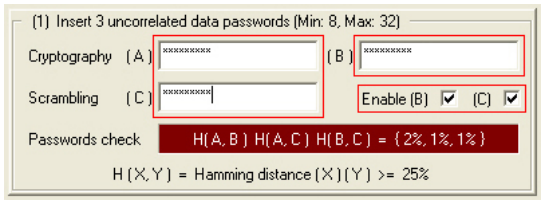
DATA HIDING STEP BY STEP

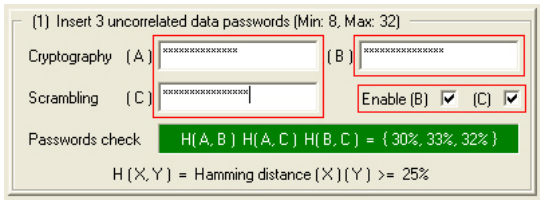
BEGIN:

(*Hide*)	Go to hiding panel

Select *Hide*.

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 three separate passwords. Each password has to be different (at bit level) and at least 8 characters long. Password type and number can be easily customized disabling the second (B) and/or the third (C) password. Disabled passwords will be set as the first (A) password.

Example: “DataPssw1” (A) “DataPssw2” (B) “DataPssw3” (C)

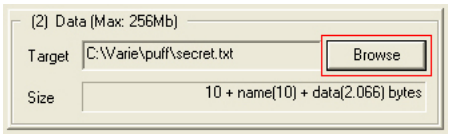
(A) **01000100 01100001 01110100 01100001 01010000 01110011 01110011 01110111 00110001**
(B) **01000100 01100001 01110100 01100001 01010000 01110011 01110011 01110111 00110010**
(C) **01000100 01100001 01110100 01100001 01010000 01110011 01110011 01110111 00110011**
(**A** ∩ **B**) 98%, (**A** ∩ **C**) 99%, (**B** ∩ **C**) 99%, HAMMING DISTANCE < 25% **KO**

Example: “FirstDataPssw1” (A) “SecondDataPssw2” (B) “AnotherDataPssw3” (C)

(A) **01000110 01101001 01110010 01110011 01110100 01000100 01100001 01110100 01100001** …
(B) **01010011 01100101 01100011 01101111 01101110 01100100 01000100 01100001 01110100** …
(C) **01000001 01101110 01101111 01110100 01101000 01100101 01110010 01000100 01100001** …
(**A** ∩ **B**) 70%, (**A** ∩ **C**) 67%, (**B** ∩ **C**) 68%, HAMMING DISTANCE ≥ 25% **OK**

SUGGESTIONS FOR BETTER RESULTS
WHAT IS DENIABLE STEGANOGRAPHY?

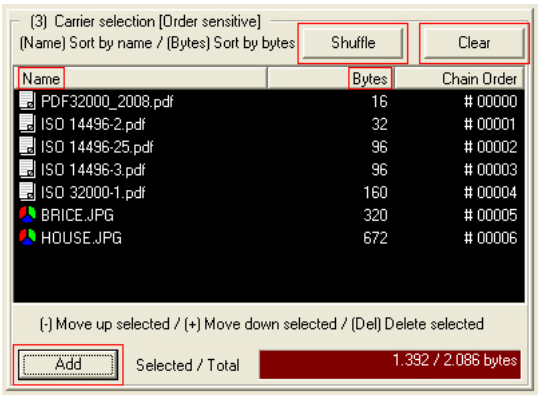
STEP 2:

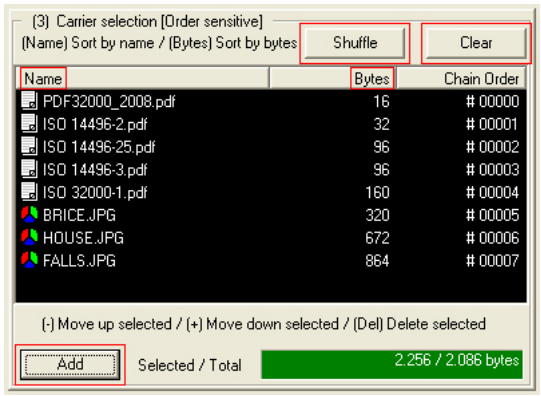


(*Browse*)	Select a file

Choose the secret data you want to hide (typically a zip/rar/… archive).

STEP 3:

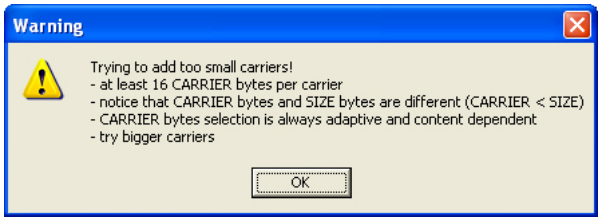




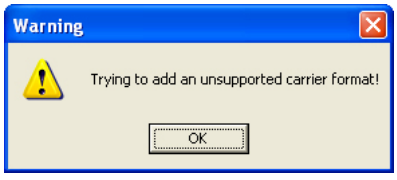
(*Shuffle*)	Random shuffle all carriers
(*Clear*)	Discard all carriers
(*Add*)	Add new carriers to the list
(*Name*)/ (*Bits*)	Sort carriers by name/bits
(*+*)/(*-*)	Move selected carriers up/down
(*Del*)	Delete selected carriers

Until *selected bytes* < *total bytes* try
- adding new carriers
- increasing bit selection level

(I)

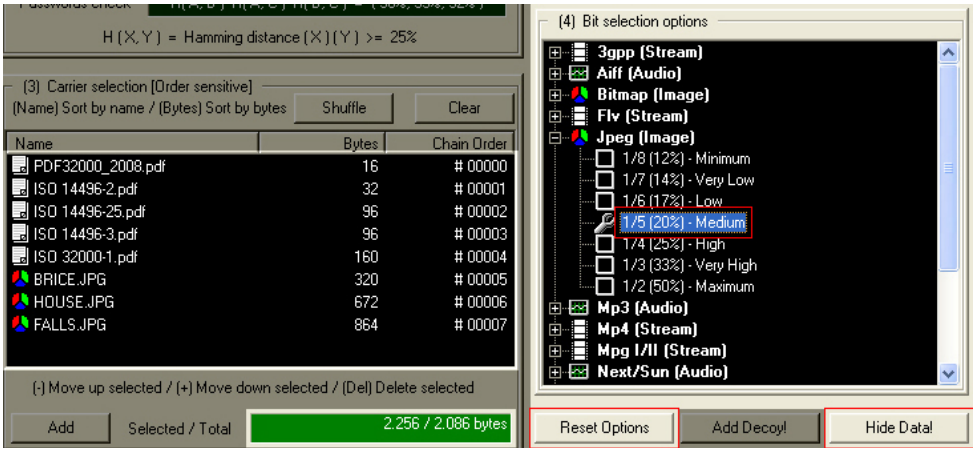


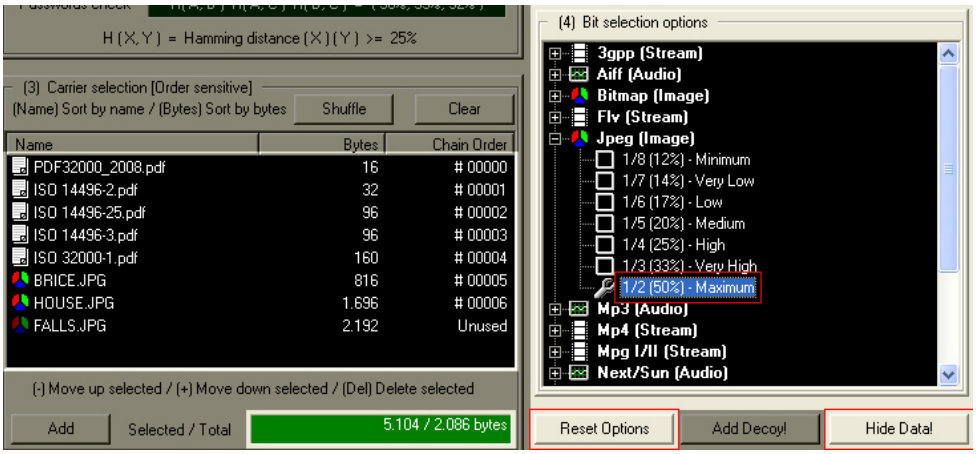
(II)



Some carriers will not be added because of steganography-process constraints
- (I) not enough carrier bytes (carrier bytes ⊂ carrier size)
  WHAT IS STEGANOGRAPHY?
- (II) unsupported format
  SUPPORTED FORMATS IN DETAIL

STEP 4:





(*Reset Options*)	Reset all bits selection level to normal
(*Add Decoy!*)	Add a decoy (deniable steganography)
(*Hide!*)	Start hiding

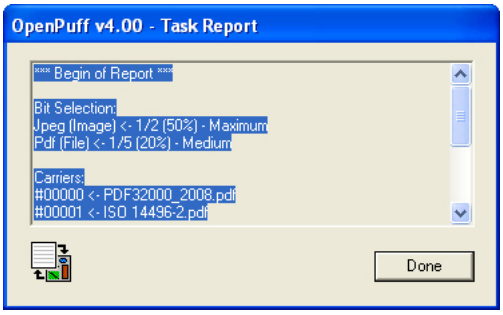
After

- typing twice the same password, at least 8 chars
- selecting a non-empty file to hide
- adding enough carrier bits
- adding a decoy (optional)

start the hiding task

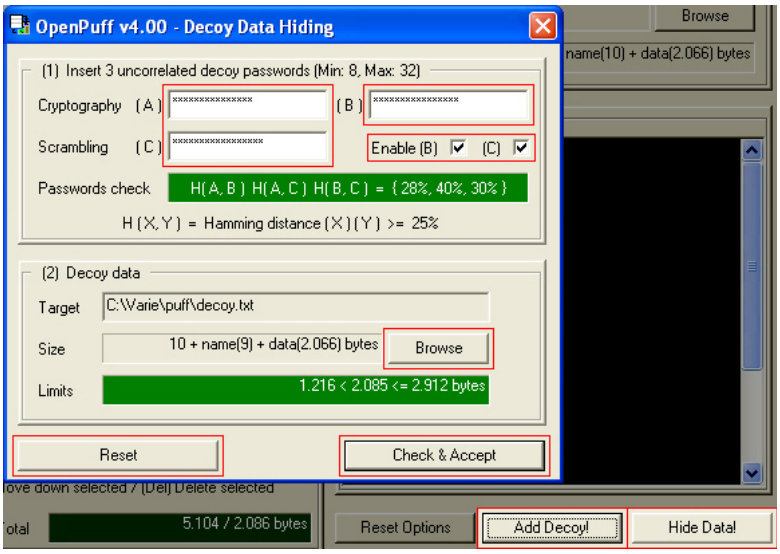
OPTIONS: BITS SELECTION LEVEL

TASK REPORT:



End report summarizes all information needed for a successful unhiding.

STEP 4 – (OPTIONAL):



(*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
(*Browse*)	Select a file
(*Reset*)	Reset password and file
(*Check & Accept*)	Check password correlation and file size

You can also add a decoy password and decoy data

- decoy passwords have to be each other **different**, and different from data passwords
- decoy password type and number can be customized like data passwords
- decoy data has to be **compatible** (by size) with sensitive data
  $\sum_{k \in \{1, N-1\}} used\_carrier\_bytes(carr_k) < Sizeof(Decoy) \leq \sum_{k \in \{1, N\}} used\_carrier\_bytes(carr_k)$

WHAT IS DENIABLE STEGANOGRAPHY?

BACK