_____

Review On : A Secure Encryption approach for Textual Data Transmission

Anagha P. Zele
Student of Master of Engineering (CSE)
Raisoni College of Engineering and
Management
Amravati, India
anaghazele12@ gmail.com

Prof. Nitin R. Chopde
P.G. Co-ordinator of CSE
Raisoni College of Engineering and
Management
Amravati, India
Nitin.chopade@raisoni.net

Prof. Dinesh S. Datar
Assistant prof of (IT)
Raisoni College of Engineering and
Management
Amravati, India
Dinesh.datar@raisoni.net

Abstract— Secure data transfer is the most important concern in today's world. Data in transit is always in danger of getting compromised Communication of information over the Internet is rapidly increasing due to the availability of the Internet and increase in transmission speed. However, confidentiality, data security, reliability issues regarding to data transmission such as , data loss are becoming serious concerns. To fulfill the need of secure transmission of text data, we proposed algorithm in next paper. Secure data transfer is the most important concern in today's world. Data in transit is always in danger of getting compromised.

_____*****_____

I. INTRODUCTION

Communication of information over the Internet is rapidly increasing due to the progression of higher availability of the Internet and the increase in bandwidth transmission speed.However, reliability issues regarding to data transmission such as confidentiality, data security and data loss are becoming serious concerns [19]. The Client requires that; the transmitted data should not be lost, damaged or manipulated. Our objective of this paper is to provide an integrated mechanism which can resolve security issues, To hide the large amount data behind the image. This work also useful to reduce the length of key file. To create unbreakable wall forstegnalyzer while extracting the secret data. To provide security to hidden message from unauthorized accesses. The transmission of digital multimedia products via internet is getting more and more popular. In that proposed method used the steganography technique to maintain the secrecy of data to hide a secret message within a cover-media and generate key for that hidden data in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another"[15]. Such as image, video, audio or text to establish secret communication between trusting parties and conceal the existence of embedded data. .

.The main objective of data hiding is to communicate securely in such a way that the true message which is embedded in any one of the digital media is not visible to the observer. That is unwanted parties should not be able to distinguish in any sense between cover-text. Steganography is used in various data hiding applications especially in intellectual property, military, personal and diplomatic applications. Various techniques used to perform steganography are available. The most popular ones are invisible inks, digital signatures, character arrangements, microdots, spread spectrum communications and covert channels. These days Steganography has moved towards digital hiding with the advancement in computer and network technologies. It provides high usability communication channels for steganography. A number of digital technologies namely movie images, text files, audio and still images that are used for digital steganography are available.[11] A secret key or stego key is required for embedding process. Stego object should look almost identical to cover message with hidden secret message present inside it. The decoding process includes interpolation of Stego object into the decoding system. The stego key is used to decodeand find the secret message.is called stego message. The stego message is transmitted over the public channel. The receiver gets the message and retrieves the message using the stego key which is same as used by the sender. In the cryptanalysis it is clear that the intercepted message is encrypted and it certainly contains the hidden message because the message is scrambled. But in the case of steganalysis this may not be true. The suspected media may or may not be with hidden message.

II. LITERATURE SURVEY

In this paper the Indra Raj Sharma andVipin Gupta proposed the performance in terms of delay, power and area of DES and Simplified DES analysed using Cadence Encounter RTL Compiler. The design analysis of Simplified DES shows leakage power is 568nW and Transition power is 169186.883nW, so the total power is 169755.035nW, the delay is 3422ps and dies area 1468μm2 on 130nm Process Technology. It is more satisfactory options for both algorithm in terms of utilization and the speed of execution[13]

In this paper the Rajashekarappa, and Dr. K M SunjivSoyjaudah proposed The SDES is a simple encryption algorithm, this is a promising method and can be adopted to handle other complex block ciphers like DES and AES[6]

In this paper, the Vimalathithan.Rand Dr.M.L.Valarmathi proposed the Genetic Algorithm for the cryptanalysisof Simplified Data Encryption Standard is presented. Thetime complexity of the proposed approach has beenreduced drastically when compared to the Brute-Forceattack. Though SDES is a simple encryption algorithm,this is a promising method and can be adopted to handleother complex block ciphers like DES and AES. The costfunction used here can be applied for other block ciphers also.[3]

In this paper the RupaliGawade, PriyankaShetye, VaibhaviBhosale and P N. Sawantdesai proposed the Steganography is a fascinating and effective method ofhiding data that has been used throughout history.Methods that can be employed to uncover such devious

tactics, but the first step are awareness that such methods even exist. There are many good reasons as well to use this type of data hiding, including watermarking or a moresecure central storage method for such things as passwords, or key processes. Regardless, the technology is easy to use and difficult to detect.[18]

In this Paper the Sheelu proposed Steganography not only prevents others from knowing the hidden information, but it also prevents others from thinking that the information even exists. If a Steganography method causes someone to suspect there is a secret information in a carrier medium, then the method has failed. Different file formats can be used as carrier in Steganography. Embedding secret information in an audio file is usually a more difficult process than embedding messages in other media. Audio Steganography methods can embed messages in WAV, AU, and even MP3 sound files. As we will hide 4 bits of secret information in each byte of the carrier. This will enhance the capacity of carrier and carrier will conceal a large amount of secret information[12]

In this paper the SouvikBhattacharyya ,PabakIndu , SanjanaDutta , AyanBiswas and GautamSanyal presented a novel approach of English text steganography method which is the improved version of the CALP. Stego text is generated by mapping each two bit of the binary sequence of the secret message through small texture/pattern changes of some alphabets of the cover text in order to achieve high level of security the CALP method generates the stego text with minimum or zero degradation as both the Jaro score and Correlation-coefficient value is very high.[4]

In this paper the ChintanDhanani and KrunalPanchal presents the stegnography techniques , because of increasing amount of security threats protection of data is required. Steganography provides security of information by hiding it in carrier. This survey paper includes the classification of steganography techniques and techniques that already been implemented to hide information in web documents. Data hidden in the web document is less suspicious in compare of other carriers because HTML WebPages are now a routine part of everyone‟s life and html document contains the considerable number of tags, attributes & other elements in which data can be hidden. We can hide information in HTML, CSS, XML, JavaScript etc. So we have more options to secure the information.[17]

In this paper the P. N. Kulkarni and P. C. Pandey proposed Multi-band frequency compression is a speech processingtechnique for improving speech intelligibility under adverse listening conditions. For use in this processing, three frequency-mapping schemes, i.e. sample-to-sample mapping, mapping by superimposition of spectral samples, and segment mapping schemes were investigated. Segment-mapping scheme achieved desired compression retaining the spectral distribution of energy, and without introducing irregular variations. The scheme needs to be further evaluated using different test materials, larger number of subjects, and different listening conditions.[1]

In this paper the Hamid Mirvaziri, KasmiranJumariMahamod Ismail and ZurinaMohdHanapi proposed the MRVLK is efficiently implemented and resistedagainst known attacks because of changing the key andblock size in each round where the key generation is anindependent process and time variant so it is reliable,fast, complex and hard enough to resists againstexisting attacks and can implement where there arespeed and memory constraints. Differential related keyattack is based on key relation so there is no chance ofgaining the key by using this method.[4]

III. PROPOSED SYSTEM

Our proposed scheme is initially encrypt the original data and hide the secured data into the original data to provide the security the hide data and compression is done to reduce the key size .The proposed model has been depicted in Fig.1 to demonstrate its flow

_____

FIGURE 2.DFD FOR DATA ENCRYPTION

FIGURE 2. DFD FOR DATA EXTRACTION

REFERENCES

[1]   P. N. Kulkarni and P. C. Pandey, "Frequency Mapping for Multi-band Frequency Compression for Improving Speech Intelligibility", Proc. 14th National Conference on Communications 2008 (NCC 2008), Bombay, India.

[2]   L. Y. POR1, B. Delina2, "Information Hiding: A New Approach in Text Steganography" , 7th WSEAS Int. Conf. on APPLIED COMPUTER & APPLIED COMPUTATIONAL SCIENCE (ACACOS '08), Hangzhou, China, April 6-8, 2008

[3]   Vimalathithan.R, Dr.M.L.Valarmathi, "Cryptanalysis of S-DES using Genetic Algorithm", International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009.

[4]   Hamid Mirvaziri, KasmiranJumariMahamod Ismail and ZurinaMohdHanapi , "Message Based Random Variable Length Key Encryption Algorithm" Journal of Computer Science 5 (8): 573-578, 2009 ISSN 1549-3636

[5]   Souvik Bhattacharyya, PabakIndu2,SanjanaDutta ,Ayan Biswas4and GautamSanyal, "Text Steganography using CALP with High Embedding CapacitySouvik", Journal of Global Research in Computer Science Volume 2, No. 5, May 2011.

[6]   SimarPreet Singh, and Raman Maini , "COMPARISON OF DATA ENCRYPTION ALGORITHMS" , International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011,

[7]   Rajashekarappa, Dr. K M SunjivSoyjaudah, "Comparative Cryptanalysis of Simplified-Data Encryption Standard Using Tabu Search and Simulated Annealing Methods" , International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN : 2278-800X, www.ijerd.com Volume 5, Issue 3 (December 2012), PP. 07-12 7.

[8]   YoussefBassil, "A TWO INTERMEDIATES AUDIO STEGANOGRAPHY TECHNIQUE", Journal of Emerging Trends in Computing and Information Sciences (CIS), ISSN: 2079-8407, Vol. 3, No.11, November 2012

[9]   S.S. Divya, M. Ram Mohan Reddy, "HIDING TEXT IN AUDIO USING MULTIPLE LSB STEGANOGRAPHY AND PROVIDE SECURITY USING CRYPTOGRAPHY" , INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 1, ISSUE 6, JULY 2012 ISSN 2277-8616

[10] Pandurangarao N. Kulkarni , Prem C. Pandey ,, Dakshayani S. Jangamashetti, "Multi-band frequency compression for improving speech perceptionby listeners with moderate sensorineural hearing loss" , Speech Communication 54 (2012) 341–350

[11] Lavkush Sharma1, Bhupendra Kumar Pathak2 and NidhiSharma3 , "Breaking of Simplified Data Encryption Standard Using Binary Particle Swarm Optimization" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012 ISSN (Online): 1694-0814

[12] RoopamBamal, Dr.V.P Singh Kaushal, "STEGANOGRAPHY: A MODERN DAY ART AND SCIENCE FOR DATA HIDING", International Journal of Latest Research in Science and Technology ISSN
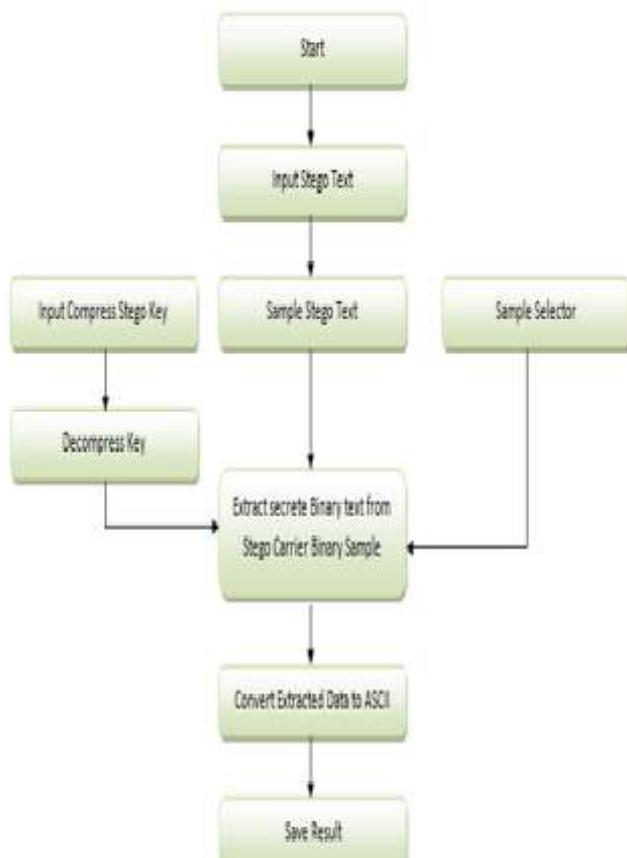
20

_____

(Online):2278-5299Volume 2,Issue 4 :Page No.9-14, July - August (2013).

[13] Sheelu, " Enhancement of Data Hiding Capacity in Audio Steganography" , IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 3 (Jul. - Aug. 2013), PP 30-35.

[14] Indra Raj Sharma1, Vipin Gupta2, "Comparative Analysis of DES and S-DES Encryption Algorithm Using Verilog Coding",

[15] Gurpreet Singh, Supriya , "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security" , International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013

[16] SoumyenduDas,Subhendu Das, "Steganography and Steganalysis: Different Approaches".

[17] W. Bender,D. Gruhl,N. Morimoto,A. Lu, "Techniques for data hiding" , IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996.

[18] ChintanDhanani, KrunalPanchal, "Steganography using web documents as a carrier: A Survey", Steganography using web documents as a carrier: A Survey | ISSN: 2321-9939.

[19] RupaliGawade, PriyankaShetye, VaibhaviBhosale, P N. Sawantdesai, "Data Hiding Using Steganography For Network Security", International Journal of Advanced Research in Computer and Communication EngineeringVol. 3, Issue 2, February 2014.

[20] Shiladitya Bhattacharjee1, Lukman Bin Ab. Rahim2, Izzatdin B A Aziz, " A Secure Transmission Scheme for Textual Data with Least Overhead", 978-1-4799-2361-8/14/$31.00 ©2014 IEEE.

Author Profile

Anagha P. Zele received the BE from SGBAU Amravati University and pursuing ME (CSE) From G. H. Raisoni College of Engineering & Management, Amravati. Her Research interest include Network security.

Prof. Nitin R. Chopade He is currently an Assistant Professor with the G.H Raisoni College of Engineering and Management, Amravati SGBAU Amravati University.

Prof. Dinesh S. Datar He is currently an Assistant Professor with the G.H Raisoni College of Engineering and Management, Amravati SGBAU Amravati University.