

“STEGANOGRAPHY AND ITS IMPACT ON IT”

Ms. Shilpa Gogia

Assistant Professor, Dept. of Electronics & IT, S.D.College, Ambala Cantt

Abstract— This paper describes the steganography and its impact on information technology. All over the world we have to transfer the information. This has been done only due to the invention of technology. But the most important is the privacy of the information. Steganography is a technique to make the data private. This helps in hiding the data from unauthorized persons. Data can be hidden in any content like audio, video or image.

I. INTRODUCTION

We need to communicate for our survival. It is an essential human need. With the advent of technology this communication has become easier and faster. With this easy and faster communication everyone needs this communication to be private and secure. Steganography is the way to communicate securely. It is the process of hiding a secret message within a larger one in such a way that someone can not know the presence or contents of the hidden message. It hides the existence of the message itself in such a way that it becomes difficult for an observer to figure out the hidden message.

II. STEGANOGRAPHY

Steganography is derived from Steganos and graphial means “covered writing” where covered means not only hiding the data but also hiding the fact of transmission of data. This concept is being used throughout the ages. Early in World War II, invisible ink was used to hide the data. [H.S. Zim(1948)]. Hidden tattoos were used in ancient times. Kings used to shave the head of the person and write a secret message on his scalp. One more method used during those days is Tablet Wax [N.F.Johnson and S. Jajodia (1998)].

III. STRUCTURE OF STEGANOGRAPHY

Secret information can be stored in any multimedia file i.e. audio ,video or image and these are known as ‘audio steganography’, ‘video steganography’ or ‘image steganography’. Out of these image steganography is most widely used because pictures or images are more frequently used over the communication in comparison to audios or videos. The basic structure of Steganography is made up of the given components:

- The secret message (M), can be plain text, cipher text or any type of data
- The cover media(C) that holds the hidden data/secret message.

- The stego image (S), which is cover image after the secret message is embedded in it.
- A stego-key (K) or password may be used to hide and unhide the message.

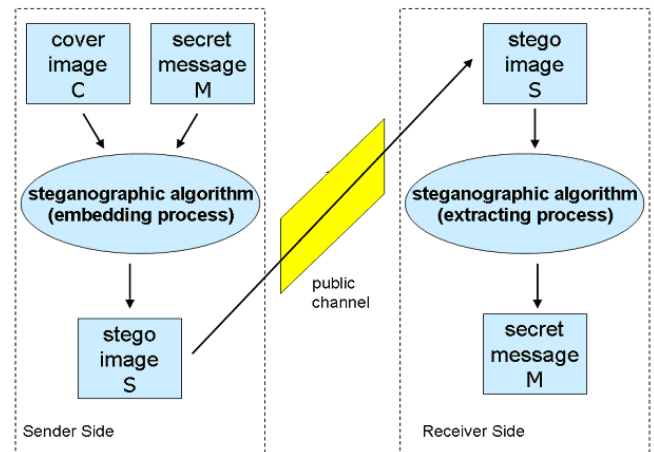


Fig. 1 Steganographic Model

IV. TYPES OF STEGANOGRAPHY

Steganography is divided into five types:

- 1) Text Steganography
- 2) Image Steganography
- 3) Audio Steganography
- 4) Video Steganography
- 5) Protocol Steganography

A. Text Steganography

Text Steganography is hiding secret messages in text. message. Sender sends a series of integer numbers to the receiver with a prior agreement that the secret message is hidden within the respective position of subsequent words of the cover text. Text based Steganography can be easily altered by unwanted parties.

B. Image Steganography

Image Steganography is hiding Secret messages in images. Any text, image and any other media can be hidden in a digital image.

C. Audio Steganography

Audio steganography is concerned with embedding information in a cover speech in a secure way. Secret

message is embedded into digitized audio signal. By hiding the information using a cover or host audio the existence of the information is concealed during transmission.

D. Video Steganography

Video files generally consist of images and sounds, so most of the techniques for hiding data into images and audio are applicable to video media. It has the advantage of good stability, but the disadvantage is its small capacity.

E. Protocol Steganography

Messages are embedded into commonly used TCP/IP protocols.

V. RELATED WORK

Many researchers have worked in this field. A method to hide data in binary images, including scanned text, figures, signatures was proposed by Min Wu and Bede Liu[15] in 2004. Miroslav Dobsicek[7] in the field of image security, has developed an application of steganography in 2004 where the content is encrypted with one key and can be decrypted with several other keys. In 2007 El-Emam[8] proposed a steganography algorithm to hide a large amount of data with high security. An approach to hide data inside the audiovisual files was introduced by Warkentin et al.[23] in 2008. A public key method of Steganography under standard cryptographic steganographic algorithm based on logical operation by Vijay Kumar Sharma et al. in 2012.

A survey paper on hybrid cryptography and steganography is given by Apoorva Shrivastava and

Different image based techniques are used:

- Least Significant Bit Insertion
- Masking and Filtering
- Algorithms and Transformations

The simplest and the most common steganographic technique is the Least Significant Bit embedding (LSB). This technique provides to embed the data into the least significant bit.

VI. IMPACT ON INFORMATION TECHNOLOGY

Steganography leaves a great impact on IT as it is used in almost every region. Communication and data transfer has become a part of life. No field can work without the transfer of data.

E-commerce, On line Education, Industry ,T.V. broadcasting, Smart Identity Cards where details of individuals is embedded, Military purposes etc. Secrecy of data is very necessary for all this .

Steganography serves this purpose.

VII. DISCUSSION AND FUTURE WORK

After reviewing the various papers in area of steganography it is found that a lot of work has been done in the field of Steganography as well as in Image Steganography. Most of the Steganography techniques are suitable to hide data either text or binary message. Image steganography is most popular used technique. Future scope requires increase in data security, increase in the hidden capacity of data without any remarkable change in the cover image data so that integrity of the stego image is maintained and there should not be any distortion. Although implementations have been done in this field. Further a lot more work is required to do in the steganography.

VIII. CONCLUSION

The Paper gives the review of Steganography and its impact on IT. The paper suggested more future research to improve integrity and data capacity of cover age so that the impact of steganography on information technology becomes remarkable.

REFERENCES

- [1] Adel Almohammad "Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility" A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing, Brunel University, August,2010.
- [2] Arvind Kumar and Km. Pooja "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.
- [3] M. Bachrach, and F.Y. Shih, "Image steganography and steganalysis,"Wiley Interdisciplinary Reviews: Computational Statistics, Vol. 3, pp. 251-9, 2011.
- [4] Cheddad, A., J. Condell, K. Curran, & P. Mc Kevitt. "A skin tone detection algorithm for an adaptive approach to steganography". Signal Processing, 89(12): 2465-2478. doi: 10.1016/j.sigpro.2009.04.022, 2009.
- [5] S.K. Bandyopadhyay, Debnath Bhattacharyya, Swamendu Mukherjee, Debashis Ganguly, Poulumi Das, "A Secure Scheme for Image Transformation", August 2008, IEEE SNPD Page(s) 490-493
- [6] Samir Kumar Bandyopadhyay & Sarthak Parui proposed "A Method for Public Key Method of Steganography" International Journal of computer Applications(0975-8887) Volume 6-No.3,September,2010
- [7] Dobsicek, M., "Extended steganographic system", In: 8th Intl. Student Conf. On Electrical Engineering, FEE CTU 2004, Poster 04.
- [8] El-Emam N.N. (2007)." Hiding a Large Amount of Data with High Security using Steganography Algorithm", Journal of Computer Science 3 (4), pp 223-232.
- [9] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn "Information Hiding A Survey"Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062 {1078, July 1999.
- [10] Farid,H."Image forgery detection". Signal Processing Magazine, IEEE, 26(2): 16-25. doi: 10.1109/msp.2008.931079, 2009.
- [11] J. Fridrich, "Steganography in Digital Media: Principles",Algorithms, and Applications, Cambridge, England: Cambridge University Press; 2009.
- [12] J.C. Ingemar, M.L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, "Digital watermarking and steganography", Burlington: Morgan Kaufmann; 2008.
- [13] N.F. Johnson, and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, IEEE, Vol. 31, pp. 26-34, 1998.
- [14] R. Krenn, "Steganography and steganalysis," An Article, Santa Barbara, California, January 2004,

available from: <http://www.krenn.nl/univ/cry/steg/article.pdf>
[Last accessed on 1 November 2013]

[15] Min Wu, Member, IEEE and Bede Liu, Fellow, IEEE, "Data Hiding in Binary Image for Authentication and Annotation", IEEE Trans. Image Processing, volume 6, Issue 4, Aug. 2004 Page(s): 528-538

[16] Mohammad Tanvir Parvej and Adnan Abdul-Aziz Gutub "RGB Intensity based Variable –Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference, 2008

[17] T. Morkel, J.H.P. Eloff, and M.S. Olivier, "An overview of image steganography" in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, pp. 1-12, 29 Jun.-1 Jul. 2005.

[18] Angela D. Orebaugh "Steganalysis: A Steganography Intrusion Detection System", George Mason University

[19] Petitcolas, F.A.P." Introduction to information hiding". In S. Katzenbeisser & F. A. P. Petitcolas (Eds.), Information hiding techniques for steganography and digital watermarking (pp. 1-12). Boston, London: Artech House, 2000.

[20] Rajkumar Yadav "Study of Information Hiding Techniques and their Counterattacks: A Review Article", International Journal of Computer Science & Communication Networks, Vol 1(2), 142-164, Oct-Nov 2011.

[21] Banasthali Vidyapith, Rjasthan "Image Steganography Techniques: A Review Article", Bulletin of Engineering, Faculty of Engineering, Hunedoara, Romania, July-September, 2013.

[22] Vikas Tyagi, "Data Hiding in Image using least significant bit with cryptography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012

[23] Warkentin M., Schmidt M.B. and Bekkering E. (2008). "Steganography and Steganalysis" Premier reference Source – Intellectual Property Protection for Multimedia Information technology, Chapter XIX, pp 374-380.