System-on-System (SoS) Architecture for Secure Bio-medical Imaging

Sang-Jin LEE, Yeon-Ho KIM, Kyung-Chang PARK, Yun-ki HONG, Younggap YOU, Kyoung-Rok CHO, Tae Won CHO, Kamran ESHRAHGHIAN

World Class University (WCU) Program
College of Electronics and Information Engineering
Chungbuk National University, Cheongju, Chungbuk, 361-763, Korea

ABSTRACT

This paper presents an integrated approach towards implementation of a multilayered architecture based on stacked silicon for image capture and secure data transmission suitable for bio-medical devices and implementation within patient-point-of-care network. The system architecture is comprised of a CMOS based image sensor layer, memory layer, 3D-DWT (Three-dimensional Discrete Wavelet Transform), 3D-AES (Three-dimensional Advanced Encryption Standard) and RF transmitter. Each layer is independent that can be fabricated using a different technology. Chips are stacked and interconnected using Through Silicon Via (TSV) technology. The CMOS image sensor located in the top layer operates as a high definition (HD) imager. The 3D-DWT compresses the stored image prior to processing. Compressed image data is encrypted, using 3D-AES encryption layer. The 3D-AES encryption block employs 3 functional layers: key schedule, S-box and round processing. The round processors are designed as fully pipeline structures. The encrypted data is shuffled to employ fault tolerance. Encrypted and shuffled data is stored in memory or alternatively is transmitted through an RF transmitter. Since each system is interconnected through TSV, the number of the input and output buffers are reduced thereby reducing the power consumption. The system can be implemented as a core element of portable devices for transmission of images within a health care management system.

Keywords: System-on-System, SoS, Bio-medical, 3D-DWT, 3D-AES

1. INTRODUCTION

System-on-System (SoS) and 3D integration technology

As systems complexity increases the number of input and output pins also increase to accommodate extensive signal connections among circuit components. However parasitic capacitances and inductances becomes major design issue in order to devise low power and faster circuits. Three-dimensional very large scale integration can increase packing density while having the potential for improved signal propagation delay with reduced power consumption when compared with equivalent 2D counterpart. Low power and high speed circuit operation cannot be resolved through conventional silicon integrated system structure. Multi-layer silicon die stacking is a promising solution that can address low power operation requirements as well as high performance where through utilization of silicon via (TSV) being one of the most critical architectural feature in our approach to system integrations. Conventional chips are stacked to form a consolidated piece of system where each die is designed and fabricated with distinct technology that may differ from other dies. The smaller size and shorter physical dimension saves substantial parasitic effects resulting in faster and cooler circuit operation [1][2][3].

Security of private medical information

Privacy protection becomes important as medical image data are transmitted through public communication networks. Digitized medical images can be easily modified, and are subject to legal responsibility when disputes are associated with the patients. Health Insurance Portability and Accountability Act (HIPAA) of the U.S. has been effective since 2003. This act is to protect against the abuse and forgery of personal medical information through prohibition of access without formal approval or authentication. Medical images and patient records may be the target of intentional and arbitrary corruption by malicious hospital employees [4]. Encryption is an effective measure to protect medical information from eavesdropping of communication channels and forgery of stored medical records. The block cipher algorithms such as AES and ARIA are the standard methods to fulfill the secrecy requirements. The cryptic algorithms can be implemented together with other functional blocks such as discrete wavelet transform (DWT) in the same system [5][6].

Figure 1. Medical video imaging system

The medical imaging system is composed of several layers of silicon dies connected with TSVs whereby all the necessary functional blocks for imaging, compression, encryption and communication are incorporated. The system protects imaging data from intentional external attacks, and prevents malicious forgery.

This paper is organized as follows: Section 2 describes our approach towards system design and integration. Section 3 shows image capture logic. Section 4 presents a three-dimensional structure for implementation of the AES algorithm, while Section 5 gives the advantageous of the new system architecture. Finally Section 6 concludes with suggestions on applications.
2. SYSTEM DESIGN OVERVIEW

The medical video imaging system as illustrated in Figure 2 comprises a CMOS image sensor, memory, 3D-DWT, 3D-AES blocks and RF transmitter.

![Proposed system block diagram](image1)

The system captures images using the CMOS image sensor and stores them in the memory unit. The stored images then traverse through a series of decomposition, entropy encoding and compression with the 3D-DWT. The compressed image data are encrypted by the 3D-AES, and then through an RF transmitter is forwarded to the host computer [10][11].

The system based upon stacking of silicon dies. Each die may have distinct processing technology requirements. Thus the functions can be easily optimized without considering other alien characteristics of different functions. Figure 3 shows the layered physical architecture for complete imaging, data manipulation and transmission/receiver system.

![Physical layers of video imaging system](image2)

3. IMAGE CAPTURE AND COMPRESSION

**CMOS image sensor and processor/interface logic**

Conventional CMOS image sensors include pixel arrays, gain amplifiers and analog to digital converters (ADC) on the same silicon dies. Characteristics of these functional blocks differ from each other in terms of circuit and process technology. They can be made easier with improved performance when they are made separately. For example sophisticated high speed processors may be required to process the captured images [7][8][9] whereas analog process technology will be necessary for ADC.

The two die scheme employs TSV interconnection between the two stacked dies. Figure 4 shows the multi-layer of dies stacked to complete the image sensor, where pixel arrays and peripheral circuitry are accommodated into different silicon dies. Top die comprises pixel arrays, row driver and decoder, and RGB S/H (Sample and Hold). The bottom die carries the remaining functions of the sensor including gain amplifier, analog to digital converter, array control logic and serial interface.

Image data captured at the pixel arrays passes through the processors and peripherals and is stored in the subsequent memory unit. The stored image then passes through decomposition, entropy encoding and quantization and compression by the 3D-DWT unit.

![Architecture of CMOS image sensor](image3)

**Three dimensional architecture of 3D-DWT**

The 3D-DWT requires an extensive scale of memory space so that the processor can access all the image frames on the same time axis. Figure 5 shows an example of 3D-DWT architecture occupying two layers of stacked silicon dies. All the frames on the same time axis can be compressed without any significant hindrance. The architecture comprises same three PE layers. Each layer decomposes images along the direction of the z axis (time), the y axis (vertical) and the x axis (horizontal). The filter architecture is based upon daubechies 9/7 filter used in JPEG2000 [12][13].

![3D architecture of 3D-DWT](image4)

Figure 5. 3D architecture of 3D-DWT
4. **3D ADVANCED ENCRYPTION STANDARD (AES)**

**3D –AES architecture of**
The AES system has three implementation layers as illustrated in Figure 6. The upper and bottom layers carry the same round functions. The middle layer comprises S-boxes and comparison logic used for duplex system operation. The S-boxes are shared between the top and bottom layers. The AES functions are classified into two groups, namely, logic and memory layer. The logic groups are accommodated in the top and bottom dies. The memory group is in the middle die. The logic is to implement round functions except s-boxes for the “sub-bytes” operation and the key expansion. The memory is to store the s-box tables for rounds. The s-boxes in the middle layer are shared by the top and bottom layers. The round functions are pipelined. The size of the s-boxes in the pipelined stage would approximately 40% of the die area when they are implemented in the same chip.

The round logic and s-boxes are 32 bit wide and each round may consume four clock cycles. Three layers of dies are interconnected through a set of TSVs. Key expansion generates all the keys in advance based on the reception of initial key. The encrypted data is shuffled to spread error bits over the entire frame so that error correction can prevent avalanche effect on the decrypted message [16].

![Figure 6. 3D architecture of AES](image)

**Two mode operation**
The AES system has two operating modes: the dual simplex mode and the duplex mode. The system can be reconfigured into one of the two modes by selecting the respective mode. The simplex mode yields high performance by processing two streams of input data. Two independent AES systems reside in the system where each system encrypt or decrypt the incoming data. This mode does not support the high reliability being offered by the architecture. Figure 7 shows the simplex mode of AES system. Data In #1 and Data In #2 represent two independent data streams fed into the two distinct round functions of the top and bottom layers. The s-boxes in the middle layer are shared by the two data streams. The compare logic is not active in this mode.

![Figure 7. Dual simplex mode block diagram of the 3D-AES](image)

**Fully pipelined round processing**
Figure 9 shows the three dimensional pipelined round processing of 3D-AES. Each pipeline stage has its own functions. Only the s-boxes are shared between the top and bottom layers [14][15].

![Figure 9. Fully pipelined round processing of 3D-AES](image)
6. CONCLUSION

This paper presents a system on system architecture aiming at medical imaging and transmission. Multiple 2D chips in conventional systems are integrated into a consolidated three dimensional structure employing TSV and chip stacking technology. Individual dies are fabricated with optimal silicon process suitable to produce the on-board circuitry. The architecture yield several advantages over the conventional single die approach. High performance and low power is possible with this multi-layered structure. The speed of the operation improves significantly due to the shorter interconnection lengths. The length of TSV is around 40-50 micron being shorter than conventional design. The system dissipates less power due to the replacement of power hogging inter-chip I/O circuitry with inter die land-TSV structures without signal amplification. The load of the each circuit is much smaller than conventional I/O ports, and thereby the power consumption is expected to be low. The volume of the entire system can be reduced substantially when the system is integrated with other components such as pixel arrays, memories and processors. It is well suited to the other functions such as DWT for data compression. High level of secrecy extends over the personal medical records by the introduction of the block cipher algorithm. It will prevent the abuse or forgery of the disputed patient medical data.

7. ACKNOWLEDGEMENT

This work was supported by grant No. R33-2008-000-1040-0 from the World Class University (WCU) project of MEST and KOSEF through Chungbuk National University. Contributions made by H. B. Kim of Chungbuk National University is gratefully acknowledged.

8. REFERENCES
