

SECURE DATA TRANSMISSION OVER INTERNET USING IMAGE STEGANOGRAPHY

P. SARANYA, B. MURALI, K. MADHAVI, K. KUNDANA, S. KARTHEEK

P. SARANYA - CSE, SITAM COLLEGE

B. MURALI - CSE, SITAM COLLEGE

K. MADHAVI - CSE, SITAM COLLEGE

K. KUNDANA - CSE, SITAM COLLEGE

S. KARTHEEK - CSE, SITAM COLLEGE

Abstract - Steganography is the technique of hiding private or sensitive information within something that appears to be nothing but a usual image. Steganography involves hiding Text so it appears that to be a normal image or other file. If a person views that object which has hidden information inside, he or she will have no idea that there is any secret information. What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them. What this system does is, it lets user to send text as secret message inside an image file, user uploads the image and enters the text to send secretly, and gives a key or a pass word to lock the text, what this key does is it encrypts the text, so that even if it is hacked by hacker he will not be able to read the text. You will need the key to decrypt the hidden text. User then sends the image and key to the receiver and receiver first opens the image, and then he enters the key or password for decryption of text, he then presses decrypt key to get secret text of the sender. By using this method you can double ensure that your secret message is sent secretly without outside interference of hackers or crackers. If sender sends this image in public others will not know what is it, and it will be received by receiver.

Key Words: Steganography, Encryption, Decryption.

1. INTRODUCTION

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of Steganography.

Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. Steganography includes an array of secret communication methods that hide the message from being seen or discovered.

Besides cryptography, Steganography can be employed to secure information. Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and Steganography.

Steganography hides the secret message within the host data set and presence imperceptible and is to be reliably communicated to a receiver.

2. LITERATURE SURVEY

1. Stefan Katzenbeiser, Fabien A.P Petitcolas "CRYPTOGRAPHY AND NETWORK SECURITY" [Artech House](#) Books, (January 2000).
2. [Harvinder Singh](#) "A BOOK OF STEGANOGRAPHY" Lotus Press, (01-Jan-2005).
3. Ingenmar J. Cox "DIGITAL WATERMARKING AND STEGANOGRAPHY" Morgan Kaufmann, (2008) .

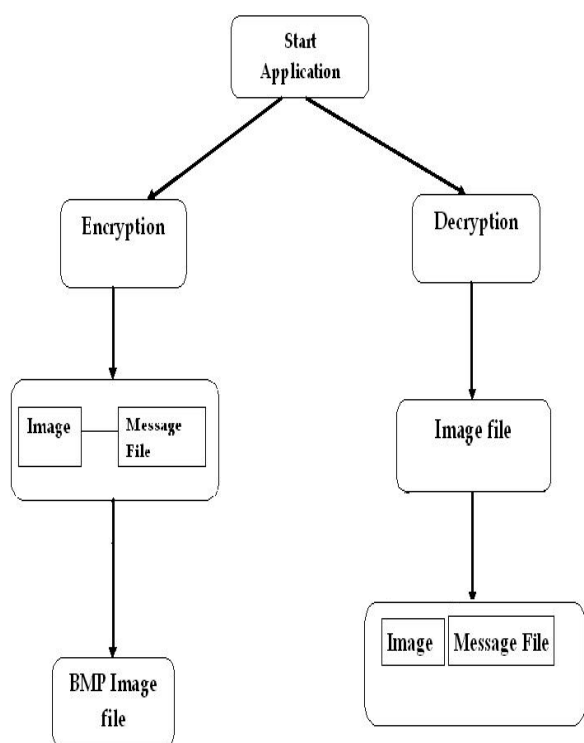
3. Problem Statement

The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. One disadvantage of linguistic Steganography is that users must equip themselves to have a good knowledge of linguistics. In recent years, everything is trending toward digitization. And with the development

of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the Steganography techniques, and then be transmitted through the internet rapidly.

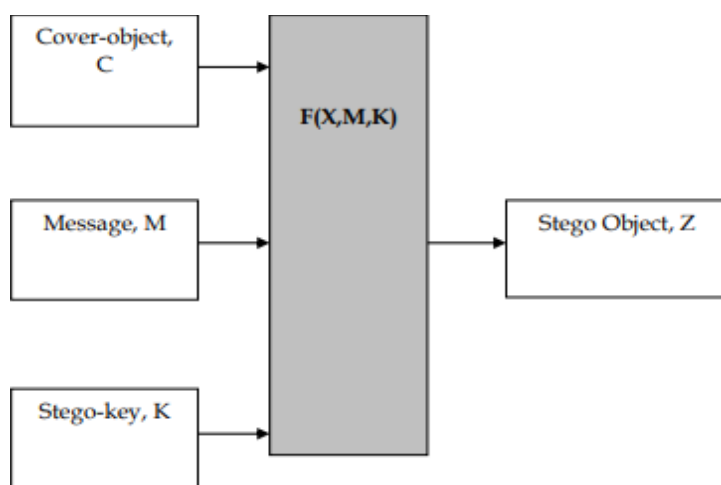
4. Overview

- The word Steganography comes from the Greek “Seganos”, which mean covered or secret
- “graphy” mean writing or drawing.
- Therefore, Steganography means, literally, covered writing.
- It is the art and science of hiding information such its presence cannot be detected and a communication is happening.
- A secret information is encoding in a manner such that the very existence of the information is concealed.
- The main goal of this projects it to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hider data.



5. STEGANOGRAPHY

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that Steganography involves hiding informationso it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of Steganography is to hide a file inside another file.



6. APPLICATIONS

Steganography is applicable to, but not limited to, the following areas. The area differs in what feature of the steganography is utilized in each system.

- 1) Confidential communication and secret data Storing.
- 2) Protection of data alteration.
- 3) Access control system for digital content distribution.

6. CONCLUSIONS

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day.

Steganography can be used for hidden communication. We have explored the limits of Steganography theory and practice. We printed out the enhancement of the image Steganography system using LSB approach to provide a means of secure communication. A Stego-key has been applied to the system during embedment of the message into the cover image.

This Steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside there. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that Steganography is not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the “digital world”.

ACKNOWLEDGEMENT

With immense pleasure, we are publishing this paper as a part of the curriculum of B.Tech. Computer Science & Engineering. It gives us proud privilege to complete this paper work under the valuable guidance of Principal for providing all facilities and help for smooth progress of paper work. We would also like to thank all the Staff Members of Computer Science & Engineering Department, Management, friends and family members, Who have directly or indirectly guided and helped us for the preparation of this paper and gives us an unending support right from the stage the idea was conceived.

REFERENCES

- [1]. Ahsan K., and Kundur D., “Practical Internet Steganography: InData Hiding in IP” found online at <http://www.ece.tamu.edu/~deepa/pdf/txsecwrksh03.pdf>. Krish nankoil.
- [2]. Anderson R.J. and Petitcolas F.A.P., “On the Limits of steganography,” J. Selected Areas inComm., vol. 16, no.4, 1998, pp. 474–481.
- [3]. Bailey, K. and Curran, K. “An evaluation of image-based steganography methods”. InternationalJournal of Digital Evidence, Fall 2003.
- [4]. Chapman, M. Davida G, and Rennhard M.. “A Practical and Effective Approach to Large-ScaleAutomated Linguistic Steganography” found online at <http://www.nicetext.com/doc/isc01.pdf>.
- [5]. Dai Y., Liu G., and WangBreaking Z., “Predictive-CodingBased Steganography and Modification for Enhanced Security”, IJCSNS International Journal of Computer Science and Network Security, vol.6 no. 3b, March 2006.
- [6]. Chin-Chen Chang , Iuan-Chang Lin, and Yaun-Hui YU, “ A new Steganographic method for color and gray scale image hiding”, Computer Vision and Image Understanding, 20 December 2006.
- [7]. Shareza Shirali, M.H, “A new Approach to Persian/Arabic Text Stegraphy”, Computer and Information Science, 2006, ICISCOMSAR 2006, 5th IEEE/ACIS International Conference, 10- 12 July2006 pp 310-315.
- [8]. Fabien A.P., and Petitcolas, “Information Hiding: Techniques for Steganography and Digital Watermarking.”, 2000.
- [9].National Academy of Sciences, How do Wavelets work? National Academy of Sciences, <http://www.beyonddiscovery.org/content/view.page.asp?I=1956>, 2003 .
- [10].Digital Watermarking for Digital Media, Information Science Publishing.