Data Security Using Compression and Encryption Techniques

Madhumita Panda
Assistant Professor, Computer Science
SUIIT, Sambalpur University, Odisha, India.

Abstract- Data security and confidentiality is a challenging issue in the present time. Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to the important information. Cryptography protects users by providing functionality for the encryption of data and authentication of other users. Compression is the process of reducing the number of bits required to store or transmit data. This paper aims to implement two commonly used cryptography algorithms AES and DES for data security. The data is first encrypted and decrypted and the time is noted. Then again the same data is compressed using LZW and then encrypted and decrypted and again time is noted. Simulation results are given at the end and seen that compression and then encryption of data give better results.

Keywords- Cryptography, Data compression, AES,DES,LZW.

I. INTRODUCTION

In today's digital world, Security is required to ensure that information remains confidential and only access by authorized users. Main goals of security are Confidentiality, Authentication, Data Integrity, Non-repudiation and Access control. Data compression is known for reducing storage and communication costs. It involves transforming data of a given format, called source message to data of a smaller size format called code word [1].Data Compression use less disk space (saves money) makes data transmission easy and hence more data can be transferred via internet. It increase speed of data transfer from disk to memory[2]. The rest of the paper is organized as follows. Section II gives a brief introduction to cryptography and Section III gives a brief introduction on Compression. Section IV of this paper gives an overview of the encryption algorithm used and the compression technique used for our experiments .Section V presents the experimental results. Finally section VI concludes the paper with future work.

II. CRYPTOGRAPHY

ryptography is the art and science of securing messages from undesirable individuals by converting it into a form indiscernible by its attackers while it is stored and transmitted. It is a fundamental building block for building information systems. The main goal of cryptography is to keep the data secure from unauthorized access [3]. In cryptography terminology, messages are called plaintext or clear text. The process of disguising the message in such a way as to hide its original content is called encryption. The encrypted message is called cipher text. The process of returning a cipher text to plaintext is called decryption. On the basis of key used, cipher algorithms are classified as asymmetric key algorithms, in which encryption and decryption is done by two different keys and symmetric key algorithms, where the same key is used for encryption and decryption [4].Some symmetric key algorithms includes DES, TRIPLE DES, AES, RC4, RC6, BLOWFISH and some examples of asymmetric key algorithm are RSA,ECC etc.

III. COMPRESSION

Data compression implies sending or storing a smaller number of bits. Compression is the reduction in size of data in order to save space or transmission time [5].It is the most important and vital approach for modern communication systems for reducing the communication costs and increasing the transmission rate by using the available bandwidth effectively[2].In general, compression methods are classified as either lossless or lossy. In lossless compression, restored data and original data are identical i.e. there is no loss in the data. This method is necessary for many types of data like executable code, bank records, and text articles etc. where we cannot afford to lose even a single bit of information. E.g., Runlength coding, Huffman coding, LZW compression, Arithmetic coding, lossless predictive coding. Lossy compression is the type of compression, in which the restored data is not identical to the original data i.e. there is some loss in the data. This compression is mostly used for compressing multimedia data, audio, video, image, etc. It is also used for a number of applications in which some amount of error is tolerable.E.g. transform coding, wavelet coding, Lossy predictive coding techniques

IV. METHODOLOGIES

a. Compression Technique

LZW

LZW compression is a lossless compression. It compress a file into a smaller file using a table-based lookup algorithm invented by Abraham Lempel, Jacob Ziv, and Terry Welch. It is a 'dictionary based' compression algorithm that scan a file for sequences of data that occur more than once [6]. These sequences are then stored in a dictionary and references are put where-ever repetitive data occurred [6].

b. Cryptographic Techniques

AES

Advanced Encryption Standard (AES) is a new encryption standard recommended by NIST to replace DES and has a Non-Feistel structure, which is based on a sophisticated mathematical design. It encrypts 128 bit block size with 128/192/256 bit key for 10/12/14 rounds. The complete specification and the above structure of AES encryption scheme can be found in [7].

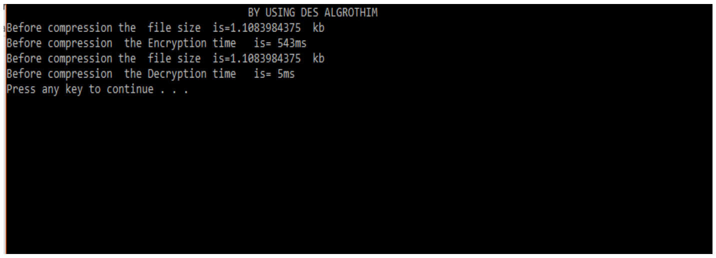
DES

Data Encryption Standard (DES) is a symmetric key block cipher and was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology)[8]. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block [9] [10].

V. SIMULATION RESULTS

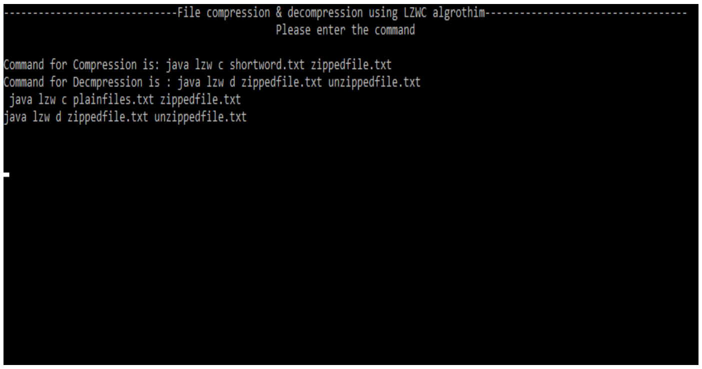
The performance comparison of the Algorithm(DES,AES) mentioned above was conducted on text file. The text file was first encrypted and decrypted and the time was noted. Then the same text file was first compressed using LZW algorithm and then encrypted and again time was noted.

The simulation was conducted on a laptop with windows 64bit, processor i5 and CPU 1.70GHZ with 4GB RAM. 1, 2, 5 and 10 KB was generated as the test subjects. The AES, DES Algrothim were used with key size 128, 64 bits.



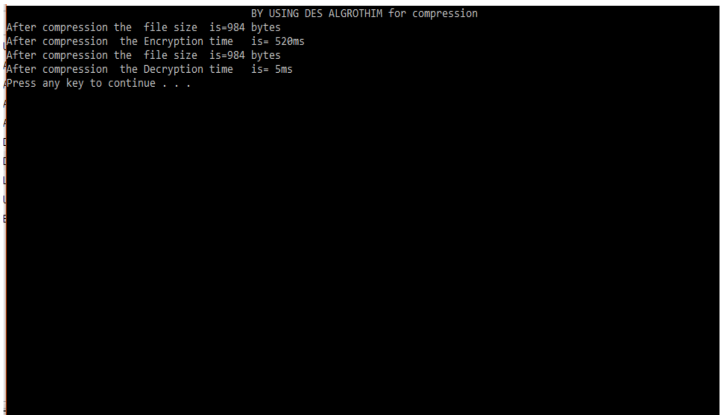
```
                                        BY USING DES ALGROTHIM
Before compression the  file size  is=1.1083984375  kb
Before compression  the Encryption time   is= 543ms
Before compression the  file size  is=1.1083984375  kb
Before compression  the Decryption time   is= 5ms
Press any key to continue . . .
```

Fig.1: Encryption and Decryption time using DES algorithm



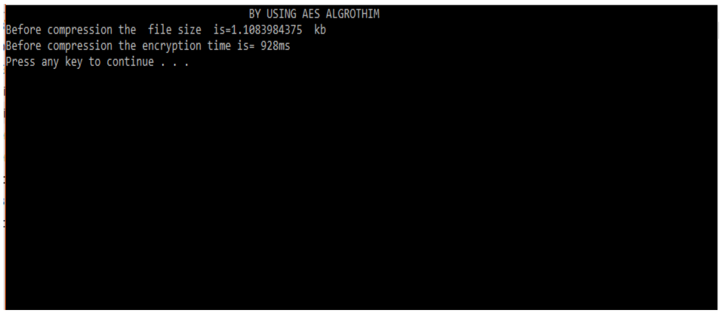
```
-----------------------------File compression & decompression using LZWC algrothim----------------------------------
                                              Please enter the command

Command for Compression is: java lzw c shortword.txt zippedfile.txt
Command for Decmpression is : java lzw d zippedfile.txt unzippedfile.txt
 java lzw c plainfiles.txt zippedfile.txt
java lzw d zippedfile.txt unzippedfile.txt
```

Fig.2:.LZW Compression



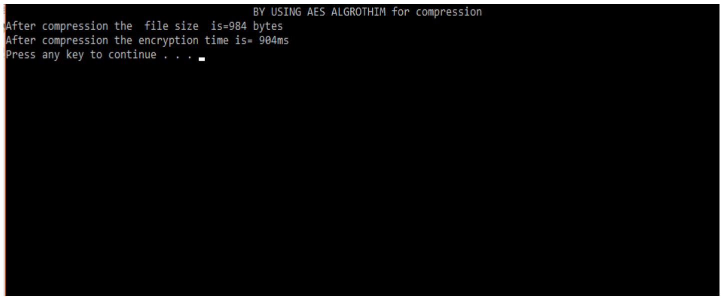
```
                                        BY USING DES ALGROTHIM for compression
After compression the  file size  is=984 bytes
After compression  the Encryption time   is= 520ms
After compression the  file size  is=984 bytes
After compression  the Decryption time   is= 5ms
Press any key to continue . . .
```

Fig.3: Encryption and Decryption Time after Compression for DES



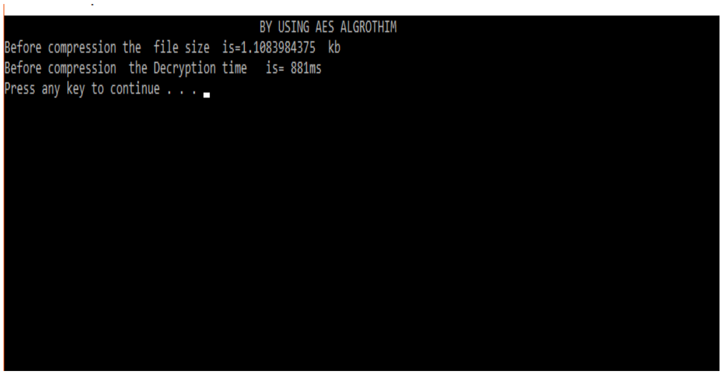
```
                                        BY USING AES ALGROTHIM
Before compression the  file size  is=1.1083984375  kb
Before compression the encryption time is= 928ms
Press any key to continue . . .
```

Fig.4: Encryption time for AES algorithm



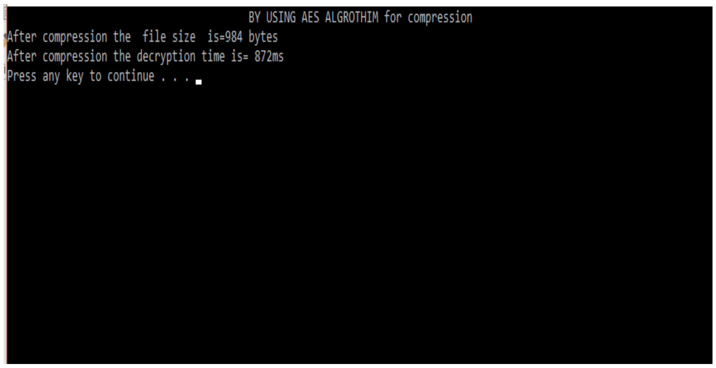
```
                                        BY USING AES ALGROTHIM for compression
After compression the  file size  is=984 bytes
After compression the encryption time is= 904ms
Press any key to continue . . .
```

Fig.5: Encryption time for AES algorithm after Compression



```
                                        BY USING AES ALGROTHIM
Before compression the  file size  is=1.1083984375  kb
Before compression  the Decryption time   is= 881ms
Press any key to continue . . .
```

Fig.6: Decryption time for AES algorithm



```
                          BY USING AES ALGROTHIM for compression
After compression the  file size  is=984 bytes
After compression the decryption time is= 872ms
Press any key to continue . . .
```

Fig.7: Decryption time for AES algorithm after Compression

VI. CONCLUSION AND FUTURE WORK

The experimental results shows clearly(from Fig.3,Fig.5,Fig.7) that for both the algorithms(AES,DES) the encryption and decryption time reduces much if files are compressed and then encryption techniques are applied on them.In this paper we have used compression and encryption techniques separately. In future to gain more better results, we aim to used compression and encryption technique at the same time.

VII. REFERENCES

[1]. T.SubhamastanRao, M.Soujanya, T.Hemalatha, T.Revathi, “Simultaneous data compression and encryption” (IJCSIT) International Journal of Computer Science and Information Technologies, ISSN 0975-9646, Volume2(5), 2011.

[2]. Lone, Quaiser Bashir, Mir Imtiyaz Hussain, and Ms Monisa. "Cryptography Encryption and Compression Techniques." International Journal of Allied Practice, Research and Review, ISSN 2350-1294, Vol. IV,July, 2017.

[3]. Diaa Salama Abd Elminaam, Hatem Mohamad Abdual Kader, Mohiy Mohamed Hadhoud, “Evalution the Performance of Symmetric Encryption Algorithms”, International journal of network security vol.10,No.3,pp,216-222,May 2010 .

[4]. Jonathan Knudsen, Java Cryptography, 2nd Edition, O’Reilly, 2011.

[5]. Haroon Altarawneh, Mohammad Altarawneh “Data Compression Techniques on Text Files: A Comparison Study” International Journal of Computer Applications, (0975 – 8887), Volume 26– No.5, July 2011.

[6]. MohiniChaudhari, Dr. KanakSaxena “Fast and Secure Data Transmission using Symmetric Encryption and Lossless Compression” International Journal of Computer Science and Mobile Computing, ISSN 2320– 088X, Vol. 2, Issue. 2, February 2013.

[7]. J. Daemen and V.Rijmen, “AES Proposal: Rijndael” ,1999.

[8]. Shanta, yoti Vashishtha,―Evaluating the performance of Symmetric Key Algorithms:AES (Advanced Encryption Standard) and DES (Data Encryption Standard)‖ IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ,pp.43-49 .

[9]. http://www.vocal.com/cryptography/rc4-encryption-algoritm/

[10]. Prashanti.G, Deepthi.S & Sandhya Rani.K. ”A Novel Approach for Data Encryption Standard Algorithm”.