International Research Journal of Computer Science (IRJCS)
Issue 01, Volume 4 (January 2017)
ISSN: 2393-9842
www.irjcs.com

Data Compression and Encryption Technique for Secure Data Transfer

Ayyub Ali [1], Dr.Mohammad Mazhar Afzal [2]
Department of Computer Science and Engineering, Glocal University, Saharanpur

Abstract - Securing data 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. Data compression is the art of reducing the number of bits needed to store or transmit data.

Keywords- Encryption technique, Data compression, Channel Overhead, Pattern recognition.

I. INTRODUCTION

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Security goals for data security are Confidential, Authentication, Integrity, and Non-repudiation. Data compression is needed because it allows the data to be stored in an area without taking up an unnecessary amount of space. Data encryption is known for protecting information from eavesdropping. It transforms data of a given format, called plaintext, to another format, called cipher text, using an encryption key. Currently compression and encryption methods are done separately.

II. CRYPTOGRAPHY

Human being from ages had two inherent needs − (a) to communicate and share information and (b) to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. The word 'cryptography' was coined by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing.

Within the context of any application to application communication, there are some specific security requirements including: -

Authentication: *The process of providing one's identity.*
Confidentiality: *Ensuring that no one can read the message except the intended receiver.*
Integrity: *Assuring the receiver that the received message has not been altered in any way from the original.*
Non-repudiation: *A mechanism to prove that the sender really sends this message.*

There are two types of cryptographic schemes:
Symmetric (private key) cryptography and asymmetric cryptography, each of which described below:

III. SYMMETRIC OR SECRET-KEY CRYPTOGRAPHY

Symmetric algorithms are keyed algorithms where the decryption key is the same as the encryption key. These are conventional cryptographic algorithms where the sender and the receiver must agree on the key before any secured communication can take place between them.

ISSN: 2393-9842
www.irjcs.com

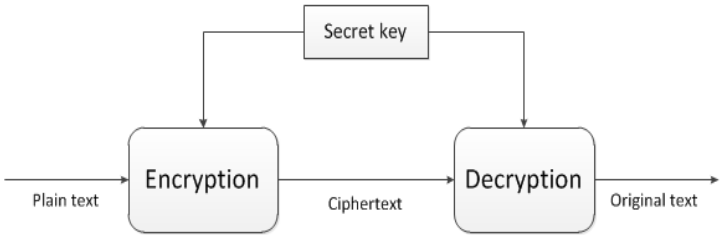

Fig.1 Symmetric Key Crypt.

There are two types of symmetric algorithms:

Block ciphers: A cryptosystem in which encryption/decryption is done on blocks of data. The full message is divided into fixed length blocks, then each block is encrypted/decrypted and the blocks are grouped to get the plaintext/ciphertext. Common block sizes are 64 and 128 bits. Examples of Block ciphers are DES and the AES.

Stream ciphers: An encryption method that uses continuous input, as opposed to fixed length blocks of data. Stream ciphers encrypt plaintext one byte or one bit at a time. Examples of Stream ciphers are RC4 cipher and the one-time pad

IV. ASYMMETRIC OR PUBLIC-KEY CRYPTOGRAPHY

Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

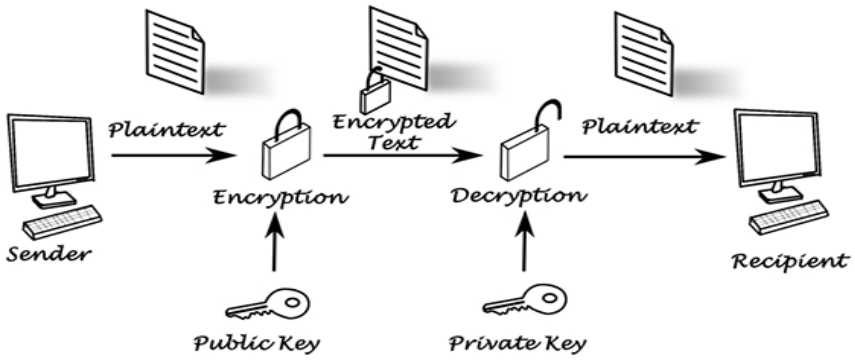

Fig. 2 Asymmetric Key Cryptography

V. COMPRESSION

The more information being dealt with, the more it costs. In spite of this, most digital data are not stored in the most compact form. Rather, they are stored in whatever way makes them easiest to use, such as:ASCII text from word processors, binary code that can be executed on a computer, individual samples from a data acquisition system, etc. Typically, these easy-to-use encoding methods require data files about twice as large as actually needed to represent the information. Data compression is the general term for the various algorithms and programs developed to address this problem. A compression program is used to convert data from an easy-to-use format to one optimized for compactness. There are different methods of encoding called: run-length, Huffman, and delta encoding. The last two are elaborate procedures that have established themselves as industry standards: LZW and JPEG.

VI. COMPRESSION-CRYPTO SYSTEM

Many systems and devices perform compression transparently, but some give users the option to turn compression on or off. Compression can be performed more than once on the same file or piece of data, but subsequent compressions result in little to no additional compression and may even increase the size of the file to a slight degree, depending on the algorithms.

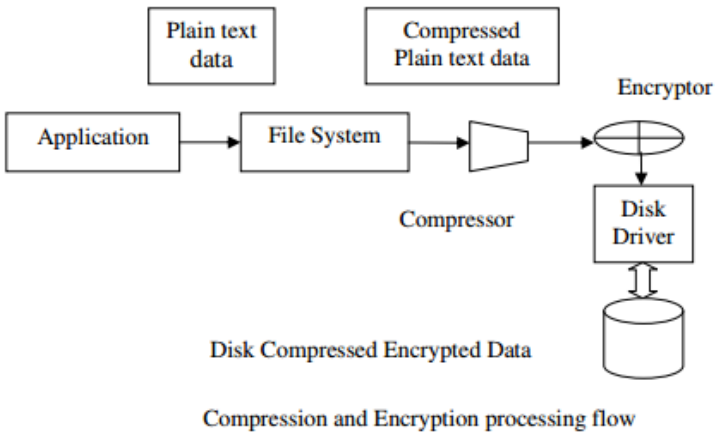

Fig. 3 Compression Crypto System

VII. LITERATURE REVIEW & RELATED WORK

A lot of works have been carried out by researchers on the concept of Enhancing Data Security through encryption and pattern matching algorithm Jayaram P, Ranganatha H R, Anupama H S [1] had suggested theaudio data hiding techniques can be used for a number of purposes other than covert communication or deniable data storage, information tracing and finger printing, tamper detection. As the sky is not limit so is not for the development. Man is now pushing away its own boundaries to make every thought possible. [2] M.Baritha Begum and Y.Venkataramani, had proposed a novel algorithm, the new compression with encryption and compression (CEC) to secure and compress the data. This algorithm compresses the data to reduce its length.

The compressed data is encrypted and then further compressed using a new encryption algorithm without compromising the compression efficiency and the information security. This CEC algorithm provides a higher compression ratio and enhanced data security. The CEC provides more confidentiality and authentication between two communication systems. [3] Chung-E Wang, had suggested cryptographic methods for concealing information during data compression processes. These include novel approaches of adding pseudo random shuffles into the processes of dictionary coding (Lampel-Ziv compression), arithmetic coding, and Huffman coding. An immediate application of using these methods to provide multimedia security is proposed. [4] Ruchita Sharma and Swarnalata Bollavarapu, had suggested to implement various cryptography algorithm for data security. The data will be first compressed using compression techniques and then encryption techniques will apply and then comparative analysis will be carried out for different combinations of compression and encryption techniques. If encryption and compression are done at the same time, then it takes less processing time and more speed. [5] Ajit Singh and Rimple Gilhotra, had suggested a scheme which uses the concept of compression and data encryption. In first phase the focus has been made on data compression and cryptography. In the next phase they have emphasized on compression cryptosystem. [6] Bobby Jasujaand and Abhishek Pandya, had proposed an algorithm which uses the compression and data encryption techniques. Firstly, data size is reduced through various compression techniques in order to increase the data transfer rate. Then the compressed data is encrypted to raise its security. Thus, technique proposed is useful in reducing data size, raising data transfer rate and providing security during communication.In the proposed system, encoded string is created from an input string of symbols and characters based on entropy encoding technique like arithmetic coding that can be used to achieve high level of compression in the present network topologies for exchange of data with more security and compression.

VIII. PATTERN MATCHING TECHNIQUE

Pattern matching is the act of checking a given sequence of tokens for the presence of the constituents of some pattern. In this proposed method, the system uses cryptographic mechanism and data compression to provide the security of the data. To ensure the safety of network, various network security measures are taken. However, numerous malicious contents, such as intrusions, viruses, spam, spyware, can still outplay firewalls by hiding themselves in the payload of packets. Many pattern or string matching architectures have been proposed in recent years for network security. Most of the researches focus on pattern matching issue for network intrusion detection and prevention system. The problem of pattern matching considers a text „T" of length „n" and a pattern of length „m" with the goal to find all the locations where the pattern matches the text. Algorithms for pattern matching have been widely studied for decades due to its broad applicability.

IX. CONCLUSION

We can study the encryption mechanism and different compression technique. This uses the pattern matching to reduce the channel overhead. By using this method, the system can reduce unwanted space and also can minimize the time required for transmission of data from source to destination.

REFERENCES

[1] Jay ram P, Ranganatha H R, Anupama H S ―INFORMATION HIDING USING AUDIO STEGNOGRAPHY A SURVEY The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011
[2] M. Baritha Begum and Y. Venkataramani- A New Compression Scheme for Secure Transmission, International Journal of Automation and Computing, 10(6), December 2013, 578-586, DOI: 10.1007/s11633-013-0756-3
[3] Chung-E Wang – Cryptography in Data Compression
[4] Ruchita Sharma and Swarnalata Bollavarapu –Data Security using Compression and Cryptography Techniques The
[5] Ajit Singh and Rimple Gilhotra - DATA SECURITY USING PRIVATE KEY ENCRYPTION SYSTEM BASED ON ARITHMETIC CODING The International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011
[6] Bobby Jasujaand and Abhishek Pandya - Crypto-Compression System: An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding, International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 21, April 2015
[7] Aman Kumar, Sudesh Jakhar, Sunil Maakar, "Distinction between Secret key and Public Key Cryptography with existing Glitches", Volume: 1, 2012.
[8] Jian L and Ligan S, Study on Chaotic Cryptosystem for Digital Image Triple Data Encryption Algorithm Modes of Operation, ANSI X9.52 - 1998.
[9] Abadi, M., and Needham, R. "Prudent Engineering Practice for Cryptographic Protocols," IEEE Transactions on Software Engineering, (22:1), 1996.
[10] D. K. Kamran Ahsan. "Practical Data Hiding in TCP/IP", Workshop on Multimedia Security at ACM Multimedia, 2002. Jain Ankit, "Steganography: A solution for data hiding"