International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Steganography: The Art of Encrypting and Decrypting Information with Different Hiding Tools and Command Prompt

Pushpendra Saini[1], Anu Singla[2], Rekha Lagarkha[3], Aishwarya Yadav[4], Pooja Soni[5]

[1,2,5]A. P. J. Abdul Kalam Institute of Forensic Science and Criminology, Bundelkhand University Jhansi, Uttar Pradesh, India
[3,4]Department of Chemistry, Bundelkhand University, Jhansi, Uttar Pradesh, India

Abstract
The concealing information within other non-secret data to hide its existence. It involves embedding secret messages or data within innocuous carriers, like images, audio files, or text. This hidden information is often encrypted to enhance security. Steganography focuses on maintaining the secrecy of the communication. The efficiency of two steganography tools Shusssh and SteganographX Plus freely available on internet. Different file format of images (JPEG, JPG and BMP) were analysed by Windows-based Command Prompt Utility and two different steganography tools (Shusssh! and SteganographX Plus).

Keywords: Steganography, Shusssh and SteganographX Plus, encrypted, steganography tools

Introduction

The term "covered writing" (steganography) is derived from the Greek terms "stegos," which means "cover," and "grafia," which means "writing". Information is only concealed in images with image steganography. Steganography is a type of anti-forensic technology that is used to hide sensitive information behind a cover medium. Steganography, which is the process of hiding tiny multimedia data in much larger multimedia data, such as an image, text, file, or video, can be defined. A method of hiding a picture inside another image is called image steganography. While using picture steganography, the cover image is modified so that the hidden information is not apparent, making it less suspect than when using cryptography. On the other hand, Steganalysis is used to find any hidden data that has been covered up by an image and to extract any hidden messages that may be present **(Sumathi et al, 2013).**

Steganography Mediums

There are many kinds of Steganography techniques available based on the type of thing that has to be secured.

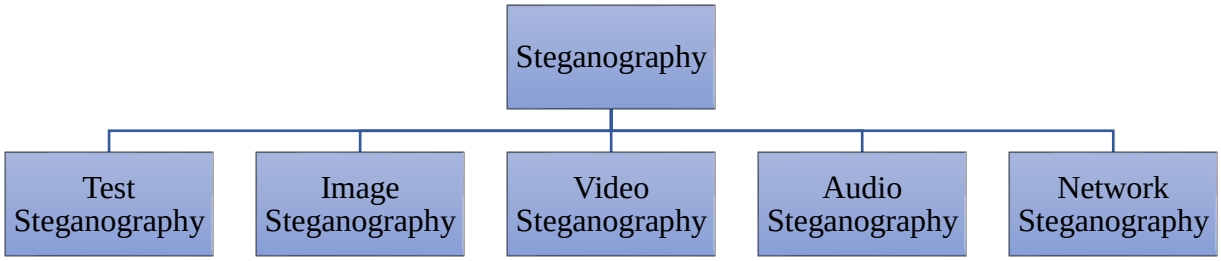

Fig.1Different Mediums to achieve steganography

Text Steganography

In this technique, for information hiding, capital letters, white spaces, the number of tabs, and many others are used. By using an embedding algorithm to create a stego-text, a secret message (or embedded data) will be hidden in a cover text. The stego text will subsequently be sent to a receiver via a communication channel, such as the Internet or a mobile device. The receiver must apply a recovery method that is parameterized by a stego-key to extract the secret message in order to recover the secret that was sent by the sender. To prevent unauthorized parties from discovering and/or recovering the embedded data, the hiding process is controlled by a stego-key **(Por, 2008)**.

Image Steganography

The technique of hiding a picture inside another image is called image steganography. When using picture steganography, the cover image is modified so that the hidden information is not visible**(Sindhu, 2020)**.

Video Steganography

Video steganography uses digital video formats to conceal all kinds of information. The discrete cosine transform (DCT) adjusts the value (for instance, from 7.667 to 8), which is undetectable to the human eye, in this method for concealing information in video image frames. Video steganography uses Mp4, AVI, etc. as its video formats. Most effective methods for blending data into images and audio are also applicable to video media because video files typically contain both images and sounds. When using video steganography, the sender uses a video sequence as the cover media to deliver the secret message to the recipient. In order to create a "stego-video," the optional secret key "K" can also be used when embedding the secret message into the cover media. Following that, the receiver receives the stego-video over a public channel. The secret message is extracted from the stego-object at the receiving end using the extracting algorithm and the secret key **(Deshmukh and Rahangdale, 2014).**

Audio Steganography

Voice Over Internet Protocol (VOIP) demand made audio steganography one of the most important mediums. Since audio is used to conceal information in this method, the term "audio steganography" has been coined. Digital audio formats like WAVE, MPEG, and others are used for audio steganography **(Sindhu and Singh, 2020).**

Network Steganography

These protocols are used as the carrier in this technique's cover object selection, which includes network protocols like UDP, ICMP, and others. Nowadays, almost everyone communicates online. Whether it be

through Facebook, Whatsapp, email, video calls, or voice calls, all communication takes place over networks. P2P, TCP/IP, HTTP, and other protocols are all useful, but the best feature of network steganography is that it allows us to use any network protocol to transmit messages by hiding them in headers, packets, etc **(Singh et al, 2017).**

Materials and Methodology

In the present study total 3 image sample belonging 3 different file formats (JPEG, JPG and BMP) were analysed by using two different steganography tools (**Shusssh!** and **SteganographX Plus**) and **Command Prompt** based on windows was used as. The message "**My Name Is Pushpendra Saini**" in the format of text was used as encryption in different image file. **SteganographX Plus** tool offer password protection feature to encrypt and decrypt during steganography. The encryption key "**123456789**" was used during analysis on **SteganographX Plus** tool.

Shusssh! is a simple tool to hide a message inside any picture. Simply select "Encrypt Text" and load an image by clicking the "Load Image" button. Type your message in the "Insert Message:" text area and click Proceed button to save the image with a hidden message on the desired location. And for the decrypting text from the encrypted image; select "Decrypt Text" load the image and click Proceed button to view the hidden message.

Fig.2 Shusssh!Tool

SteganographX Plus is a freeware for hiding secret messages inside BMP images. It is just 496 KB in a ZIP file and no installation is required to use this software. It is a very simple and user-friendly program. It supports only numbers while entering the encryption key. You can use it to encrypt or decrypt text inside a BMP file. Supply the correct password to extract the hidden text. This software must be present at both ends while encrypting or decrypting.

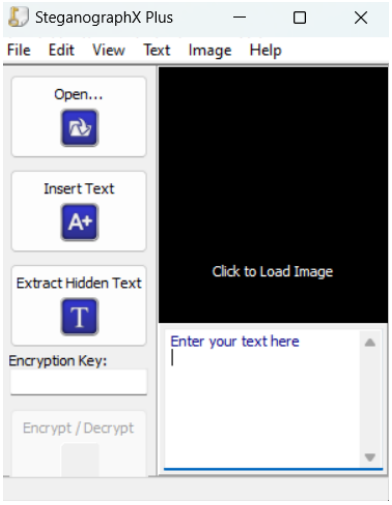

Fig.3 SteganographX Plus Tool

Command Prompt is windows-based platform where any data in all formats can be hidden in any data (image, audio, video, etc.). But the data to be hidden must be compressed into a zip document. A txt extension file can be hidden in a video or audio file without zipping the text file and the secret txt file can be accessed by opening the video or audio file using a notepad (any text editor).

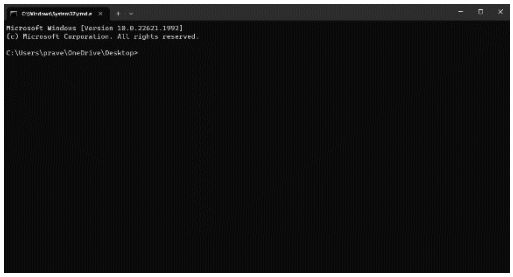

Fig.4 Command Prompt

Results

The result of the present study has been summarised in the form of table 3-5. The result of the image encrypted by **Shusssh! Tool**, **SteganographX Plus** and **Command Prompt** shows difference in the size while other parameters remain same.

Table. 1 Comparison Between Normal Image and Stego Image by Shusssh! Tool

S.No	Parameters	Normal Image	Stego Image
1	Type of File	JPEG	JPEG
2	Size	5.21 kb (5,342 bytes)	5.25 kb (5,382 bytes)
3	Size on Disk	8.00 kb (8,142 bytes)	8.00 KB (8,142 bytes)
4	Dimension	183*275	183*275
5	Width	183	183
6	Height	275	275
7	Horizonal Resolution	96	96
8	Vertical Resolution	96	96
9	Bit depth	24	24

Image is found increased by .04 kb from Normal Image 5.25 kb (5,3822 bytes) to Stego Image 5.21 kb (5,382 bytes).

Table. 2 Comparison Between Normal Image and Stego Image by SteganographX Plus Tool

S.No	Parameters	Normal Image	Stego Image
1	Type of File	BMP	BMP
2	Size	148 kb (1,51622 bytes)	148 kb (1,51578 bytes)
3	Size on Disk	156 KB (1,59744 bytes)	152 KB (1,55648 bytes)
4	Dimension	275*183	183*275
5	Width	275	275
6	Height	183	183
7	Horizonal Resolution	96	96
8	Vertical Resolution	96	96
9	Bit depth	24	24

Image is found decreased by 44 bytes from Normal Image 148 kb (1,51622 bytes) to Stego Image 5148 kb (1,51578 bytes) but Image is found decreased by 4 kb from Normal Image 156 KB (1,59744 bytes) to Stego Image 152 KB (1,55648 bytes).

Table. 3 Comparison Between Normal Image and Stego Image by Command Prompt Utility

S.No	Parameters	Normal Image	Stego Image
1	Type of File	JPG	JPG
2	Size	27.5 kb (28182 bytes)	27.5 kb (28,236 bytes)
3	Size on Disk	28 kb (28,672 bytes)	28 KB (28,672 bytes)
4	Dimension	720*409	720*409
5	Width	720	720
6	Height	409	409
7	Horizonal Resolution	96	96
8	Vertical Resolution	96	96
9	Bit depth	24	24

Image is found increased by 54 bytes from Normal Image 27.5 kb (28182 bytes) to Stego Image 27.5 kb (28,236 bytes).

Discussion

On the basis of the results obtained from comparative analysis of open-source steganography software and command prompt utility based on windows platform, it is concluded that command prompt can be easier and safer alternative providing almost similar results to that of the open-source steganography. Moreover, the comparative analysis of two open-source tools Shusssh! and SteganographX Plus revealed that SteganographX Plus offer password protection feature, but has a limitation that it supports only image file in BMP format.

References

1. **Abduallah, W. M. and Rahma, A. M. S.(2016)** "A Review on Steganography Techniques", *American Scientific Research Journal for Engineering, Technology, and Sciences*, *24*(1), 131–150.
2. **Abdulrazzaq, S. T.; Siddeq, M. M. and Rodrigues, M.(2020)**"A Novel Steganography Approach for Audio Files", *SN Computer Science*, 1(2).
3. **Cheddad, A.; Condell, J.; Curran, K. and Kevitt, P. M.(2010)**"Digital Image Steganography: Survey and Analysis of Current Methods", *Signal Processing*, 90(3), 727–752.
4. **Deshmukh, P. R. and Rahangdale, B.(2014)**"Data Hiding using Video Steganography", *International Journal of Engineering Research and Technology*, 3(4).
5. **Hussain, M.; Wahab, A. W. A.; Idris, Y. I. B.; Ho, A. T. S. and Jung, K.(2018)**"Image Steganography in Spatial Domain: A Survey", *Signal Processing-image Communication*, 65, 46–66.
6. **Kumar, A. and Pooja, K.(2010)** "Steganography- A Data Hiding Technique", *International Journal of Computer Applications*, 9(7), 19–23.
7. **Lin, E. T. and Delp, E. J.(1999)** "A Review of Data Hiding in Digital Images", *Computer Vision and Pattern Recognition (CVPR)*, 274–278.
8. **Morkel, T.; Eloff, J. H. P. and Olivier, M. S.(2005)** "An Overview of Image Steganography", *Information Security for South Africa*, 1–11.
9. **Por, L. Y. (2008)** "Information Hiding: A New Approach in Text Steganography", *Journal of Systems and Software*, 85(10), 2385-2394.
10. **Rajkumar, G. P. and Malemath, V. S.(2017)** "Video steganography: Secure Data Hiding Technique", *International Journal of Computer Network and Information Security*, *9*(9), 38–45.
11. **Raghavan, S. V. (2012)** "Digital Forensic Research: Current State of the Art", *CSI Transactions on ICT*, 1(1), 91-114.
12. **Sindhu, R. and Singh, P.(2020)**"Information Hiding using Steganography", *International Journal of Engineering and Advanced Technology*, 9(4), 1549–1554.
13. **Singh, N.; Bhardwaj, J. and Raghav, G. R.(2017)** "Network Steganography and its Techniques: A Survey", *Procedia Computer Science*, 171, 1810-1818.
14. **Subramanian, N.; Elharrouss, O.; Al-Maadeed, S. and Bouridane, A.(2021)** "Image Steganography: A Review of the Recent Advances", *IEEE Access*, 9, 23409–23423.
15. **Sumathi, C. P.; Santanam, T. and Umamaheswari, G.(2013)** "A Study of Various Steganographic Techniques used for Information Hiding", *International Journal of Computer Science & Engineering Survey*, 4(6), 9–25.
16. **Thampi, S. M.(2008) "**Information Hiding Techniques: A tutorial review", *Engineering, Technology & Applied Science Research*, 9(1), 3681-3684.
17. **Zhang, K. A.; Cuesta-Infante, A.; Xu, L. and Veeramachaneni, K.(2019)** "SteganoGAN: High-Capacity Image Steganography with GANs", *IEEE Transactions on Information Forensics and Security*, 14(5), 1280-1295.