OpenPuff

Steganography & Watermarking Tool

Michael Chesbro, Ph.D., CCIA, CCIP

February 22, 2014

The word "steganography" comes from the Greek words *steganos*, meaning hidden or covered, and *graphia*, meaning to write. Thus, steganography refers to hidden writing or to methods for concealing messages. The advantage of steganography is that it allows sensitive information to be hidden in mundane and innocuous carrier files. Steganography is not new. It has been used at least since the time of ancient Greece. Today with modern computers and the rapid exchange of information across the Internet, steganography allows information to be shared with individuals in areas and in situations where their communications are monitored and their freedom of expression and association is repressed. This paper discusses the OpenPuff - Steganography & Watermarking Tool.

OpenPuff - Steganography & Watermarking Tool

One of the most popular steganography programs is OpenPuff (http://goo.gl/GmB6c0). OpenPuff is freeware and provides the user with the ability to encrypt and hide data in audio

(wav), image (bmp, jpg, png), and stream (Mp3, Mp4, Vob) carrier files, as well as in pdf files and a few other file types as well. OpenPuff focuses on the security of your hidden information, and is highly recommended for anyone who needs to exchange information securely and covertly.

OpenPuff safeguards hidden information by encrypting the data and protecting it with up to three different passwords. At least one password of eight characters is required to hide data with OpenPuff. Additional passwords increase the security of the hidden data. Hidden data can also be split across multiple carrier files, allowing large amounts of sensitive information to be concealed. OpenPuff further protects hidden information by adding a large amount of random data (noise) to the information before it is encrypted and hidden.

A special feature of OpenPuff is '*Deniable Steganography*' which allows two separate sets of data to be concealed in a carrier file. This allows someone to hide both sensitive information and decoy information. If forced to disclose the passwords protecting the hidden data, a user can give up the decoy passwords, revealing non-incriminating information, while sensitive information still remains hidden and protected by a separate set of secret passwords.

OpenPuff also allows one to insert a hidden string of up to 32 characters into a carrier file. This is a type of digital watermark. This digital watermark can be revealed, without the need for a password, using the CheckMark function in OpenPuff. This digital watermarking function can be used to identify and track files posted to public forms or shared with selected groups of people.

OpenPuff is fairly easy to use, but there is a little bit of a learning curve for people unfamiliar with the software. For example, because OpenPuff saves a carrier file (with hidden data) as the same name as the file used to create that carrier file, these files must be saved to separate locations / folders. Trying to create a carrier file from a photo on your desktop and then save the photo with hidden data back to the desktop generates an error but does not identify what caused the error. The error message just states: "Couldn't create target: [Filename]." Other errors can be generated when a user tries to hide too much data in a small carrier file, or when OpenPuff password strength requirements are not met when hiding data in a carrier file. In general,

however, with several minutes of practice any person with basic computer skills will be able to easily use OpenPuff to conceal sensitive information.

Using Steganography

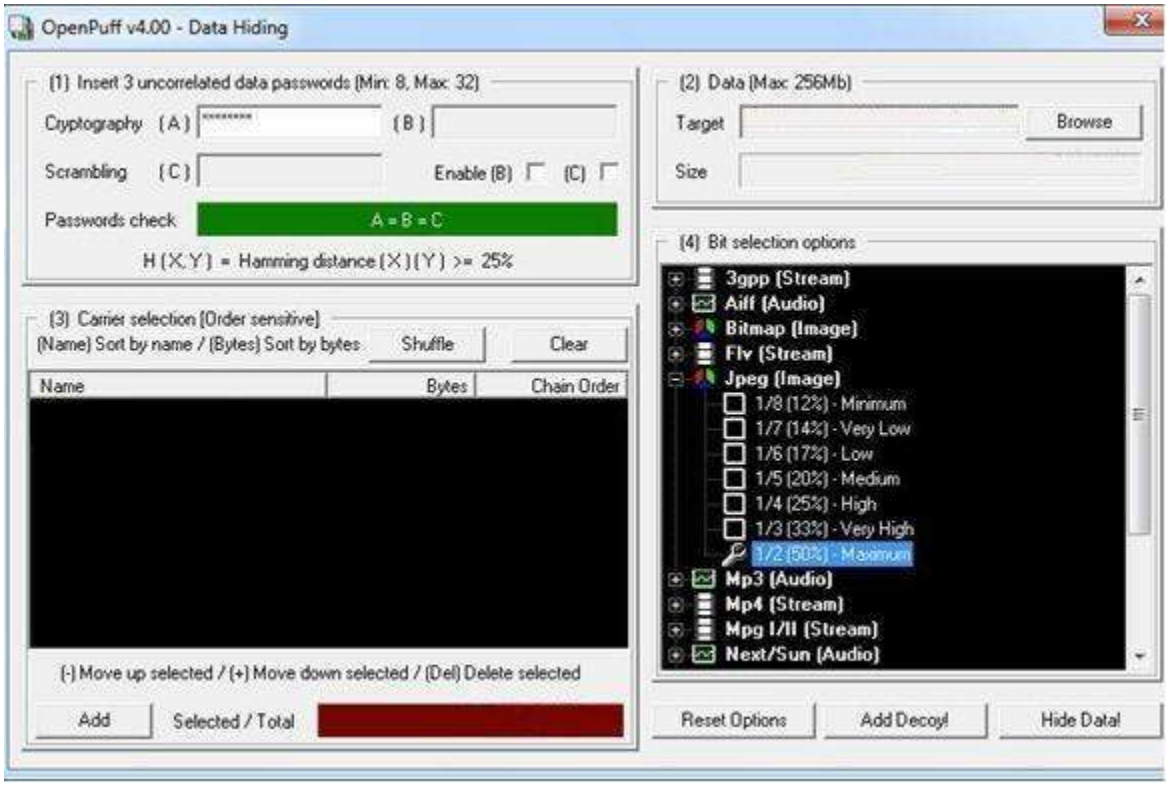
A primary purpose of steganography is to hide sensitive information from censors, abusive regimes, spies, and thieves. Information that appears to be mundane, innocuous, and perhaps even a little bit boring will attract little attention. Information that is encrypted, using PGP for example, may not be able to be decrypted and read by an adversary, but the use of encryption may cause an adversary to believe that the message contains sensitive or illicit information, whether it does or not. In some places the use of strong encryption may be restricted or prohibited. Steganography allows encrypted information to be hidden from prying eyes.

When using steganography to transmit information there should be a plausible reason for sending a file to someone in the first place. Just sending attached photos or files without any associated comments or context can appear suspicious. Instead of sending a file to someone directly, an innocuous photo might be posted to a web-page or on-line forum. Anyone that wanted to do so could copy the photo, but only someone with OpenPuff and knowledge of the correct passwords could recover any hidden information that the photo might contain.

It should be noted that because of the way some social media sites, like Facebook, process posted photos, information hidden using OpenPuff, and other steganography programs, may be corrupted or destroyed in photos uploaded to these sites. If using a social media site to exchange information using steganography it is important to conduct tests to ensure that data integrity is maintain in uploaded files.

Steganography works well to hide small amounts of sensitive data in otherwise innocuous information. The greatest limitation of steganography is that carrier files must be significantly larger than the data being hidden. You can't hide the text of a large book in a small image file. Large amounts of data are best hidden in audio (wav) or stream files (Mp4), and OpenPuff does this quite well. With OpenPuff you can also split large amount of data over multiple carrier files.

As with all security tools, it is important to practice using OpenPuff to become proficient, and to be able to take full advantage of the capabilities of the software. OpenPuff is an important tool for security researchers and for anyone who needs to share sensitive information.



Conclusions

OpenPuff is certainly not the only steganography tool available. There are several other steganography tools available (some of which are quite good), but in the opinion of the author OpenPuff is the best steganography tool currently available. OpenPuff's ability to encrypt data, conceal that data in several different types of carrier files, split data over multiple carrier files, and provide for the hiding of decoy data to help guard against coercion – forcing someone to disclose passwords used to protect hidden information – makes OpenPuff must have security software.

Download the OpenPuff user's manual: http://embeddedsw.net/doc/OpenPuff_Help_EN.pdf

OpenPuff Homepage - EmbeddedSW.Net:
http://embeddedsw.net/OpenPuff_Steganography_Home.html