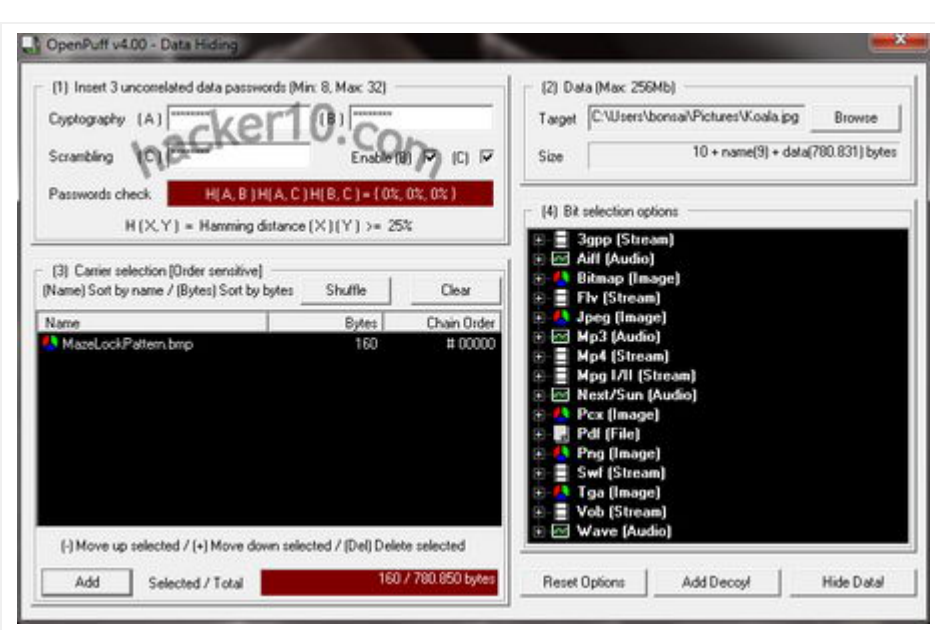
Steganogaphy and hidden watermarks with OpenPuff

OpenPuff is a portable steganography tool supporting images, audio, video and Flash Adobe animation carrier files, it can conceal up to 256MB of data splitting files in between multiple carriers. Before hiding data everything is securely encrypted with AES, scrambled, whitened and encoded, this reduces the chances of anything hidden being detected by specialist tools, you must always remember to erase the original carrier files. If a computer forensics expert has access to both files and can compare them he should be able to prove that one of them contains hidden data even if it can not extracted because everything inside the has been encrypted. OpenPuff has sixteen different encryption algorithms you can use, this makes extracting data even more difficult as only the creator will know what cipher has been used, the tool supports well known secure algorithms like AES, Serpent and Twofish and more obscure ones, like Mars, Anubis or Clefia, a high speed block cipher developed by Sony Corporation intended for use in Digital Rights Management.

To stop steganalysis, the detection of hidden data, encrypted files are scrambled with a second layer using a pseudo random number generator (CSPRNG) seeded with a user chosen password with data shuffled using random indexes, a third security layer whitens scrambled data adding a high amount of ramdom noise with hardware entropy and the final fourth security layer encodes whitened data using a non-linear function. Very paranoid types can add a decoy file for deniable steganography, just like Truecrypt hidden container works, in OpenPuff you can reveal a password to an innocuous text and keep the real hidden message from view with a second password. Another feature is the ability to hide a mark inside a video, audio or photograph, useful for when you privately distribute a confidential file to a selected group of people, if the file is later on found leaked on the internet you can check the mark and track down the leak source.



OpenPuff steganography freeware

The software interface is a little overwhelming for the steganography novice and drag and drop doesn't work, you have to select everything manually, but security experts should appreciate things like a window with bit selection options showing a huge list of supported carrier files and the ideal data percentage that can be hidden in each different extension to avoid detection, with a third optional password seeding the scrambling CSPRNG, you can use up to three passwords to hide data inside a file, the other end will have to know all of them to decrypt it.

Thanks to the support for a wide range of carrier files (*.bmp, .jpg, .png, .mp3, .vob, .mp4, .3gp, .flv, .swf, .pdf*, etc) the program makes it easy to embed hidden data anywhere on the Internet, from a blog to a photo sharing site like Flickr, saving you from having to personally contact a source, which could compromise his identity, but if you are hiding data in multiple files to decrypt them the other end will have to order the files in the right sequence. OpenPuff needs a little practise to get everything right but it is one of the most complete steganography tools I have seen and it has some unique features.