JOURNAL OF SEMICONDUCTOR TECHNOLOGY AND SCIENCE, VOL.17, NO.3, JUNE, 2017
https://doi.org/10.5573/JSTS.2017.17.3.465
ISSN(Print) 1598-1657
ISSN(Online) 2233-4866

Enabling Energy Efficient Image Encryption using Approximate Memoization

Seongmin Hong[1], Jaehyung Im[1], SM Mazharul Islam[1], Jaehee You[1], and Yongjun Park[2]

***Abstract*—Security has become one of the most important requirements for various devices for multi-sensor based embedded systems. The AES (Advanced Encryption Standard) algorithm is widely used for security, however, it requires high computing power. In order to reduce the CPU power for the data encryption of images, we propose a new image encryption module using hardware memoization, which can reuse previously generated data. However, as image pixel data are slightly different each other, the reuse rate of the simple memoization system is low. Therefore, we further apply an approximate concept to the memoization system to have a higher reuse rate by sacrificing quality. With the novel technique, the throughput can be highly improved by 23.98% with 14.88% energy savings with image quality loss minimization.**

***Index Terms*—Crypto processor, approximation, memoization, AES, SSIM, FPGA implementation**

I. INTRODUCTION

As multi-sensor based embedded systems are broadly introduced, security concerns have become one of the major issues. As a result, many commercial and governmental organizations are beginning to require security features for their systems. To meet this demand, various cryptographic algorithms have been developed and applied to the systems. Traditionally, cryptographic computation is performed using software implementation under general purpose processor based systems. However, software implementation of cryptographic algorithms incurs severe performance degradation since cryptographic computation requires high CPU resources with low energy efficiency.

To solve this inefficiency, hardware implementation is widely adopted in the form of specialized hardware accelerators. As these hardwired accelerators perform cryptographic computation efficiently, original program performance can be maintained with minimal power overhead for adding security features. The AES (Advanced Encryption Standard) is one of the most widely used cryptographic algorithms in hardware security because it is fairly strong as shown in Fig. 1(a). Though many previous ideas were introduced to design faster hardware for AES algorithm such as pipelining and parallelization, they still suffer from high power consumption with large hardware overhead [3, 7].

When the AES algorithm is applied to image transfer systems as shown in Fig. 2, reducing power overhead while maintaining high throughput is more important since the data throughput requirement for high-definition image transfer is much higher than for other protocols. To this end, we propose an energy efficient image encryption module using a hardware memoization technique as shown in Fig. 1(b). Memoization is a technique to store the results of complex computations to special storage and reuse the previously calculated result when having the same input [1]. Though the memoization technique is generally known not to be effective for cryptographic algorithms due to the low

Manuscript received Mar. 12, 2017; accepted May. 21, 2017
[1] Dept. of Electronic and Electrical Engineering, Hongik University, Korea
[2] Division of Computer Science and Engineering, Hanyang University, Korea
E-mail : yongjunpark@hanyang.ac.kr

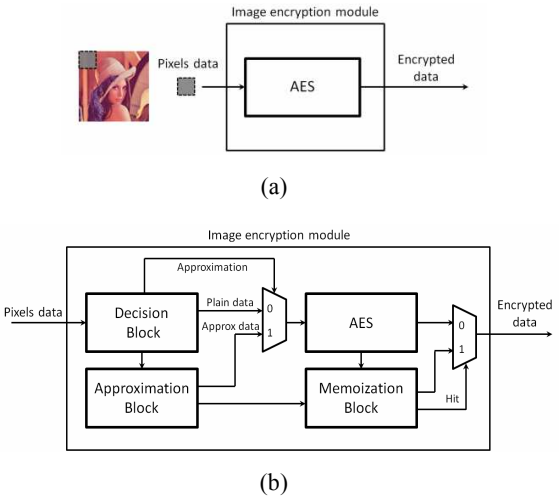


Fig. 1. (a) Conventional image encryption, (b) The proposed image encryption using approximate memoization.

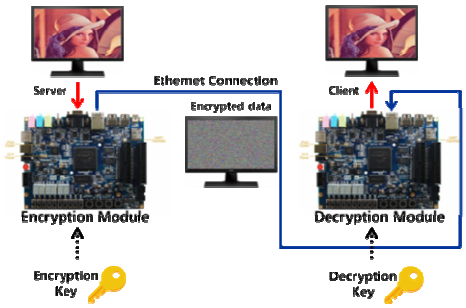


Fig. 2. An example of secure image transfer systems.

reuse rate, it is well matched to image encryption systems because there is a high possibility that neighboring pixels have the same or similar RGB values [2]. However, the reuse rate with a simple memoization system is not as high as expected since most pixel values are slightly different from each other in reality, even though they look the same to human's perception. To increase the reuse rate, we further adopt approximation, which is a technique to improve performance by lowering accuracy, to the memoization system. In this work, we approximate the pixels when the quality degradation is not perceivable by the human eye. Our experiment shows that the approximate memoization system can improve performance and energy efficiency by 23.98% and 14.88%, respectively.

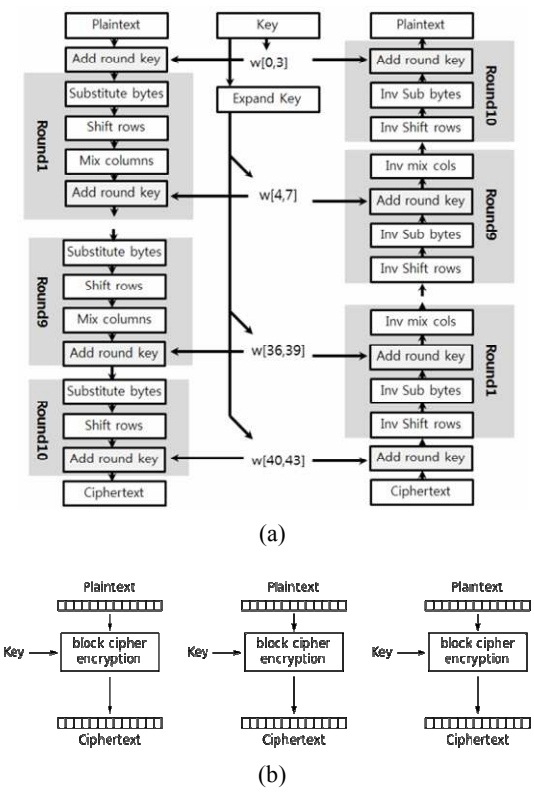


Fig. 3. (a) The AES algorithm, (b) ECB encryption mode.

II. BACKGROUND

1. AES Algorithm

AES [4] is one of the most widely used encryption algorithms. This work uses the 128 bit key length with 10 rounds execution for 128 bit data encryption. The entire AES algorithm is shown in Fig. 3(a), which is quite complex as each round consists of 4 operations: Substitute Byte, Shift Row, Mix Column, and Add Round Key. We designed the AES hardware with a feedback structure, which means that hardware for one round is implemented and it is used iteratively with updated input. The block cipher mode we used is the ECB mode [10] as shown in Fig. 3(b).

2. Image Quality Metric

There have been many research studies on Image Quality Assessment (IQA) techniques. Several widely used metrics are Mean Error (ME), Mean Absolute Error (MAE), Mean Square Error (MSE), and Peak Signal to

Table 1. Parameters of the Structural Similarity Index

	Parameters
μ_x, μ_y	*Average of x, Average of y*
σ_x, σ_y	*Varience of x, Varience of y*
σ_{xy}	*Covarience of x & y*
c_1, c_2	$(k_1L)^2$, $(k_2L)^2$ *are used to avoid division by zero*
L	*Dynamic range of image pixels, typically* $2^{\#of\ bits}-1$
k_1, k_2	0.01, 0.03 *by default*

Noise Ratio (PSNR) [5]. The main drawback of these approaches is that these IQAs treat each pixel separately rather than assessing them together with their background information. Due to this, the results from these IQAs are purely mechanical and mathematical, which comply with the Mean Opinion Score (MOS) very poorly. The MOS is obtained by taking the average of scores given by human testers. These MOS scores are the closest to the Human Visual System (HVS) evaluation of images.

Due to the drawbacks of conventional IQAs, researchers have devised improved ways to measure the quality of images. Among these modern IQAs, the Structural Similarity Index (SSIM) [6] is one of the best, which is expressed as follows with parameters in Table 1:

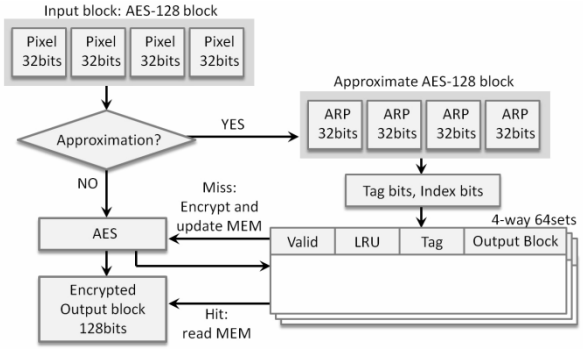
$$SSIM(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)}$$

SSIM is a perceptual metric to quantify image quality degradation of a test image compared to the original image. As a result, the evaluation based on SSIM is highly similar to MOS evaluation. For this paper, we have chosen SSIM as the IQA which is the closest to the MOS evaluated by HVS among the following five IQAs: Mean Error (ME), Mean Absolute Error (MAE), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM).

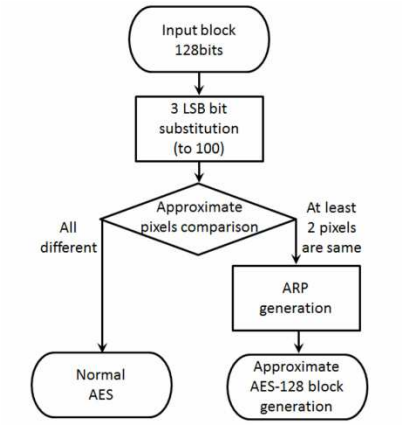
III. PROPOSED SYSTEM

1. System Overview

Memoization is a technique to minimize the repeated computing overhead from the same input combinations,



(a)



(b)

Fig. 4. (a) The system overview, (b) Approximation decision flow.

by storing the computation result in a lookup table (LUT) and reuse the result from the LUT when possible. Therefore, it improves the performance and energy efficiency since the first computation overhead is much higher than to read the result value of the computation from the LUT in terms of speed and power. The efficiency of memoization highly depends on the frequency of redundant computations [8].

An overview of the proposed memoization-based image encryption system is illustrated in Fig. 4(a). It first examines the continuous input pixel blocks for whether memoization can be applied to them. If the block is determined not to be used in memoization, it just performs the normal AES encryption process. However, if the block is determined to be used for memoization, it then applies the approximation process to the blocks. Based on the approximated block, it checks if the encryption result from the block input is already stored in the LUT from the previous execution. If the previous result is saved in the LUT, it is used for the AES result

data directly without AES computation. If not, the normal AES encryption process is performed from the approximate input data, and the result is saved to the LUT for future reuse opportunities.

As the input size of the AES-128 algorithm is 128 bits and each image pixel is 32 bit-size RGBA format, every group of 4 neighboring image pixels should be packed into the 128 bit block. Therefore, the system continuously generates the AES-128 input blocks from the serial input image data stream.

Based on every AES-128 input block, the system determines whether the block can be used for memoization through approximation. The intermediate approximation step is required because the pixel data of the original image files generally cannot have exactly the same value even when they look similar to neighboring pixels, and therefore, the expected reuse rate from the original pixel data is extremely low.

In order to increase the reuse probability and minimize loss of image quality, we apply a smart approximation process to the AES-128 block as shown in Fig. 4(b). In this process, as higher-order bits are more important than lower-order bits for image quality, we decided to consider only 5 MSB bits of each 8 bit color segment of all pixel data inside an AES-128 block. We then compare the total 20 bits consisting of four 5 MSB bits from RGBA color of four pixels inside an AES-128 block. If more than 2 pixel values are the same among 4 pixels, we decide to perform an approximation process to generate an Approximate Representative Pixel (ARP) from the major pixel and use the memoization process since four pixels in the AES-128 block are considered to be similar to each other. A more detailed explanation of the parameter selection process is shown in Section 3.2. An ARP consists of 20 MSB bits from the major pixel and 12 LSB bits with four 100 binary values as shown in Fig. 5, and an approximate AES-128 block is composed of the four ARPs as shown in Fig. 4(a).

The LUT for memoization is implemented similar to a typical cache structure, which is a 4 way set-associative cache (64 sets) with a pseudo LRU replacement policy [12]. Among 20 MSB bits of an ARP, 6 bits are used as an index, and the remaining 14 bits are used as the tag. More specifically, (4, 3) bits from Red and Green values and (3) bit from Blue and Alpha values are used to select a target set as indicated in Fig. 5. Each entry stores the

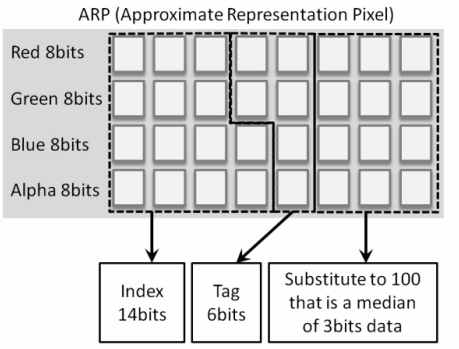


Fig. 5. An approximate representative pixel (ARP).

128-bit AES encryption data from the corresponding approximate AES-128 block.

When accessing the LUT with an approximate AES-128 block, a hit means that a saved result exists, and therefore the system stops the encryption process and brings the result directly from the LUT entry. However, if a miss happens, the system continues the encryption process and stores the result to the LUT entry for a future reuse opportunity.

2. Approximation Design Space Exploration

To find an optimal approximation-based memoization system, we try to maximize the reuse rate while retaining fair image quality by examining various types of system architectures. As discussed in Section 2.2, SSIM is used for image quality measurement rather than other simple metrics. This is because SSIM checks the visual similarity of two images similar to human visual systems, while other metrics simply calculate the image data value difference. In this paper, we decide that an original image and its approximate image are visually the same when the SSIM index value of them is higher than 0.95.

Two different design parameters are considered for design space exploration: the number of approximate LSB bits per image pixel, and the number of the same approximate pixels for approximate representative block selection. A detailed explanation of these two considering factors is as follows:

- Number of approximate LSB bits per image pixel: As the human eye cannot recognize the small difference between pixel values, several LSB bit values of RGBA format can be transformed to a pre-defined value. A large number of pre-defined bits

highly enhances the reuse rate of memoization as discussed so far. However, it should be chosen carefully because it may incur severe image quality loss.

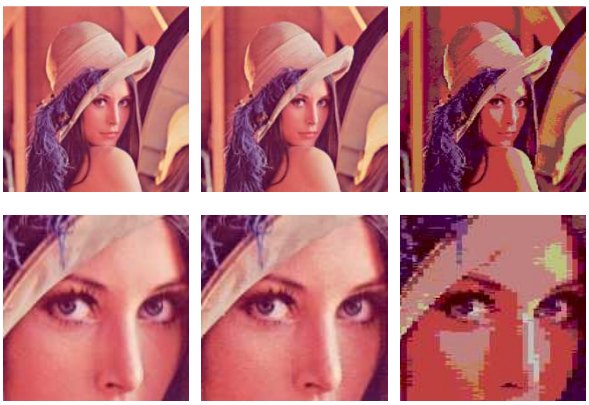
- Number of same approximate pixels for approximate representative block selection: As an approximate AES-128 block consists of four ARPs, the policy to choose the ARP is another important factor. If the ARP is chosen only when all the approximate pixels are the same, the image quality will be maintained but the reuse rate will be dramatically lower because approximation would not be applied at all for most cases. However, if the ARP is chosen from one of different approximate pixels, the reuse rate will be higher but the image quality will be degraded due to the different pixels inside the block.

Among different configurations, varying the number of pre-defined LSB bits from 0 to 6 and the minimum required number of same approximate pixels for ARP selection from 2 to 4, the system with ARP selection from the minimum two same pixels having 3 pre-defined LSB bits is selected to the optimal choice based on performance and image quality considerations. A detailed discussion is shown in section 4. Note that the pre-defined 3 LSB bit value is the median value (100) for each RGBA factor.

IV. Experimental Setup and Results

1. Experimental Setup

Architecture variations are first implemented in C for design space exploration, and the final design is written in RTL Verilog and synthesized with Altera Quartus Prime 16.0. Quartus is also used to measure logic utilization and performance simulation. In order to measure power consumption, Powerplay Power Analyzer is used by including a vcd file from gate level simulation. Altera Cyclone 5 5CSEMA5F31C6 [13] is used as the target FPGA device, and the evaluation is done on the Altera DE1-SoC board [13]. Four 512x512 size color images of Lena, Mandrill, Peppers, and Parrots are selected as test images from various widely used images in image processing research [9].



(a) (b) (c)

Fig. 6. Comparison of images with different level of approximation (a) Original image, (b) 3 bits (SSIM: 0.993), (c) 6 bits (SSIM: 0.825).

In this section, we first show the image quality difference by varying the approximation level of an example image. We then choose an optimal approximation configuration and LUT structure based on the SSIM index and the reuse rate. Finally, we compare logic utilization, performance, and energy efficiency of the proposed system and the baseline.

2. Experimental Results

Fig. 6 shows the image quality comparison of images generated from different levels of approximation from the original Lena image [9]. Fig. 6(a) is the original image, and Fig. 6(b) is the decrypted image of encrypted data generated from the proposed approximate memoization system using ARP generation with minimum 2 same 3 LSB bit approximate pixels. As shown in Fig. 6(b), the image does not show perceivable image degradation and the SSIM index is 0.993, which is higher than the minimum acceptable SSIM index (0.95).

However, the Fig. 6(c) image, from the system using ARP with minimum 2 same 6 LSB bit approximate pixels, shows high perceivable image degradation, and the SSIM index is lower than 0.95, as expected.

To determine the effects of differing architectural features, the measurements for SSIM index and ideal reuse rate (100% hit rate), were obtained as shown in Fig. 7 and 8. The X-axis on the graphs shows the width of pre-defined LSB bits, and the Y-axis shows the SSIM index and the reuse rate. Three different minimum

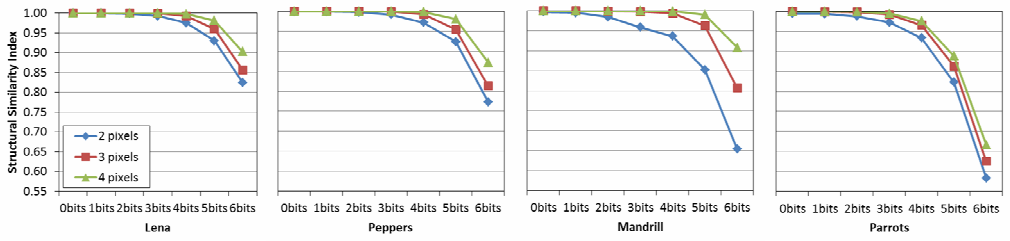


Fig. 7. SSIM comparison for different approximation levels.

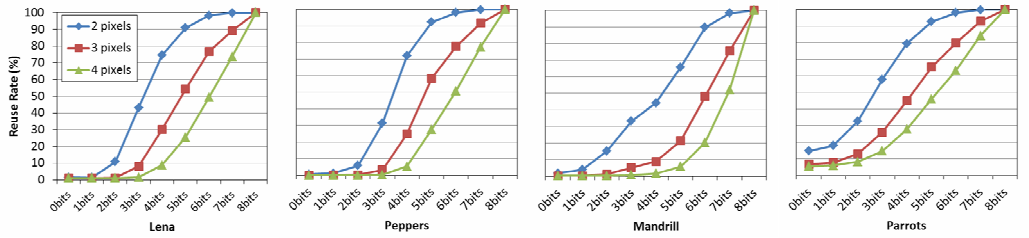


Fig. 8. Reuse rate comparison for different approximation levels.

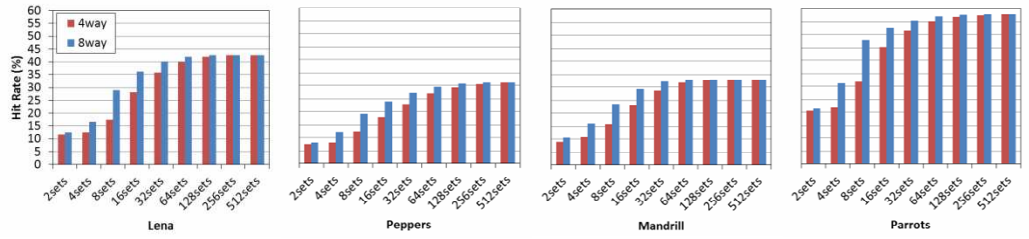


Fig. 9. Hit rate comparison for LUTs with different number of sets and ways.

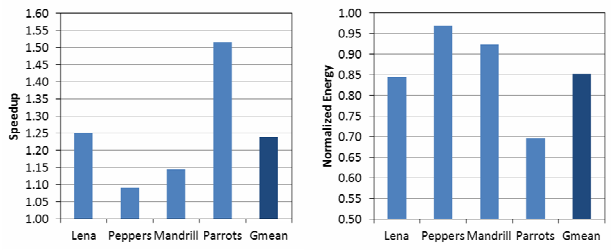
numbers of the same approximate pixels for ARP selection were considered from 2 to 4. Based on these sets of graphs, we decided on the optimal architecture with these two guidelines: 1) the SSIM index must be higher than the minimum value of 0.95, and 2) an architecture with the highest reuse rate will be selected among the qualified ones. Based on Fig. 7, architectures with up to 3 LSB bits for 2 pixels and up to 4 LSB bits for other pixels are able to successfully maintain the image quality within the SSIM index requirement. The architecture with ARP selection from the minimum two same pixels having 3 pre-defined LSB bits was selected as the final choice among these qualified variations due to the highest reuse rate (Fig. 8).

Fig. 9 shows the LUT hit rates for 4-way and 8-way associativity with increasing number of sets from 2 to 512. The hit rates highly increase initially but saturated at some point. As the hit rate saturated at 32-64 sets, a 4 way structure with 64 sets was chosen to be the final design compared to an 8 way structure with 32 sets since higher associativity usually incurs more power consumption.

Table 2. Comparison of the proposed and baseline architectures.

	Proposed Design	Baseline AES
Device	CycloneV 5CSEMA5F31C6	CycloneV 5CSEMA5F31C6
Target frequency (MHz)	100	100
Logic utilization (in ALMs)	1,503 / 32,070 (5%)	1,118 / 32,070 (3%)
Total registers	866	576
Total block memory (bits)	36,800 / 4,065,280 (<1%)	0 / 4,065,280 (0%)

Table 2 shows the implementation details when synthesizing the proposed and baseline architectures for the target FPGA device. Based on the table, the approximation based memoization system requires more logic gates and memory elements due to the additional



(a) (b)

Fig. 10. Performance of the proposed design over the baseline (a) Speedup, (b) Normalized energy consumption.

approximation control logic and the LUT structure. We also measured the performance and the total energy consumption for running image encryption of four reference images to determine the effectiveness of our design. Fig. 10 shows that the proposed design achieves 23.98% Speedup and 14.88% Energy savings on average over the baseline design.

V. Related Work

Previous work has improved AES performance using parallelization [3] or subpipelining [7]. However, these studies show fair performance improvement but suffer from low energy efficiency since parallelization requires multicore processors and subpipelining requires additional feedback structure. A recent work [1] on GPUs proposes to apply memoization by removing massive redundant computations for graphical applications but is orthogonal to our research because it is not relevant to data encryption and approximate computing. Approximate computing is now introduced to image processing as shown in [11] but most works use simple image metrics such as mean square errors without consideration of human perception. In order to solve this, the SSIM metric is introduced as an image quality assessment (IQA) to consider human perception [6].

VI. Conclusion

As the image resolution standard has become higher, design of an efficient image encryption system has become the most important challenge for image transfer systems. In this paper, we propose to introduce a hardware memoization technique with approximation to the baseline image encryption system. With extensive design space exploration, our system offers 23.98% higher geo-mean performance and 14.88% lower energy consumption than the baseline encryption system with minimum image quality loss based on human perception.

Acknowledgments

This work was supported in part by the National Research Foundation of Korea (NRF) grants funded by the Korea government (MSIP) (No. NRF-2015R1C1A1A01053844 and No.NRF-2015K2A1A2070541). This work (Grants No. C0409630) was also supported in part by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2016.

References

[1] Jose-Maria Arnau, et al, “Eliminating Redundant Fragment Shader Executions on a Mobile GPU via Hardware Memoization,” *ISCA (2014)*

[2] Adnaan Ahmed, et al, “Image Steganography By Closest Pixel-pair Mapping,” *ICACCI (2014)*

[3] Akshay Desai, et al, “Parallelization of AES algorithm for disk encryption using CBC and ICBC modes,” *ICCCNT (2013)*

[4] J. Daemen et al, “AES Proposal: Rijndael, ”

[5] Marta Mrak, et al, “Picture Quality Measures in Image Compression Systems,” *EUROCON (2003)*

[6] Zhou Wang, et al, “Image Quality Assessment: From Error Visibility to Structural Similarity,” *IEEE trans. on image processing. 13 (2004)*

[7] Xinmiao Zhang and Keshab K. Parhi, “High-Speed VLSI Architectures for the AES Algorithm,” *IEEE trans. VLSI 12 (2004)*

[8] Carlos Alvarez, et al, “Fuzzy Memoization for Floating-Point Multimedia Applications,” *IEEE trans. on computers 54 (2005)*

[9] USC-SIPI Image Database: http://sipi.usc.edu/database/.

[10] Ebru Celikel, et al, “Parallel Performance of DES in ECB Mode,” *IEEE international symposium on computer networks (2016)*

[11] Jie Han and Michael Orshansky, “Approximate Computing: An Emerging Paradigm For Energy-Efficient Design,” *IEEE ETS (2013)*

[12] Hassan Ghasemzadeh, et al, "Modified pseudo LRU replacement algorithm," *Engineering of Computer Based Systems (2006)*
[13] Altera DE1-SoC User Manual: https://www.altera.com/support/training/university/boards.html#de1-soc.

Seongmin Hong received the B.S degree in 2016 and is currently pursuing the M.S degree in the Department of Electronic and Electronical Engineering from Hongik University. His research interests include digital integrated circuit and accelerators.

Jaehyung Im received the B.S degree and the M.S degree in the Department of Electronic and Electronical Engineering from Hongik University in 2015 and in 2017. His research interests include digital integrated circuit and accelerators.

SM Mazharul Islam received the B.Sc. degree in 2016 from Bangladesh University of Engineering & Technology and is currently pursuing the M.S degree in the Department of Electronic Engineering from Hongik University. His research interests include digital image processing and machine learning.

Jaehee You received the B.S. degree in Electronics Engineering from Seoul National University, Seoul, Korea, in 1985, and the M.S. and Ph.D. degrees in Electrical Engineering from Cornell University, Ithaca, NY, in 1987 and 1990, respectively. In 1990, he joined Texas Instruments, Dallas, TX, as a Member of Technical Staff. In 1991, he joined the School of Electrical Engineering, Hongik University, Seoul, Korea, as a faculty member, where he is currently supervising the Semiconductor Integrated System Laboratory. His current research interests include integrated system design for display image signal processing, image-based home networking, and perceptual image quality enhancement systems.

Yongjun Park is currently an Assistant Professor in the Division of Computer Science and Engineering, Hanyang University, Seoul, Korea. His research interests include compilers and computer architectures for various computer systems. He has a Ph.D in electrical engineering from the University of Michigan, Ann Arbor, MI, USA (2013). He is a Member of the IEEE.