THE INTEGRATION OF VARIOUS COMPRESSION TECHNIQUES WITH AES AND DES FOR EFFICIENT ENCRYPTION

Abstract

With the advancements in the area of information and communication technologies, we are now moving from 5G towards 6G-grounded systems. The employment of such paradigms will result in the generation of a huge volume of data named big data because of the high bandwidth and low latency. The main issue that should be taken care of during today's technological systems is the efficient and secure transmission and processing of this data. For this purpose, compression and encryption are the best candidates to achieve this goal. To analyze the computational performance of the integration of compression encryption, the proposed study combined the compression algorithms named Huffman Coding, LZW technique, and Run Length Encoding with symmetric encryption algorithms named Data Encryption Standard (DES) and Advanced Encryption Standard (AES). The experiment was performed with these different combinations using the 32 bytes file, while the codes are implemented in Visual Studio IDE using the Go language. The resultant data shows that the utilization of compression-encryption can enhance the computational performance and the target of effective and secure communication can be achieved.

Keywords: 6G, AES, Go language, Computational performance, Big data.

1. Introduction

The number of devices (sensors) connected is increasing very rapidly on daily basis, and it is now the time of the Internet of Everything (IoE) instead of IoT. For such approaches, high throughput, less latency, and vast coverage are required. 6G is the optimal candidate for achieving all these characteristics to have effective communication. The increase in the number of connected devices means a huge volume of data over the internet, which will result in various security issues. It needs time to bring efficient and secure communication paradigms for the smooth and reliable working of Artificial Intelligence (AI)-based smart systems. The practice of expressing certain material while using fewer data to do so is generally referred to as data compression. The method of encoding the provided information in fewer bits is known as data compression. In the present era of communication, it is playing a very important function [1]. The process of data compression can be seen in figure 1.

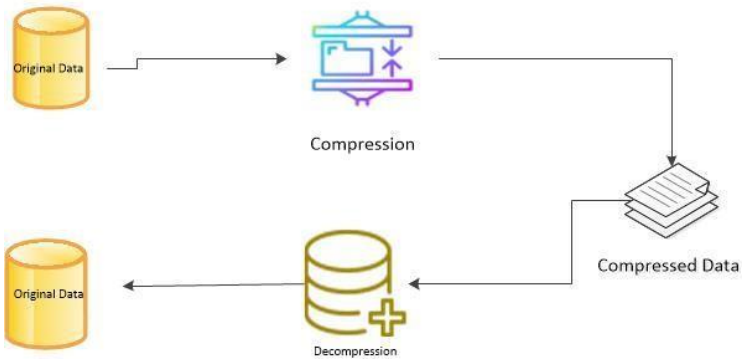

Figure 1 Data Compression

Encryption involves transforming plain text (or any other type of data) into cipher text. It is extremely crucial for safe communication. Symmetric or Asymmetric encryption (separate keys

for encryption and decryption) is both possible. The original data will only be accessible to the intended recipient [2]. The overall encryption process is shown in figure 2.

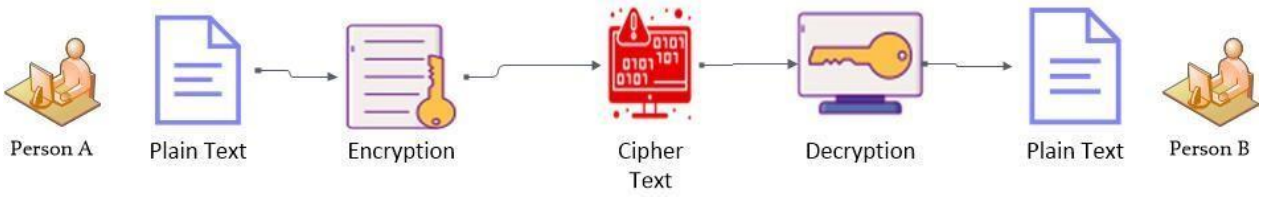

Figure 2 Encryption

1.1 Huffman Coding

Huffman coding provides a more advanced and effective lossless compression method that converts symbols in a data source to binary codes, resulting in the most common letters generating the shortest binary codes and the least common having the largest [3]. The main steps involved in the process of Huffman coding are given in algorithm 1.

Step 1: Start.
Step 2: Sort input symbols according to decreasing likelihood.
Step 3: Consolidate two of the least likely symbols into a single subgroup.
Step 4: Give the top and bottom branches, respectively, the numbers 0 and 1.
Step 5: Does the number of unmerged nodes exceed one?
If yes, repeat step 3 to 5.
Else
Step 6: Stop, scan the branches' changeover bits from top to bottom to create code-words.
Step 7: End

Algorithm 1 Huffman Coding

1.2 LZW Compression

Abraham Lempel, Jacob Ziv, and Terry Welch developed the global lossless data compression technique known as Lempel-Ziv-Welch (LZW). One of the Adaptive Dictionary approaches is LZW compression. The dictionary is constructed concurrently with the encoding of the data. Therefore, on-the-fly encoding is possible. It's not necessary to convey the dictionary. At the receiving end, a dictionary may be created on the spot. If the dictionary becomes overflowing, we must re-initialize the dictionary and slightly expand each of the code words [4]. The main procedure of LZW compression is given in algorithm 2.

Step 1: Start.
Step 2: Let x be the first input symbol.
Step 3: WHILE there are still more characters.
Step 4: y = next character.
Step 5: IF x+y is already in the table.
x = x+y
ELSE
Display the code for x
Step 6: Insert x+y into the table.
Step 7: x = c.
Step 8: END WHILE
Step 9: display the code for x.
Step 10: End.

Algorithm 2 LZW Compression

1.3 Run Length Encoding

Run length encoding (RLE) reduces the size of a sequence of characters by more effectively resembling a subsequence made up of runs of the same character. A tuple that includes the start and outcome of a run is substituted for it. The beginning is the position of the substring's first item, and the value is the letter that appears there [5]. The process of RLE is explained in algorithm 3.

Step 1: Start.
Step 2: Select the first symbol from the input sequence.
Step 3: Add the chosen item to the string's final location.
Step 4: Add the count to the target sequence after counting the symbol's following appearances.
Step 5: If the input sequence's endpoint isn't attained, select the following symbol and return to the starting position 2, 3, and 4.
Step 6: End.

Algorithm 3 Run Length Encoding

1.4 AES Encryption

AES is a symmetric block encryption algorithm with a defined block size that's employed to safeguard private data. AES uses 10, 12, and 14 encryption repetitions with key sizes of 128, 192, and 256 bits supported. A round-key obtained from the encryption key is mixed with the data during each round [6]. The architecture of AES encryption is shown in algorithm 4.

Step 1: Start.
Step 2: Read a plain text.
Step 3: Select a key.
Step 4: Perform SubBytes operation.
Step 5: Do the ShiftRows.
Step 6: Utilize the MixColumns computation.
Step 7: Add round key.
Step 8: Repeat step 4-step 7 according to the chosen Scheme (without including MixColumns operation in the last round).
Step 9: End.

Algorithm 4 AES Encryption

1.5 DES Encryption

A common private key is used by the cryptosystem DES to encrypt and decode data. DES method applies a predetermined piece of sequence in plaintext bits and encodes it by performing several steps into cipher text of identical size and every block is 64 bits. There are 16 similar operating cycles or steps. There is also a first and last permutation, denoted by the letters IP and FP, respectively [7]. Algorithm 5 explains the DES encryption system.

Step 1: Start.

Step 2: Read a 64 bits plain text.

Step 3: Perform initial permutation on it.

Step 4: Two halves of 32 bits are achieved from step 3.

Step 5: 16 rounds of encryption are performed on each half.

Step 6: Both the half are combined and final permutation is carried out on it.

Step 7: A 64 bits encrypted string was obtained.

Step 8: End.

Algorithm 5 DES Encryption

The main aim of the proposed study is to discuss the efficiency in the computational performance using the reliable combination of compression encryption. The study also aims:

- ✓ To discuss the existing literature related to the area of research.
- ✓ To obtain statistical data about various compression encryption techniques.
- ✓ To realize how to select an effective combination.

The article is structured as follows: The project idea is summarized in Section 1. Section 2 provides a summary of the methods employed to examine the case. Section three of the report goes into further depth on the specifics of how it was used. The main subject of Section 4 is the investigation's findings. Section 5 examines the full body of research.

2. Related Work

Carpentieri [8] has investigated the use of both compression and encryption on digital records. To be effective and secure, communication should be built on a scheme defined as two activities that are diverse and occasionally at odds with one another. Compression and cryptography are these two procedures. The adversary of compression is unpredictability, while on the other hand, encryption has to infuse randomization into the electronic data to ensure protection. Poor security, ineffective picture propagation, and inefficient image storage are becoming major issues. Tong et al. [9] have presented a brand-new picture lossless compression coupled encryption technique utilizing chaotic maps with all source data unaltered. According to empirical results, the reduced data size is around 50% of the actual file size, achieving a respectable lossless compression ratio. Additionally, the encryption system satisfies several safety checks. For large datasets, the privacy of electronic patient records (EPR) is a major problem. The EPR information for the hospital setting was protected using a compression-then-encryption-based dual watermarking technology, which results in many noteworthy characteristics. The potential of the suggested strategy for telemedicine has been demonstrated through trials on a sizable quantity of patient records. Furthermore, the suggested technique is superior in terms of resilience and reliability when compared to the current approaches [10]. Hameed et al. [11] have suggested a method that allows smooth and encrypted transfer of the Ecg waveform from the detector to the screen utilizing buffer blocks, peak detection, compression, and encryption mechanisms. It was discovered that the suggested system's discrete wavelet transform, Huffman coding, and Cipher Block Chaining-Advanced Encryption Standard algorithm could provide rebuilt waveforms of a top standard than those produced by unencrypted compression.

One of the best methods for protecting information when saving and delivering them over a network connection is encryption. Ashila et al. [12] have suggested an approach utilizing AES-Huffman in conjunction to create lossless compressed encrypted documents. when the compression step is carried out after encryption. Entropy following encryption and compression and the avalanche effect (AE) was used to determine the degree of file privacy. According to the test findings, it has been shown that AES encryption causes files to grow by about 25% of their initial dimensions. But the encrypted file code shrunk by around 30% after Huffman compression. The analysis showed the use of arithmetic coding with the AES (Advanced Encryption Standard) technique to secure and condense content. The basic experiment includes first encoding the material arithmetically, then encrypting it via the AES method, and then transmitting the data. The information is encrypted and interpreted at the other end to create the user data. The ability of the paper to simultaneously encode, decode, and compress data is a benefit. The source file size is 128 bits or 256 bits in AES, therefore the goal is to use digital arithmetic coding to compress the data before encryption [13].

Nowadays, since everything is accomplished via information technology, there is a much greater demand for cryptography. By integrating Huffman coding to shorten the content, Kumari et al. [14] have tried to enhance the privacy of internet data. The practiced approach is an attempt to compact, protect, and conceal the data. It outlines the process by employing different encryption

algorithms one at a time, and the goal is to achieve the level of protection possible out of the solutions that are already in place. The suggested strategy is applied in MATLAB2016a, and the results obtained in this research demonstrate that this approach is superior to the previous methods. Joshi and Sharma [15] have used the LZW technique to do data immersion. Then, using the AES method, resilience is achieved. Lastly, computerized data is embedded in an encrypted picture using a spatial approach. Research is conducted using actual dataset images. Results for quality factors demonstrate that the suggested approach preserved SNR and PSNR values with excellent data resilience. Encrypting the digital data may be used to overcome the ownership issue. This method starts by clustering human readable texts and encrypting them using AES and Elliptic Curve Encryption (ECC). Next, it utilizes compression to generate cipher blocks, and eventually, it attaches the MAC address and the AES key encrypted by ECC to generate all of the encrypted messages. The findings of the method's explanation and application demonstrate that it may decrease encryption time, decryption time, and overall operating computational burden without sacrificing safety [16].

3. Methodology

Compression and encryption of data are two different procedures but somehow they are interrelated. Both can be applied for achieving randomness in the input data. In today's modern communication systems, the computational performance and security of data are the most essential requirements. In this article, the compression-encryption algorithms are employed in combination to analyze the performance in terms of time. The procedure followed in the study is that first the input data is compressed using various algorithms and then the AES and DES encryption techniques are applied to it as shown in figure 3.

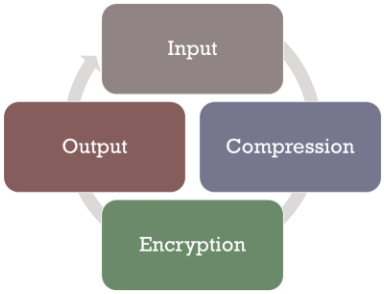

Figure 3 Methodology

The main structure of the performed study is given in figure 4.

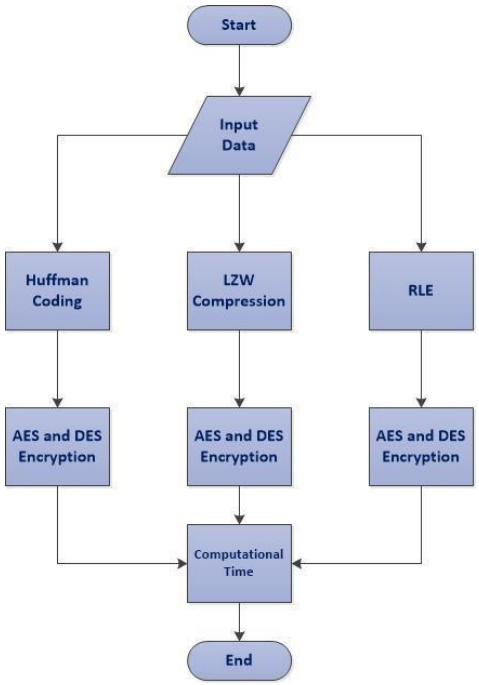

Figure 4 Architecture of the Method

After the compression of input data using each compression technique, the encryption algorithms were applied to the resultant compressed data separately. All the codes of the used algorithms were implemented in Visual Studio using the Go language.

4. Results and Discussion

In the proposed article, the performance of different compression techniques with AES and DES encryption was analyzed. The resultant data revealed that the integration of compression encryption greatly depends on the type of data and requirements of a user. The study shows that an effective combination of compression and encryption can achieve the goal of efficient and secure processing and transmission of data in today's modern technological approaches like the Internet of Everything (IoE). With the characteristics like high bandwidth and low latency of 6G, these procedures should be considered in the first place. The overall results are discussed below.

4.1 AES and Compression

The data extracted from the combined implementation of various compression algorithms with AES is shown in figure 5. It can be realized that the encryption time can be greatly reduced with these combinations. Overall, the time taken for encryption can be represented in chronological order as AES+RLE > AES > AES+LZW > AES+Huffman. It can be concluded that the AES-Huffman combination is very efficient in terms of computational time.

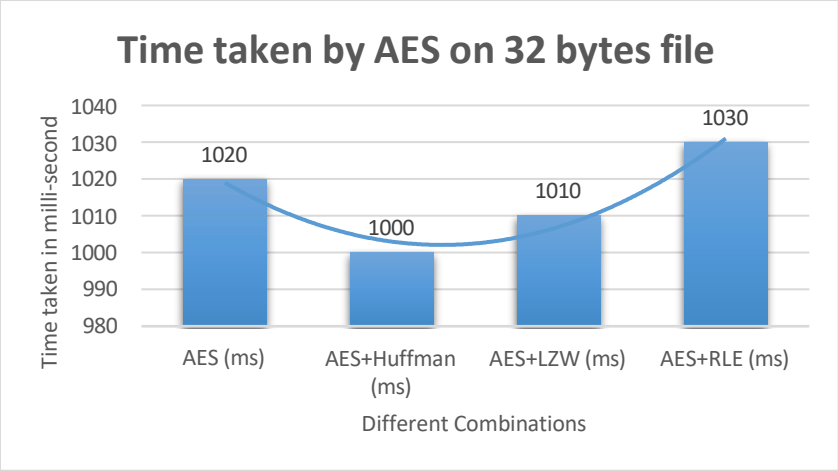

Figure 5 AES and Compression

4.2 DES and Compression

The effective integration of DES with different compression algorithms achieved some interesting results as shown in figure 6. The time complexity was minimized efficiently. The obtained data can be represented in chronological order as DES > DES+RLE > DES+Huffman > DES+LZW. So, the most efficient one is the DES+LZW combination.

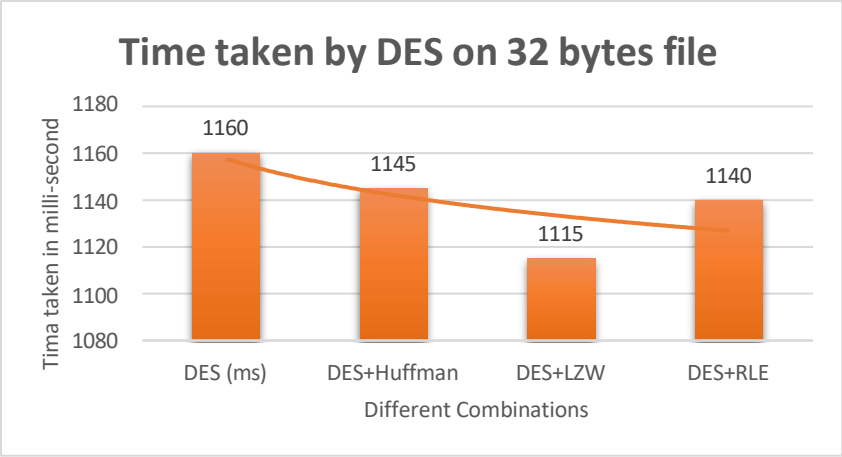

Figure 6 DES and Compression

The whole data obtained from the study is shown in figure 7.

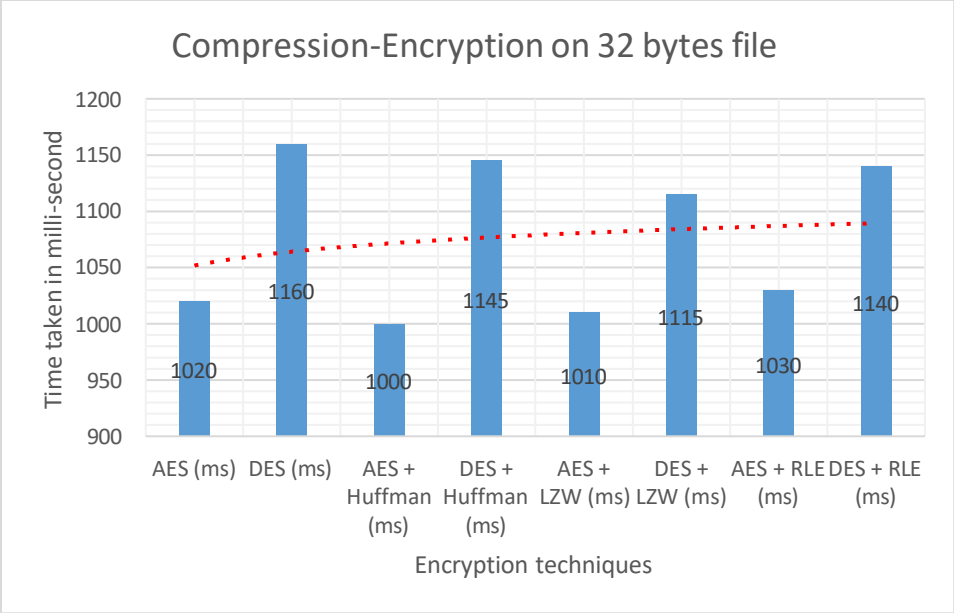

Figure 7 AES, DES, and Encryption

5. Conclusion

Because condensed data is much more dependable and manageable, data compression is a crucial aspect of information safety. Data that has been compressed well is reliable, safe, and simple to communicate. Cryptography is the basis for any secure and reliable communication technique which allows the end users to communicate securely and confidentially. The techniques of compression were integrated with Huffman Coding, LZW, and RLE encryption, and their performance was studied. The study shows that the encryption time can be greatly minimized with the employment of compression and encryption in integration.

References:

[1] J. D. A. Correa, A. S. R. Pinto, and C. Montez, "Lossy Data Compression for IoT Sensors: A Review," *Internet of Things,* vol. 19, p. 100516, 2022.

[2] R. Bhanot and R. Hans, "A review and comparative analysis of various encryption algorithms," *International Journal of Security Its Applications,* vol. 9, no. 4, pp. 289-306, 2015.

[3] A. Moffat, "Huffman coding," *ACM Computing Surveys,* vol. 52, no. 4, pp. 1-35, 2019.

[4] H. Dheemanth, "LZW data compression," *American Journal of Engineering Research,* vol. 3, no. 2, pp. 22-26, 2014.

[5] B. Strasser, A. Botea, and D. Harabor, "Compressing optimal paths with run length encoding," *Journal of Artificial Intelligence Research,* vol. 54, pp. 593-629, 2015.

[6] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, and C.-H. Tsai, "AES-128 based secure low power communication for LoRaWAN IoT environments," *Ieee Access,* vol. 6, pp. 45325-45334, 2018.

[7] K. Logunleko, O. Adeniji, and A. Logunleko, "A comparative study of symmetric cryptography mechanism on DES AES and EB64 for information security," *Int. J. Sci. Res. in Computer Science Engineering,* vol. 8, no. 1, 2020.

[8] B. Carpentieri, "Efficient compression and encryption for digital data transmission," *Security Communication Networks,* vol. 2018, 2018.

[9] X.-J. Tong, P. Chen, and M. Zhang, "A joint image lossless compression and encryption method based on chaotic map," *Multimedia Tools Applications,* vol. 76, no. 12, pp. 13995-14020, 2017.

[10] A. Anand, A. K. Singh, Z. Lv, and G. Bhatnagar, "Compression-then-encryption-based secure watermarking technique for smart healthcare system," *IEEE MultiMedia,* vol. 27, no. 4, pp. 133-143, 2020.

[11] M. E. Hameed, M. M. Ibrahim, N. Abd Manap, and A. A. Mohammed, "A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES," *Future generation computer systems,* vol. 111, pp. 829-840, 2020.

[12] M. R. Ashila, N. Atikah, E. H. Rachmawanto, and C. A. Sari, "Hybrid AES-Huffman Coding for Secure Lossless Transmission," in *2019 Fourth International Conference on Informatics and Computing (ICIC)*, 2019, pp. 1-5: IEEE.

[13] P. S. Mukesh, M. S. Pandya, and S. Pathak, "Enhancing AES algorithm with arithmetic coding," in *2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)*, 2013, pp. 83-86: IEEE.

[14] M. Kumari, V. Pawar, P. J. I. J. o. N. S. Kumar, and I. A. Vol, "A novel image encryption scheme with Huffman encoding and steganography technique," *International Journal of Network Security Its Applications,* vol. 11, 2019 2019.

[15] A. K. Joshi and S. Sharma, "Reversible data hiding by utilizing AES encryption and LZW compression," in *Proceedings of International Conference on Recent Advancement on Computer and Communication*, 2018, pp. 73-81: Springer.

[16] T. Yue, C. Wang, and Z.-x. Zhu, "Hybrid encryption algorithm based on wireless sensor networks," in *2019 IEEE international conference on mechatronics and automation (ICMA)*, 2019, pp. 690-694: IEEE.