[Windows] Best free steganography program (i.e. hide files within other files)

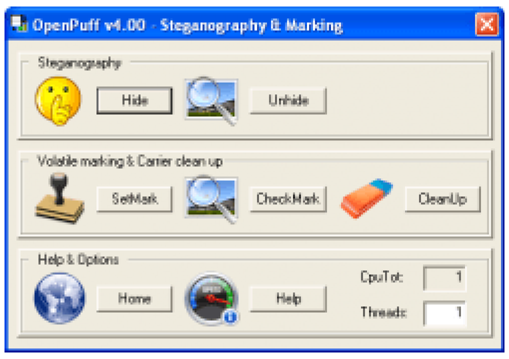
Posted By *Ashraf* On April 15, 2013 @ 12:15 AM In Best Free Windows Software | 9 Comments

A popular way for people to protect their files is encryption, using programs like TrueCrypt and AxCrypt [1] to prevent unauthorized access to data. The only problem with encryption is it is typically obvious that a file is encrypted. Steganography is a different method of preventing unauthorized access to data and files that solves that problem.

What steganography does is it allows you to do is hide files within other files. For example, you can hide a Word file inside an JPG image. On the outside the JPG image is a normal JPG image; it even opens and is viewable like a JPG image. However, under the JPG image is the hidden Word file which can be extracted by the people who know it is there.

Best Free Steganography Program

[6]*Program Name:* OpenPuff [7]



Developer: Cosimo Oliboni

Download Size: 5 MB

Version Reviewed: 4.00

Supported OS: Windows

Pros

Allows you to hide any file (regardless of type) inside an image (BMP, JPG, PNG, TGA, PCX), audio (AIFF, MP3, NEXT/SUN, WAV), video (3GP, FLV, MP4, MPG, SWF, VOB), or PDF file

Note: Files that hold hidden files are called "carriers"

Can hide one file split across multiple carriers

Hidden files cannot be accessed without a password

Allows you to enter up to three passwords, making it harder for someone to crack (aka they must know all three passwords); if you don't want to use all three passwords, you can use only one or two

Can hide files as large as 256 MB

Can hide a "decoy" file along with your main hidden file

When the password(s) for the decoy file is entered OpenPuff shoots out the decoy file and the password(s) for the main hidden file is entered OpenPuff shoots out the main hidden file. The idea here is you can give someone the password(s) for the decoy file if you are forced to reveal the password(s).

When hiding a file inside carrier(s), uses four levels of security to ensure files are safe: encryption, scrambling, whitening, and encoding

Can insert a hidden "mark" (i.e. text watermark) on carriers

Has a built-in ability to "clean" carriers (i.e. remove hidden files from carriers)

Makes it extremely hard for someone to accidentally unhide hidden files. Hidden files can only be extracted when: a) the password(s) are known b) the correct carrier is selected or carriers are selected in the right order, if multiple carriers were used and c) the same bit selection is used that was used when file being originally being hidden

Aside from file size and date and time accessed, carriers remain untouched and work as normal. For example, if you use a carrier as an image then that carrier remains an image that you can view even after using it as a carrier

Is portable and open-source

Cons

Has a learning curve, although the curve isn't too big — learned the program isn't too difficult

The method to unhide (i.e. need password(s), carrier(s) in same order, and correct bit selection) can make it a bit annoying for people to unhide files (e.g. if you forget what order the carriers were in or if you forget which bit selection you had used)

Has an inherent limit on how many bytes of data one carrier can hold; this limit varies from carrier file to carrier file. Having this limit isn't that big of an issue (it has to do with the way OpenPuff works and its enhanced security measures). What is an issue is there is no way of knowing how many bytes of data a specific carrier can hold until you actually load it into OpenPuff, which can make it annoying to find a large enough carrier to hold your hidden file

Can only hide one file at a time; no batch processing is supported nor can you hide multiple files inside the same carrier

Note: You can get around the one-file-per-carrier(s) restriction by ZIPing or archiving the files you want to hide before throwing them in OpenPuff

Would be nice to have more selection for carrier file types, such as ZIP or RAR

When selecting carriers for hiding files, by default "All files" is enabled and you are shown all file types even though you cannot use all file types as carriers. This may result in you accidentally selecting an unsupported file type which will cause you go to back and select again. This can get annoying

Cannot hide files larger than 256 MB

Program window cannot be minimized or resized, only closed

Discussion

TrueCrypt is known and respected as one of the best, if not the best, encryption tools primarily due to how it goes above and beyond encryption — all the other features it has are what make TrueCrypt special, like plausible deniablility. Similarly, OpenPuff is an excellent steganography program not just because it can do steganography; there are tons of programs that can do steganography. Rather, OpenPuff is exemplary because it goes above and beyond steganography thanks features such as its multiple layers of protection, ability to use decoy files, ability to split one file across multiple carriers, portability (yep, doesn't need to be installed), and more.

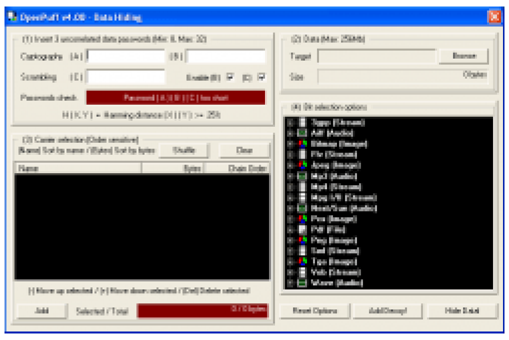
In fact, my two favorite features of OpenPuff are plausible deniability (the decoy feature) and its ability to split one hidden file across multiple carriers. These two features are awesome simply because they allow for added security that most other steganography programs lack. The other feature I like in OpenPuff is the fact that it uses four layers of protection to ensure your hidden files stay hidden until you unhide them with OpenPuff; OpenPuff encrypts, scrambles, whitens, and encodes all hidden files, making it extremely (extremely) hard for someone to gain access to your files without your password.

In terms of features, OpenPuff rocks. I cannot think of or find a steganography program that provides more security than OpenPuff. Where OpenPuff falls down is its usability.

You see OpenPuff has a butt-ugly interface and has options that are not necessarily self explanatory. It isn't that the program is impossible to use or understand, but newbies to OpenPuff will definitely scratch their head asking themselves "what does this do" at multiple stages of the program; however, once you learn OpenPuff, it is a breeze.

When you first run the program, you can prompted with the main-program window that has the following options:

Hide (hide a file)
Unhide (unhide hidden file)
Mark (add text watermark to carrier(s))
UnMark (remove text watermark from carrier(s))
CleanUp (remove hidden file from carrier(s))



[8]When you go to Hide, you are prompted with the Data Hiding window in which you must specify five parameters:

Password. By default you are asked by OpenPuff to enter three different passwords of minimum eight characters each, all of which must be used to unhide the file you are about to hide. If you don't want to use three passwords, you can manually disable up to two of them so that you only use one password.
File you want to hide. You can hide any file of any file format you want. You can only hide one file at a time — you cannot hide multiple files inside one carrier.
Carriers. Carriers are the files that hold your hidden file. You can have one carrier or as many carriers as you want; if you use multiple carriers, your hidden file is split among the carriers and you can only unhide your file if you use all carriers. Not only that must it is important to remember the order of the carriers you have used because you must load the carriers in the exact same order when you go to unhide your file, otherwise you will not be able to unhide.
OpenPuff is unable to use all file types as carriers; there is a specific list of file types that can be used as carriers by OpenPuff: BMP, JPG, PNG, TGA, PCX, AIFF, MP3, NEXT/SUN, WAV, 3GP, FLV, MP4, MPG, SWF, VOB, and PDF.
It is important to note, because of the way OpenPuff works with its advanced security measures, each carrier can only hold a certain amount of data. This amount of data varies from file to file. OpenPuff tells you exactly how much data a carrier can hold once you load the carrier inside OpenPuff. There is a "Selected / Total" bar at the bottom of the program window that tells you how many bytes your carrier can hold (Selected) and how many it needs to hold your hidden file (Total). The bar is red if the carrier you selected is too small. If this is the case, you either need to pick a different carrier or use multiple carriers until the bar turns green.
Bit selection. This is probably the most confusing of all things when hiding files. Bit selection has to do with behind-the-scenes algorithms OpenPuff uses. However, you don't really need to worry about what OpenPuff is doing behind the scenes. Rather, you need to understand that via this setting, you can increase the amount of bits a carrier can hold. By default carriers are set to the Medium setting; if you want a carrier to hold more bytes, you can change up to Maximum. To change bit selection, you need to click on the option for the particular file type of carrier you are using. If you are using multiple different file types as carriers, you need to modify the setting for each file type.
It is important to remember what bit selection you use because you must select the same bit selection when unhiding files, otherwise you won't be able to unhide files.
(OPTIONAL) Decoy. OpenPuff has the ability to allow you to insert a "decoy" file. Like you set a password for your hidden file, you must select a password for your decoy file. Then, when you go to unhide your hidden file, if you enter the password for your hidden file then you are given your hidden file; if you enter the password for your decoy, then you are given the decoy file. The idea here is you can give someone the password for the decoy file if you are ever forced to reveal your password.
Once you are done with that, you hit the Hide Data button and OpenPuff hides your file inside the carrier(s) you selected. The whole process is a bit confusing at first but becomes second nature if you use the program often.

Overall, OpenPuff has its shortcomings but it is the best free steganography program I have ever used. Highly recommended.