



## Nascondere documenti in un'immagine o in altri tipi di file con OpenPuff

La **steganografia** è una tecnica che si prefigge, come obiettivo, quello di **nascondere informazioni importanti** in modo tale che non possano cadere nelle mani di malintenzionati, aggressori, concorrenti e curiosi. Le radici sono antiche: i primi utilizzi della steganografia risalirebbero, secondo alcuni studi, addirittura al 440 a.C. Lo storico greco Erodoto (484 a.C. - 425 a.C.) menziona due esempi di impiego della steganografia nella sua opera "Le storie". La tecnica fu poi teorizzata nel 1500 dall'abate Tritemio.

Nel campo dell'informatica, due interlocutori possono "mascherare" i propri messaggi "sotto mentite spoglie" inserendo il testo da mantenere segreto all'interno di file di diverso tipo (documenti, file audio e video, immagini,...).

Il concetto su cui si basa la steganografia è racchiuso nel suo stesso nome che deriva dai termini greci *stèganos* ("nascosto") e *gràfein* ("scrittura"): questa tecnica si pone di fornire un certo livello di sicurezza **mediante segretezza**.

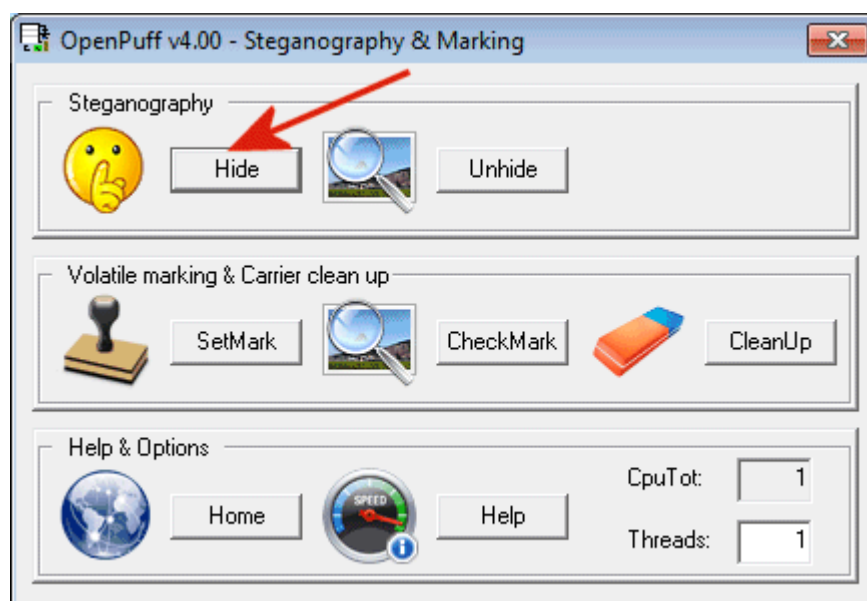
I software steganografici più validi non si limitano però a nascondere il messaggio da proteggere all'interno di una certa tipologia di file ma aggiungono una difesa in più, data dall'uso della **crittografia** sul testo in chiaro.

**OpenPuff** è un software freeware sviluppato e distribuito da un programmatore italiano che, tra l'altro, ne fornisce anche il codice sorgente. L'autore Cosimo Oliboni presenta la sua applicazione utilizzando lo slogan "*yet not another steganography software*", a rimarcare il fatto che OpenPuff contiene una serie di funzionalità "esclusive" che lo distinguono dai tanti programmi steganografici disponibili in Rete.

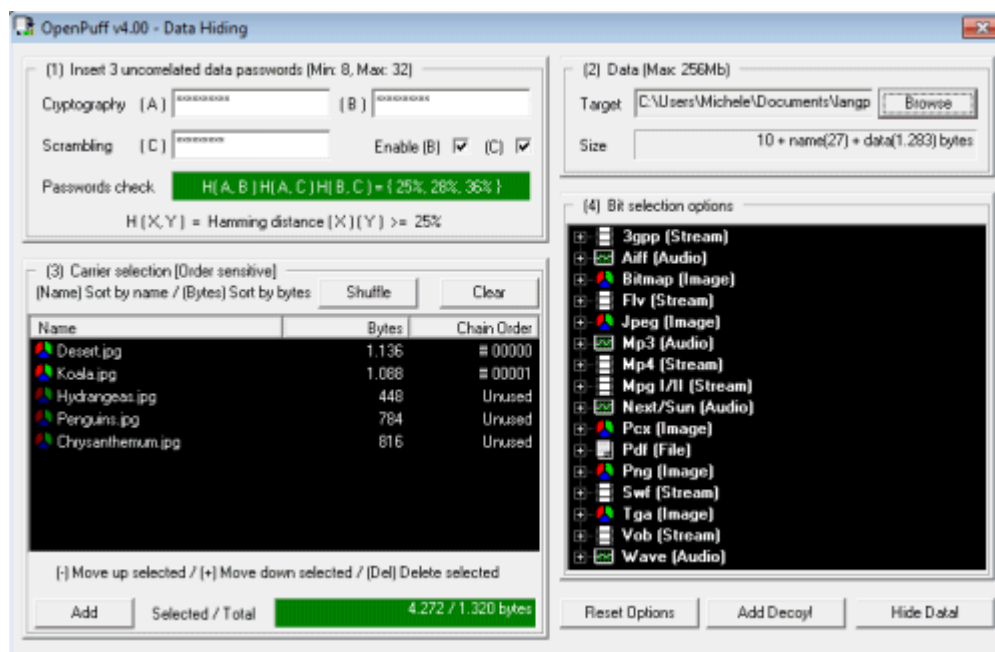
OpenPuff, innanzi tutto, è compatibile con tutte le versioni di Windows, non necessita di un account dotato di diritti amministrativi per essere avviato (non provoca neppure la comparsa degli avvisi di UAC) ed è portabile. A tal proposito, va osservato che dopo aver estratto il contenuto dell'archivio compresso di OpenPuff e fatto doppio clic sul suo eseguibile, il programma si avvierà immediatamente senza aggiungere alcun tipo di informazione nel registro di Windows ed astenendosi dal creare o modificare qualunque file sul disco fisso.

Il software provvede ad acquisire i file indicati dall'utente, li cifra utilizzando uno degli algoritmi supportati quindi ne salva una o più porzioni in più file di vario genere (BMP, JPG, PNG, MP3, WAV, MP4, MPG, FLV, SWF, PDF,...). Questi ultimi vengono definiti "*carrier files*" dal momento che sono utilizzati come "contenitori" per il trasporto delle informazioni sensibili.

Per nascondere un file contenente dei dati importanti all'interno di un'immagine o di un elemento multimediale, basta fare clic, dalla finestra principale di OpenPuff, sul pulsante *Hide* (riquadro *Steganography*):



La finestra che apparirà a video consente di specificare tre password (devono essere differenti l'una dall'altra) per proteggere le informazioni aggiunte ai vari file che fungeranno da contenitori. L'utilizzo di tre password differenti consente di fidare sul livello di sicurezza più elevato. Per specificarne solamente una o due, basta agire sulle caselle *Enable (B)* ed *Enable (C)*.

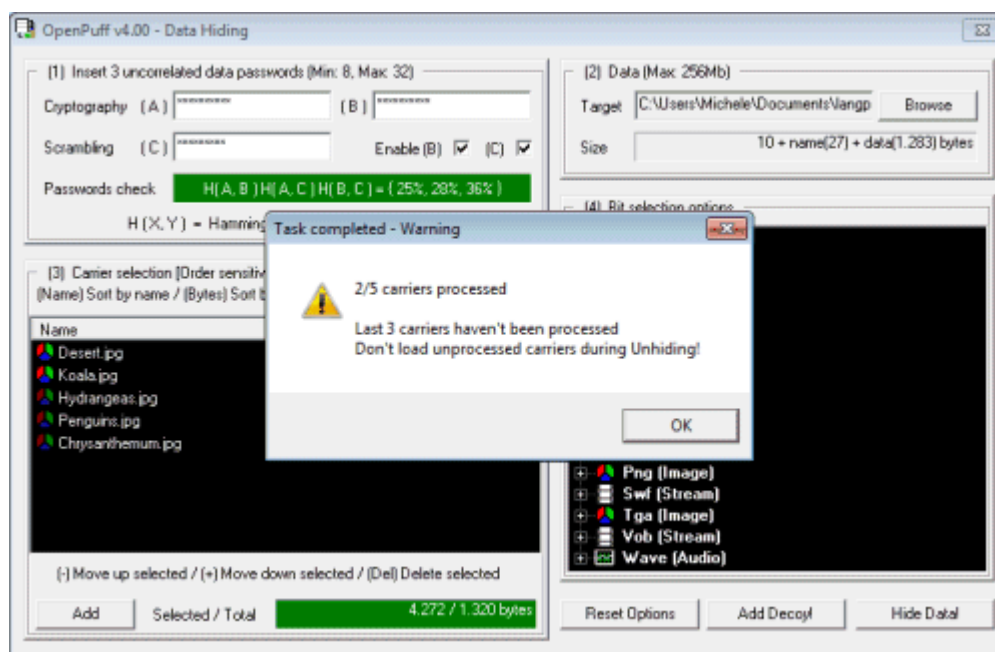


È necessario che la dimensione complessiva del *carrier file* che si specifica sia notevolmente superiore a quella del file che s'intende nascondere. Tipicamente, per ogni singolo MB oggetto dell'operazione di steganografia si dovrà disporre di un file *carrier* pesante circa 5 MB.

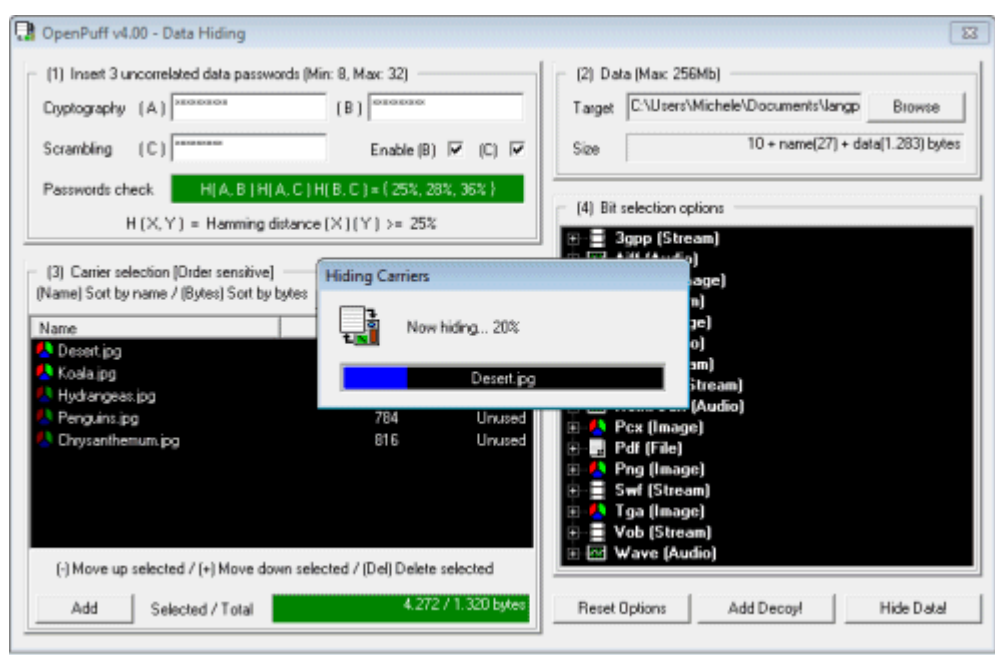
Dopo aver indicato (riquadro *Data*) il documento od il file da nascondere (deve avere dimensioni massime di 256 MB), si dovrà provvedere a specificare uno o più file-contenitore nel riquadro *Carrier selection*. Bisognerà aggiungere nuovi file-contenitore sintanto che la casella *Selected / Total* non si colorerà di verde.

Terminata la procedura, si dovrà fare clic sul pulsante *Hide Data!*, in basso a destra, per inserire, in forma cifrata il documento od il file indicato nel riquadro *Data* all'interno del o dei *carrier*.

Se i file *carrier* specificati sono in numero superiore al necessario, OpenPuff esporrà il seguente messaggio d'avviso:



La comparsa del messaggio non sta a significare che qualcosa è andato storto. Piuttosto, OpenPuff ricorda che per estrarre i file nascosti, ci si dovrà limitare a selezionare, dal supporto di memorizzazione, solo i file *carrier* utilizzati, nell'esatto ordine (nel nostro caso, il file *Desert.jpg* prima e *Koala.jpg* poi).



Per effettuare la procedura inversa e, quindi, annullare l'operazione steganografica, basta tornare alla finestra principale di OpenPuff e cliccare sul pulsante *Unhide* (riquadro *Steganography*).


OpenPuff, agendo sul pulsante *SetMark* consente anche di inserire una firma (una stringa di caratteri arbitraria) all'interno di uno o più file. Si tratta di uno strumento in più che permette di attestare che uno o più oggetti siano di propria produzione.

Utilizzando la tecnica della steganografia si hanno notevoli vantaggi. Oltre, nel caso di OpenPuff a poter fidare - a difesa dei propri dati - su di un elevato grado di sicurezza derivante dall'impiego di solidi algoritmi crittografici e dall'uso di tre password di protezione, servendosi della steganografia si può negare che una certa informazione sia in proprio possesso. Questa possibilità si rivela particolarmente utile allorquando qualcuno cerchi di estorcere

dati sensibili ed informazioni importanti che debbono restare segrete.

L'importante – si tratta di un punto che l'autore di OpenPuff ha più volte evidenziato – è che i file *carrier* non siano in alcun modo modificati. Diversamente, non si sarà più in grado di recuperare il contenuto in essi nascosto.

Cliccando qui è possibile scaricare un completo manuale in formato PDF (in italiano) che illustra molti dettagli tecnici sul funzionamento di OpenPuff.

 **OpenPuff** è prelevabile gratuitamente cliccando qui.

---

di *Michele Nasi* (pubblicato giovedì 12 luglio 2012)



Gli interessati ad utilizzare il materiale pubblicato sulle pagine de ISoftware.it sono pregati di richiedere l'autorizzazione. Lo staff de ISoftware.it non è responsabile per i danni che le informazioni contenute in queste pagine possono arrecare al vostro sistema. Tutti i marchi citati in queste pagine sono copyright dei rispettivi proprietari.