Fast & Secure Data Transmission using Symmetric Encryption & Lossless compression

Rajashri

Department of Information Technology, SVERI's College of Engineering, Pandharpur

Abstract

"HuffmanZip" software lets you reduce the overall number of bits and bytes in a file so it can be transmitted faster over slower Internet connections, or take up less space on a disk. Domain File compression is a System Based Software. The software will be done using Core Java. It can use in the System as a utility. The type of compression we will use here is called **lossless compression**. The user need not depend on third party software's like winzip, winrar, Stuff etc. the software can be used to compress files and they can be decompressed when the need arises. For implementing this Software we want to use algorithms **Huffman algorithm** The Domain File Compression mainly include 5 modules

1. Compress file or folder: - This module helps us to compress a file or folder. The compressed file will have a .huf extension that has been given at the development time. We can send the compressed file over the internet so that users having this software can decompress it.

2. Decompress a file or folder: - This is the reverse process of file compression. Here we can decompress the compressed file and get the original file.

3. View files in the compressed file: - Here we can view the list of files inside our compressed file. We can view the files before decompressing and decide to decompress or not.

4. **Set icon and extension**: - This is additional feature in our project. We can set our own extension to the compressed file. More than that we can specify the style of icon for the compressed file. Users will also be given a option to change the icon as per their preference.

Introduction

Internet based communications are evolving at a tremendous rate. The Internet has facilitated the development of a worldwide 'Virtual Community' free from the constraints of time and geography. Due to the internet there is no distance between a person located in one place and experts around the globe. Through Telemedicine is becoming popular in the specialties of radiology, pathology, critical care and psychiatry, where data is in the form of image. The internet has become a hostile environment with both wired and wireless channels offering no inherent assurance of confidentiality. It is required to ensure confidentiality and security for transmitting certain multimedia data over the internet. Encryption of data has become an important way to protect data resources especially on the Internet, intranets and extranets. The another challenge in multimedia applications is the transport services to both discrete media such as text and digital images and continuous media such as audio and video with limited bandwidth and huge data size. With the huge demand for bandwidth due to the large data transmitted in multimedia applications, it becomes necessary to apply compression algorithms on transmitted data. So the best way of fast and secure transmission is by using compression as well as encryption of multimedia data. In the literature it has been seen that the dual approach of image compression & encryption is carried out in any one of the following ways based on the order of these two processes.

1. Individual or independent compression and encryption

a) Compression followed by Encryption (CE): In this sequence an intruder have less cleave to access image but encryption may again increase the size.

b) Encryption followed by Compression (EC): In this sequence size is not again increased but an intruder may have more clues to access the image. In some case sequence size decreased so not efficiently compressed.

2. Joint Compression and Encryption (JCE):

This approach is recently used which may be fast as compared to previous two but procedure is complicated. Encryption applied by different researchers by means of encrypting algorithm which encrypt the entire or partial multimedia bit sequence using a fast conventional cryptosystem . Much of the past and current research targets encrypting only a carefully selected part of the image bit stream in order to reduce the computational load, and yet keep the security level high. The encryption can be performed either using Symmetric key cryptography or by using Asymmetric key cryptography. If same key is used for encryption and decryption then

it is called as Symmetric key cryptography and if the different key is used for encryption and decryption then it is called as Asymmetric key cryptography. Image compression algorithms are used use to reduce the amount of data required to represent a digital image and the basis of the reduction process is the removal of spatial and psychovisual redundancies. Mathematically, visual data compression typically involves transforming (encoding) a 2-D pixel array into a statistically uncorrelated data set. Two types of compression are lossless compression and lossy compression. If same image can be generated from the compressed image then it is Lossless compression otherwise it is lossy compression.

PROPOSED SYSTEM

The aim of proposed system is to develop a system of improved facilities. The proposed system can overcome all the limitations of the existing system. The system provides data accuracy and save disc space. The existing system has several disadvantages and many more difficulties to work well. The proposed system tries to eliminate or reduce these difficulties up to some extent. The proposed system is file/folder compression or decompression based on the Huffman algorithm and GZip algorithm. The proposed system will help the user to consume time. The proposed system helps the user to work user friendly and he can easily do the file compression process without time lagging. The system is very simple in design and to implement. The system requires very low system resources and the system will work in almost all configurations. It has got following features Ensure data accuracy, minimize manual data entry, minimum time needed for the various processing, greater efficiency, better service.

Advantages of Proposed System:

The system is very simple in design and to implement. The system requires very low system resources and the system will work in almost all configurations. It has got following features

- Ensure data accuracy and Save disk space
- Minimum time needed for the file compression
- Greater efficiency and Better Service
- Protection from virus and Easy to send via E-mail
- Maximum Compression rate is 2 GB.
- The user need not depend on third party software's like winzip, winrar, Stuff

Existing System

Existing system refers to the system that is being followed till now. The main disadvantage of this system is that the users depend on third party software's like winzip, winrar, Stuff etc.

The existing system requires more computational time, more manual calculations, and the complexity involved in Selection of features is high. The other disadvantages are lack of security of data, Deficiency of Data accuracy, Time consuming etc.

To avoid all these limitations and make the working more accurately the system needs to be computerized.

Draw backs of Existing System:

- Lack of security of data.
- Deficiency of Data accuracy
- Time consuming.
- The users depend on third party software's like winzip, winrar, Stuff etc.