ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Secure Data Transmission Scheme by Using Encryption Based Technique: A Review

Nikita D.Dongare [1], Prof. V.T. Gaikwad [2], Prof H.N. Datir [3]

ME Student, Department of CSE, Sipna C.O.E.T Amravati, Maharashtra, India[1]

Associate Professor, Department of IT, Sipna C.O.E.T Amravati, Maharashtra, India[2]

Assistant Professor, Department of IT, Sipna C.O.E.T Amravati, Maharashtra, India[3]

ABSTRACT: Security of data transmitted through internet has put a number of challenges. Reliability issues regarding to data transmission such as confidentiality, data security and data loss are becoming serious concerns. For overcome this problem we combine two techniques that are encryption and compression, which provides a strong backbone for its security and reduces extra overhead. In this paper, we describe the encryption mechanism, which uses the pattern matching to reduce the channel overhead and also uses the compression technique. 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. This system can maintain the security by using encryption mechanism. This scheme extends security by incorporating pattern recognition, data encryption using encryption technique, and reduces extra overhead by data compression technique.

KEYWORDS: Channel Overhead, Pattern recognition, Encryption technique, and Data compression.

I. INTRODUCTION

Nowadays communication over social media is growing vastly, so that the security level between sender and receiver must be kept secret, hence the transmission of information between end system and server can be done successfully. To maintain security this system can using the concept of cryptography, in this the system used pattern matching mechanism. The Client requires that the transmitted data should not be lost, damaged or manipulated by any unauthorized third party. Data lost can also result from network congestion due to extra overhead, so the system can reduce the overhead by pattern matching and also maintain space complexity.

The exponential growth of the internet and free accessibility to all users across the globe, security of data across Internet has become a prime concern and the increase in bandwidth transmission speed. The efficiency of the propose system will be calculated by the information loss during the transmission. This technique reduces channel overhead, reduces the information loss, and high Bandwidth requirement. It maximizes the data security during data transmission over the network.

II. LITERATURE REVIEW & RELATED WORK

Several 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.

Z. Jalil, A. M. Mirza [2], had suggested the Watermarking is an emerging research area for copyright protection and authentication of multimedia content. In this paper, a new watermarking technique is specified that uses combined image and text watermark and encryption. First we embedded a watermark in to text using the algorithm described previously. After embedding watermark into text, a watermark key is generated. Then we encrypted the text with RSA. This provides an additional level of security for text documents. Later the cipher text is decrypted and watermark is extracted. Then extracted watermark is compared with original watermark to prove authenticity.

X. Zhou, Z.Wang,W. Zhao,S. wang,[3] had worked on the Security Theory and Attack analysis for Text Watermarking, Security problems with text watermarking are greatly completely different from those of alternative multimedia system watermarking, in terms of its specific needs and characteristics of text watermarking. the protection

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

theory of text watermarking is projected during this paper, and therefore the following security topics are discussed: (i) the classification and application of text watermarking; (ii) the classification and analysis of attacks; (iii) the watermarking model and security countermeasures.

J. K. Pal; J. K. Mandal [4], were introduced Random Block Length Based Cryptosystem through Multiple Cascaded Permutation Combinations and Chaining of Blocks,In this paper a four stage character/bit level cryptography technique (RBCMCPCC) has been projected, wherever the primary 3 steps take input block of length 128 bit, 192bit and 256 bit, separately, and develop intermediate blocks of identical lengths exploitation identical lengths of keys in every step. The fourth stage generates final cipher blocks supported random session-keys.

U. Mehta; K.S. Dasgupta; N.M. Devashraye,[5] had worked on the Survey of Test Data Compression Technique Emphasizing Code Based Schemes, As a results of the emergence of recent fabrication technologies and style complexities, commonplace stuck-at scan tests aren't any longer spare. the amount of tests and corresponding information volume increase with every new fabrication method technology.

Ning; Z. Jie,[6] had worked on A multipurpose audio watermarking scheme for copyright protection and content authentication To make digital audio watermarking accomplish each copyright protection and content authentication with localization, a unique utile watermarking theme is projected during this paper.

L Hemme; L. Hoffmann, [7] had suggested that the Differential Fault Analysis on the SHA1 Compression Function, In FDTC 2009, Li et al. printed a DFA attack against the biracial block cipher SHACAL1.This block cipher well consists of the compression operate of the hash operate SHA1 aside from the ultimate addition operation. SHA1 compression operate as a primitive in an exceedingly keyed hash operate like HMAC-SHA1 or in an exceedingly key derivation operate it'd be of some interest if the attack of Li et al. additionally applies to the SHA1 compression operate.

M.A.D.Suarjaya,[8]"A New Algorithm for Data Compression Optimization" **:** In this paper the author propose a new algorithm for data compression, called j-bit encoding (JBE). This algorithm will manipulates each bit of data inside file to minimize the size without losing any data after decoding which is classified to lossless compression. This basic algorithm is intended to be combining with other data compression algorithms to optimize the compression ratio. The performance of this algorithm is measured by comparing combination of different data compression algorithms. This paper proposes and confirms a data compression algorithm that can be used to optimize other algorithm. An experiment by using 5 types of files with 50 different sizes for each type was conducted, 5 combination algorithms has been tested and compared. This algorithm gives better compression ratio when inserted between move to front transform (MTF) and arithmetic coding (ARI). Because some files consist of hybrid contents (text, audio, video, binary in one file just like document file), the ability to recognize contents regardless the file type, split it then compresses it separately with appropriate algorithm to the contents is potential for further research in the future to achieve better compression ratio.

M. Sharma, [9]"Compression Using Huffman Coding" **:** In this paper, the author has analyzed Huffman algorithm and compare it with other common compression techniques like Arithmetic, LZW and Run Length Encoding. The author has concluded that arithmetic coding is very efficient for bits and reduces the file size dramatically.RLE is simple to implement and fast o execute. LZW algorithm is better to use for TIFF, GIF and Textual Files.

Shanmugasundaram and R. Lourdusamy,[10] “A Comparative Study of Text Compression Algorithms” : There are lot of data compression algorithms which are available to compress files of different formats. This paper provides a survey of different basic lossless data compression algorithms. Experimental results and comparisons of the lossless compression algorithms using Statistical compression techniques and Dictionary based compression techniques were performed on text data. Among the statistical coding techniques the algorithms such as Shannon-Fano Coding, Huffman coding, Adaptive Huffman coding, Run Length Encoding and Arithmetic coding are considered.

III. DATA HIDING AND STEGANOGRAPHY

Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. The art of concealing the original information within the other information is known as Steganography [11][12]. It can be further categorized into three types such as

- Format based.
- Random and
- Statistical generations and linguistic method [13].

Water marking is one of the examples of this approach. Steganography and cryptography are closely related. Cryptography scrambles messages so it can’t be understood. Steganography on the other hand, hide the message so

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

there is no knowledge of the existence of the message. The message in Steganography may or may not be encrypted. If it is encrypted, then a cryptanalysis technique is applied to extract the message.

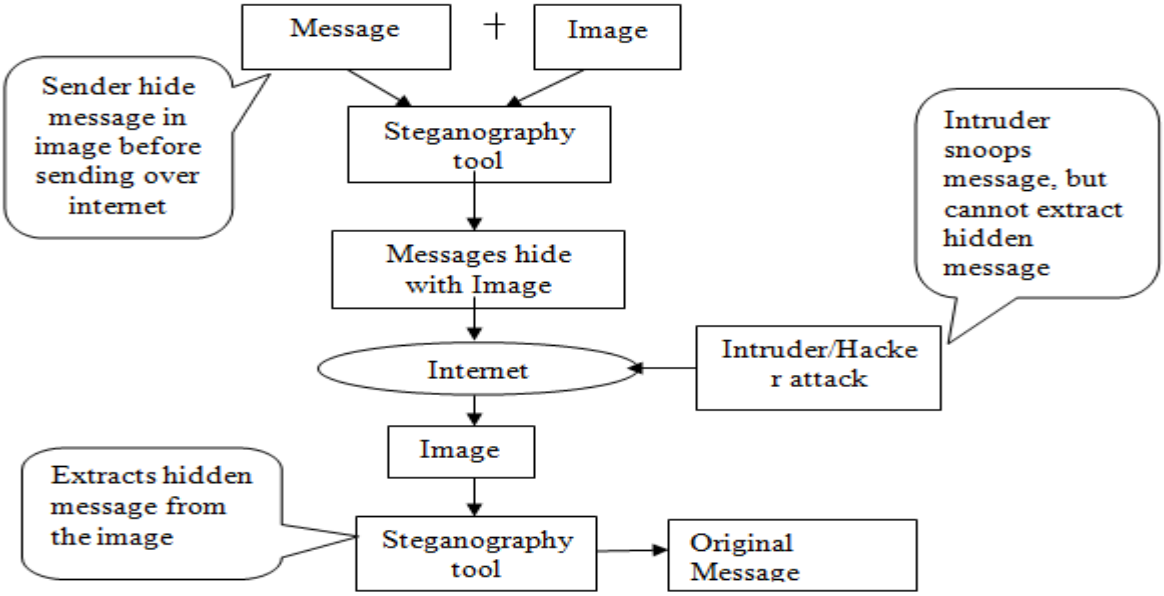

Fig.1 Steganography on an Internet

➢ Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.

➢ It is also possible to simply use Steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source.

➢ Steganography can also be used to implement watermarking. The main difference is on intent, while the purpose of Steganography is hiding information.

➢ E-commerce allows for an interesting use of Steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder.

➢ Paired with existing communication methods, Steganography can be used to carry out hidden exchanges.

➢ The transportation of sensitive data is another key use of Steganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see one. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them.

IV. CRYPTOGRAPHIC MECHANISM

It is the art of protecting information by transforming or encrypting it into an unreadable format, called cipher text .The secret key is used to decrypt the message into plain text. It can be classified into two types, including,

- Public-key cryptography
- Private-key cryptography [14].

In public key cryptography two keys are used, one for encryption and another for decryption while in the private key cryptography, the single key is used for both encryption and decryption .It is also called as asymmetric & symmetric key [15].

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

The purpose of a cryptographic mechanism is to provide a security function in a given environment and in combination with other mechanisms .The minimum size of symmetric keys to be used until 2010 is 80 bits. The minimum size of symmetric keys to be used beyond 2010 is 100 bits. The minimum recommended size of symmetric keys is 128 bits. The use of keys containing fewer than 80 bits would appear to be risky. 56-bit keys are clearly insufficient and it is generally accepted at the moment that 64-bit keys can be attacked, although not everyone can make such a computation. However, such attacks have been made, specifically in the public environment. Management of keys is a quite separate problem that is sometimes just as complex as determination of encryption and integrity algorithms. Therefore, this problem is dealt with in a document dedicated to it. This document is entitled "Management of cryptographic keys – Rules and recommendations for management of keys used in cryptographic mechanism".

V. PATTERN MATCHING TECHNIQUE

Pattern matching is a procedure to check a perceived sequence of tokens for the presence of constituents of some predefined pattern. In this proposed technique, the system use cryptographic mechanism, pattern generation and matching technique to provide security confidentiality, and integrity. This system can introduce the scheme to provide better security, by finding the weakness of existing techniques. Computer network has become an essential part of our daily life. To ensure the safety of network, various network security measures are taken. Being the most widely deployed one, firewall ensures information transfer from trusted sources to destinations by inspecting the packet headers.

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. Lately, researchers started to look at this problem in the context of secure two-party computation due to growing interests in private text search. In this setting, one party holds the text whereas the other party holds the pattern and attempts to learn all the locations of the pattern in the text (and only that), while the party holding the text learns nothing about the pattern.

➢ Need of Pattern Matching

Pattern matching is the process of checking a perceived sequence of string for the presence of the constituents of some pattern. In contrast to pattern recognition, the match usually has to be exact. Pattern matching concept is used in many applications Following figure shows the different application.

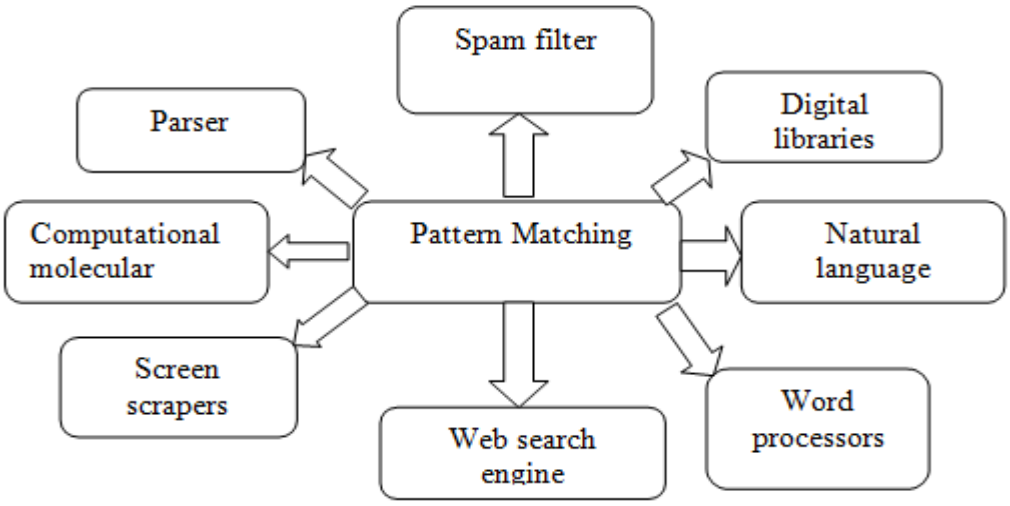

Fig.2 Applications of Pattern Matching

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

The patterns generally have the form sequences of pattern matching include outputting the locations of a pattern within a string sequence, to output some component of the matched pattern, and to substitute the matching pattern with some other string sequence (i.e., search and replace).

VI. CONCLUSION & FUTURE SCOPE

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. This technique reduce channel overhead, reduce the information loss, and high bandwidth requirement. It maximizes the data security during data transmission over the network. This is the main advantage of this approach. As the compression technique reduces the output file in very small size, so the channel overhead will be significantly low.

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. Z. Jalil, A. M. Mirza ,"Text Watermarking Using Combined Image-plus-Text Watermark" , IEEE, 2010
3. X. Zhou, Z..Wang,W. Zhao,S. wang,"Performance Anlysis and Evaluation of Text watermarking", IEEE, 2009
4. J. K. Pal; J. K. Mandal, "A Random Block Length Based Cryptosystem through Multiple Cascaded Permutation Combinations and Chaining of Blocks," December 2009
5. U. Mehta; K.S. Dasgupta; N.M. Devashraye, "Survey of Test Data Compression Technique Emphasizing Code Based Schemes," Aug. 2009.
6. C. Ning; Z. Jie, "A multipurpose audio watermarking scheme for copyright protection and content authentication," June 2008
7. L. Hemme; L. Hoffmann, "Differential Fault Analysis on the SHA1 Compression Function," Sept. 2011
8. M.A.D. Suarjaya, "A New Algorithm for Data Compression Optimization", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 8, 2012, pp.14-17
9. M. Sharma, "Compression using Huffman Coding " IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010
10. S. Shanmugasundaram and R. Lourdusamy, "A Comparative Study of Text Compression Algorithms" International Journal of Wisdom Based Computing, Vol. 1 (3), December 2011
11. Dauneria; K. Indu, "Encryption Based Data Hiding Architecture with Text Pattern and Authentication Verification," Computer and Information Technology Workshops, 2008. CIT Workshops 2008. IEEE 8th International Conference on, vol., no., pp.236-241, 8-11 July 2008
12. W. Jinwei; L. Guangjie; L. Shiguo, "Security Analysis of Content-Based Watermarking Authentication Framework," Multimedia Information Networking and Security, 2009. MINES '09. International Conference on, vol.1, no., pp.483-487, 18-20 Nov. 2009
13. C. Ning; Z. Jie, "A multipurpose audio watermarking scheme for copyright protection and content authentication," Multimedia and Expo, 2008 IEEE International Conference on, vol., no., pp.221-224, June 23 2008-April 26 2008
14. J. K. Pal; J. K. Mandal, "A Random Block Length Based Cryptosystem through Multiple Cascaded Permutation Combinations and Chaining of Blocks," Fourth International Conference on Industrial and Information Systems, ICIIS 2009, 28–31December2009, SriLanka.
15. Y. Ji; K. Hongbo, "FPGA implementation of dynamic key management for DES encryption algorithm," Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011International Conference on , vol.9, no., pp.4795-4798, 12-14 Aug.2011