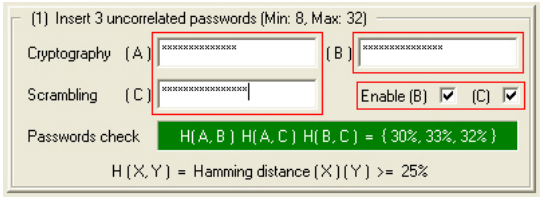
DATA UNHIDING STEP BY STEP

BEGIN:

(*Unhide*)	Go to unhiding panel

Select *Unhide*.

STEP 1:

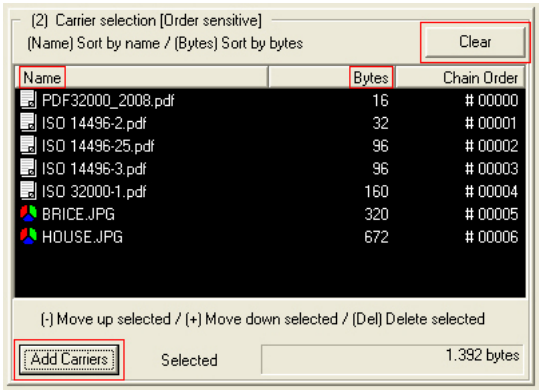


(*Cryptography A*)	First password (cryptography keys)
(*Cryptography B*)	Second password (cryptography CSPRNG)
(*Scrambling C*)	Third password (scrambling CSPRNG)
(*Enable B*)	Second password enable/disable
(*Enable C*)	Third password enable/disable

Insert your passwords (secret to get secret data, decoy to get decoy data), enabling only those used at hiding time.

SUGGESTIONS FOR BETTER RESULTS
WHAT IS DENIABLE STEGANOGRAPHY?

STEP 2:

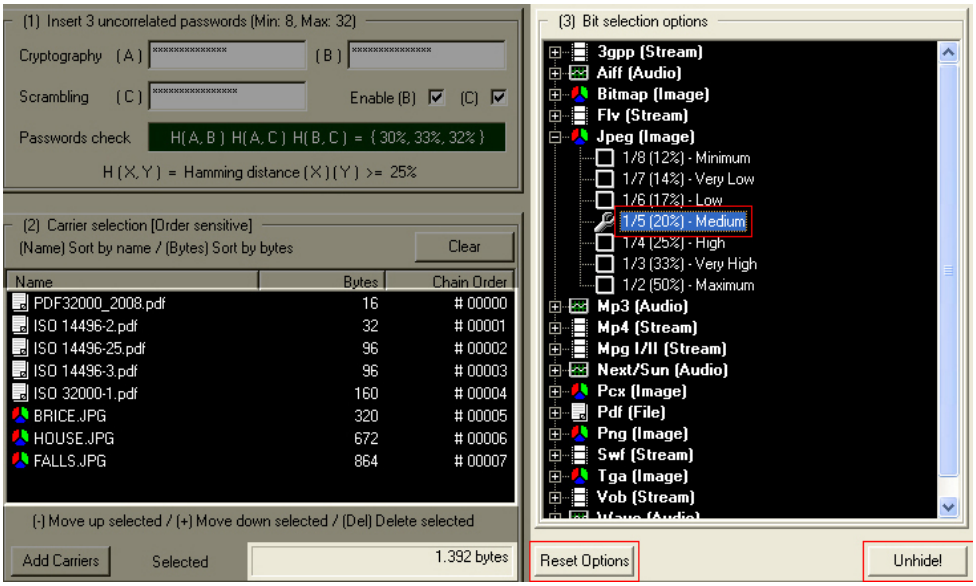


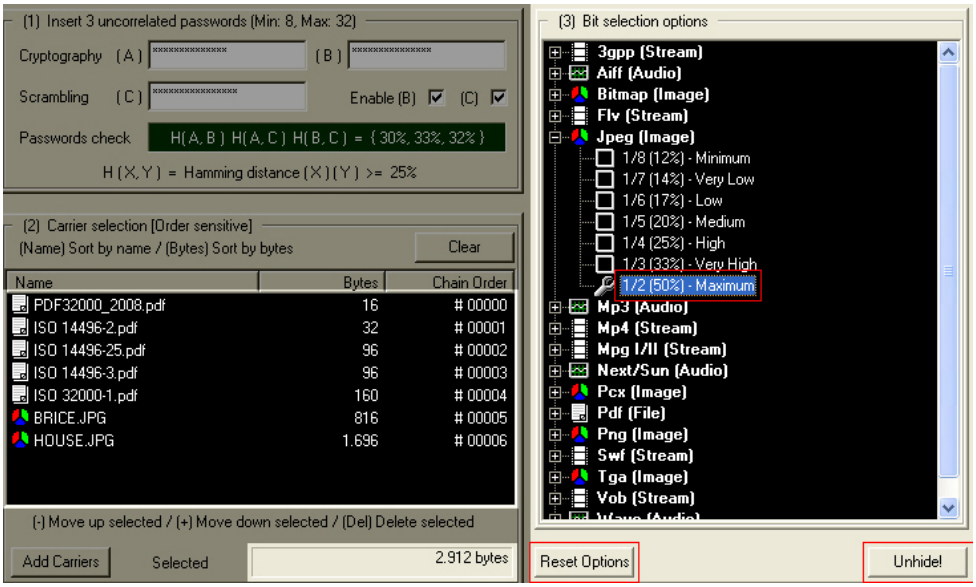
(*Clear*)	Discard all carriers
(*Add*)	Add new carriers to the list
(*Name*)/ (*Bits*)	Sort carriers by name/bits
(*+*)/(*-*)	Move selected carriers up/down
(*Del*)	Delete selected carriers

Add all the carriers that have been processed during the hide task.

SUPPORTED FORMATS IN DETAIL

STEP 3:





(*Reset Options*)	Reset all bits selection level
(*Unhide!*)	Start unhiding

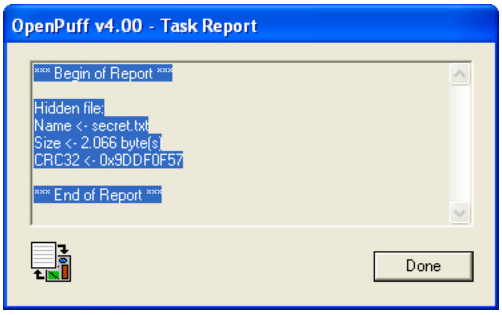
After

- typing twice the same password
- adding all the carriers, in the right order
- setting all bits selection levels to the original value

start the unhiding task

OPTIONS: BITS SELECTION LEVEL

TASK REPORT:



If carriers have been added in the right order, with the original bits selection levels, OpenPuff will be able to reconstruct the original data. For better security, data will be reconstructed only after a successful CRC check.

Even the slightest change in one of the carrier could damage the data and prevent every unhiding try.

BACK