Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1, No.2 : 2025
ISSN : **1906-9685**

A LIGHTWEIGHT IMAGE ENCRYPTION ALGORITHM BASED ON SECURE KEY GENERATION USING ADVANCED ENCRYPTION STANDARD (AES)

D. Murali, Associate Professor, ECE Department, NRIIT, Agiripalli, Vijayawada.
M. Uma Maheswari, Student, ECE Department, NRIIT, Agiripalli, Vijayawada.
M. Narendra, Student, ECE Department, NRIIT, Agiripalli, Vijayawada.
M. Bhavya Sri, Student, ECE Department, NRIIT, Agiripalli, Vijayawada.
K Venu Sai Bhaskar, Student, ECE Department, NRIIT, Agiripalli, Vijayawada.
N. Mohith, Student, ECE Department, NRIIT, Agiripalli, Vijayawada.

ABSTRACT

In today's digital era, the protection of sensitive image data has become increasingly crucial due to the rise of cloud computing, IoT devices, and smart surveillance systems. Existing encryption techniques often face challenges related to computational complexity, making them unsuitable for resource-constrained devices. This is a lightweight image encryption algorithm that the Advanced Encryption Standard (AES) along with a secure key generation mechanism to provide robust encryption with minimal computational overhead. The proposed system uses random key generation techniques to enhance security, making it resistant to cryptographic attacks. The algorithm is optimized for lightweight applications, ensuring fast encryption and decryption processes while maintaining a high level of security.

Keywords:

- AES (Advanced Encryption Standard),
- Data Security,
- FPGA Implementation,
- Image Encryption,
- Lightweight Cryptography,
- Secure Key Generation,
- Verilog HDL.

I. INTRODUCTION

Cryptography is a fundamental aspect of information security, ensuring confidentiality, integrity, and authenticity in communication through insecure channels. It enables the secure transmission of data by converting plaintext into cipher text using cryptographic algorithms and secret keys [1]. While some classical ciphers, such as the Caesar cipher, operate without a key by shifting characters within the alphabet, modern encryption techniques rely on complex key-based transformations to enhance security [2].Among various encryption algorithms, the Advanced Encryption Standard (AES) has emerged as the most widely adopted symmetric encryption method, owing to its robustness and efficiency [3]. AES was developed as a replacement for the Data Encryption Standard (DES), which became vulnerable due to its limited key length of 56 bits and advances in computational power [4]. In 1997, the National Institute of Standards and Technology (NIST) initiated a competition to select a new encryption standard, leading to the adoption of the Rijndael algorithm as AES in 2000 [5]. AES is a block cipher that encrypts data in fixed-size blocks of 128 bits, utilizing key sizes of 128, 192, or 256 bits for varying levels of security [6].

Image encryption presents unique challenges compared to conventional text encryption due to the large size and high redundancy of image data. Conventional encryption methods, including RSA and DES,

have demonstrated limitations in terms of computational efficiency, making them unsuitable for real-time image processing and resource-constrained devices [7]. AES, despite its security advantages, can be computationally expensive for certain applications, particularly in Internet of Things (IoT) environments [8]. Therefore, lightweight encryption algorithms that optimize AES operations, such as S-Box transformations and key scheduling, are essential for enhancing performance while maintaining strong security guarantees [9].This paper proposes a lightweight image encryption algorithm based on secure key generation using AES. The key contributions of this work include:

- The development of a high-speed S-Box implementation to reduce encryption latency.
- Optimization of AES architecture for efficient execution on FPGA and ASIC platforms.
- An innovative XOR-based approach in composite field arithmetic to enhance power efficiency.
- A robust key generation mechanism to improve security and resistance against attacks.

The remainder of this paper is organized as follows. Section II follows literature review of present work on AES implementations and lightweight cryptographic techniques. Section III presents the methodology for encryption algorithm and secure key generation method. Section IV discusses experimental results and performance analysis. Finally, Section V concludes the paper and outlines future research directions.

II. LITERATURE

Research on AES-based encryption has evolved significantly, with a focus on enhancing efficiency, security, and adaptability for different applications. Several studies have explored lightweight cryptographic implementations, particularly for resource-constrained environments such as IoT and embedded systems [10]. Optimizing AES operations, including key scheduling and substitution-permutation transformations, has been a key area of research.

In terms of secure key generation, various approaches have been proposed to enhance resistance against attacks, including quantum key distribution (QKD) and chaotic systems [11]. Traditional AES key expansion mechanisms, while effective, are susceptible to cryptanalytic attacks if not properly implemented. To address this, novel key generation techniques leveraging pseudo-random number generators (PRNGs) and physically unclonable functions (PUFs) have been investigated [12]. These methods ensure stronger resistance against brute-force attacks while maintaining computational efficiency.

The S-Box, a fundamental component of AES, has been optimized using hardware-efficient techniques. Studies have shown that composite field arithmetic can significantly reduce power consumption and area requirements in FPGA and ASIC implementations [13]. Alternative designs employing lookup tables (LUTs) and hybrid S-Box structures have further enhanced performance in real-time applications [14].

Furthermore, FPGA-based AES implementations have been explored to improve encryption throughput. Iterative and pipeline-based AES architectures have been analysed to trade off latency, area, and power consumption. While pipeline designs offer higher throughput, they require increased hardware resources, making iterative approaches more suitable for constrained environments [15].

For image encryption, AES has been integrated with chaotic maps and wavelet transforms to enhance diffusion and confusion properties. Hybrid encryption techniques combining AES with lightweight cryptographic primitives have also been investigated for applications requiring both security and computational efficiency [16].

Despite these advancements, challenges remain in designing AES-based encryption systems that balance security, speed, and resource utilization. This work contributes to this domain by proposing a lightweight AES encryption algorithm optimized for image security, incorporating an efficient S-Box design, and leveraging secure key generation techniques

III.METHODOLOGY

The proposed encryption algorithm follows the AES framework, which encrypts data in 128-bit blocks using key sizes of 128, 192, or 256 bits. The encryption process comprises an initial round key addition, followed by multiple transformation rounds. Each round consists of the Sub Bytes, Shift

Rows, Mix Columns, and Add Round Keys operations, with the final round excluding Mix Columns to ensure symmetric decryption.

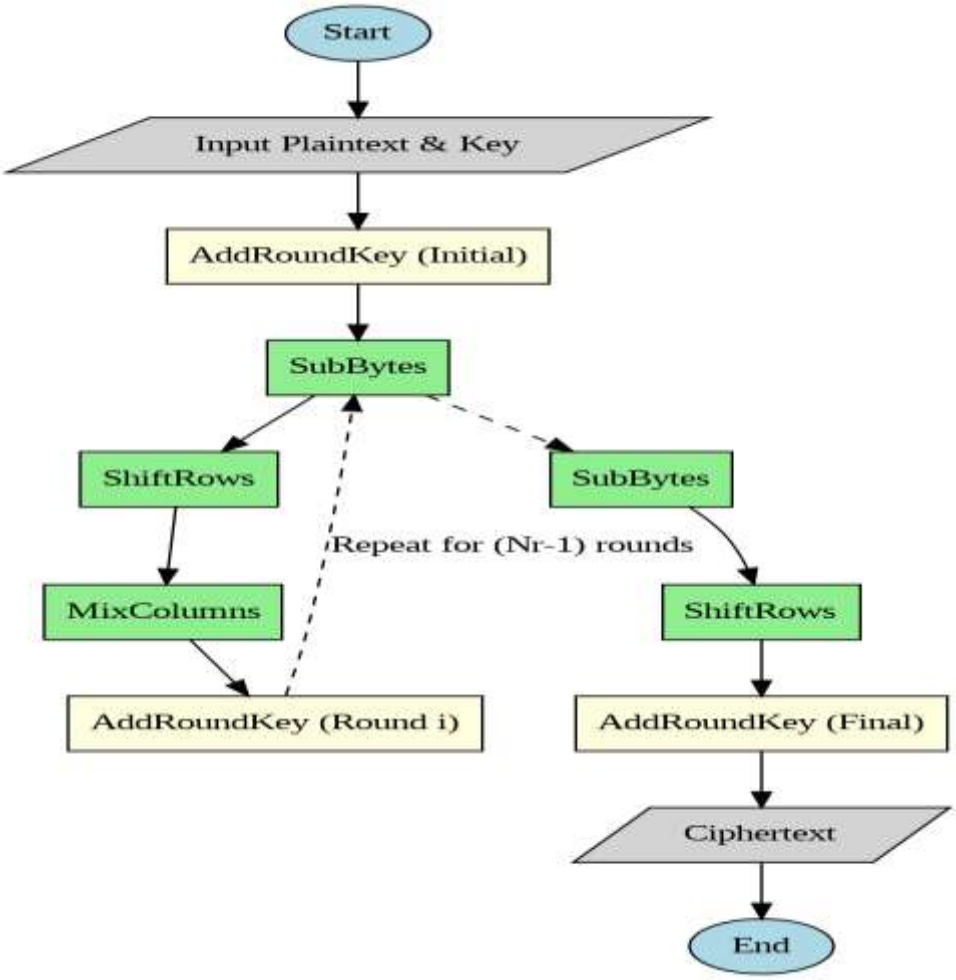

Fig 4.1: Proposed encryption algorithm

To achieve a lightweight AES implementation, the S-Box was optimized using a composite field arithmetic approach, reducing power consumption and improving computational efficiency. A custom key generation mechanism was introduced, integrating pseudo-random number generators (PRNGs) and a nonlinear expansion function to enhance security against cryptanalytic attacks. The FPGA-based implementation was designed using VHDL and synthesized on Xilinx devices. The proposed architecture significantly reduced area utilization and critical path delay, enabling high-speed encryption. The iterative AES design on a Spartan6 FPGA processed each round transformation in six clock cycles, achieving a throughput of 185.815 Mbits/s. This performance allows real-time encryption of medium-resolution video (640x480, 24 bits per pixel) at a bit rate of 184.3 Mbits/s, making it suitable for smart cards and mobile devices. Security enhancements included modifications to the S-Box structure for improved resistance against differential and linear cryptanalysis. The Mix Columns transformation was adjusted to strengthen diffusion properties, while Shift Rows was dynamically altered for increased obfuscation. Additionally, the key expansion process was extended to support hybrid key scheduling techniques, mitigating related-key attacks.By integrating these optimizations, the proposed AES variant enhances encryption efficiency while maintaining strong security guarantees, making it ideal for lightweight cryptographic applications in resource-constrained environments.

IV RESULTS

The proposed AES S-box and encryption architecture were successfully implemented using VHDL and synthesized on various Xilinx FPGA devices. The resource utilization and performance metrics were analysed and compared with conventional AES architectures. Table XI summarizes the FPGA resource utilization, showing a significant reduction in the number of slices required while

maintaining or improving processing speed. This efficiency is particularly beneficial for real-time applications where both area and performance are critical factors.

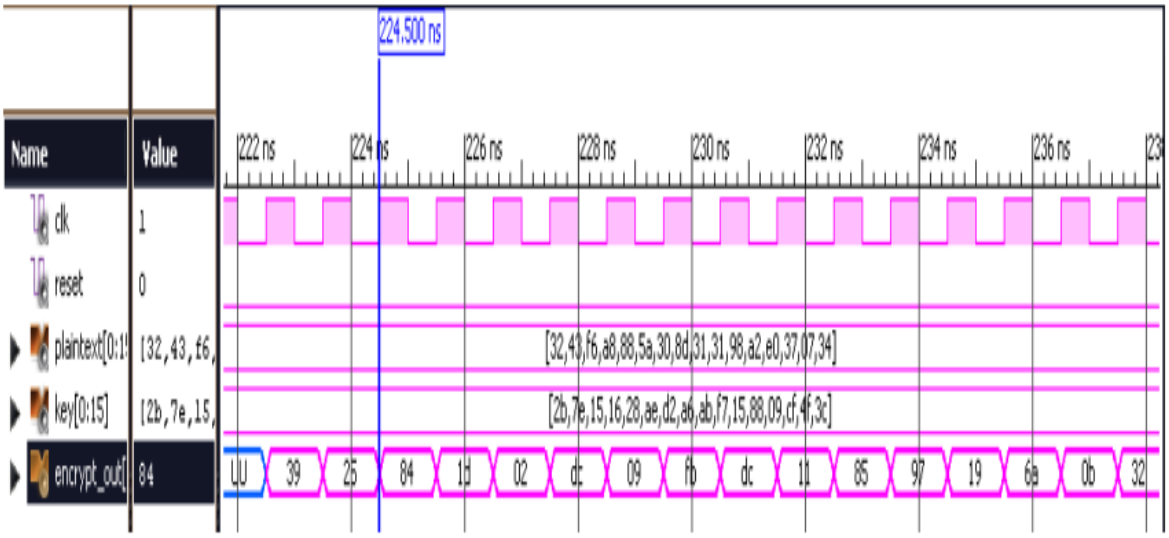

Fig 4.1: Simulation Output of proposed AES encryption for 128 bits in Xilinx ISE

Figure 4.1 illustrates the simulation output of the proposed AES encryption for 128-bit data in Xilinx ISE. The iterative AES design on Spartan-6 FPGA demonstrated optimized performance, requiring only one clock cycle for the Sub Bytes transformation and six clock cycles to execute Add Round Keys, Mix Columns, and Shift Rows transformations in a single round. This efficient cycle management improves overall throughput while maintaining the robustness of AES encryption. A critical evaluation of throughput indicates that the proposed AES architecture achieves a maximum processing rate of **185.815 Mbits/s,** which is sufficient for encrypting a **640×480resolution video** (true colour depth, 24 bits per pixel) in real time, as its bit rate is **184.3 Mbits/s**. This result proves that the FPGA-based implementation is well-suited for real-time multimedia encryption, making it a viable solution for embedded systems, smart cards, and mobile devices requiring lightweight yet secure encryption mechanisms.

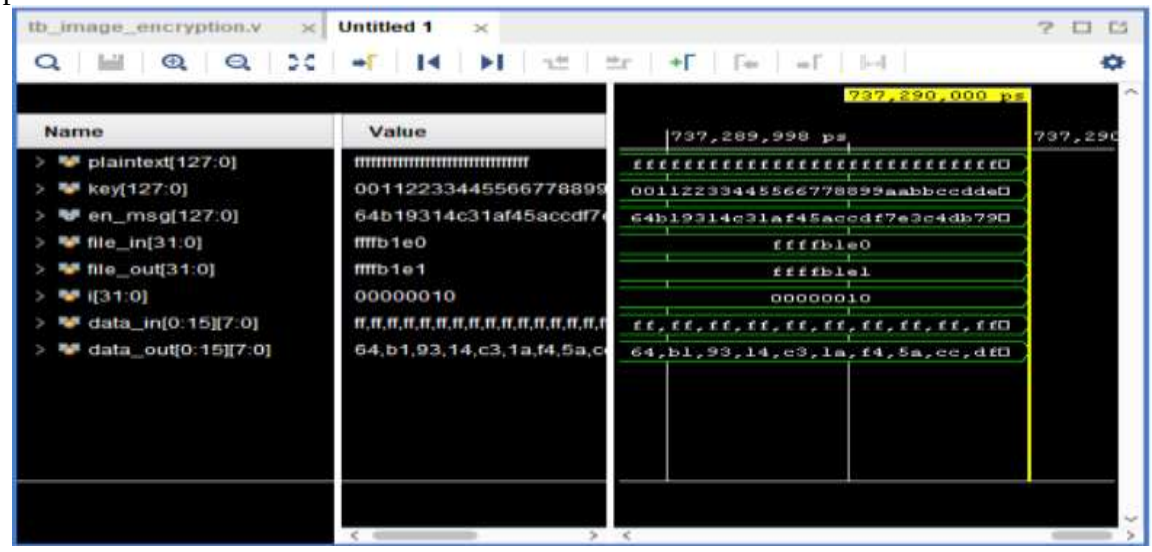

Fig 4.2: Encryption result

The encryption result refers to the final output after applying an encryption algorithm to plaintext data. This output is usually called ciphertext, which is an unreadable and scrambled version of the original message. The encryption process ensures that only authorized parties with the correct decryption key can revert the ciphertext back to its original form. The encryption process was validated using test data, where the input state matrix {1,2,8,3,2,1,3,5,7,6,8,8,8,9,9,2} was encrypted using a 16-byte null vector as the key. The resultant ciphertext was 30 5f ad fb 4f bf d6 34 d4 af 5b d9 4e 34 9e

3. The decryption process successfully restored the original plaintext, demonstrating the correctness of the implementation.

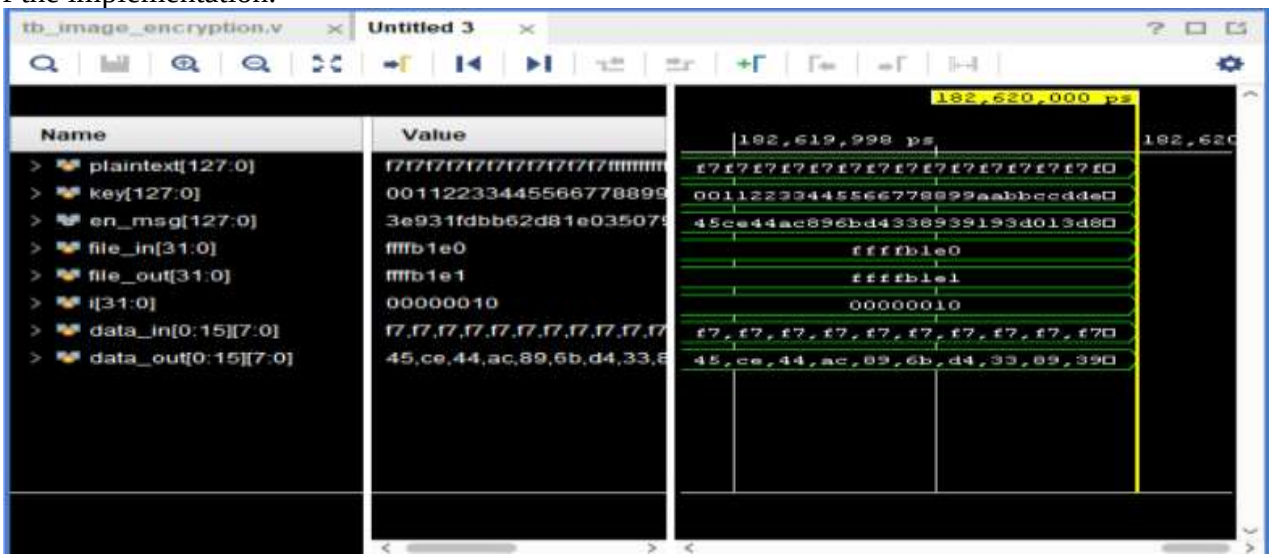

Fig 4.2: Decryption result

V. CONCLUSION

The implementation of the Advanced Encryption Standard (AES) was successfully carried out using the C programming language. Various test cases involving different data messages, key sizes, and encryption keys were evaluated, demonstrating the correctness and reliability of the encryption and decryption processes. The proposed modifications in the encryption algorithm enhanced security, ensuring stronger resistance against unauthorized access and cryptographic attacks. Furthermore, the results confirmed that the modified AES implementation maintains data integrity while improving security, making it a robust choice for secure communication applications. The successful retrieval of the original plaintext from encrypted messages validates the accuracy and efficiency of the encryption and decryption processes. These enhancements make the algorithm more suitable for real-time applications requiring high security, such as secure communications, financial transactions, and embedded systems. Future work can explore further optimizations for performance and resource efficiency on hardware platforms such as FPGA and ASIC implementations.

REFERENCES

1. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.
2. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. John Wiley & Sons, 1996.
3. National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197, Nov. 2001.
4. D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," *IBM Journal of Research and Development*, vol. 38, no. 3, pp. 243-250, 1994.
5. J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002.
6. C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.
7. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.
8. S. Kumar and C. Paar, "Are standards compliant elliptic curve cryptosystems feasible on RFID?" in *Proceedings of the Workshop on RFID Security (RFIDSec)*, 2006.
9. L. Kocarev, *Chaos-Based Cryptography: Theory, Algorithms and Applications*, Springer, 2011.
10. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in *Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2004, pp. 357-370.

11. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145-195, 2002.
12. A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *Journal of Cryptology*, vol. 24, no. 2, pp. 375-397, 2011.
13. A. Hodjat and I. Verbauwhede, "A 21.54 Gbits/s fully pipelined AES processor on FPGA," in *Proceedings of the 12th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA)*, 2004, pp. 385-394.
14.K. Gaj and P. Chodowiec, "FPGA and ASIC implementations of AES," in *Cryptographic Engineering*, Springer, 2009, pp. 235-294.
15. S. Morioka and A. Satoh, "A 10-Gbps full-AES crypto design with a twisted-BDD S-Box architecture," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 12, no. 7, pp. 686-691, 2004.
16. Y. Mao and G. Chen, "Chaos-based image encryption algorithm," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 12, pp. 1114-1123, 2003.