Video Steganography Utilizing .avi Files as Carriers

Micheal Dieterle, Jerry Reimer, Divine Puplampu
Department of Information Technology and Management, Illinois Institute of Technology
201 East Loop Road, Wheaton IL 60189

ABSTRACT

This paper examines the use of video steganography to hide other information in .avi carrier files. The intended .avi carrier files are converted into .bmp frames using a web app that performed file format conversions. We then used a steganography tool called OurSecret to insert whatever information we wished to conceal inside of the bitmap frames and locked the contents with a password if so desired. We then recompile the altered and unaltered bitmap frames into one .avi video file using BmpSeq. The end result is a .avi file that contains some discretely hidden message of the creator's choosing.

General Terms

Documentation
Theory
Security
Experimentation
Verification

Keywords

video steganography
.avi RIFF
.avi steganography
steganography
OurSecret
.avi to .bmp Conversion
.bmp
bitmap
sequence

PROBLEM

Groups as diverse as social activists, government agents and officials, journalists, and terrorists all hold in common the need for a means to unobtrusively hide information and messages. The ability to effectively hide and extract hidden messages to and from innocuous carrier files can be the difference in preventing sensitive government information from falling into the wrong hands or repelling hostile forces. Advances in computing technology have made the use of steganography, the practice of hiding messages, images, or files within another message, image, or file[3], accessible to a much larger range of individuals. Likewise the use of more complex file types as carrier files for hidden information has grown. Video file formats have even begun to see use as carrier types. However, no application exists for performing stenographic processes in .AVI videos. They are no applications for hiding and extracting data in .avi videos, so to prove that data could be hidden and extracted in .avi videos is important.

HYPOTHESIS

We are trying to prove the concept that data can be hidden within .avi videos. In this particular procedure, we will prove that data can be hidden into and extracted from .avi videos by breaking up the .avi video into a series of .bmp images and hiding the data in the images before recompiling the images into a .avi video.

INTRODUCTION

The .avi video file type in particular is examined in this paper. .avi stands for audio video interleave. The file format contains both audio and video with synchronous playback ability. It possesses a large storage size which makes it ideal as a container. It can carry a large variety of compression types. "AVI has become the most popular container file format used for watching video on the PC"[2]

AVI files are derivatives of RIFF files, and within the single chunk of .AVI data with the RIFF file is the AVI's header, body, and index sub-chunk of it's data.

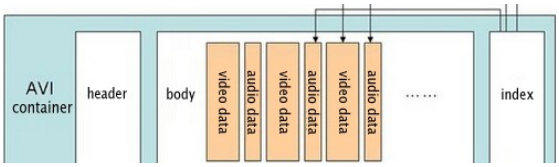

Figure 1: .avi Data Chunk [2]

Within the header is information about the frame rate, resolution, width and height of the video. The body contains the audio and visual data in virtually any compression scheme. The index points to where each piece of audio and visual data is.[2]

PROCEDURE

The process of breaking the .avi into .bmp frames, hiding the hidden information inside of the .bmp frames, and finally recompiling the .bmp into a single and almost identical .avi file will be examined in depth. The first step in hiding information inside of an .avi file is to find or create an .avi video file that you know is clean and unaltered in anyway. Once you have a clean .avi file use an online file format converter to break the .avi file file into .bmp frames.

When you have ready both your .bmp files derived from your original .avi file and the target file containing the information you wish to conceal, download and open the program OurSecret. OurSecret is a steganography tool which hides files and text information within image files. It hides the data by using the least significant bit steganographic method. It can also hide data in the header and footer[4]. Load in however many .bmp frames are necessary to contain the information you wish to hide while maintaining the integrity of the carrier file. If you desire to you may put a password over the hidden information contained in the file to add an extra layer of security.

After you have hidden all the information you desire to hide within your carrier .bmp frames, use AVIEdit to recompile and sequence the frames into an .avi video. Then, you can send the .avi video to the recipient. Once the recipient has received the .avi video with the hidden data within it, they will break the .avi video back up into a .bmp image series using the same application that the sender used, so that the same number of .bmp images is made by the recipient from the .avi video as the sender had. We used the application Aoao Video to Picture Converter[1].

Once the .avi video is broken down by the recipient into .bmp images, the recipient can start recovering the hidden data from the .avi file using OurSecret. Just browse for the images with the hidden data, type in the password, if any, to recover the data, and click “unhide” on the application, and you hidden data is now revealed.

RESULTS

The proof of concept that data can be hidden and extracted from .avi videos has been proven to work. Even though there are no applications specifically for hiding data in .avi files, there are ways to hide data in .avi files and extract it.

CONCLUSION

Although .avi steganography is possible with only a moderate level of computer proficiency, it would be nice to have an application with a GUI interface, so that less technical users could hide and extract data in .avi videos.

REFERENCES

[1] Aoao Video to Picture Converter. (n.d.). Retrieved December 1, 2014, from http://www.aoaophoto.com/video-to-picture-converter/video-to-picture.htm

[2] “AVI (Audio Video Interleaved) – Video Container and Format”. N.p. n.d. Web. 23 Sept. 2014. Retrieved from http://www.ezr8.com/avi

[3] Fridrich, J. & Goljan, M. & Soukal, D. (2004). "Searching for theStego Key". Proc. SPIE, Electronic Imaging, Security,Steganography, and Watermarking of Multimedia Contents VI5306: 70–82. Retrieved from http://www.ws.binghamton.edu/fridrich/Research/Keysearch_SPIE.pdf

[4]Steganography software OurSecret hides text inside photos. (n.d.). Retrieved December 1, 2014, from http://www.hacker10.com/computer-security/steganography-software-oursecret-hides-text-inside-photos/