



# StegTorrent

- 2003-04-22: Version 2.0.0.1 [released](#)
- 2003-04-17: StegTorrent is a [SourceForge project](#) now
- 2003-04-15: Version 0.1.2.1 [released](#)

Just installed StegTorrent and eager to try it out? Here is a [sample stego image](#).

[intro](#)

[what](#)

[why](#)

[how](#)

[help](#)

[install](#)

[operate](#)

[faq](#)

update: 2003-04-22  
[xhtml](#) 1.1 + [css](#) 2.0

SOURCEFORGE.NET

stegtorrent and this doc  
 © [henry 'pj' james](#)  
[bittorrent](#) © bram cohen  
[steghide](#) © stefan hetzl

## what

StegTorrent is both a concept and an user friendly, graphical tool implementing this concept. The basic idea is to hide [BitTorrent](#) metainfo (.torrent files) into images or sounds. StegTorrent provides an easy interface to restore the .torrent files (somewhat) automatically from those special images or sounds. From the end user's point of view, these images and sounds should be usable just like normal torrents to retrieve files via the BitTorrent protocol.

## why

Firstly, a general purpose of [steganography](#) is the protection of privacy. This also applies to StegTorrent. For whatever reasons, if a person wants to publish .torrent files without drawing attention (e. g. avoid being [googled](#)), she can do so by embed the torrents into JPEG files. Even if these JPEG files themselves get googled, it's still hard for a third party to detect the torrents hidden within.

Secondly, steganography is a cryptographical process, and plain data are embedded into cover data with a crypto secret (called "watchword" in StegTorrent). This can be used as a kind of access control. Of course, there are lots of other (and better) ways to encrypt a .torrent file, but the point here is the *combination* of both hiding and protecting, creating an extra level of security. Also, the possibility of placing the watchword into the cover image, either as [human readable text](#), or by suggestion and association through subjects in the image, makes it very hard, if not impossible, to automatically scan larger amount of images for embedded .torrent files.

Thirdly, the idea of merging .torrent files and media files brings a positive side effect to StegTorrent, making it useful even without any privacy and security concerns. While choosing media files as cover data, it is possible to pick such files which have a descriptive and/or demonstrative function regarding the target of the torrents. For instance, rather than having the poster of a movie and a torrent for it's trailer, why not just *embed* the torrent into the poster image?

The idea of applying steganography to .torrent files strucked me one night out of sudden. And the more I think about it, the more useful it appears to me. I believe it's perfectly possible to find even more beneficial aspects of it than those I'm already aware of right now.

## how

StegTorrent is designed as an easy user interface only, it has neither integrated functions to retrieve data via the BitTorrent protocol, nor does it do the steganographical work itself. Instead, it relies on an Open Source, command line tool called [steghide](#) to extract plain files out of stego files. Once properly installed, StegTorrent will call steghide internally when it's

needed. The user does not need to bother with it. After the .torrent file is restored, StegTorrent can launch it using whatever program .torrent files are associated with in the user's current system. Normally, this would be BitTorrent.

In fact, StegTorrent is not limited to BitTorrent and .torrent files at all. It can be used as a general GUI for steghide's extraction function since it doesn't really care about what kind of file it restores. However, StegTorrent refuses to directly launch files other than \*.torrent for obvious security reasons (like if the restored file is a virus or spyware). It can still show restored non-.torrent files in Windows Explorer and let the user decide what to do with it.

Currently StegTorrent only provides an interface to restore plain files from stego files, not for creating such stego files. If the user wants to embed a torrent into an image, she needs to use steghide directly. It is just a single command to type in, and described [below](#).

---

## install

StegTorrent is released in a ZIP archive. Just extract the whole archive wherever you want using whatever unzip tool you prefer.

Then you need steghide. This is a *must*, without it StegTorrent wouldn't work. You can download steghide from its official [website](#). There, at the download page, click "for Windows: steghide.exe with libraries". What you get is again a ZIP file, and you need to extract at least "steghide.exe" (one file) and "cyg\*.dll" (five files) into the *very same* directory you placed StegTorrent earlier. (If you are a Cygwin user, which is very unlikely, you don't need to extract all the "cyg\*.dll" files, but only those not included in your Cygwin installation. In fact, take care of possible version conflicts of duplicated libraries.) As a result, "STorrent.exe" and "steghide.exe" should lie in the same directory.

Now you can start StegTorrent by (double) clicking "STorrent.exe". When StegTorrent starts, it checks if "steghide.exe" can be found where it's supposed to be. If not, an error message will appear. Otherwise simply continue.

## operate

The easiest way to use StegTorrent is via drag 'n' drop. If you're using Internet Explorer, you can simply drag a stego image (where a .torrent file is hidden within) from your IE over to StegTorrent. (Technically the image file in your browser cache will be dropped into StegTorrent.) Unfortunately this does not work with Mozilla or Opera, since each browser has its own logic and its own way to handle drag 'n' drop. The way IE does it just happens to fit the operation of StegTorrent. (I like to explicitly point out that I'm an "advanced" Mozilla user and frequent Opera user, too, and only takes IE when it has to be.)

But even aside of Internet Explorer, drag 'n' drop is possible from Windows Explorer to StegTorrent. (Again I must say I hate Windows Explorer and almost never use it. I use [GeoShell](#) as system shell and [FAR](#) as file manager.) If you are not a friend of drag 'n' drop at all (like myself), you can still click on "..." or press Ctrl+O to browse for the stego file, or directly enter its file name the hardcore way.

After telling the StegTorrent what stego image/audio/file to handle and clicking "Restore", you are asked for the watchword. If you have not been told what watchword to use, try the default "BitTorrent". If that's not the correct one, StegTorrent will show you an error message and let you retry. In some cases, the watchword may be written in readable text on

the stego image, or it could be suggested by the content of the stego image (or audio). Does the stego image show a forest, you may want to give "forest" a try.

With any luck, you've typed in the correct watchword. After StegTorrent restores the original file successfully, it shows you the file name (with full path) and offers you to open it right away or show it in Windows Explorer. If the file is not "\*.torrent", the "Open" button will be disabled, so you won't mistakenly install a virus and/or spyware your evil enemy packed into a picture of a naked young girl and sent to you claiming it were a torrent for some hardcore action pr0n.

The StegTorrent window is "Always on Top" by default. This can be changed within its system menu (left click the icon or right click the titlebar or the title in Windows taskbar) or by simply pressing Ctrl+T. A "Minimize to System Tray" option *may* be added in a future version.

## faq

I got an error saying "steghide: the distribution method saved in the stego header is unknown (file corruption ?)." What does it mean?

It means you most probably typed in the wrong watchword.

Your pathetic little proggy sux! I wanna crack the stego file maself to get the torrent.

```
steghide.exe extract -H -sf <stego_file>
```

This thing is cool! How do I hide my own torrents into such stego (image/audio) files?

```
steghide.exe embed -H -E -pf <plain_file> -cf <cover_file> -sf
<stego_file>
```

The <plain\_file> would be your .torrent file, the <cover\_file> an arbitrary JPEG, BMP, WAV, or AU file (these are the only file types supported by steghide). The <stego\_file> would obviously be the stego file to create. You can only embed one .torrent file into a cover file at a time.

I suggest you use a JPEG file as cover file. The size of the JPEG file should be at least 3 to 4 times as large as the plain (.torrent) file you want to hide. Regarding the content of the image, something related to the actual target of the torrent would be fitting and also raises less suspicion in case you name the stego file similar to the torrent. Ideal cover files are, for example, photographs containing noisy subjects with lots of colors (e. g. landscape, flowers, downtown traffic) because they are easier to manipulate without making much visual difference. Compare the resulted stego image to the original cover image, also compare the size of these both files. The little their size difference is, the better your choice of image has been.

For normal cases, I recommand you to use the default watchword "BitTorrent". If you don't like it, but have no reason to keep the watchword secret, either, you may consider adding the watchword as text onto the image. This can be done with any image editing software.

Can I use any other steganographical tools/libraries instead of steghide?

Theoritically of course. But StegTorrent in its current form can only interact with

steghide. As far as I know, there is no common protocol or format for steganographical tools, so the encrypted data they create are also incompatible to each other. steghide is simply the best Open Source tool I can find for StegTorrent's purpose. If you know [better](#), feel free to [tell me](#).