Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 3, March-2017

A Survey on Steganography and Different Types

Twinkal J. Patel[1], Chandresh D. Parekh[2]

[1]*Cyber Security Dept., Raksha-Shakti University*
[2]*Cyber Security Dept., Raksha-Shakti University*

ABSTRACT : The use of internet has grow rapidly form last few year. This growth has increased the demand for techniques that can ensure information security. The Feature of information hiding has received much attention in the recent years as security of information has become a big concept in this internet era. We are also surrounded by a world of secret communication, where human of all types are transmitting information as innocent as an encrypted credit card number to an online-transaction and as insidious as a terrorist plot to hijackers. Steganography is a technigue where information theory, spread spectrum, and cryptography technologies are brought together to satisfy the need of privacy for Internet. Security of data is a challenging issue and transmitting the Secured data is again most challenging. Data hiding from intruders and also hiding the fact that any data is hidden is one of the techniques to hide the data in a secure manner called Steganography. In this paper I have analalyze steganography and its types, its uses, how it is different from cryptography and Model of Steganography.

KEYWORDS – Steganography,Cryptography,Types,Steganalysis.

I.INTRODUCTION

The internet is a large collection of networks. It is connects places all over the world. Internet is the rapidly growing technologies in the present time. This growth has focused attention on one of the important aspect of internet viz. information security.Internet is a public network, secure the information on internet is very important. Various techniques including cryptography, steganography etc are used to secure data on the internet. Cryptography *is a* method of storing and transmitting data in a particular form , such that it is not understandable to anyone other than the intended sender and recipients.cryptography are both ways to secure information from unwanted parties but neither technology alone is perfect and can be compromised. Steganography is the technique that hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused data in regular files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information, such that the existence of information is concealed to everyone except for the intended sender and receiver. The strength of steganography can amplified by combining it with cryptography.

II.STEGANOGRAPHY TYPES

Steganography can be broadly classified into Five types on the basis of the type of the cover media used viz. text steganography, image steganography, audio,video and Protocol steganography.

Image steganography : A steganography technique that uses images as the cover media is called an image steganography. images are the mostly used among other types of steganography. Many different image file formats exist, most of them for specific applications. The conventional image steganography algorithm is LSB embedding algorithm.

All Rights Reserved, @IJAREST-2017

Audio steganography: A steganography technique that uses audio as the cover media is called an audio steganography. It is the most challenging task in steganography. This is because the human auditory system has a large dynamic range that it can listen over.

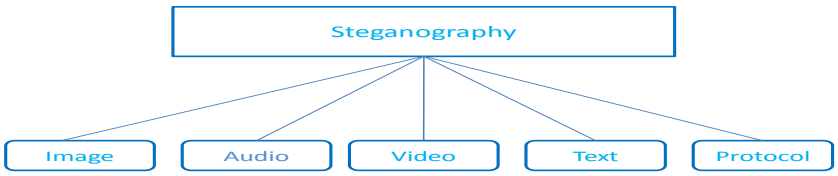

Fig 1.Types Of Steganography

Video Steganography : This technique is uses video as a cover media so it is called video steganography.The Video file should be undetectable by attacker.

Text steganography : Text Steganography is uses text as the cover media so it is called a text steganography. Text files have a very small amount of redundant data to hide a secret message. So it is difficult type of steganography.

Protocol Steganography: Protocol steganography is the technique of embedding information within messages and network control protocols used in network transmission.
A network packet has packet headers, user data and packet trailers. So during some of the layers of the network model, steganography can be used When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography.

III.COMPARISON OF STEGANOGRAPHY AND CRYPTOGRAPHY

Steganography and cryptography are closely related. Cryptography is the converts plain text into cipher text so it can't be understood and Steganography hide the message so there is no knowledge of the existence of the message. Cryptography is given the cipher text as final result, while steganography is the stego-media.Steganography and cryptography are both ways to protect data from unwanted parties but neither technology alone is perfect. The strength of Steganography can be amplified by combining it with cryptography.

IV.STEGANOGRAPHY MODEL

Steganographic system has a cover file that is used to cover the original message and the steganography algorithm to carry out the required object as shown in Fig. 2. The result is a stego-file which has the message inside it, hidden. This file is then sent to the receiver where the receiver retrieves the message by applying the de-steganography. The goal of modern steganography is to keep the message undetectable.

There are carriers below to be the cover-object

1. Network Protocols TCP, IP and UDP
2. Audio that using digital audio format like wav, midi, avi, mpeg, mpi and voc
3. File and Disk that can hides and append files by using the slack space
4. Text such as null characters,like morse code including html and java

All Rights Reserved, @IJAREST-2017

5. Images file bmp, gif and jpg, where they can be both color and gray-scale.

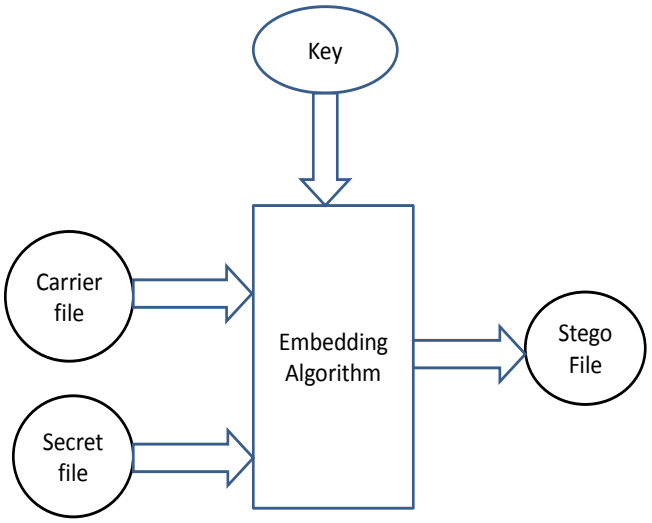

Fig 2. Steganography Model

V.USES OF STEGANOGRAPHY

Steganography can be used for digital watermarking, ecommerce, and the transport of sensitive data.Digital watermarking involves embedding hidden image or file to show ownership.This is useful for protecting copyright of the owner. In current e-commerce transactions, most users are protected by a username and password.But there is no real method of verifying that the user is the actual card holder. In Biometric finger print scanning,combined with unique session IDs embedded into the fingerprintimages via steganography, allow for a very secure option to open ecommerce transaction verification.Paired with existing communication methods, steganography can be used to carry out hidden exchanges. Governments are used two types of hidden communications: those that support national security and those that do not. Digital steganography provides vast potential for both types. Businesses may have similar concerns regarding new product information.

VI.TYPES OF ATTACKS

Attacks on hidden information may take several forms: detect,extract, and disabling, destroy or modify hidden information or data.

The possible attacks on a stego media can be one of the following:
1.Stego-only attack:
Only the stego-object is available for analysis.
2.Known carrier attack:
the original cover, object and stego object are both available.
3.Known message attack:
A message is known.
4.Chosen stego attack:

All Rights Reserved, @IJAREST-2017

The steganography tool (algorithm) and stego-object are known.
5.Chosen message attack:
The steganalyst obtains a stego-object from steganography algorithm of a chosen message.This attack is intended to find patterns in the stego-object that may point to the use of specific steganography tools or algorithms.
6.Known stego attack:
The stegonography algorithm is known and both the original and stego-object are available.

VII.COMBINATION OF STEGANOGRAPHY AND CRYPTOGRAPHY

The steganography and cryptography differ in the way they are evaluated: steganography fails when the ”enemy” is able to access the content of the cipher message, while cryptography fails when the ”enemy” detects that there is a secret message present in the steganography medium. Steganography and Cryptography both techniques can be combined to produce better protection of the message.

VIII.STEGANALYSIS

Steganalysis is the science of detecting hidden information . The aim of steganalysis is to break steganography and the detection of stego image is the goal of steganalysis..
Steganalysis deals with three important categories:

1.Visual attacks :
It reveal the presence of hidden information, which helps to separate the image into bit planes for more analysis.
2. Statistical attacks :
This type of the attack are similar to visual attack. The idea of the statistical attack is to compare the frequency distribution of a potential cover file with the theoretically expected distribution of the cover file.If the new data does not have the same statistical profile as the standard data is expected to have,then it probably contains a hidden message. Statistical attacks has two types 1) passive and 2) active. Passive attacks involves with identifying presence or absence of a covert message or embedding algorithm used.Active attacks is used to investigate embedded message length or hidden message location or secret key used in embedding.
3. Structural attacks :
The format of the data file is different when information is embedded.The attacker may detect the presence of a message by examine statistical profile of the bits.These changes to the data file usually fall into easily detectable pattern that gives an indication of a hidden message.After hiding process the attacker will not see which steganography program was used.

IX.CONCLUSION

Steganography is the art and science of writing hidden messages in such a way that no one can see that message except the sender and receiver.Steganography and Steganalysis are most important topic because now a days,the use of internet is grow.This paper,Basic concept of steganography,different types of steganography,its uses,difference between steganography and cryptography,steganalysis has been reviewed .

ACKNOWLEDGMENT

I thankful to my prof. Chandresh D.Parekh who has encourage and help me to do my work.I finished my paper under his advice.

All Rights Reserved, @IJAREST-2017

REFERENCES

1) Mohit Garg, A Novel Text Steganography Technique Based on Html Documents, International Journal of Advanced Science and Technology Vol. 35, October, 2011 129.
2) M. Pavani1, S. Naganjaneyulu2, C. Nagaraju3, A Survey on LSB Based Steganography Methods, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2464-2467
3) VIJAY KUMAR SHARMA ,2VISHAL SHRIVASTAVA, A STEGANOGRAPHY ALGORITHM FOR HIDING IMAGE IN IMAGE BY IMPROVED LSB SUBSTITUTION BY MINIMIZE DETECTION Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1© 2005 - 2012 JATIT & LLS
4) Pratap Chandra Mandal, **Modern Steganographic technique: A Survey** International Journal of Computer Science & Engineering Technology (IJCSET)
5) Arvind Kumar Km. Pooja,A Data Hiding Technique, International Journal of Computer Applications (0975 – 8887)Volume 9– No.7, November 2010
6) Hemang A. Prajapati1, Dr. Nehal G. Chitaliya, **Secured and Robust Dual Image Steganography: A Survey, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization)Vol. 3, Issue 1, January 2015**
7) **Divyanshu Tripathi1, Yash Kumar Singh2, Rohit Singh, A Review on Digital Image Steganography with its Techniques and Model, IJSART – Volume 2 Issue 4–APRIL 2016 ISSN [ONLINE]: 2395-1052**
8) https://en.wikipedia.org/wiki/Steganography
9) http://www.webopedia.com/TERM/S/steganography.html
10) http://steganography-info.blogspot.in/2008/04/steganography-and-attacks.html

All Rights Reserved, @IJAREST-2017