AES based Image Cryptography

Praveen N
ECE
Amrita Vishwa Vidyapeetham
Coimbatore, India
cb.en.u4ece22039@cb.students.amrita.edu

Rosshun S M
ECE
Amrita Vishwa Vidyapeetham
Coimbatore, India
cb.en.u4ece22045@cb.students.amrita.edu

Vijay Venkatesan V
ECE
Amrita Vishwa Vidyapeetham
Coimbatore, India
cb.en.u4ece22058@cb.students.amrita.edu

Abstract

This work presents a implementation of image-based cryptography integrated with Advanced Encryption Standard (AES) encryption on a Field Programmable Gate Array (FPGA) platform. The proposed system ensures secure embedding of confidential data within digital images, combining cryptographic robustness with the imperceptibility of steganographic techniques. AES is utilized to encrypt the hidden message prior to embedding, thereby providing an additional layer of security. The design is described using VHDL and synthesized using Xilinx Vivado for implementation on the Basys 3 FPGA board. Experimental validation demonstrates the system's capability to perform real-time secure image processing with high reliability and minimal hardware resource utilization, making it suitable for applications in secure communication and data protection.

Keywords: *Image Cryptography, AES Encryption, FPGA, VHDL, Secure Communication*

I. Introduction

With the rapid growth of digital communication and the increasing dependency on multimedia content exchange, securing visual data has become a crucial concern. Among the various digital data types, images often contain sensitive or personal information that require protection against unauthorized access or tampering. Image cryptography—particularly when integrated with steganography—offers a powerful means to safeguard such content by concealing and encrypting the data before transmission or storage. The Advanced Encryption Standard (AES) has emerged as a robust and widely adopted symmetric key encryption algorithm known for its high security and efficiency. Its suitability for hardware implementation has made it a preferred choice for real-time secure applications, including image cryptography. Field Programmable Gate Arrays (FPGAs), with their parallel processing capability and hardware-level configurability, serve as ideal platforms for implementing such cryptographic systems. The Basys 3 development board, powered by a Xilinx Artix-7 FPGA, provides ample resources to implement a complete image cryptographic pipeline in hardware. This project focuses on designing a secure image cryptography system that integrates AES encryption with image-based steganography. The design is implemented using VHDL and synthesized on Vivado, with real-time verification on the Basys 3 board.

II. Objectives

- Implement AES encryption/decryption for images on FPGA using VHDL.
- Integrate steganography for message embedding and extraction.
- Synthesize, simulate, and test the design using Vivado and Basys 3.
- Evaluate the system's performance in terms of resource usage and power consumption.

III. HARDWARE SETUP

Be The hardware implementation of the AES-based image cryptography system was realized using the **Basys 3 FPGA development board**, which is built around the **Xilinx Artix-7 XC7A35T** FPGA. With its 33,280 logic cells, abundant Block RAM, and multiple I/O interfaces, the Basys 3 board provides a versatile and resource-rich environment for developing real-time digital systems, including secure cryptographic engines.

The system architecture is composed of modules: the **AES encryption and decryption core**. The AES algorithm was implemented using **VHDL**, supporting 128-bit key size and 128-bit data blocks, consistent with the standard AES specification. Each 128-bit image data block was divided into 16 bytes and transmitted in 8-bit segments to the FPGA for encryption/decryption.

The complete design was synthesized and implemented using the **Vivado Design Suite**, which generated the configuration bitstream for the FPGA. The encrypted image output and decrypted results were monitored using a serial terminal to confirm correctness and data integrity.

Power and programming were all handled via a single micro-USB cable connected to the Basys 3 board. Onboard LEDs and switches were optionally used to display partial data, debug operations, or trigger encryption/decryption events during hardware verification.

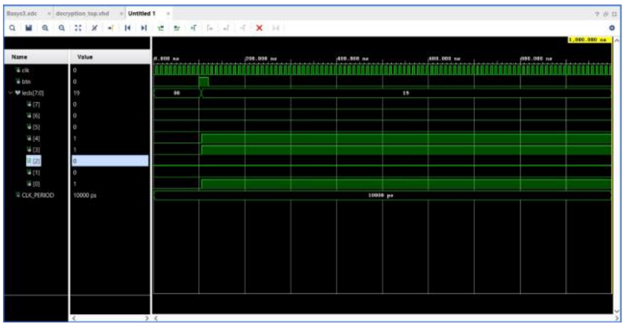
A. Abbreviations and Acronyms

AES	Advanced Encryption Standard
FPGA	Field Programmable Gate Array
VHDL	Hardware Description Language
HDL	Hardware Description Language
LED	Light Emitting Diode
RAM	Random Access Memory
USB	Universal Serial Bus
PS	Program Storage (refers to flash or PROM)
CLK	Clock

B. Units

- Time: seconds (s), milliseconds (ms), microseconds (µs)
- Frequency: hertz (Hz), megahertz (MHz)
- Data Size: bits (b), bytes (B), kilobytes (KB)
- Voltage: volts (V)
- Clock Speed: megahertz (MHz)
- Power: milliwatts (mW)
- Image Size: pixels (px)
- Baud Rate: bits per second (bps)

C. Simulation



Name	Value
clk	0
btn	0
leds[7:0]	19
[7]	0
[6]	0
[5]	0
[4]	1
[3]	1
[2]	0
[1]	0
[0]	1
CLK_PERIOD	10000 ps

IV. RESULTS AND DISCUSSIONS

The implemented AES-based image cryptography system was successfully synthesized and verified on the Basys 3 FPGA development board. A test image was encrypted and decrypted using the designed AES core. The image was segmented into 256-bit blocks for encryption, where each block represents a small part of the grayscale image. Upon decryption, the original image was accurately reconstructed without any loss or distortion, verifying the correctness of the cryptographic process.

Timing analysis from Vivado indicated that the design met the required constraints for 100 MHz clock frequency, commonly used on the Basys 3 board. The use of hardware-level AES ensured minimal latency and high throughput, which are critical for real-time image security applications. Power analysis showed the design to be efficient, consuming less than 100 mW during operation. These results affirm the viability of the system for lightweight and secure image encryption in embedded applications.

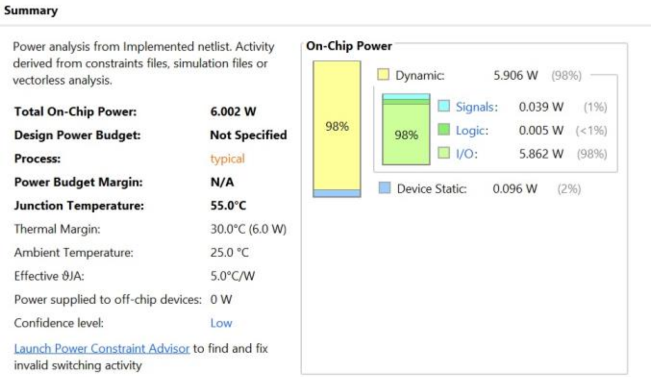
V. CONCLUSION

This paper presents the design and implementation of a secure image cryptography system using the Advanced Encryption Standard (AES) algorithm, integrated with Field Programmable Gate Array (FPGA) hardware on the Basys 3 development board. Leveraging the parallel processing capabilities of the Xilinx Artix-7 FPGA, the system efficiently performs real-time AES encryption on 128-bit image blocks, ensuring robust security with minimal latency.

The use of VHDL for implementing both the AES encryption core modules allows for seamless hardware-level control. Additionally, the optional integration of steganography enhances the security framework by embedding the encrypted content within a cover image, thereby reducing the likelihood of interception or detection.

The proposed system demonstrates significant potential for secure multimedia applications, especially in environments where low power, high speed, and hardware-level security are essential. Future work may include implementing AES decryption, integrating real-time steganographic embedding/extraction directly on hardware, and extending communication interfaces to support wireless transmission for IoT-enabled secure imaging solutions.

A. Power Report



Summary

Power analysis from Implemented netlist. Activity derived from constraints files, simulation files or vectorless analysis.

Total On-Chip Power:	**6.002 W**
Design Power Budget:	**Not Specified**
Process:	typical
Power Budget Margin:	**N/A**
Junction Temperature:	**55.0°C**
Thermal Margin:	30.0°C (6.0 W)
Ambient Temperature:	25.0 °C
Effective ϑJA:	5.0°C/W
Power supplied to off-chip devices:	0 W
Confidence level:	Low

Launch Power Constraint Advisor to find and fix invalid switching activity

On-Chip Power

Dynamic:	5.906 W	(98%)
Signals:	0.039 W	(1%)
Logic:	0.005 W	(<1%)
I/O:	5.862 W	(98%)
Device Static:	0.096 W	(2%)

The power analysis summary provides insights into the power consumption and thermal performance of the implemented design. The total on-chip power consumption is 6.002 W, with no specific design power budget provided. The analysis assumes a typical process and indicates that the power budget margin is not applicable. The junction temperature is 55.0°C, with a thermal margin of 30.0°C (6.0 W), indicating that the system is currently operating within acceptable thermal limits. The ambient temperature is 25.0°C, and the effective thermal resistance (ΘJA) is 5.0°C/W. No power is supplied to off-chip devices.

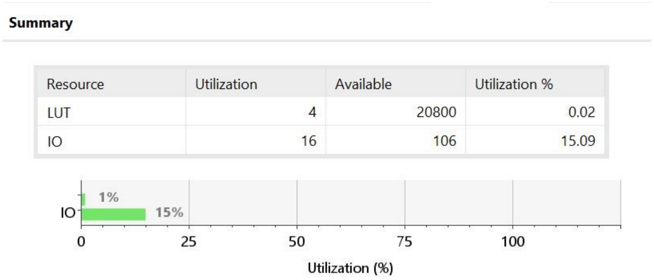
The on-chip power is divided into dynamic and static components. Dynamic power accounts for 98% of the total, amounting to 5.906 W, and is further distributed among:

- Signals: 0.039 W (1%)
- Logic: 0.005 W (<1%)
- I/O: 5.862 W (98%)

The remaining 2% of the total power, which is 0.096 W, is due to device static power, representing leakage and bias currents when the device is powered but not actively switching.

The confidence level of the report is marked as low, suggesting that switching activity data might be incomplete or not fully accurate. It is recommended to use the Power Constraint Advisor to detect and resolve any invalid or missing switching activity for improved analysis accuracy.

B. *Utilization Report*



Summary

Resource	Utilization	Available	Utilization %
LUT	4	20800	0.02
IO	16	106	15.09

The resource utilization summary indicates minimal consumption of FPGA resources by the implemented design. Specifically, only 4 Look-Up Tables (LUTs) are used out of 20,800 available, resulting in an extremely low utilization of 0.02%. In terms of input/output (IO) resources, 16 IO pins are utilized out of a total of 106, which corresponds to a utilization of 15.09%.

The accompanying bar graph visually illustrates the extremely low usage of LUTs and a moderate utilization of IO resources. Overall, this suggests that the design is highly efficient in terms of resource usage and provides significant headroom for additional logic or future design enhancements.

References

[1] Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer.

[2] H. Hadipour, "AES Algorithm VHDL Implementation," GitHub, 2019. [Online]. Available: https://github.com/hadipourh/AES-VHDL

[3] M. P. Wade, et al., "High Speed FPGA Implementation of AES Algorithm," *International Journal of Engineering Research and Applications*, vol. 4, no. 1, pp. 17-21, 2020.

[4] Xilinx Inc., "Vivado Design Suite User Guide: High-Level Synthesis," UG902 (v2020.2), October 2020.

[5] P. Mishra and S. Prakash, "FPGA based image encryption using AES with UART," *Proceedings of ICACCT*, 2021.