minor report plag check

by Mohit B

Submission date: 27-Nov-2022 09:02PM (UTC+0530)

Submission ID: 1964106950

File name: report_for_plag_1_1.pdf (118.61K)

Word count: 723

Character count: 3883

MINOR-1 PROJECT
END TERM REPORT

For

Hybrid Compression-Encryption Algorithm

Submitted By

Specialization	SAP ID	Name
CCVT	500087456	Mohit Bishesh
CCVT	500086385	Shiv Pratap Singh
CCVT	500087109	Yuvraj Pundir
CCVT	500084917	Anant Garg

Department of Systemics

School of Computer Science

UNIVERSITY OF PETROLEUM & ENERGY STUDIES,

DEHRADUN- 248007. Uttarakhand

Prof. Sandeep Pratap Singh.
Project Guide

Dr. Neelu J.
Cluster Head

1. Introduction

With the advancement of time, there is rapid innovation and development in the field of technology and tech industries. Many new Software and applications have been developed especially when we talk about social media or other software connecting people.

So here comes cryptography which plays a vital role in securing the data and maintaining the privacy of the users. Technically, cryptography refers to the encryption technique which helps us to convert the plain text to cyphertext with the help of appropriate algorithms. This technique can be used to apply to almost all kinds of soft or digital files available including PDF, word, images, etc.

Advanced encryption standard (AES), 3DES, and Data encryption standard (DES), a are thecommon but very famous symmetric- cryptographic algorithms being used. Whereas theadvanced encryption standard is one of the best cryptographic algorithms and hence it is being used as a security standard for the National institute of standards and technology (NIST).

But it must be noted that some of the researchers claim that AES has a slight side effect on the file size as it increases the size of the file after encryption. This side effect can be negated with the help of compression algorithms. There are two types of compression techniques - Lossless compression and Lossy compression. Lossless compression is a technique in which there is no data loss and the data of the content of the file is completely reversed during the decryption process.

Whereas lossy compression is a compression technique in which some non-critical parts of the data are removed and there is a certain loss in the data. For better accuracy, especially when we have critical data, lossless compression is always the first choice.

So finally, the integration of a cryptographic algorithm i.e. AES (used here), and a compression technique (like Huffman Encoding) is a better idea that not only reduces the file size but also increases the security and is hence helpful in maintaining the security and privacy of the users in case of connecting platforms or if we are sharing our file contents.

2. Literature Review

In the research done by author [1] it was proven that after AES encryption, the size of the file was increased by 25% but after applying Huffman encoding the encrypted file code decreased by 30%. Also, a considerable amount of change in entropy and Avalanche effect if observed after applying Huffman encoding.
In the research done by author [2] it was shown that AES has higher space complexity as compared to DES, while DES has higher time complexity as compared to DES.

3. Problem Statement

Advanced Encryption Standard is a widely used and recognized encryption algorithm. Although the algorithm provides strong and reliable encryption, it does so on the cost of making the file size slightly larger. Therefore, there is a need to negate this drawback. Huffman encoding can be coupled with AES to produce compressed lossless encrypted files without compromising security.

4. Objectives

- To implement AES and DES to generate ciphertext from plaintext.
- To compare file size of ciphertexts generated by AES and DES respectively.
- To compress plain text using Huffman Encoding and then perform encryption.
- To compare the size of compressed ciphertext with normal ciphertext.

5. Methodology (tentative at synopsis time and exact at end term time)

- Input plaintext will be taken.
- Generating of cipher text of input string using AES or DES algorithm.
- File size of generated ciphertext will be noted.
- Compression of input plaintext using Huffman encoding.
- Encryption of compressed input plaintext.
- Calculation of compression factor for each ciphertext generated with respect to the encryption technique used.

6. Conclusion

By performing our project, we have successfully concluded that we can use a combination of advance encryption standard (AES) to encrypt our files as well as to reduce the size of our file which in turn increases the efficiency and security of our file.

This combinational approach also reduces the bandwidth requirement, time of delivery and other resources needed for the transmission of loss less data.

minor report plag check

ORIGINALITY REPORT

8%	6%	4%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to De Montfort University Student Paper	2%
2	pubmed.ncbi.nlm.nih.gov Internet Source	2%
3	Anu Aryal, Shoko Imaizumi, Takahiko Horiuchi. "Hierarchical Scrambling Method for Palette-Based Images Using Bitwise Operation", Bulletin of the Society of Photography and Imaging of Japan, 2016 Publication	1%
4	prataponblog.blogspot.com Internet Source	1%
5	"M817 Block 2 week 9 symmetric encryption WEB097768", Open University Publication	1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		