz. It has occupied only 19% of resources available on target FPGA , consumes very low power. The proposed on chip communication architectures compared with device utilization on FPGA and power consumed.

Keywords: *SoC, FPGA, Encryption and Decryption, Micro Blaze*

--***--

1. INTRODUCTION

SoC architectures are used to provide the required computational power for novel embedded systems. The ITRS predicts that while manufacturing complex SoC will be feasible, the production cost will grow rapidly as the costs of masks is raising drastically. The growing complexity of embedded systems leads to a large in their development effort. At the same time, the market dynamics for these systems push for shorter and shorter development times. The NRE cost associated with the design and tools of complex chips is growing rapidly. To address these issues, a platform based design methodology is proposed. The main objective of this design methodology is to increase the re-use of soft cores and IPs. The SoC consists of both hardware, and the software controlling the soft processor or DSP cores, peripherals and interfaces. The design flow for a SoC aims to develop this hardware and software in parallel.

Most SoCs are developed from pre-designed hardware blocks for the hardware, together with the software drivers that control their operation. The hardware blocks are put together using EDA tools. The software modules are integrated using a Software development environment. In this paper, a novel soft processor based SoC architecture is proposed for Image encryption and decryption, which is based on shared processor local bus (PLB) and developed using Xilinx Platform Studio (XPS)[1][2].

Proposed SoC has three layers, hardware layer which is based on soft processor (Micro Blaze), Standalone OS layer which has low level drivers for different controllers and interfaces and application layer which is developed using above two layers as shown in Figure1[3].

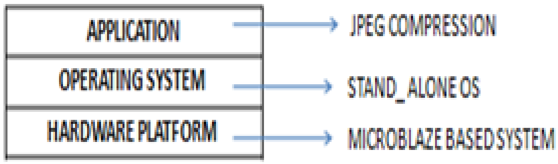

Figure 1: Layered Structure of SoC

2. MICRO BLAZE SOFT PROCESSOR

The micro blaze embedded processor soft core is a reduced instruction set computer (RISC) optimized for implementation in Xilinx Field Programmable Gate Arrays (FPGAs).

Compared to other general purpose processors, micro blaze is quite flexible with a few configurable parts and capable of being extended by customized co-processors. There are a number of on-chip communication strategies available including a variety of memory interfaces. The operating frequency of micro blaze on spartan-6 SP605 kit is 83.33Mhz. Hence we use micro blaze soft-core processor in order to develop hardware platform for JPEG compression application.

Micro blaze processor has an instruction decoding unit, 32x32 bit general purpose register file, arithmetic unit and special purpose registers. In addition, it has an instruction pre fetch buffer. The arithmetic unit is configurable, as shown in core block diagram. The Barrel Shift, Multiplier, Divider and FPU are optional features. Micro blaze processor has a three- stage pipeline: fetch, decode and execute. For most of instructions, each stage takes one clock cycle. There is no branch prediction logic. Branch with delay slot is supported to reduce the branch penalty. Micro blaze is a Harvard architecture processor, with both 32-bit I-bus and D-bus. Cache is also an optional feature. Three types of buses, FSL, LMB and OPB are available. FSL bus is a fast co-processor interface. LMB is one-clock-cycle, on-chip memory bus while OPB is a general bus with arbitration.

MicroBlaze has an orthogonal instruction set architecture. It has thirty-two 32-bit general purpose registers and up to eighteen 32-bit special purpose registers, depending on configured options.

3. PROPOSED SoC ARCHITECTURES

We proposed two On Chip Communication architectures. First one is based on IBM Coreconnect Bus Processor Local Bus(PLB) and second on chip communication is AMBA AXI interconnect[3] System on chip for Image encryption and decryption has three layers as shown in figure 1. The three layers are hardware platform followed by operating system (OS) and the required application that is to be carried out. In this third layer is Image encryption and decryption. First layer is hardware platform. It is generated using micro blaze. Micro blaze is flexible and can be configurable customized soft core processor. Second layer is operating system. Standalone OS is used for controlling hardware platform. The application is developed using the two layer. Hardware platform for the image encryption and decryption requires components like, Block RAM, Instruction Local Memory Bus controller , Data Local Memory Bus controller, Micro blaze Debug Module, UART, System_ACE controller for Compact flash, Multiport Memory controller for DDR3 SDRAM, PLB-Bus. All these hardware components are configured for Image encryption and decryption. Its architecture is as shown in the figure 2a. And second On chip communication architecture is based on AMBA AXI Interconnect for Image encryption and decryption as shown in Figure 2b[4][5].

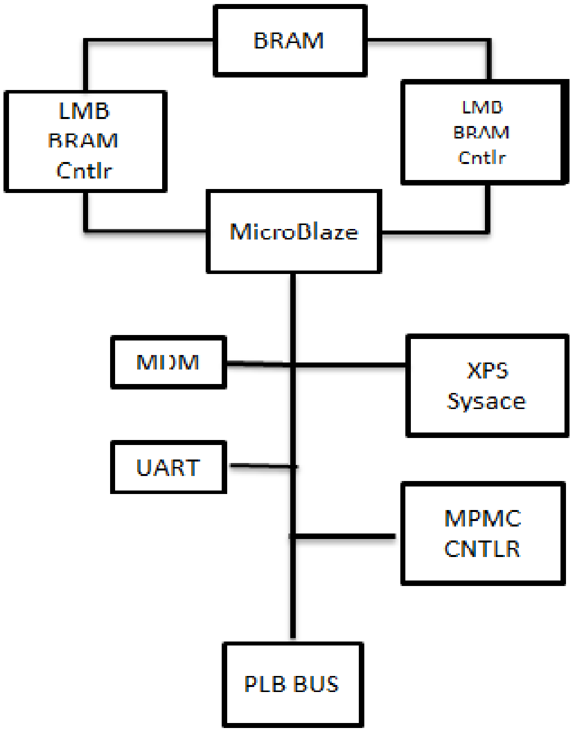

Figure 2a. PLB Based SoC

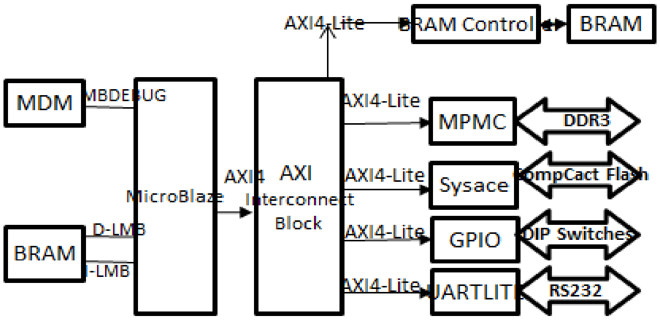

Figure 2b.AXI Based SoC

4. IMAGE ENCRYPTION AND DECRYPTION

The Image encryption and decryption is developed on proposed SoC using AES algorithm. Embedded C is used to develop the AES algorithm and to access images from Compact flash. AES comes in three favors, namely AES - 128, AES - 192, and AES-256, with the number in each case representing the size (in bits) of the key used. All the modes are done in 10, 12 or 14 round depends on the size of the block and the key length chosen. AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4*4 matrix that is called the state. The algorithm begins with an Add round key stage followed by nine rounds of four stages and a tenth round of three stages which applies for both encryption and decryption algorithm [6] [7] [8].

These rounds are governed by the following four stages:

- Substitute Bytes
- Shift rows
- Mix columns
- Add round key

The tenth round Mix columns stage is not included. The first nine rounds of the decryption algorithm are governed by the following four stages:

- Inverse Shift rows
- Inverse Substitute Bytes
- Add round key
- Inverse Mix columns

Again the tenth round Inverse Mix columns stage is not included. The Overall flow of the encryption and decryption algorithm of the AES algorithm is show in Figure 3.

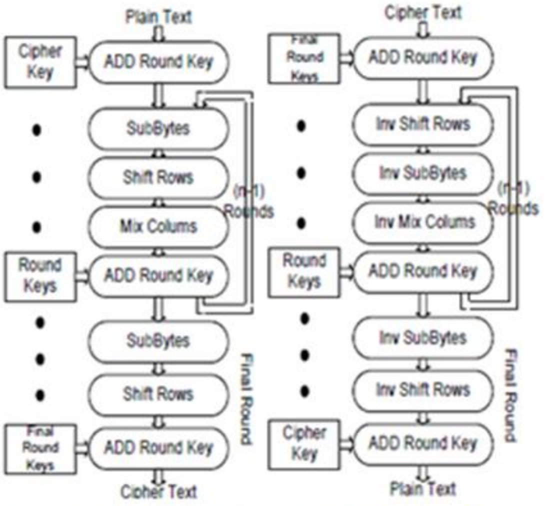

Figure 3 : Design Flow for AES Algorithm

5. IMPLEMENTATION

This AES algorithm is implemented for the text. But It can be used for the images, pdf file formats, any other types of documents. For every image there will be a header and footer which gives the information regarding resolution, pixels, starting and ending of image. In order to acquire the proper image this header and footer information should be proper so we need not to encrypt this part and the remaining part which contains pixel information will be encrypted and decrypted. In this paper jpeg images are used for the encryption and decryption. First copy the header part into the encryption file. The header part does not go for the encryption to support the jpeg format. After copying the header part in the encrypted file, encrypt the remaining data using AES algorithm and then copy the footer part without encryption. For the decrypted image, use the same procedure. The header and footer part does not go for the encryption or decryption to support jpeg format.

6. RESULTS

Proposed On chip communication architectures for image encryption and decryption has been implemented using Xilinx EDK tool and Image encryption and decryption application developed using SDK tool. Device utilization of two communication architectures are compared as shown in figure 5.Figure 5 provides how many SLICEs and LUTs are used for proposed SoC design. On chip power detail are as shown in figure 6, provides power consumption of PLB based SoC, AXI based SoC. The SoC occupied only 19% resources and it is area efficient design. The design consumes very low power of 0.67 W. Experimental results as shown in figure 4 provides encrypted and decrypted images with original image and takes only 45 sec for both encryption and decryption process. The proposed design has been evaluated with 83.33MHZ. AXI based SoC has better performance when compared with PLB based SoC.

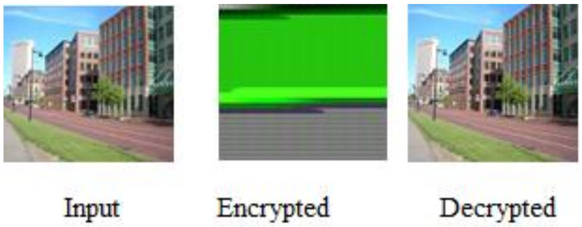

Figure 4 :Encrypted and Decrypted Images

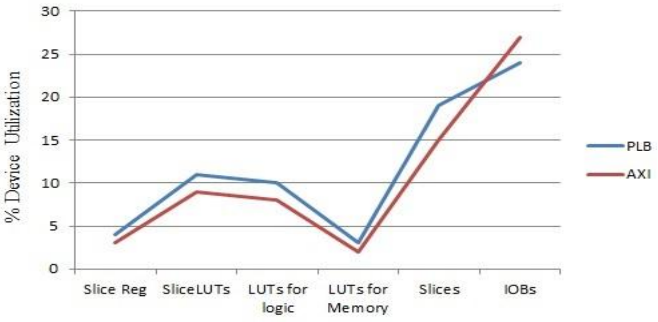

Figure 5 : Device Utilization

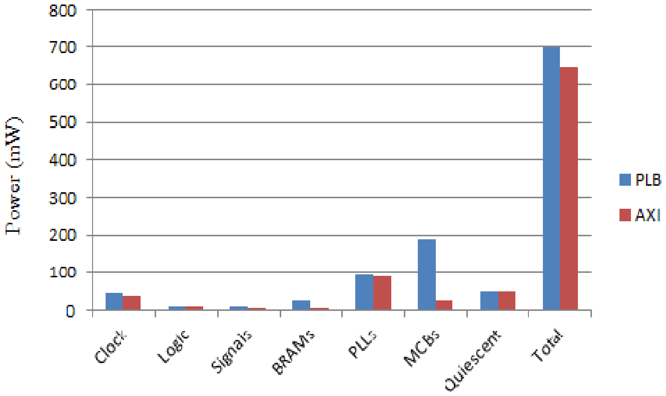

Figure 6 : On Chip Power

7. CONCLUSIONS

In this paper, a novel shared bus based SoC architecture and AXI based SoC has been proposed and implemented on Spartan 6 FPGA using single soft processor. The effectiveness of design flow and SoC architecture is illustrated by experimental results obtained from the image encryption and decryption on proposed SoC design. In comparison to hardware methods and software methods which are often used to implement cryptographic applications, proposed SoC offers fast prototyping , area efficient and consumes less power. This work can be extended to research on HW/SW portioning and Multi Processors SoC (MPSoC) with shared bus

REFERENCES

[1]. Shaila S Math, Manjula R B, “Survey of system on chip buses based on industry standards”, Conference on Evolutionary Trends in Information Technology(CETIT), Bekgaum,Karnataka, India, pp. 52, May 2011

[2]. ARM, AMBA Specifications (Rev2.0). [Online]. Available at http://www.arm.com, 1999

[3]. ARM, AMBA AXI Protocol Specification (Rev 2.0). [Online]. Available at http://www.arm.com, March 2010

[4]. IBM, Core connect bus architecture. IBM Microelectronics. [Online]. Available:http://www.ibm.com/chips/products/coreconnect, 2000

[5]. Silicore Corporation, Wishbone system-on-chip (soc) interconnection architecture for portable ip cores, (Rev B.3). [Online]. Available at http://www.opencores.org/projects.cgi/web/wishbone/wishbone, Sept 2002

[6]. ARM, AMBA AXI protocol specifications, Available at, http://www.arm.com, 2003

[7]. National Institute of Standards and Technology, “Federal Information Processing Standard Publication 197, the Advanced Encryption Standard (AES),” Nov. 2001.

[8]. William Stalling, Cryptography and Network Security: Principles and Practices, Principles and Practices, 4th ed. Prentice Hall, 2006.

[9]. Charles H Roth, Jr. Digital Systems Design Using VHDL, Thomson, India Edition 2007.

[10]. Atul Kahate, Cryptography and Network Security, Second Edition, Tata McGraw-Hill Edition 2008.

[11]. Abdulkarim Amer Shtewi, Bahaa Eldin M. Hasan, Abd El Fatah .A. Hegazy “An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems” IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2,pp.226-232 February 2010.

[12]. P.Karthigaikumar, Soumiya Rasheed “Simulation of Image Encryption using AES Algorithm” IJCA Special Issue on “Computational Science - New Dimensions & Perspectives” NCCSE, pp166-172, 2011.

[13]. Mr. Atul M. Borkar, Dr. R. V. Kshirsagar, Mrs. M. V. Vyawahare “FPGA Implementation of AES Algorithm” IEEE, pp.401-405, 2011.

[14]. Xinmiao Zhang, Keshab K. Parhi, Fellow, “High-Speed VLSI Architectures for the AES Algorithm” IEEE Transactions on vlsi systems, vol. 12, no. 9, pp.957-966, September 2004.

[15]. Manoj. B, Manjula N Harihar “Image Encryption and Decryption using AES” IJEAT, Volume-1, Issue-5, June 2012.