Application of the Advanced Encryption Standard for Image Processing and Performance Analysis

Prithwi Narayana Bhat M G[1],
[1]M-Tech student, VLSI Design and Embedded Systems, Bangalore Institute of Technology, Bengaluru, India.

Hemanth Kumar A R[2],
[2]Professor and HOD, Department of ECE, Bangalore Institute of Technology, Bengaluru, India.

ABSTRACT **-** Based on the analysis of multiple existing implementations in this study, we provide a balanced hardware design and implementation for AES here. One of the most popular cryptographic algorithms is AES, which has a key size that can be adjusted between 128 bits, 192 bits, and 256 bits with a data block size of 16 bytes. In the suggested design, the AES algorithm is implemented using Verilog and Xilinx Vivado 2018, which reduces operation time and the number of clock cycles required to encrypt and decode the message as compared to VHDL implementation. AES's larger key size confers greater secrecy than DES's.

Keywords: Xilinx Vivado 2018, Verilog HDL, AES.

1. INTRODUCTION

1.1 The National Institute of Standards and Technology (NIST) of the United States chose AES in 2001 to replace the outdated Data Encryption Standard (DES). The primary function of cryptography is data transport in applications like internet security. It has reliable safe communication and secure data transmission. A lot of security concerns, like data privacy on unsecured networks, arise with wireless communication. It has become an essential technique for preventing attacks and protecting user information. Every cryptography technique conducts the two operations of encryption and decryption. During the encryption procedure, the initial communication (plain text) is transformed into a coded message (cipher text). Messages are decrypted and then transformed back to plain text. **Figure.1.** Points to keep in mind: AES is a block cipher; key sizes range from 128 to 256 bits. Each block of data has a 128-bit encryption key. The same key is utilized for both encryption and decryption in the symmetric encryption algorithm known as AES. As a result, it is quicker and more effective than asymmetric encryption techniques like RSA.

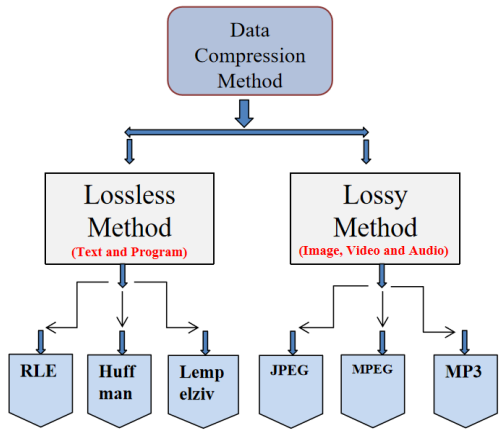

Figure.1. Data Compression Technique.

Data Compression classifies into two ways lossless compression and lossy compression. Lossless compression is a kind of data compression algorithm that permits the information to be totally compressed and decompressed without any loss of the original information. RLE methods are utilized to lesser data size for storage and transmitting content.

1.2 Encryption

The study of information encryption and decryption is known as cryptography. Ciphertext and plaintext are terms used to describe different types of data in the computer world. Key components of an encryption system include:

1. Plaintext (message not encrypted).
2. An encryption algorithm that acts as a safe's locking mechanism.
3. Key (operates like the combination to the safe).
4. Ciphertext, which an encryption key creates from a plaintext message.

1.3 Decryption

It decodes the information such that it can be decrypted by a trustworthy person who knows the secret password. The rounds' steps are easy to undo because they each have an opposite that can be used to undo the adjustments.Each of the 128 blocks is processed via 10, 12, or 14 rounds, depending on the key size. Decryption techniques. Information sent over the Internet is accessible to unauthorized individuals and organizations for review and access. Therefore, data is encrypted to reduce data theft and loss.

1.4 Run Length Encoding (RLE)

In 1983, Hitachi received a patent for run-length encoding. Due to its suitability for palette-based bitmap images like computer icons, RLE was a popular image compression technique on the internet before the advent of more complicated formats like GIF. It is also suitable for simple graphics and animations with lots of redundant pixels. Lossless compression is a sort of data compression technology without any degradation of the original data. RLE techniques are used to store, process, and transfer material with less data. decryption.

For example, if the input data is, [5,5,8,9,9,9,9,9,9,30,30,30,22,22,22,22,22,22,12,12].

Then the output data sequence will be [(5,2), (8,1), (9,6), (30,3), (22,6), (12,2)].

1.5 Compression and Decompression

1.5.1 Compression

Compression is a method for reducing the size of a file or data collection without losing any crucial information. To reduce the amount of data, compression techniques use a variety of algorithms and strategies. It Includes followings:

Run-Length Encoding (RLE): A shorter representation is used to replace many instances of the same value, such as "AAAABBB" becoming "A4B3."

Huffman Coding: based on their probabilities, assigning shorter codes to the data's more frequent symbols or patterns.

Dictionary-Based Compression: Putting common patterns into a dictionary and replacing them with references well-known dictionary-based compression called Lempel-Ziv-Welch (LZW) is utilized in file formats like GIF and ZIP.

Transform Coding: Redundancy can be more effectively compressed by applying mathematical adjustments to the data to create a new representation.

1.5.2 Decompression

Decompression is the process of restoring compressed data to its original state. Data decompression is required in almost all circumstances involving compressed data, including lossless and lossy compression. Data decompression, like data compression, depends on a variety of approaches.

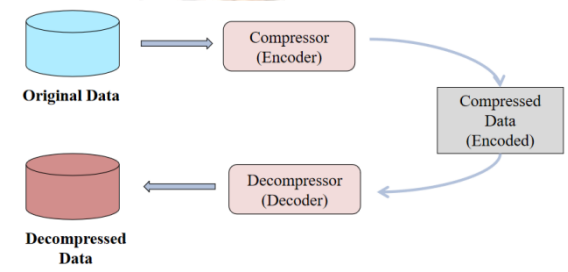

Figure.2. Simple Block diagram of Compression and Decompression.

The choice of compression algorithm is influenced by the type of data, the desired compression ratio, the importance of retaining data fidelity, and the specific use case. In particular situations, different algorithms might perform better. It's crucial to remember that decompressing compressed data is necessary before accessing or using it.

Factors	AES
KeyLength	128,192 and 256
Block Size	128
Block Size	Excellent
ExcecutionTime	MoreFast

Table 1. Comparision of Lossy and Lossless compression.

2. LITERATURE REVIEW

Mahesh B. Neelagar et al. [1] explained in the description "Designing of AES algorithm using Verilog." Since encrypted data lacks the patterns that compression systems use to achieve compression, it appears random. The key and data blocks are 56 and 64 bits in size, respectively, and there are 16 round operations.

Hayder Waleed et al. [2] provided a "Run length implementation with compression technique" in which the given data sequence is encoded using 8 bits for the data value and 3 bits for the counter value to increase compression ratio.

Giuseppe Baruffa et al. [3] An improved approach for on-chip clustering and lossless data compression of HL-LHC pixel hits was described in "An Improved Algorithm for On-Chip Clustering and Lossless Data Compression of HL-LHC Pixel Hits.,"

S. Sarika et al. [5] "Improved Run Length Encoding Scheme For Efficient Compression Data Rate," which describes AES, explains how it works. The adoption of AES for future compression and decompression technology implementation has been well-proposed here, according to reports.

Swetha Annangi et al. [6] In the article "RTL Design Of Efficient Modified Run Length Encoding Architectures Using Verilog HDL," the performance and analysis of an effective Run length architecture are discussed. RLE is built for image processing utilizing verilog HDL in order to analyze the performance parameter.

Keshav Kumar et al. [10] The article "A Design Implementation and Comparative Analysis of Advanced Encryption Standard (AES) Algorithm on FPGA".

3. PROPOSED METHODOLOGY

Design and implementation process includes a number of crucial processes and elements. AES works with fixed-size blocks of data, typically 128 bits, and employs a symmetric key for both encryption and decryption operations. These operations are repeatedly applied to the input data, which leads to confusion and diffusion, in order to achieve a high level of security. It is thought to be secure against known cryptographic attacks when used properly and with the appropriate key size. The AES algorithm's basic block diagram is shown in **Figure.3.** Now that AES is built into the CPU, applications that use it for encryption and decryption can operate more quickly and securely (with throughput of several GB/s). Even though the AES algorithm has been around for 20 years, we haven't succeeded in breaking it because, even with today's technology, it is impossible.

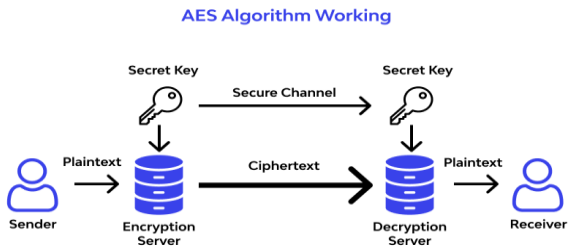

Figure.3. AES Block diagram.

In order to make the required changes, software implementations typically include working with bytes and bitwise operations. For high-speed encryption and decryption, hardware systems typically use specialized circuits like field-programmable gate arrays (FPGAs) or application-specific integrated circuits (ASICs).

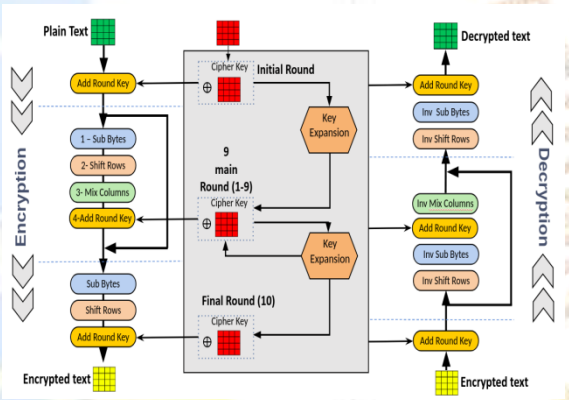

Figure.4. Flowchart of Encryption and Decryption.

AES Verilog implementation consists of a number of modules that work together to perform encryption and decryption operations. The flow diagram for both encryption and decryption is shown in **Figure.4.** above. The encryption algorithm creates the cipher text C as specified in (1) using the inputs of the message P and the key K.

$$C = EK(P) \quad (1)$$

The notation used in (1) shows that the plaintext P is used to produce the cipher text C, with the specific function being decided by the key K's value. This is done by applying the encryption method E. (2) shows the inverse transformation that the decryption algorithm D performs as a result of the encrypted text C.

$$P = DK(C) \quad (2)$$

3.2 Types of INPUT

The two sorts of data that can be inserted here are text and images. The input data I used for this work is shown in the figures below.

Figure.5. Coloured Image.

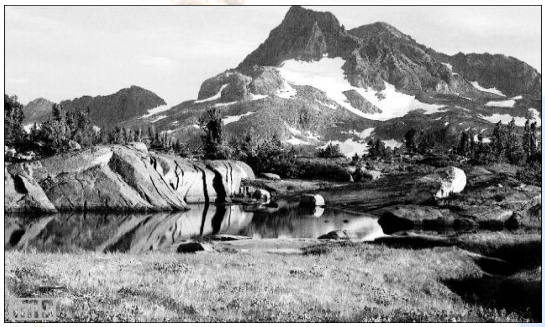

Figure.6. Black and White Image.

That will provide information on the power and space usage for the photos up top. I used MATLAB to convert images into hexadecimal values, which will translate the images into their hexadecimal numbers. Then, in order to use Xilinx Vivado 2018, we must include that converted file in our verilog HDL code.

Coloured Images: The image data's binary representation, not the precise color components or their values, **Figure.5.** is how the encryption process works. It's crucial to remember that employing AES to encrypt an image will produce a ciphered image that looks like random noise or jumbled data.

Black and White: Each pixel in a black-and-white image is either "black" (represented by the number 0) or "white" (represented by the number 1) **Figure.6.** The image data is split into 128-bit blocks (or multiples thereof) and AES encryption is applied separately to each block to encrypt a black-and-white image.

3.1.1 RGB Value

The RGB model uses combinations of red, green, and blue light in varying intensities to create colors. These values typically range from 0 to 255, with 0 signifying no intensity (no color) and 255 signifying maximum intensity (full color). An image pixel with the RGB values (255, 0, 0), for example, might be used to depict a fully saturated red color since the red component is at its highest intensity (255), while the green and blue components are at their lowest intensities (both 0). Here are a few illustrations of RGB color values:

- Absolute red is (255, 0), for example.
- (0, 255, 0) is the ideal shade of green.
- "Pure blue" is (0, 0, 255).
- White is made up of the colors red, green, and blue in the ratio (255, 255, 255).
- Black is created when all components of color are absent (0, 0, 0).

The RGB color model is used by digital displays, computer monitors, and other electronic devices.

4. Results and Synthesis Reports

4.1 Results

4.1.1 Simulation Results and Synthesis Reports.

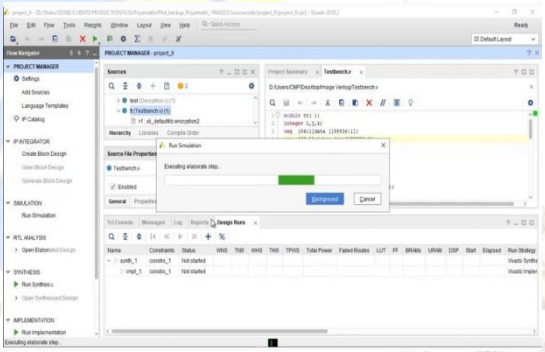

Figure.7. Run Simulation panel.

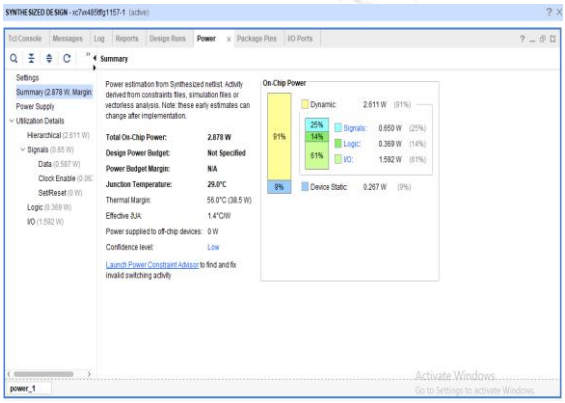

Figure.8. Synthesis Report of AES

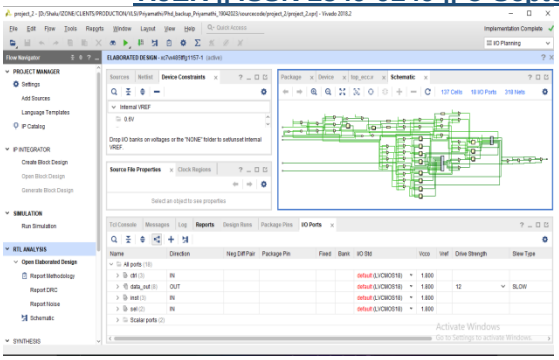

Figure.9. RTL diagram for AES.

The double-and-add-always (DAAA) strategy for ECPM is used in place of the traditional DAA method to protect the processor from SPA attacks. It consumes more energy than the conventional DAA technique because PA and PD are performed at each cycle. The cost-effective SPA defense for our processor is created using the DAA algorithm with unified PA.

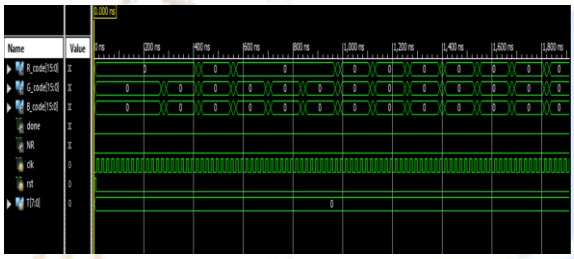

Figure.10. Simulation output of image

The recommended AES processor offers SPA high resilience by quickly multiplying points with a significantly smaller amount of space being used. The comparison findings for both RLE and AES are shown in **Table 2.**

Table 2. Comparison of RLE and Proposed AES.

Parameter	RLE method	AES method
Key Size	56 bits[1]	128 bits
Data Block Size	64 bits[3]	128 bits
Number of Round Operations	16[1]	10

For the planned system to be successful, the participants must have confidence in their capacity to contribute to the objectives and benefits envisaged. As systems get more intricate, there is a rising need for education and training. Before being given instructions on the new application software, the users must first get the necessary basic training in computer awareness.

Table 3. Power and Delay reports of images.

Image	Power (In mW)	Delay (nS)
Coloured	1.298663	5.23
Black & White	0.698695	2.5

5. Conclusion and Future Scope

5.1 Conclusion

During this process, modified Verilog HDL structures for AES compression and decompression were produced. The designed modules are simulated and synthesized using Xilinx Vivado 2018. In this method. The proposed AES, which is designed in Verilog and tabulated in a comparison table for coloured and Black and White image, optimizes the performance and operation time needed for both procedures.

The outcomes demonstrate that switching to Verilog from VHDL shows power and delay. Fewer clock cycles reduces the power usage.

5.2 Future Scope

Reduce the circuit complexity while compressing product data with the hybrid AES and AES algorithm by adding more inputs and fewer outputs to the compressor (as needed). Even if new technologies and threats are developed and improved upon, AES is likely to continue playing a vital role in secure communication and data protection for the foreseeable future.These are only a few examples of the kinds of domains where the possibilities of AES's potential future scope can be researched. As technology advances and new issues arise, further research and innovation will help AES maintain its relevance in data and communication security.

REFERENCES

[1] S. Sarika et al. “Improved Run Length Encoding Scheme For Efficient Compression Data Rate”, 2020 7th Int.conf.on Advanced encryption standards (AES), 2020.

[2] Joseph Sunil et al. “Implementation of AES Algorithm on FPGA and on software”, AES (Advanced Encryption Standard) is an algorithm which is used to protect electronic data, April, 2020.

[3] Hayder Waleed et al. “Run length implementation with compression technique”, data sequence is encoded by using 8 bits for data value and 3 bits for counter value to improve the compression ratio.2020

[4] Dr. Chris Bailey et al. “lossless bio-signal compression circuit with 250 femtoJoule performance per bit”, International Journal of Advances in Engineering and Management (IJAEM) Sep 2019

[5] Giuseppe Baruffa et al. “An Improved Algorithm for On-Chip Clustering and Lossless Data Compression of HL-LHC Pixel Hits”, ISPECE 2018.

[6] Ayan Banerjee et al. “An Efficient Image Compression Algorithm for almost Dual-ColorImage Based onK-Means Clustering, Bit-Map Generation and RLE.”2010.

[7] Lokireddi Phani Kumar et al. “Implementation of Speech Encryption and Decryption using Advanced Encryption Standard” IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India.

[8] Soumya, Mahesh B Neelagar et al. “Designing of AES algorithm”, 4th International Conference for Convergence in Technology (I2CT) SDMIT, ujire. 2018.

[9] Xilinx “XA Spartan-3E FPGA Family”, [Online] Available: http://www.xilinx.com/products/silicon devices/fpga/xaspartan-3e/.

[10] Micron Technology Inc., ”2, 4, 8Gb: x8/x16 Multiplexed NAND Flash Memory Features” datasheet, 2gb nand m29b 1.fm, Revision I 1/06 EN, 2004.

[11] P. T. Dao, X. J. Li and H. N. Do, ”Lossy compression techniques for EEG signals”, 2015 International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, pp. 154-159.

[12] Held, Gilbert et al. “Data Compression: Techniques and Applications, Hardware and Software Considerations”, second edition, John Wiley & Sons, New York, NY, 1987.

[13] G. Higgins, S. Faul, R. P. McEvoy, B. McGinley, M. Glavin, W. P. Marnane, W. P., and E. Jones et al. “EEG compression using JPEG2000: How much loss is too much?”, In IEEE Engineering in Medicine and Biology Society (EMBC), 2010 Annual Intl. Conference of the IEEE (pp. 614-617).