July 21, 2011 Computer Forensics, Cyber spying, Forensics 0 Comments

Steganography and Digital Watermarking Tools

 On 2010 Moscow communicated with a ring of alleged spies in America by encoding instructions in otherwise innocent-looking images on public websites. It's a process called steganography. Steganography is a smart way to hide data into other files, called carriers.

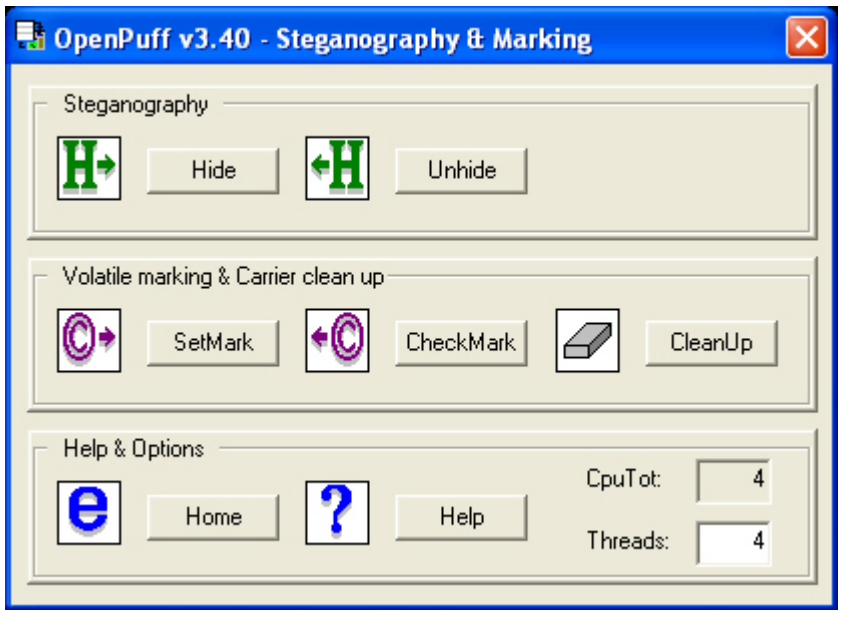
Modified carriers will look like the original ones, without perceptible changes. The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.

Today we can use some free tools to create covert transmission for any sensitive data or to protect your copyright. Protecting files copyright is by using Watermarking which is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners.

Still images, video, music, text, and software are all easily copied and illegally distributed, causing the authors to lose out on considerable income in royalties. By embedding identifying information in a file, watermarking software enables authors to control the distribution of and to verify ownership of their digital information.

First tool is OpenPuff a freeware steganography tool for Microsoft Windows created by Cosimo Oliboni and still maintained as independent software author. The program is notable for being the first steganography tool (version 1.01 released on December 2004) that:

- Let's users hide data in more than a single carrier file. When hidden data are split among a set of carrier files you get a carrier chain, with no enforced hidden data theoretical size limit (256Mb, 512Mb, … depending only on the implementation)
- implements 4 layers of hidden data obfuscation (cryptography, scrambling, whitening and encoding)
- extends deniable cryptography into deniable steganography



The current version is OpenPuff 3.40 and released on the 18th of July.

Another interesting tool is QuickStego which lets you hide text in pictures so that only other users of QuickStego can retrieve and read the hidden secret messages. Once text is hidden in an image the saved picture is still a 'picture', it will load just like any other image and appear as it did before. The image can be saved, emailed, uploaded to the web as before, the only difference will be that it contains hidden text.