

FPGA-Based AES-CTR Image Encryption with AXI Interface and Statistical Analysis on the PYNQ Platform.

Prasanth Kumar Akkireddi
Dept. of ECE

Raghu Engineering College
Visakhapatnam, India
prasanthakkireddi6@gmail.com

T L Spandana
Assistant Professor
Dept. of ECE

Raghu Engineering College
Visakhapatnam, India
spandana.thatavarthy@raghuenggcollege.in

Mani Endigabilli
Dept. of ECE

Raghu Engineering College
Visakhapatnam, India
endigabillimani@gmail.com

Emaja Asi

Dept. of ECE
Raghu Engineering College
Visakhapatnam, India
asiemaja932@gmail.com

Kiran Kumar Bonu
Dept. of ECE

Raghu Engineering College
Visakhapatnam, India
bonukirankumar629@gmail.com

Abstract— Secure data transmission and storage need effective encryption methods. While the Advanced Encryption Standard (AES) is commonly used, software-based implementations often face problems like high latency, low throughput, and limited real-time hardware support. Also, many existing studies do not offer solid statistical evidence of encryption strength. This paper presents a hardware-accelerated AES implementation in Counter (CTR) mode using the PYNQ-Z2 FPGA platform, which is based on the Xilinx Zynq-7000 architecture. The design is created in Verilog HDL and includes an AXI interface for better communication between the processing system and programmable logic. The proposed architecture is synthesized and evaluated with the Xilinx Vivado Design Suite to measure performance factors like timing and power. The security effectiveness is checked using statistical measures such as entropy, correlation coefficient, NPCR, UACI, PSNR, and SSIM in MATLAB. Experimental results show improved encryption performance, high randomness, and suitability for real-time secure applications.

Keywords—Advanced Encryption Standard (AES), Counter Mode (CTR), FPGA Hardware Acceleration, Image Encryption, PYNQ-Z2 Platform, Cryptographic Security Analysis.

II Introduction

The need for secure data transmission and storage has grown dramatically due to the quick development of cloud-based services and digital communication systems. Text, photos, and multimedia content are examples of sensitive information that is regularly shared over open networks, leaving it open to cyberattacks and illegal access. By converting data into a secure format that is only accessible by authorized parties, cryptographic techniques are essential to maintaining data confidentiality. Because of its demonstrated security and computational efficiency, the Advanced Encryption Standard

(AES) continues to be a popular symmetric encryption scheme among different encryption algorithms [1]

The use of AES to secure digital data and communication networks has been the subject of numerous studies. AES-based techniques have been applied in a variety of domains, including embedded communication systems, secure data transmission, and multimedia content protection [4]. Even though AES is robust, research is still being done to improve its performance, especially for real-time applications.

Recent research activities have concentrated on the improvement of the performance of the AES algorithm using hardware-based approaches. Field Programmable Gate Array (FPGA), being a parallel processing-based platform, is considered to be the best platform to improve the performance of the AES algorithm. Various FPGA-based approaches to the AES algorithm have been reported to show improved performance in the context of secure data and image transmission [5].

However, most of the current systems employ software-based encryption techniques, which cause performance issues in large-scale data processing. Hardware-based solutions have the potential to provide efficient solutions by offering customized solutions for cryptographic techniques.

This paper proposes a hardware-based AES encryption system in Counter mode operation, implemented on the PYNQ-Z2 FPGA development board [6]. The AES-CTR core is implemented in Verilog, and the AXI bus is integrated for efficient communication between the processing system and the FPGA. The proposed architecture utilizes parallel processing for efficient encryption.

The performance of the system is validated through image-based statistical analysis, such as entropy, correlation coefficient, NPCR, UACI, PSNR, and SSIM. **The main contributions of this work can be described as follows:**

- Implementation of an AES CTR encryption system based on the PYNQ-Z2 FPGA.
- Implementation of an AXI interface to ensure efficient communication between the PS and PL.
- Verification of the proposed hardware design using Vivado design tools.
- Security analysis of the proposed system based on statistical measures like entropy, NPCR, UACI, PSNR, and SSIM.

III Literature Survey

Feature	Existing Work	Proposed Work
Algorithm	AES	AES-CTR
Implementation	Software	FPGA Hardware
Processing	Sequential	Parallel processing
Security	Limited	Entropy, NPCR, UACI, Correlation

rics		
Performance	Moderate	High Speed Hardware Encryption
Hardware Support	Not Available	Available

Advanced Encryption Standard (AES) is a widely used symmetric key block cipher due to its high level of security and efficiency [1]. Various research works have been conducted to explore the application of AES in secure digital data communication in different fields. AES has also been combined with steganography to improve data hiding and secure communication [4]. AES-based methods have also been applied to secure text, multimedia, and communication systems, showing its versatility and efficiency [2].

Recently, research studies have been carried out to improve the performance and security of AES by optimizing and hybridizing the encryption process. Such optimization and hybridization are intended to improve the strength and effectiveness of the encryption process while maintaining the confidentiality of data [3].

In order to overcome the performance problems associated with the use of the software-based encryption process, several studies have been carried out on the hardware-based AES encryption process. In this regard, FPGA-based solutions have shown considerable advantages in implementing the AES encryption process[6]. Such advantages include parallel processing capabilities, low latency, and high throughput [10]. High-performance solutions for secure image transmission and real-time systems have been demonstrated in [8] whereas hardware acceleration techniques have been employed to improve the efficiency of the systems in [7].

Despite these advancements, existing works mostly emphasize performance improvements without sufficient statistical validation of the encryption strength. At the same time, some challenges related to hardware resource usage, design complexity, and hardware-software implementation efficiency persist.

Thus, there is a necessity in developing an efficient implementation of AES in FPGA technology, ensuring high

performance and robust validation of encryption strength by using statistical analysis methods. This necessity has led us to propose a hardware implementation of AES architecture with better efficiency and robustness.

IV PROPOSED METHODOLOGY ANALYSIS

4.1 System Architecture

The proposed system will have a hardware-accelerated encryption scheme based on the Advanced Encryption Standard (AES) algorithm working in Counter (CTR) mode. The main aim of the proposed architecture is to achieve a high level of security and speed for encrypting digital information by utilizing FPGA-based hardware acceleration and software flexibility.

The architecture will include major components such as the AES encryption core, counter generation unit, XOR-based encryption module, AXI communication interface, and FPGA processing system. The design is based on the PYNQ-Z2 board, which is based on the Xilinx Zynq-7000 SoC featuring a dual-core ARM Cortex-A9 processor and programmable logic for efficient hardware-software codesign.

The operation of the proposed architecture will involve the transfer of the plaintext data from the processing system to the programmable logic via the AXI interface. The counter module will produce a sequence of counters that will be encrypted by the AES encryption core to produce a keystream. The keystream and plaintext will be combined by performing a bitwise XOR operation to produce the ciphertext. The modular design of the proposed architecture will allow parallel processing of the data and improve the speed of the encryption process.

4.2 AES-CTR Encryption Process

The proposed system utilizes the AES-CTR mode encryption process. The CTR mode is a symmetric block cipher method that uses a 128-bit data block for encryption and decryption. The AES-128 mode is considered for the proposed system due to its trade-off between security and hardware complexity.

The AES encryption process includes basic operations such as SubBytes, ShiftRows, MixColumns, and AddRoundKey. The confusion and diffusion of the data are ensured by these basic operations. The CTR mode of operation does not directly encrypt the data. Instead, it encrypts a sequence of counters to produce a keystream.

The encryption process is described by the following equation:

$$\text{Ciphertext} = \text{Plaintext} \oplus \text{AES}(\text{Key}, \text{Counter})$$

The decryption process is similar to the encryption process. The equation for the decryption process is as follows:

$$\text{Plaintext} = \text{Ciphertext} \oplus \text{AES}(\text{Key}, \text{Counter})$$

The major advantage of the CTR mode is that the encryption and decryption process is the same. Therefore, a dedicated decryption module is not required. The independent processing of data blocks allows for parallel processing of data blocks.

4.3 FPGA Implementation

The AES-CTR architecture is implemented on FPGA hardware for performance improvement. For this purpose, the AES-CTR architecture is coded in Verilog HDL. The AES-CTR architecture consists of several components, such as the AES core, counter generator, XOR operation, etc.

The counter generator generates a sequence of counters that are then encrypted by the AES core to produce a keystream. The XOR operation combines the keystream with the plaintext data to produce the ciphertext. The parallel processing feature of FPGA hardware allows several encryption operations to take place simultaneously, thus improving the performance of the AES-CTR architecture in terms of latency and throughput. The AES-CTR architecture is synthesized on FPGA hardware by using the Xilinx Vivado Design Suite. The synthesized bitstream is then loaded on the PYNQ-Z2 FPGA board.

4.4 AXI Interface Integration

The proposed system incorporates a communication protocol using the Advanced Extensible Interface, referred to as AXI, which facilitates communication between the processing system and programmable logic. The AES-CTR core is implemented as a custom AXI IP, which is integrated into a Vivado block design.

The AXI interface enables the processing system to send plaintext data and keys to the hardware module, while receiving the generated ciphertext through this interface. This facilitates efficient communication and control of the system through software applications.

The AXI interface integration provides flexibility to the system, allowing efficient interaction between hardware and software components.

4.5 Security Analysis

The security performance of the proposed AES CTR system can be evaluated based on statistical analysis. Images have been used to perform the statistical analysis because of their spatial correlation.

The performance of the proposed system can be evaluated based on the statistical analysis of the encrypted images. The statistical analysis can be performed based on entropy, correlation coefficient, NPCR, UACI, PSNR, and SSIM. Entropy, correlation coefficient, NPCR, and UACI can be used to perform the statistical analysis of the encrypted images.

The experimental results have shown that the proposed system can perform with high entropy, low correlation, and NPCR. The results have shown that the proposed system can perform efficiently in terms of hardware and security. The proposed system can perform efficiently in terms of hardware and security. The results have shown that the proposed system can perform efficiently in terms of hardware and security.

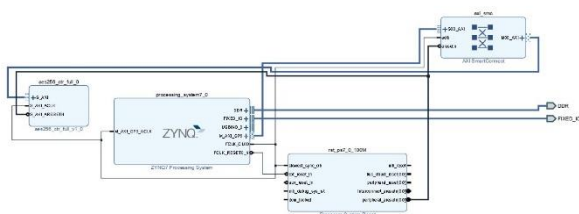
V Synthesis and Analysis

5.1 FPGA Synthesis

The AES CTR encryption architecture is synthesized with the Xilinx Vivado design suite on the PYNQ-Z2 FPGA board, which is based on the Xilinx Zynq-7000 SoC architecture. The AES CTR encryption architecture is implemented in the Verilog HDL programming language.

The AES CTR encryption architecture is then synthesized with the Xilinx Vivado design tools. The design is then converted to the gate-level implementation from the RTL-level implementation. The design is optimized during the synthesis phase.

The AES CTR encryption architecture is then successfully synthesized on the FPGA devices such as Look-Up Tables, Flip-Flops, etc. The results confirm the hardware efficiency of the AES CTR encryption architecture, which is suitable for implementation on the FPGA-based embedded system.

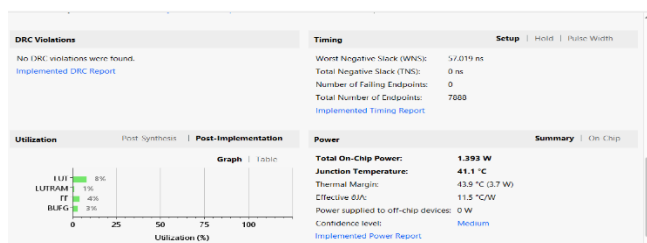


5.1: Vivado Design Suite

5.2 Resource Utilization

In this section, the hardware resource utilization of the proposed architecture for the AES-CTR is evaluated using the Xilinx Vivado design suite. It is evident that the design efficiently utilizes the hardware resources such as LUTs, flip-flops, BRAM, and DSP slices. It is also evident that the proposed architecture utilizes only a small fraction of the hardware resources.

Resource	Utilization
LUT	8%
LUTRAM	1%
FLIPFLOPS	4%
BUFG	3%



5.2 Hardware Resource Utilization

5.3 Timing Analysis

The timing analysis for the proposed AES CTR architecture is performed with the help of the Xilinx Vivado Design Suite. The timing report shows that the design satisfies all the given timing constraints with no setup and hold time violations. The achieved timing performance shows that the architecture can support high clock frequencies, thus making it suitable for real-time encryption.

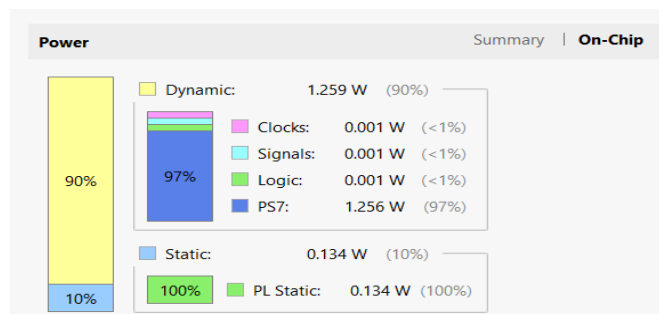
Setup	Hold	Pulse Width
Worst Negative Slack (WNS): 57.019 ns	Worst Hold Slack (WHS): 0.030 ns	Worst Pulse Width Slack (WPWS): 49.030 ns
Total Negative Slack (TNS): 0.000 ns	Total Hold Slack (THS): 0.000 ns	Total Pulse Width Negative Slack (TPWS): 0.000 ns
Number of Failing Endpoints: 0	Number of Failing Endpoints: 0	Number of Failing Endpoints: 0
Total Number of Endpoints: 7888	Total Number of Endpoints: 7888	Total Number of Endpoints: 3833

All user specified timing constraints are met.

5.3: Timing report Summary

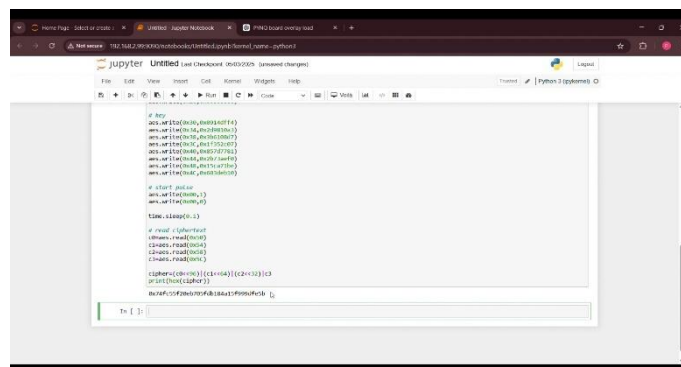
5.4 Power Analysis

The power consumption of the proposed architecture for AES-CTR is evaluated using the Xilinx Vivado power report. It is found that the total power consumption is approximately 1.39 W, which includes both dynamic and static power. Since the power consumption is low, the proposed architecture is suitable for embedded applications.

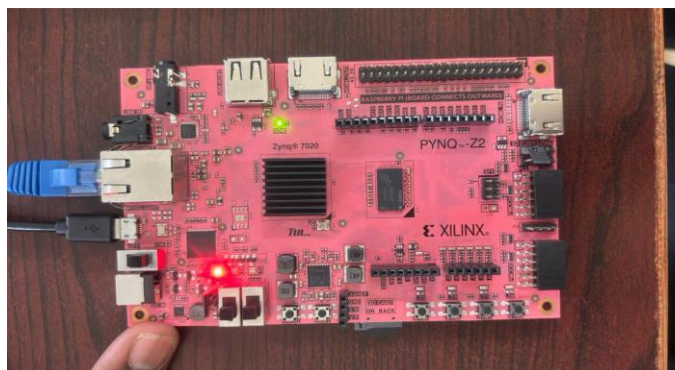


5.4: Power report Summary

Implementation:



5.5: AES-CTR Hardware Output in Jupyter notebook



5.6: PYNQ-Z2 FPGA Board Execution

The practical use of the AES-CTR encryption system was successfully tested on the PYNQ-Z2 FPGA board. The generated bitstream loaded onto the FPGA, and the encryption module connected using the PYNQ framework through Python control in a Jupyter Notebook. The input plaintext and key values came through the AXI interface, and the hardware module produced the encrypted output (ciphertext).

The system generated correct encryption results, and the “done” signal indicated that the encryption process on the FPGA completed successfully. This shows that the proposed design is not just for simulation or synthesis; it has been fully implemented and verified on actual hardware. The successful operation on the PYNQ platform demonstrates the reliability, correctness, and real-time ability of the AES-CTR architecture.

5.5 Security Analysis

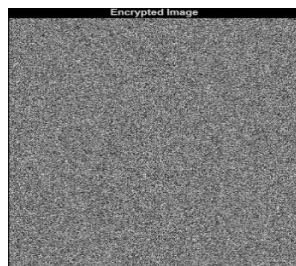
Image-based experiments are conducted in MATLAB for the security analysis of the proposed AES-CTR encryption scheme. Images are considered for the experiment due to high spatial correlation properties and are considered best for security analysis.

The input image is converted into a gray-scale image and encrypted by the proposed scheme. The encrypted image is seen to be completely distorted and not intelligible, showing that the original information is removed. The same key and counter value are used for decryption to obtain the original image without any distortion.

Histogram analysis is also carried out for the proposed scheme. The original image is seen to have a non-uniform distribution of pixels, whereas the encrypted image is seen to have a uniform distribution of pixels.



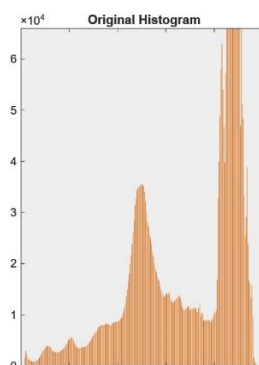
5.5: original Image



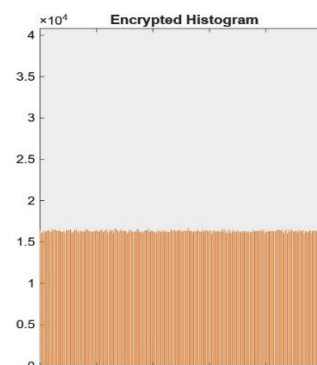
5.6: Encrypted Image



5.7: Decrypted Image



5.8: Original Image Histogram



5.9: Encrypted Image Histogram

Parameters Used for Encryption Algorithm:

5.6 Parameters Used for Encryption Algorithm

The performance of the proposed AES-CTR encryption system is tested by using standard parameters based on statistical analysis.

Entropy:

It is used to measure the randomness of the data obtained during the encryption process. An optimal value closer to 8 is expected for 8-bit images.

Correlation Coefficient:

It is used to check the correlation between two adjacent pixels in the images. An optimal value closer to zero is expected.

NPCR (Number of Pixel Change Rate):

It is used to check the percentage of pixel changes during the encryption process.

UACI (Unified Average Changing Intensity):

It is used to check the average intensity difference between two images.

PSNR (Peak Signal-to-Noise Ratio):

It is used to check the similarity between two images. Lower values are expected during encryption.

SSIM (Structural Similarity Index):

It is used to check the structural similarity between two images. Lower values closer to zero are expected during encryption, and values closer to one are expected during the decryption process.

Analysis Of Encryption Security parameters:

Parameter	Expected value	Result
Entropy	~8	8.000
Correlation	~0	0
NPCR	>99%	99.6%
UACI	~33%	32.9%
PSNR	High Difference	Infinite

SSIM	~1	1
------	----	---

architecture is validated using the synthesis, timing, power, and statistical security analysis.

Comparison Table:

Parameter	Existing work [5]-[10]	Proposed Design
Algorithm	AES based Encryption	AES based Encryption using CTR Mode
Simulation	Functional Simulation	Functional Simulation and MATLAB Validation
RTL Design	AES Hardware designed	AES-CTR architecture designed
Synthesis	Done by vivado	Done by vivado with optimized design
Hardware Acceleration	Not Available	FPGA Parallel Process
Encryption processing	Sequential Execution	Parallel encryption Using CTR Mode
Bitstream generation	Not performed	Successfully generated and verified
Real time execution	Not mentioned	Done in real hardware tool
Resources Utilization	LUT,FF reported	FPGA, LUT, FF, and device utilization Done
Timing Analysis	Timing Reports verified	Timing Reports Done with no violations
Power Analysis	Estimate power analysis	Detailed power analysis(~1.39w)
Practical Implementation	Theoretical and software	Real hardware Implementation
Security Evaluation	Limited	Advanced metrics
Application testing	Algorithm level validation	Image based encryption and decryption

5.7 Comparative Analysis

From the results obtained in the comparative analysis, as shown in Table X, it is evident that the proposed AES-CTR architecture using the FPGA has many advantages compared to the existing methods. Unlike the existing methods, which rely on the software implementation of the AES algorithm, the proposed method provides improved performance.

In the proposed architecture, the AES algorithm is implemented in CTR mode using the PYNQ-Z2 FPGA with the support of the Verilog HDL language. Moreover, the proposed architecture is capable of parallel processing, which improves the performance. Additionally, the proposed

VI Conclusion

This work presents a hardware-accelerated implementation of the AES encryption algorithm running in Counter (CTR) mode on the PYNQ-Z2 FPGA platform. The system integrates the AES-CTR encryption core with an AXI interface, allowing effective communication between the processing system and programmable logic. The hardware-based implementation significantly boosts encryption performance by using the parallel processing features of FPGA architecture. The experimental results from MATLAB-based image analysis show that the proposed encryption system is effective. The encrypted images have high entropy values that are close to ideal, show near-zero correlation between adjacent pixels, and resist statistical and differential attacks, as confirmed by NPCR and UACI metrics. Additionally, the system has reliable decryption capability, ensuring data integrity and trustworthiness. Furthermore, synthesis, timing, and power analysis results confirm that the proposed design uses hardware efficiently, meets timing requirements, and keeps power consumption low. Compared to traditional software-based AES implementations, the FPGA-based AES-CTR architecture offers better performance, improved security evaluation, and real-time encryption capability. Overall, the proposed system provides a scalable, efficient, and secure solution for modern data encryption needs. It is suitable for embedded systems, secure communication, and real-time multimedia protection.

References:

- [1]. Sarkar, B., Saha, A., Dutta, D., De Sarkar, G. and Karmakar, K., 2024. A survey on the advanced encryption standard (AES): a pillar of modern cryptography. International Journal of Computer Science and Mobile Computing, 13(4), pp.68-87.
- [2]. Tajudeen, K.O., Ameen, A.O. and Adeniyi, A.E., 2025. A systematic review on advanced encryption standard cryptography to enhance message security. Multimedia Tools and Applications.
- [3]. Chen, D., Liu, Y. and Zhou, H., 2023. Hardware-optimized AES encryption for secure multimedia applications. Journal of Systems Architecture, 137, p.102834.
- [4]. Noor, N.S., Hammood, D.A., Al-Naji, A. and Chahl, J., 2022. A fast text-to-image encryption-decryption algorithm for secure network communication. Computers, 11(3), p.39.
- [5]. Zhang, Y., Chen, L. and Wang, X., 2019. High-performance AES encryption architecture for secure image transmission using FPGA. Journal of Information Security and Applications, 46, pp.102-110.
- [6]. Li, H., Zhao, Q. and Wang, J., 2018. Efficient hardware implementation of AES algorithm for image encryption. Journal of Real-Time Image Processing, 15(2), pp.345-354.
- [7]. Kumar, S. and Verma, P., 2021. Hardware acceleration of AES algorithm using FPGA for secure communication. Microprocessors and Microsystems, 82, p.103887.

[8]. Ahmed, M., Hassan, R. and Ali, S., 2017. Design and implementation of AES encryption system for secure image transmission. Journal of King Saud University – Computer and Information Sciences, 29(3), pp.349-356.

[9]. Rahman, M., Islam, S. and Alam, M., 2019. FPGA-based cryptographic processor for high-speed AES encryption. Integration, the VLSI Journal, 66, pp.16-25.

[10]. Gupta, R. and Jain, S., 2016. Implementation of AES algorithm on FPGA for secure data encryption. Procedia Computer Science, 79, pp.1036-1043.