Network Protocols for Steganography: A Glance

Avish Dhamade, Krunal Panchal
Computer Science & Engineering Department,
L. J. Institute of Engineering & Technology,
Gujarat Technological University

***Abstract* - In the present scenario, internet is among the basic necessities of life. Internet has changed each and everybody's lives. So confidentiality of messages is very important over the internet. Steganography is the science of sending secret messages between the sender and intended receiver. It is such a technique that makes the exchange of covert messages possible. Each time a carrier is to be used for achieving steganography. The carrier plays a major role in establishing covert communication channel. This survey paper introduces steganography and its carriers. This paper concentrates on network protocols to be used as a carrier of steganograms. There are a number of protocols available to do so in the networks.**

***Index Terms* – Covert, Network, Protocols, Steganography.**

I. INTRODUCTION

Information is available over the internet freely. Also majority of persons are connected to the internet now days. So information hiding becomes major issue for the privacy seekers. The parties who want to communicate on the internet want their messages to be secret. Information hiding can be done using Cryptography, Steganography and Digital Watermarking. Fig shows the classification of information hiding.

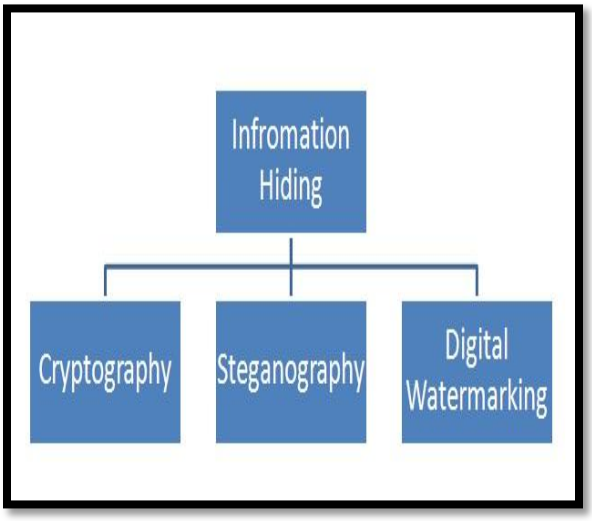

Figure 1: Classification of Information Hiding Techniques

Table shows the comparison of the three methods using various parameters as below:

Criteria/ Method	**Cryptography**	**Steganography**	**Digital Watermarking**
Carrier	Mostly text based	Any digital media	Mostly image/audio
Secret data	Plain-text	Watermark	Stego-data
Key	Necessary	Optional	-
Objective	Data protection	Secret communication	Copyright preserving
Result	Cipher-text	Stego-file	Watermarked-file
Types of attacks	Cryptanalysis	Steganalysis	Image processing
Visibility	Always	Never	Sometimes
Fails when	Deciphered	Detected	Removed/ Replaced
Flexibility	N/A	Any cover choice	Restricted cover choice
History	Modern	Ancient except digital	Modern

Table 1: Comparison of Techniques

II. STEGANOGRAPHY

Steganography is a Greek word meaning hidden writing [3]. It is a technique of communicating with others secretly. Lampson introduced this concept through prisoner's problem [1]. Steganography has changed from the ancient age to modern age. If the existence of the secret communication is revealed then steganography fails.

Ancient Steganography

Steganography is having its existence since the time of Herodotus [13]. Herodotus used it to send a message to the neighboring country. He shaved the head of his faithful slave and wrote the message on his head. Then the slave was told to move to the

destination. At the destination, head of the slave was shaved to get the secret message.
Since that time a lot of various techniques are employed for steganography. Major of them includes hiding message in stomach of hare, carving messages on wooden tablets covered with wax, use of bone dice, invisible ink, hard-boiled egg, music scores, newspaper codes, microdots and various others [13]. Of the given techniques microdots were used during the World War-II.

III. MODERN STEGANOGRAPHY

Steganography has changed a lot over the past years. It has moved from the physical carriers to digital carriers. Today's modern steganography use digital carriers like text, image, audio, video and network protocols.

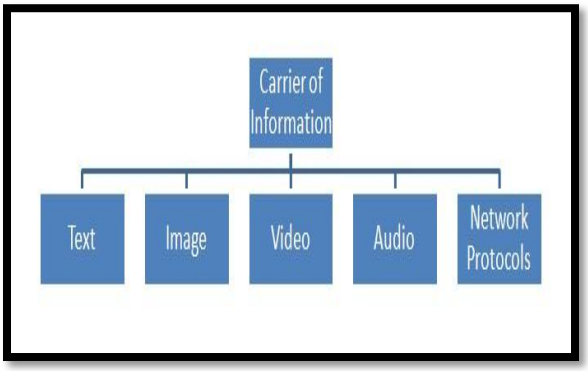

Figure 2: Types of Carriers of Information

1. Text – Text Steganography hides secret messages in text. It is somewhat difficult to achieve because of limited places to hide text in the carrier. HTML code, Huffman tree and binary file are examples of text steganography.
2. Image – Image steganography is the most used carrier. Human eye cannot find minute alterations done to the image. So it's easy to hide secret messages in the image. The original image and the stego image look almost same.
3. Video – Video steganography involves procedure same as of image. The only difference is that video is a group of images flowing in certain speed such that a constant video is obtained. Each frame can be used to store a secret message. More information can be stored in video.
4. Audio – Audio steganography is one of the difficult techniques to implement. Humans can easily find the changes made in audio. Also it requires a sound knowledge of digital signal processing.
5. Network Protocols – Network steganography is a new approach towards steganography. Many protocols are available in the layers of the network. The reserved and unused bits of the protocol fields and header fields are used to achieve steganography.

IV. BASIC MODEL OF STEGANOGRAPHY

The steganography scheme includes the first step of embedding the secret message in the desired carrier. The carrier is passed through the transmission media. The receiver extracts the message which is the reverse of embedding, to get the secret message. Below fig gives the proper flow.

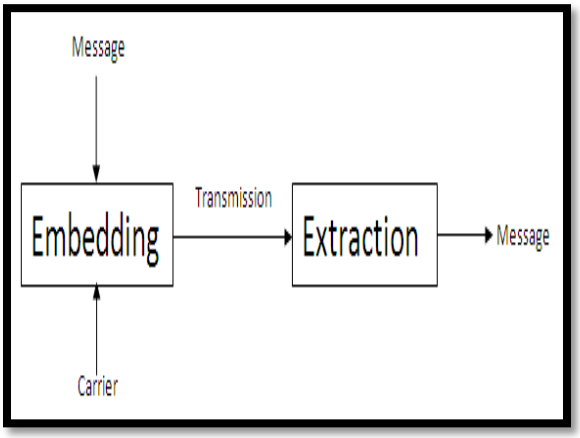

Figure 3: Basic model of Steganography

V. STEGANOGRAPHY TECHNIQUES USING NETWORK PROTOCOLS

Network steganography is a technique implementing steganography using available network protocols. The concept of covert channels was first introduced by Lampson in 1973. The term Network Steganography was first coined by K. Szczypiorski. The OSI RM (Open System Interconnection Reference Model) has 7 layers in it. The 7 layers have different protocols freely available for carrying out steganography [12].
Network steganography is done by using covert channels. Covert channels could be [12]

- Storage channels: the channels which use the reserved or unused bits of the packet header and payload are called storage channels.
- Timing channels: the channels which use the time synchronization of the packets for sending secret bits are called timing channels.

- Hybrid channels: the channels which use the strategies of storage as well as timing are called hybrid channels.

Covert Channels

There are a number of covert channel techniques in computer network protocols. They are described as follows [1]:

- **Unused Header Bits**
  Secret message could be encoded in unused or reserved bits of frame or packet headers. IP header's Type of Service (TOS) field, TCP header's Flags field, IP header's Don't Fragment (DF) bit, TCP Urgent Pointer, TCP Reset segments (RST) and IPv6 header fields could be used to hide secret bits of data.
- **Header extensions and Frame or Packet padding**
  Many protocols do support extension of the standard header. Extra padding could be done to the header to send the covert bits. IPv6 destination options header, IPv6 Hop-by-Hop, Routing, Fragment, Authentication and Encapsulating Security Payload extension headers, IP Route Record option headers and padding of the IP and TCP header could be used to hide secret bits.
- **IP Identification and Fragment Offset**
  The IP Identification (ID) header field is used for reassembling fragmented IP packets. The reassembling could be done at the receivers end by checking the identification field. The Fragment Offset is used to find in which sequence the fragments need to be reassembled. The bytes of IP ID could be multiplied by a number and could be set as IP ID. Thus the secret bit could be sent over the network.
- **TCP Initial Sequence Number Field**
  TCP Sequence Number is used to maintain data that has been transmitted and received which guarantees reliable transport. Here the secret data could be sent in the SYN/ACK or SYN/RST packets. The receiver would decrement the ACK and decodes the hidden information.
- **Checksum Field**
  IP header Checksum field could be used to encode secret information. IP header extension is added with the content such that the modified checksum is correct again. Same technique could be used for TCP Checksum. UDP Checksum is used for providing a signal if any secret information is sent.
- **Modulating the IP Time to Live Field**
  The IP Time to Live (TTL) field could be used for general marking purpose instead of communication. Also IPv6 Hop Limit Field (IPv6 equivalent of the IP TTL) is also available for covert communication.
- **Modulating Address Fields and Packet Lengths**
  Any communication protocol uses address fields to identify the address of senders and receivers. The amount of bits transmitted depends on the number of different addresses. Also the packet length fields indicate the length of headers, header extensions or messages (frames, packets). This packet length could be used to send secret bits of data.
- **Modulating Timestamp Fields**
  IP timestamp header extension can be used to transmit covert data. But it limits a packet to only 24 hops and is no longer used. TCP timestamp header options can also be used to transfer secret information over the network.
- **Packet Rate/Timing**
  In this scenario the relevant rate of the packets received at the receiver are used for handling secret bits. The covert information could be encoded by varying the packet rates resembling packet timings. The packets sent have some network constraints regarding time management. So this method has to be used in proper timely manner.
- **Message Sequence Timing**
  The acknowledgement received by the sender sometimes reveals the secret message. Acknowledgement could be sent after each frame or wait until two frames are arrived before acknowledging the first. Thus the sequence timing can be used to convey a secret message.
- **Packet Loss and Packet Sorting**
  Sometimes the loss of packets and the sorting of packets can also be used to convey a secret message. IPSec Authentication Header (AH) or Encapsulated Security Payload (ESP) can be used to complete our task.
- **Frame Collisions**
  The Ethernet Carrier Sense Multiple Access Collision Detection (CSMA/CD) mechanism can be exploited to send the secret information over the network. The covert sender jams any packets of another user and exploits the mechanism. There are many frames processing in the internet. So this entity also comes in handy.
- **Ad-Hoc Routing Protocols**
  Dynamic Source Routing (DSR) protocol is used for routing in ad-hoc networks. The header fields present in DSR routing requests like request

identification number, hop limit, clock time or address fields can be used. Also Ad-hoc On-Demand Distance Vector (AODV) protocol can be used as a covert channel.

- **Wireless LAN(WLAN)**
  There are various protocols in the IEEE 802.11 for applying network steganography. The RC4 initialization vector can be used. Retry bit and More Fragments bit of the Frame Control field and the Duration/ID field of 802.11 header fields can also be used for this purpose. The ACK frames or invalid frames are also available.
- **Hyper Text Transfer Protocol (HTTP)**
  Information is hidden in JavaScript/HTML and transported through the use of JavaScript redirects. Secret messages can be embedded into HTTP protocol headers.
- **Domain Name System (DNS) Protocol**
  An indirect covert channel can be created over the DNS protocol. The channel exploits negative caching of domain names. IP packets can be tunneled over the DNS protocol. Communication takes place between a client and a fake DNS server.
- **Other Application Protocols**
  Various other application protocols can be used as covert channels. Voice over IP (VoIP), Real-time Transport Protocol (RTP), Real-Time Control Protocol (RTCP), Secure Shell (SSH) protocol, Message Authentication Code (MAC) header and File Transfer Protocol (FTP) can be used to implement network steganography.
- **Payload Tunneling**
  Payload tunnels are covert channels that tunnel one protocol into the payload of another protocol. Mostly IP protocol is used. IP over ICMP, SSH over HTTP proxies and UDP or TCP over HTTP can be used for payload tunneling.

VI. PAPERS ANALYSIS

The following table shows the important points obtained from various protocols for network steganography. The protocol used from the appropriate layer and thus the Steganographic capacity obtained is also shown. The detection possibilities of the given protocol are also given.

No.	Title	Protocol	Capacity	Detection
1.	Network Packet Payload Parity Based Steganography [3]	UDP	1 bit/packet	Difficult
2.	Practical Internet Steganography: Data Hiding in Ip [4]	IP	Depends on selected field	-
3.	Retransmisssion steganography and its detection [5]	TCP	180 byte/s	Not easy
4.	Length Based Network Steganography using UDP Protocol [9]	UDP	456 bit/s	Not easy
5.	StegTorrent: a Steganographic Method for the P2P File Sharing Service [10]	UDP	270 bit/s	Difficult
6.	PadSteg: Introducing inter-protocol Steganography [6]	TCP and ARP	32 bit/s	Difficult
7.	Stream Control Transmission Protocol Steganography [8]	TCP and UDP	Depends on selected field	-

Table 2: Papers Discussion

VII. CONCLUSION

Steganography could be done using various carriers in which using network protocols is the latest and newest approach. Numerous protocols and their unused bits are available to attain steganography. It is been said that if 1 bit per packet data is used to transfer secret messages, a genuine website could lose 26 GB of data [1].

REFERENCES

[1] Sebastian Zander, Grenville Armitage and Philip Branch. "A Survey of Covert Channels and Countermeasures in Computer Network Protocols", Swinburne University of Technology Melbourne, Australia, IEEE Communications Surveys & Tutorials, Volume 9, No. 3, 3rd Quarter 2007, pp. 44-57.

[2] Theodore G. Handel and Maxwell T. Sandford II. "Hiding Data in the OSI Network Model", Weapon

Design Technology Group, Los Alamos National Laboratory, Los Alamos.

[3] Osamah Ibrahiem Abdullaziz, Vik Tor Goh, Huo-Chong Ling and KokShiek Wong. "Network Packet Payload Parity Based Steganography", Conference on Sustainable Utilization and Development in Engineering and Technology, IEEE 2013

[4] Deepa Kundur and Kamran Ahsan. "Practical Internet Steganography: Data Hiding in IP", In Proceedings of Texas Workshop on Security of Information Systems, April 2003.

[5] Wojciech Mazurczyk, Milosz Smolarczyk and Krzysztof Szczypiorski. "Retransmission Steganography and its detection", Warsaw University of Technology, Institute of Telecommunications, Warsaw, Poland, Springer 05 November 2009.

[6] Bartosz Jankowski, Wojciech Mazurczyk and Krzysztof Szczypiorski. "PadSteg: introducing inter-protocol steganography", Institute of Telecommunications, Warsaw University of Technology, Warsaw, Poland, ISSN 1018-4864, Volume 52, Number 2, Springer 2013.

[7] R. M. Goudar, Prashant N. Patil, Aniket G. Meshram, Sanyog M. Yewale and Abhay V. Fegade. "Secure Data Transmission by using Steganography", The International Institute for Science, Technology and Education, Vol 2, No. 1, 2012.

[8] Wojciech Fraczek, Wojciech Mazurczyk and Krzysztof Szczypiorski. "Stream Control Transmission Protocol Steganography", International Conference on Multimedia Information Networking and Security, IEEE Computer Society 2010.

[9] Anand S Nair, Abhishek Kumar, Arijit Sur and Sukumar Nandi. "Length Based Network Steganography using UDP Protocol", Department of Computer Science and Engineering, Indian Institute of Technology, Guwahati, pp. no. 726-730, IEEE 2013.

[10] Pawel Kopiczko, Wojciech Mazurczyk and Krzysztof Szczypiorski. "StegTorrent: a Steganographic Method for the P2P File Sharing Service", Security and Privacy Workshops, pp. no. 151-157, IEEE 2013.

[11] Wojciech Mazurczyk and Krzysztof Szczypiorski. "Steganography in Handling Oversized IP Packets", Multimedia Information Networking and Security, pp. no. 559-564, IEEE 2009.

[12] Jozef Lubacz, Wojciech Mazurczyk and Krzysztof Szczypiorski . "Principles and Overview of Network Steganography", Communications Magazine, Volume: 52, Issue: 5, pp. no. 225-229, IEEE 2014.

[13] Elzbieta Zielinska, Wojciech Mazurczyk, Krzystof Szczpiorski. "Development Trends in Steganography", Communications of the ACM, Volume: 57, No. 3, pp. no. 86-95, March 2014.