International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 1, Issue 1, November 2014

Web Based Communication Using Text Steganography

[1]Mr. M.Hareesh Babu,[2]Ms.M.Bharghavi
[1]M.TECH (CNIS) Scholar [2]Assistant Professor
[1][2]Department of Computer Science and Engineering,
Sree Vidyanikethan Engg College, Tirupathi, Andhra Pradesh, India
[1]police.max11@gmail.com,[2]bhargavisvec@gmail.com

Abstract- **with the increase in Internet Technologies, great amount of information is following electronically everyday over the network. Information security is a way to protect information against its confidentiality, reliability and availability. Hiding exchange of information is an important factor in the field of security. Cryptography and Steganography are two very important methods for this purpose and are both used to ensure data confidentiality. In Steganography a cover media is used to hide the existence of data where cryptography is used to protect information by transferring plain text into cipher text. Here we discusses some proposed methods, implementations of different embedding techniques and two different ways for hiding data and also a comparative analysis is made based upon some security variables. Text Steganography is applied on XML files and is further encrypted using a cryptographic algorithm.**

***Keywords*— Steganography, Cryptography, Encryption, Decryption, Cipher text, Plaintext**

I. INTRODUCTION

Secret communication has been a subject of interest for ages. With the vast expansion of Internet, massive web based information is travelling every day and securing data is a very important subject in this matter. For security reasoning, many different methods have been implemented and new methods are evolving every day. Cryptography, Steganography and Watermarking are well known ways of securing information but they all work under different mechanisms. Cryptography makes data unreadable by writing into secret code and it ensures authentication, confidentiality and integrity. Steganography hides the existence of data and it ensures transparency, robustness and capacity. Whereas, watermarking technique provides evidence for the intellectual property rights over certain content by hiding some information in it.

II. EXISTING SYSTEM

In the existing system we use the HTML file for carrying the input which is send to the receiver from the sender and the secret message is embedded by using the text-Steganographic techniques. Here we use the DES algorithm to perform cryptography. By this we encrypt the

data by the 64-bit key. Then perform embedding on the encrypted message into the html file. The resultant data is kept in a secure web page and is transferred through a communication channel.

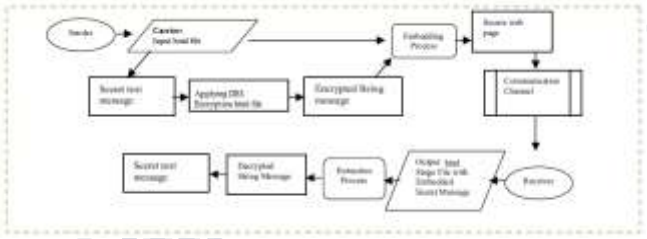

Fig.1.Existing system using DES

Disadvantages of Existing System:

HTML:

- In HTML there are no user defined tags.
- It cannot produce dynamic output alone, since it is a static language.
- Security features offered by HTML are limited.

DES :

- The 56-bit key size is the biggest defect of DES. Hardware implementations of DES are very fast. DES was not designed for software and hence runs relatively slowly

III. PROPOSED SYSTEM

In the proposed system we use the XML file as a carrier for carrying the secret message which is send to the receiver from the sender and that secret message is embedded by using the text-Steganography techniques. Here we use the AES (Advanced Encryption Standard) algorithm to perform cryptography. In this we encrypt the data by using a key of 256-bit length. Then we perform embedding process on the encrypted message to store it in an xml file.

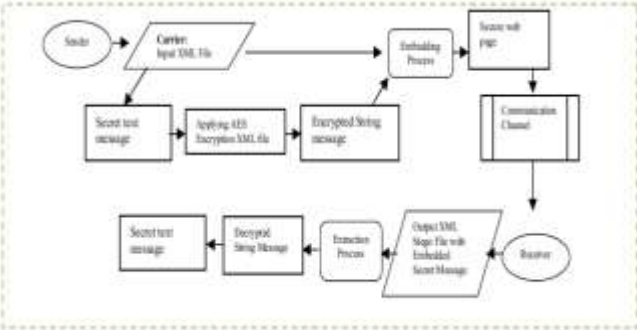

Fig.2.Proposed system using AES

Advantages of Proposed System:
XML file:

- It is a platform independent language.
- It is as easy as HTML.

AES algorithm:

- Advanced Encryption Standard not only assures security but also improves the performance in a variety of settings such as smartcards, hardware implementations etc.
- AES is federal information processing standard and there are currently no known non-brute-force direct attacks against AES.

Crypto module:

In crypto module we perform encryption and decryption. That is, encryption is done at the sender side and decryption is done at the receiver side.

- Encrypting: The secret message which sender wants to send is encrypted using the Advanced Encryption Standard (AES) algorithm.
- Decrypting: The received encrypted text which is in binary form is decrypted using the AES algorithm.

Steno module:

In steno module we perform embedding and extraction process. That is, embedding is done at the sender side and extraction is done at the receiver side.

- Embedding: In embedding process we apply the text Steganography techniques on xml file based on the cipher text that is obtained from AES algorithm.
- Extraction: This is the reverse process of Embedding at the receiver side in order to extract the cipher text from the xml file and that cipher text is given as input to the AES decryption algorithm.

Transmission module:

This module is used to send the xml file which is embedded using text Steganography techniques at the sender side and to receive that xml file at the receiver side. Here the sender has to give the path of the xml file in order to send it to the receiver and the receiver has to give path to store the received xml file.

IV. RESUITS

By creating a text file which contain plain text and here we named it as p.txt and the data which is written in it is the secret message which is to be transferred to the receiver. When we run the embedding process program, it asks for the plain text file path. We should specify the correct path. It takes the plain text present in that file and converts it into the cipher text. It displays cipher text and the length of the cipher text. If we give wrong path as input then it displays an error message saying that file does not exist and stops the execution process.

V. CONCLUSION & FUTURE ENHANCEMENTS

We have presented Text Steganography combined with Cryptography for hiding secret information using XML file to provide more security. There are nine different embedding techniques for the text Steganography, studied and applied on XML file. System has been implemented using java language for all nine methods combined with AES which has added another layer of security. All methods are measured with respect to different standards and it is analyzed that white space method, white space replacement method, color replacement method, line break method, synonyms method and acronyms methods are considered stronger and less vulnerable. Furthermore, improvements in color, synonyms and acronyms are needed to make them more practical, efficient and stronger. Techniques discussed in our project have therefore been applied on textual information and hence could also be applied on other types of data in XML files, as XML does not only contain text but multimedia based information as well and the idea could be extended toward other parts.

REFERENCES

[1] Shingo, Kyoko, Ichiro, Osamu, “A Proposal on Information Hiding Methods using XML”, Mitsubishi Research Institute, Communication Research Laboratory, Yokohama National University and The University of Tokyo.

[2] Mohammad Laheen, Sun XingMing, "Techniques with Statistics for Web page Watermarking" 2005, NSFC No.60373062

[3] Aasma, Sumbul, Asadullah, "Steganography: A New Horizon for Safe Communication through XML", 2005.

[4] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[5]http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf

BIOGRAPHY

Mr.M Hareesh Babu is a M.Tech Scholar in the Computer Science & Engg Department, Sree Vidhyanikethan Engg College. He received Bachelor of Technology (I.T) degree in 2012 from JNTUA, Ananthapur,Andhra Pradesh, India. His research interests are Computer Networks (wireless Networks), HCI, Algorithms, web 2.0 etc.

Ms.B.Bargavi is a assistant professor in the Computer Science & Engg Department, Sree Vidhyanikethan Engg College. She received Master of Technology (CNIS) degree in 2012 from JNTUA, Ananthapur,Andhra Pradesh, India. Her research interests are Computer Networks (wireless Networks), Algorithms, Database Management Systems etc.