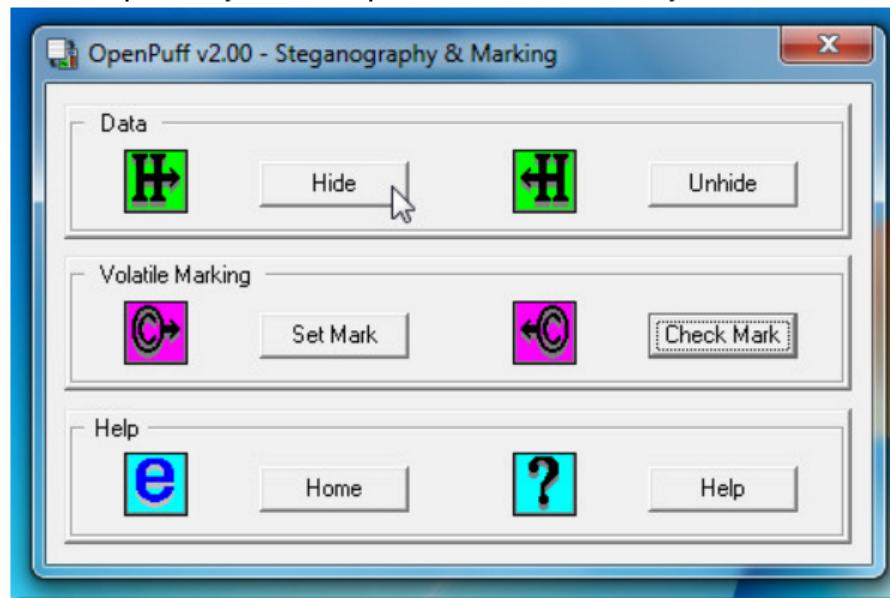


OpenPuff: Sign The Document/Application And Hide File Inside Other File

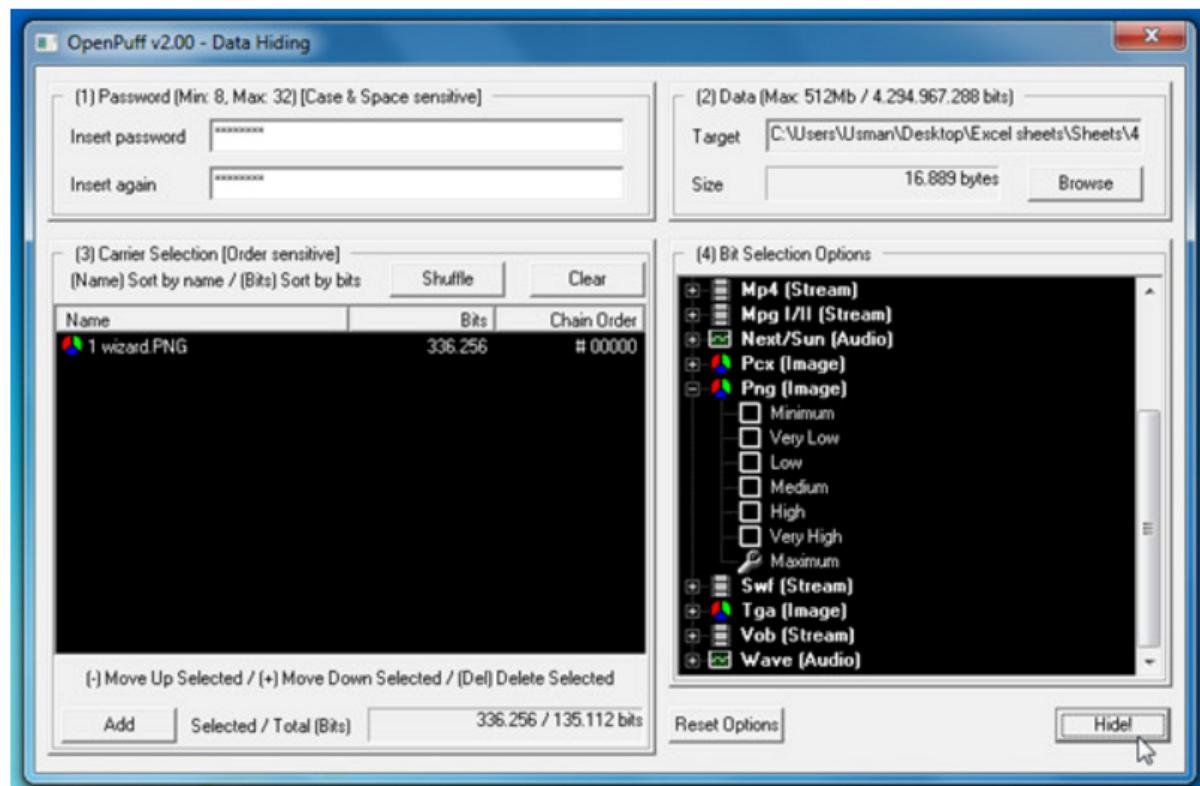
By Usman on Jul 26 2010  2 Comments

OpenPuff is a powerful Steganography and Marking tool. For those who don't know about steganography, it is a phenomenon of disguising things in an elusive manner. Here it is referring towards concealing files (data) into other file of different format. Even though steganography has been made public through various kind of tools, this application brings advanced support, such as, [password](#)-protection with an option of choosing desired carrier (file).

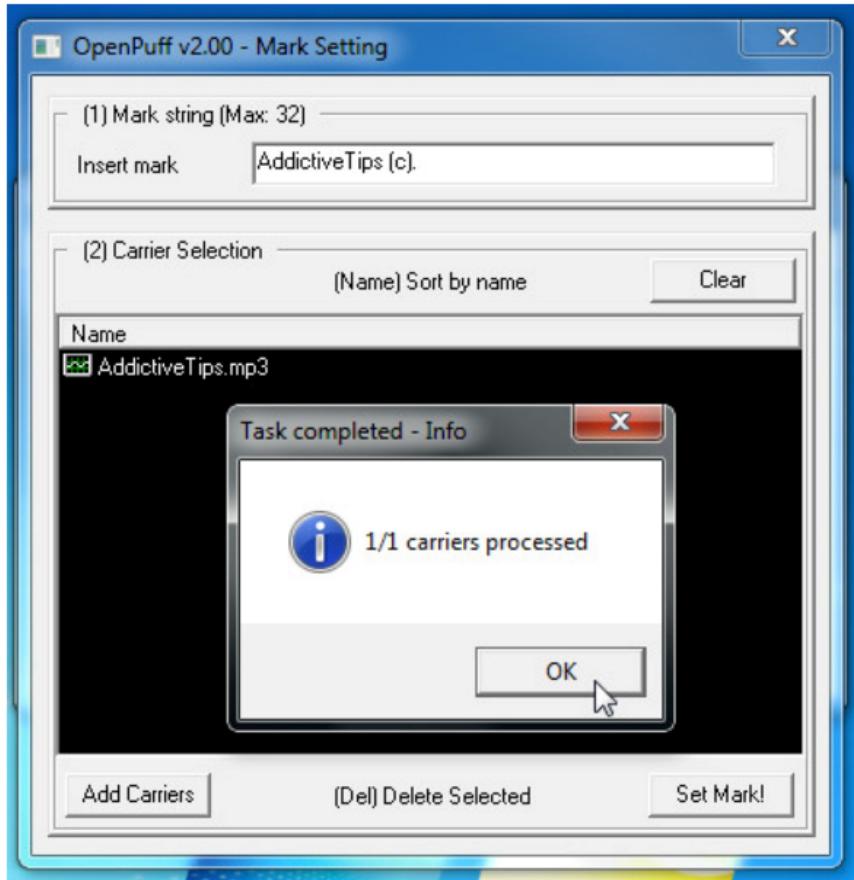
Marking will abet you in signing the file in a subtle way, which comes helpful to incorporate text into files, and when needed, you can claim ownership by showing the marked text. The interface is small and usage is self-explanatory as the steps to be taken are clearly defined. For hiding a file, click [Hide](#) button.



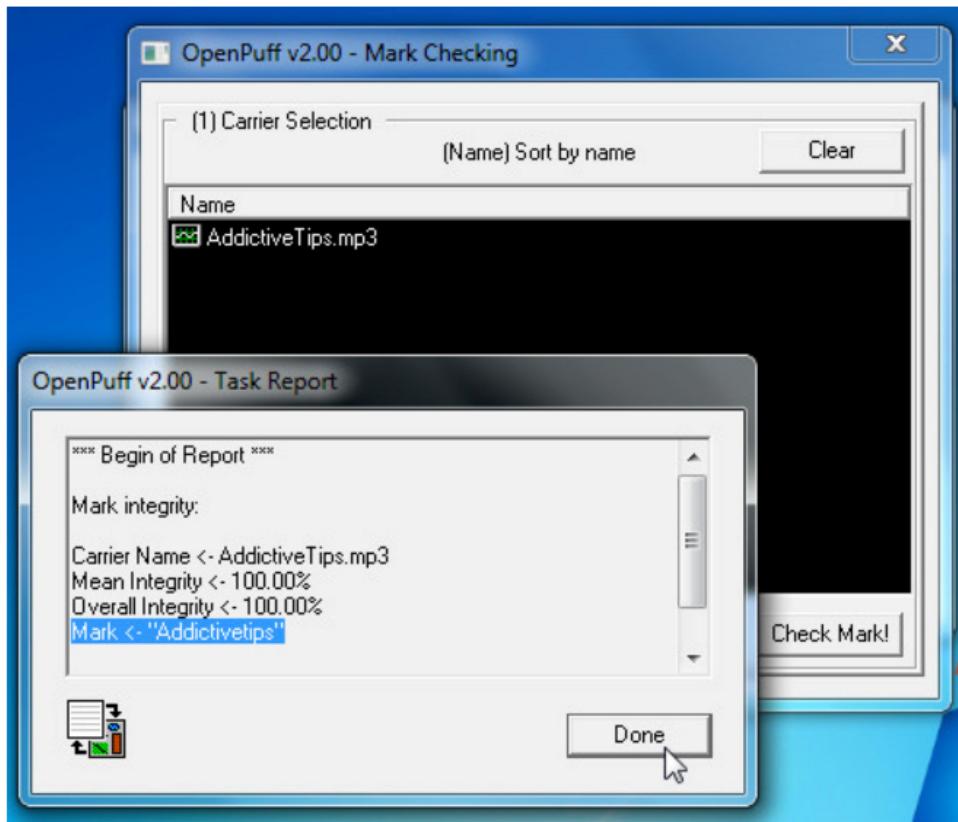
You will see the Data Hiding window, all the steps are defined to hide the file, it starts off with entering passphrase, specifying data to hide, selecting a carrier and then choosing a [file](#) format from the list. Once all the settings are in place, click Hide to specify the output folder of resultant file.



Marking a file is more simpler, clicking Mark will lead you to Marking window, where all you'd require is to insert mark text and specify the file (carrier). Clicking Set Mark will sign the file.



Besides facilitating user to hide files and insert specified mark, it lets you unhide the data and check the file mark easily. Clicking Unhide Data button will bring up window, where you'd require to enter password, choose carrier and select the file option to extract the file. For checking the file mark, specify the designated carrier and it will show you the specified mark instantly.



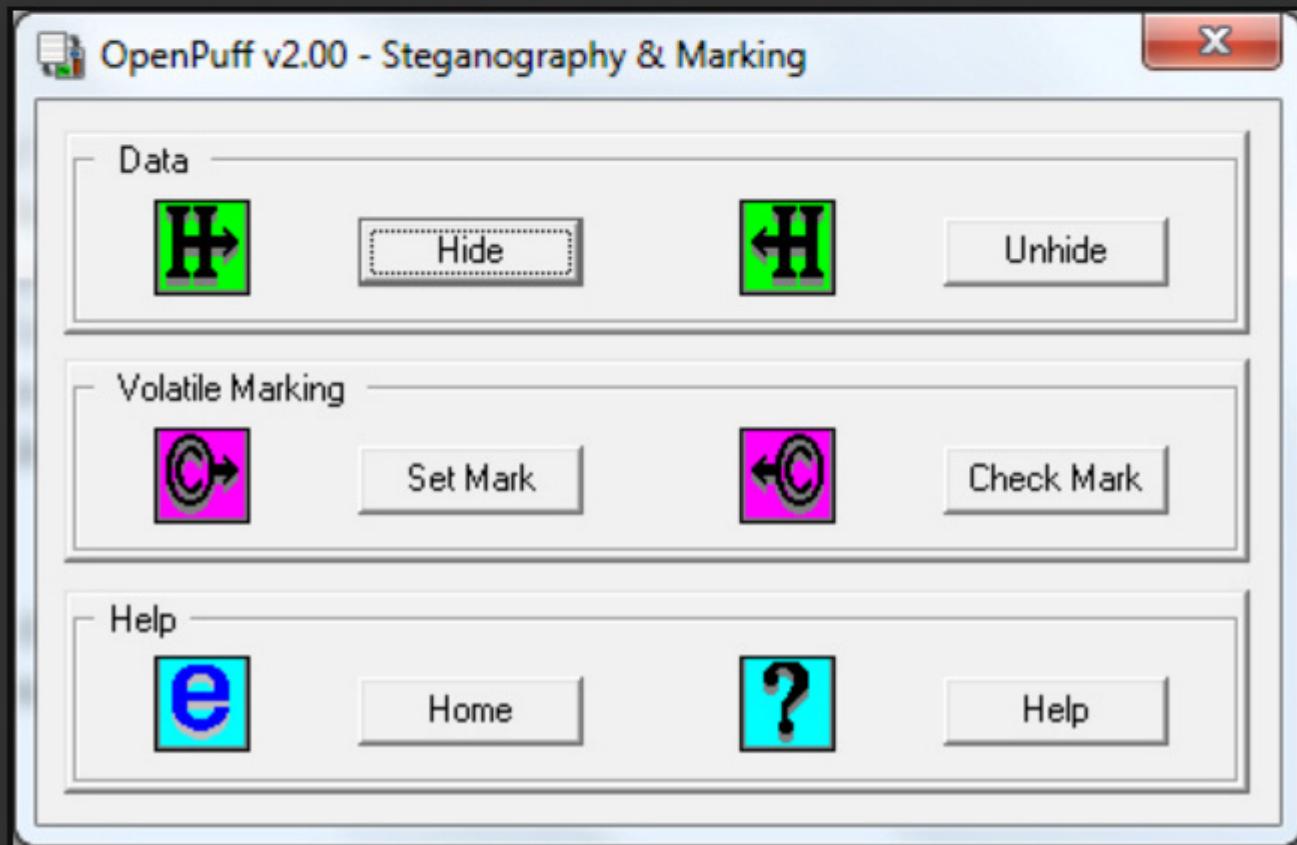
The application is of great use especially when you need to make some data private and marking comes useful in signing your file with your product or company name.

BRYAN'S DIGITAL WORLD

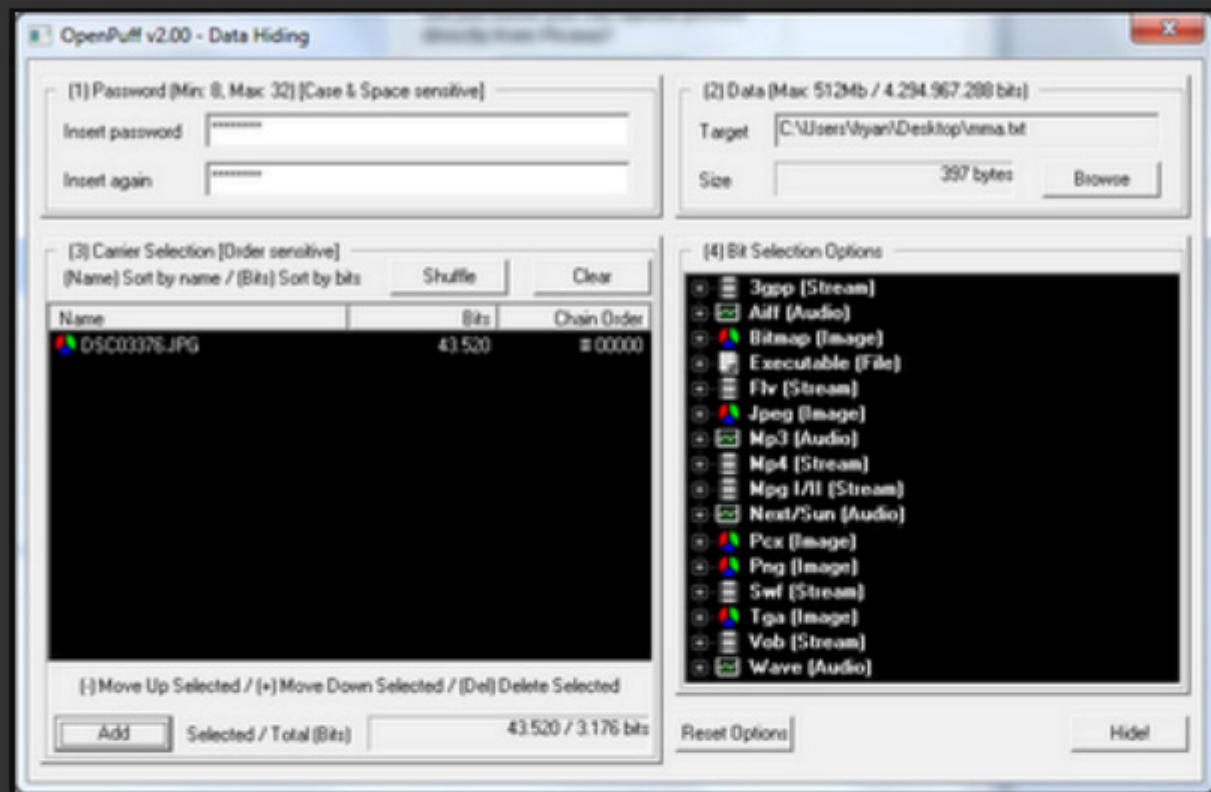
SATURDAY, JULY 31, 2010

Hide Data Or Message Inside Another File With OpenPuff

Steganography is the art and science of concealing information in such a way that no one, apart from the sender and intended recipient knows the existence of a hidden message on the visible message. You can have your own Steganography using a free and portable application called OpenPuff. This program hides data into other files, called carriers. Modified carriers will look like the original ones, without any obvious changes. It is recommended to use videos, images and audio files as carriers since these are commonly used and shared files. To conceal data, just run OpenPuff, and click Hide from the main screen.



From the Data Hiding screen, (1) Enter the password you want to use to hide the data, (2) Select the file you want to hide, (3) Choose the carrier/s where the hidden file will reside, (4) Select the Bit Options, And lastly hit Hide button to start the hiding process.



To retrieve your hidden data, from that main screen click Unhide. On the Data Unhiding screen, (1) Enter your password, (2) Select the carrier/s (3) then hit Unhide button. Aside from Hiding data, OpenPuff can also sign a file with your copyright mark (best known as Watermarking). Unlike the ordinary watermark on images, your copyright mark will be invisible but accessible by everyone (using this program).

It works on any Windows OS version. I tested it with Windows 7 Ultimate Edition.

Download [OpenPuff](#)

To stay up-to-date on Portable Apps, [subscribe now](#).

Posted by Fryan Valdez at 7:00 AM



Labels: [Cool Softwares](#), [Portable App](#), [Security](#)

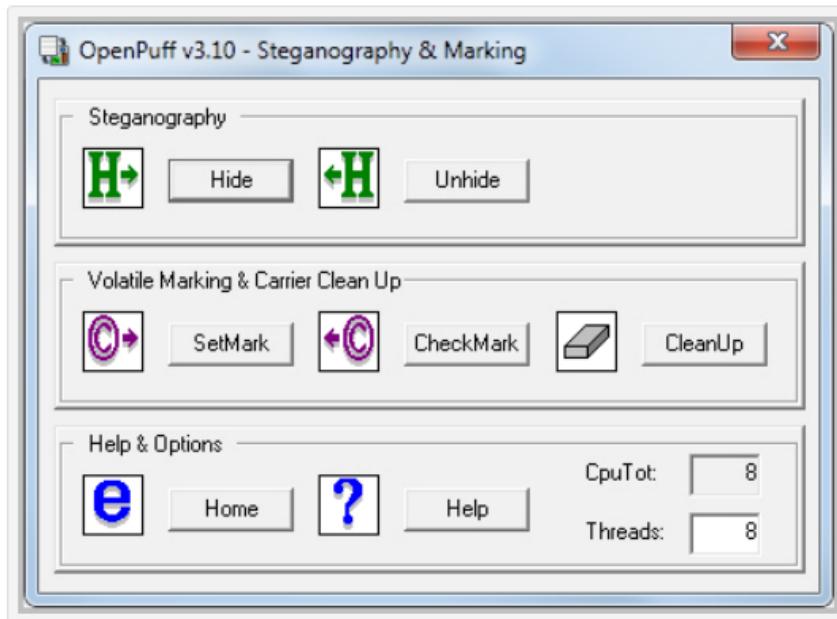
Hide Files With OpenPuff Steganography Software

BY MASTER GURU, ON NOVEMBER 16TH, 2011

Steganography, what's that again, and how does it relate to encryption? Steganography refers to techniques that censor messages or data, encryption on a other palm to techniques that strengthen a record from unapproved entrance by encrypting it. The classical instance to explain a judgment of steganography is a summary dark inside an picture file. No one, on initial look, would solely an picture record to enclose a tip message. That's what steganography is all about, concealing a data.

But it is no longer required to censor a information though protection, passwords and keys can be used to strengthen a dark information further.

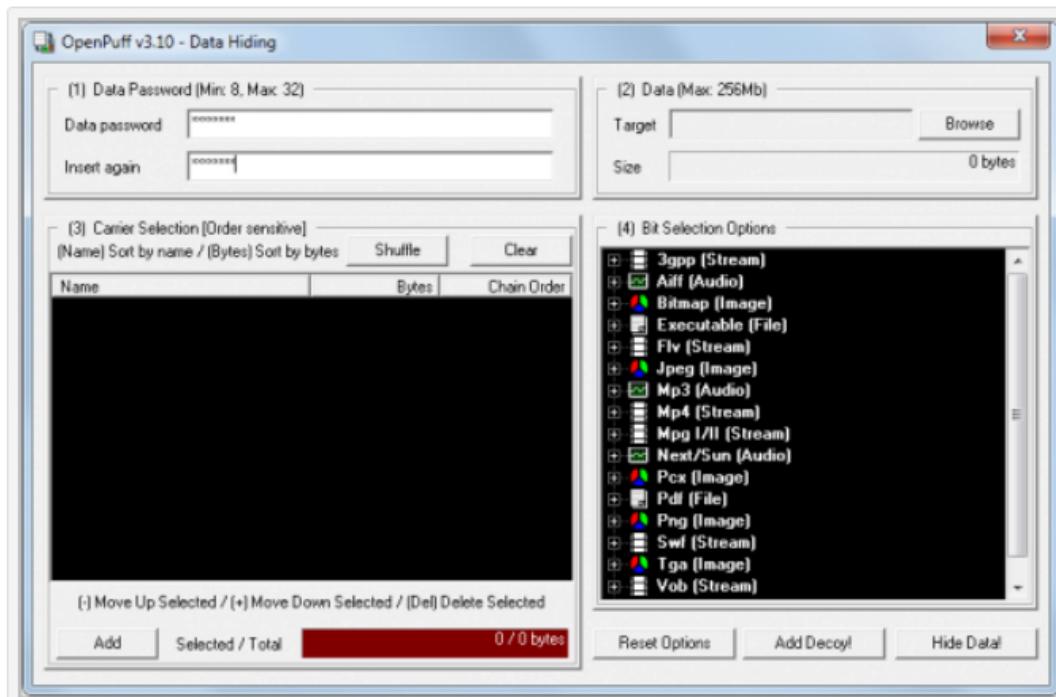
OpenPuff is a unstable steganography and imprinting module for Windows. The interface displays all accessible options when a focus is started.



Here it is probable to censor or unhide information underneath Steganography, or set, check or cleanup marks.

Hide Files, Unhide Files

You see a pattern window when we click on a censor symbol in a categorical interface.

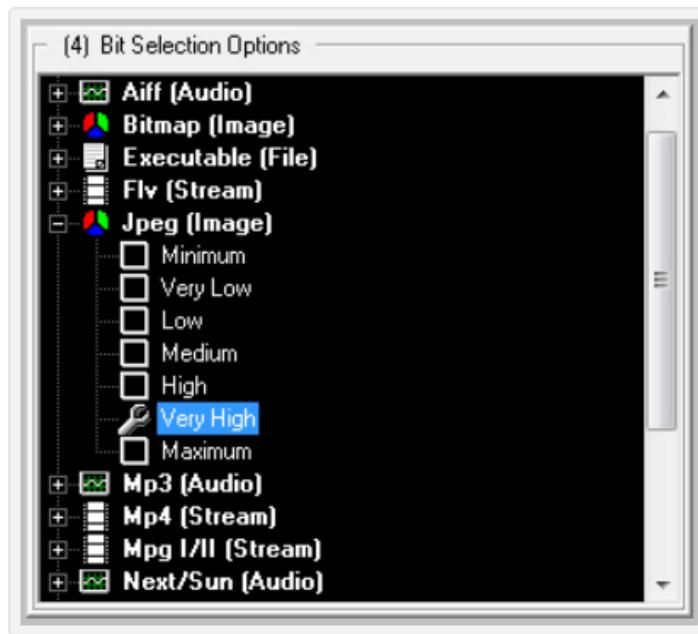


You need to mention a cue underneath (1) with a smallest length of 8 characters and a limit length of 32 characters.

A aim record is comparison underneath (2). The limit distance might not surpass 256 Megabytes. You might wish to cruise regulating an repository format like zip or rar if we need to censor mixed files.

Once we have comparison a aim record we need to name one or mixed carriers underneath (3). Carriers are a files a information gets combined to. The bytes combined to any conduit record are displayed immediately after they have been added.

You need to make certain that a carrier's accessible byte distance exceeds a distance of a comparison record that we wish to hide. For that, we can make changes to a bit preference shade (4).



One engaging choice is a ability to supplement a fake that fundamentally is a second record and cue that we could afterwards exhibit in box someone detects a dark information in a files.

A click on Hide Data processes a files by adding a information of a comparison record that we wish to censor to all of them. A save window is displayed automatically to store a processed files in a opposite folder than a strange files.

The processed files open adult routinely in concordant viewers. If we have combined information to images, they would still uncover adult as images in picture viewers.

The unhide routine fundamentally reverses a process. You still need to enter a cue that we have used to strengthen a data. Then we name all conduit files and a bit preference that we have selected. You are afterwards presented with a save as window to name a folder to save a dark record to.

Marking

Marking, or watermarking, is a second underline of OpenPuff. You can fundamentally supplement a fibre to one or mixed content files that could afterwards be used as explanation that we are a legitimate owner, for instance when copyright issues occur.

A click on set Mark opens a simple interface with options to enter a tradition fibre of adult to 32 characters and a files that need to be noted with that string.

You can afterwards use a check symbol choice to check if a symbol is still present, or cleanup to mislay outlines from files.

A video has been combined by a developer that demonstrates a capabilities of a software. It explains how to censor files and other features. An comparison module chronicle is used for a video demonstration.



[Home](#) - [Categories](#) - [Encryption Tools](#)

OpenPuff 3.40

steganography and file marking tool



[click for full size](#)

OpenPuff is a steganography and file marking tool that enables you to hide sensitive data inside images, audio files, videos and Flash files. It supports 512bit key cryptography with SHA512 password extension as well as data scrambling, data whitening and creation of decoy data. Your sensitive data can even be chained across multiple files. In addition to hiding data, the program can also be used to apply a, invisible digital watermark to any of the supported file types, allowing you to prove ownership or verify file integrity. Despite the advanced features, OpenPuff is easy to use with a self-explaining interface.

License: Freeware

Our Rating :

Price: Free

[Download Now](#)

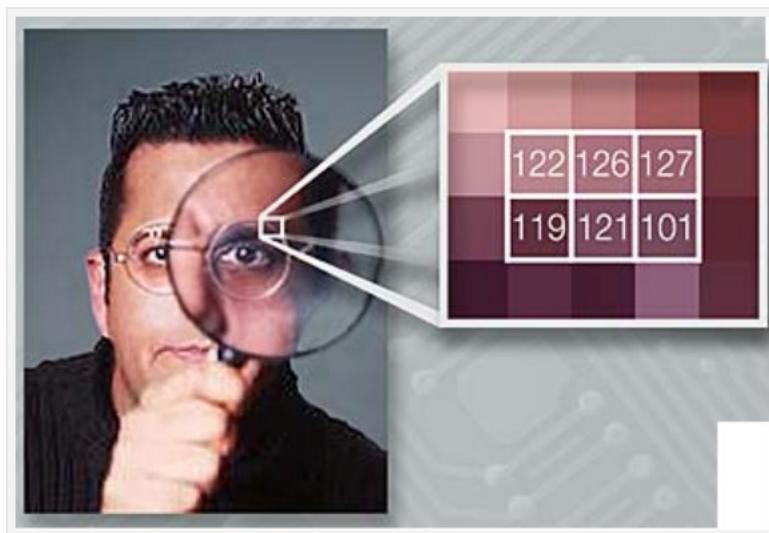
O/S: Win (All)

File size: 3661 kb

Author: [Cosimo Oliboni](#)

Last update: 07/18/2011

Steganography – The Art to Hide Data inside Image, Audio or Video Files



and ultimately get succeeded.

On the other hand, Steganography allows you to *hide data* without raising any flags. Only the desired recipient knows that some sort of sensitive information is hidden beneath the innocent looking media file. This is a useful way of secretly transferring data and information in some countries where encryption of data is not allowed.

OpenPuff – A freeware tool to Hide Data inside Image, Audio or Video Files

OpenPuff is a steganography and file marking tool that enables you to hide sensitive data inside images, audio files and videos. It supports 512bit key cryptography with SHA512 password extension as well as data scrambling, data whitening and creation of decoy data. Your sensitive data can even be chained across multiple files. In addition to hiding data, the program can also be used to apply a, invisible digital watermark to any of the supported file types, allowing you to prove ownership or verify file integrity. Despite the advanced features, OpenPuff is easy to use with a self-explaining interface.

Features of OpenPuff – The Freeware Steganography Tool to Hide Data

- Images support (BMP, JPG, PCX, PNG, TGA)
- Audio support (AIFF, MP3, NEXT/SUN, WAV)
- Video support (3GP, MP4, MPG, VOB)
- Flash-Adobe support (FLV, SWF, PDF)
- Windows Executable support (EXE, DLL)
- Multiple carriers chains (up to 256Mb hidden stream)
- Random per-block-cryptography (8 open-source algorithms)
- Strong cryptography (512bit key, password hex extension)
- Data scrambling & Whitening
- Adaptive LSB & Bits selection level
- Multithread support (up to 64 cpus) = Faster processing
- Simplified interface
- Unzip program and help in the same directory
- Portable – no need to install

If you have never heard of Steganography, then let me tell you that it is an art to hide your sensitive data inside innocent looking files like simple images, audio or video files such that the hidden data can be retrieved by the recipient easily with the help of a decoding code.

A similar process is Cryptography. But in cryptography, then encrypted files raise suspicion in the minds of other people, who happen to access the hidden data during the process of transfer. And once the suspicion is raised, there are chances that they may try to break the encryption

Ocultar archivos usando esteganografía – OpenPuff

 Techtástico, said há 9 meses

Muchos se han de estar preguntando ¿qué es esteganografía, y cuál es la diferencia con el cifrado?, bueno esteganografía se refiere a la técnica de esconder mensajes o datos (como en algunas películas que ponían un mensaje oculto en un punto), por otra parte el cifrado es para proteger archivos de accesos no autorizado mediante la encriptación del mismo. Un ejemplo sencillo para entender mejor el concepto de esteganografía es un mensaje oculto dentro de un archivo de imagen. A simple vista nadie nota nada, solo una imagen, pero en realidad pude contener un mensaje oculto. De esto es lo que trata la esteganografía, ocultar información.

Openpuff es un programa portable de esteganografía para Windows. La interfaz es amigable muestra todas las opciones disponibles cuando se inicia la aplicación.

Aquí se puede ocultar o mostrar los datos ocultos bajo esteganografía.

Ocultar archivos, mostrar archivos.

Veras una ventana de configuración cuando des click en el botón de ocultar de la ventana principal. Necesitas especificar una contraseña de un mínimo de 8 caracteres y de un máximo de 32. El archivo seleccionado no puede excederse de un tamaño de 256 Megabytes; Te recomiendo considerar la opción de usar un archivo zip o rar si quieres esconder múltiples archivos.

Una vez que tengas seleccionado el archivo destino es necesario seleccionar uno o varios archivos transportistas; estos archivos es donde los datos se agregan. Los datos que se agregan a cada operador aparecen inmediatamente después de que se han añadido.

Tienes que asegurarte de que el tamaño disponible de bytes del transportista no supera el tamaño del archivo seleccionado que deseas ocultar. Por eso, puedes realizar cambios en la pantalla de selección de bits.

Este vídeo fue hecho por el desarrollador del programa donde muestras las capacidades de este.

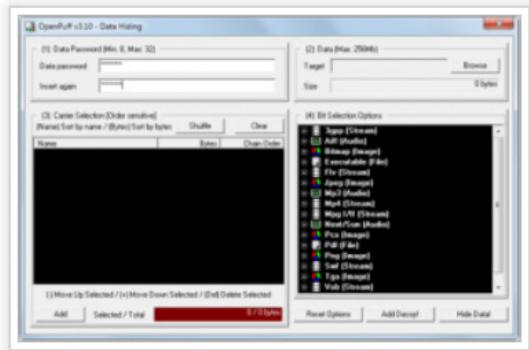
Openpuff se puede descargar de la pagina oficial del desarrollador. El programa a sido actualizado hace unos cuantos días para que no te dejes engañar por lo feo de la web. Los desarrolladores pueden descargar el código fuente de la aplicación por si quieren jugar un poco.

Ocultar mensajes detrás de una imagen: Openpuff

Ocultar mensajes detrás de una imagen: Openpuff: "

Muchos de ustedes, seguramente sabrán que existe un método muy ingenioso para **ocultar mensajes en la computadora** que consiste, en pocas palabras, en enviarlos detrás de una imagen o archivo anfitrión, lo cual permitiría que el mensaje pase desapercibido y no pueda ser visto si no se sabe de su existencia.

A este método se lo conoce como **esteganografía** y puede ser realizado gracias a algunas herramientas como **Openpuff**, las cuales permiten ocultar dichos mensajes de una forma segura e imperceptible, brindando además la seguridad de poder incluir una contraseña al archivo de forma que sólo se pueda ver lo oculto si se sabe la clave.



Este software gratuito no se puede denominar como **fácil de usar**, pero luego de que lo entendimos nos permitirá realizar el proceso en algunos minutos, pudiendo con él tanto ocultar los mensajes como verlos cuando necesitamos leerlos.

En cuanto a las **especificaciones que se dan para Openpuff**, se destaca que los archivos con los que vamos a trabajar no pueden superar en ningún caso los 256 MB, mientras que la contraseña que le asignemos para aumentar su seguridad debe oscilar entre los 8 y 32 caracteres, siendo más segura conforme se utilicen más espacios.

Aquí dejamos un video creado por un desarrollador del software que describe **cómo se usa Openpuff**.

Enlace: [Openpuff](#)

Fuente: [Techtastic](#)

Esteganografia (parte II). Escondendo arquivos dentro de músicas

Pessoal, dando continuidade as minhas pesquisas sobre esteganografia descobri que existem dezenas de softwares para esconder [arquivos](#) dentro de imagens. Mas meu intuito era aprender, e ao mesmo tempo mostrar aqui no blog como esconder arquivos dentro de outros tipos de mídias. Depois de muito procurar encontrei um software muito bom, e com uma [interface](#) bastante [prática](#) de [fácil](#) aprendizagem.

O intuito desse post é mostrar como esconder um arquivo dentro de uma mídia de áudio, pra ser mais preciso, como esconder uma mensagem(ou outro arquivo qualquer) dentro de uma música em formato .WAV.

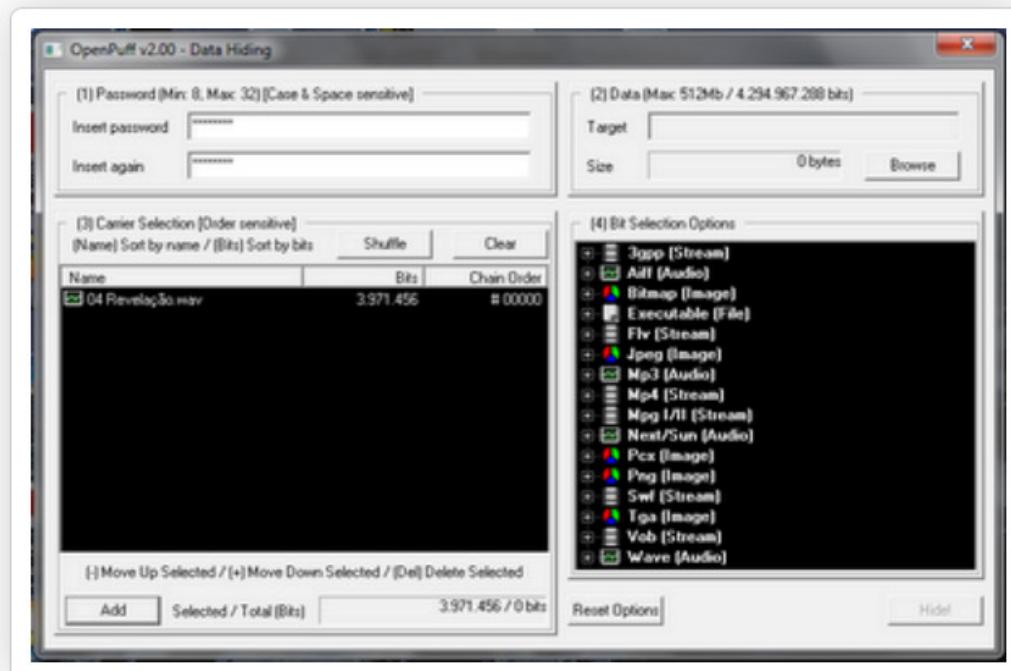
Depois de muito procurar, constatei que encontrar ferramentas de esteganografia para a plataforma Linux é bem mais fácil que para a plataforma Windows. Porém, tendo em vista que cerca de 90% dos visitantes do Blog utilizam a plataforma Windows, resolvi procurar mais e finalmente encontrei 2 softwares que prometiam esteganografar arquivos dentro de arquivos .WAV.

Após testar o primeiro surgiu um grave problema. Os arquivos depois de esteganografados ficaram inconstantes e travaram alguns dos reprodutores de áudio que tenho aqui para testar, entre eles o Windows Media Player e o Winamp. Logo o primeiro software foi descartado.

Em seguida comecei a testar o segundo software. Logo no começo o programa já começou a me impressionar, ele além de fazer esteganografia promete também criar e identificar marcas d'água. Não testei ainda como ele procede com as marcas d'água, talvez seja assunto para outro post, porém na questão de esteganografia o software se saiu muito bem. Outra vantagem do software é a Interface que como falei acima é bastante prática.

Bom, vamos deixar de conversa fiada e partir para o que interessa. O nome do software é OpenPuff e você pode fazer o download dele [aqui](#).

Utilizando o programa...



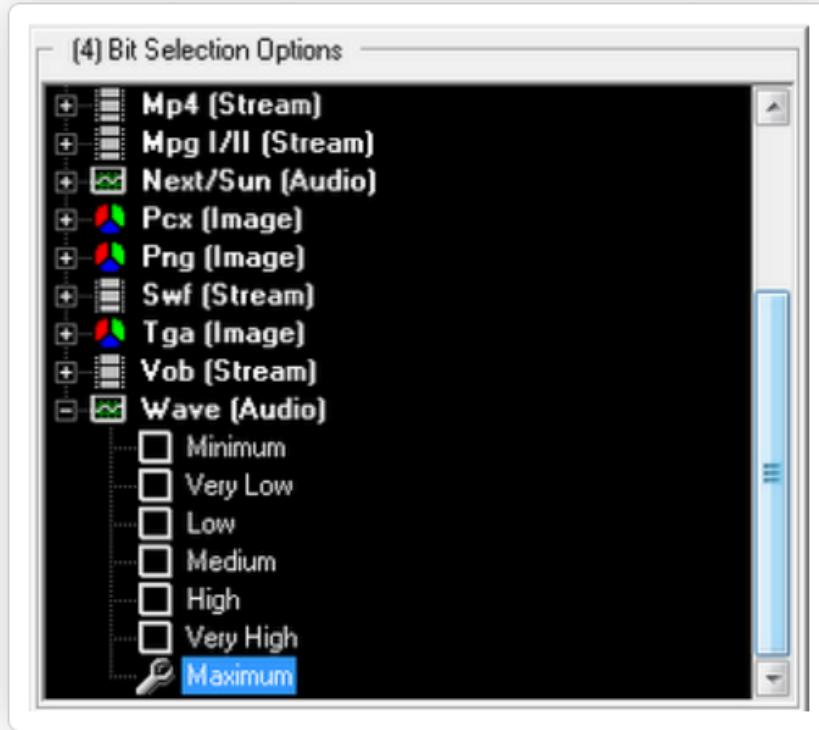
Nos campos,

(1) **Insert Password e Insert Again:** deverá ser colocado a senha para segurança da informação a ser escondida, a pessoa que quiser extrair a mensagem de dentro da música deverá conhecer a senha.

(3) **Carrier selection:** Aqui vai ser adicionado através do botão "Add" o arquivo que você vai usar como "mula", ou seja o arquivo que vai mascarar a mensagem secreta que você não quer que ninguém saiba que existe. No nosso caso vamos trabalhar apenas como extensão .WAV. Note que no exemplo foi colocado a música revelação.wav.

(2)**Data:** Neste campo será colocado o arquivo confidencial, que vai ser enviado dentro da música afim de que passe desapercebido. Através do botão "Browse" você vai procurar em seu PC o arquivo que quer enviar.

(4) **Bit Selection Option:** Neste campo você vai selecionar como vai ser dada a taxa de bits no processo de esteganografia do arquivo dentro da música. Lembrando que este fator é muito importante porquê aumenta o nível de segurança. Se você tiver a senha, mas não souber em que taxa de bits o arquivo foi escondido, não será possível extrair o arquivo corretamente de dentro da música. Clique na opção Wave conforme a imagem abaixo.



A Caixa vai expandir e você vai ter uma lista das opções de taxa possíveis. As taxas têm 7 opções que variam entre Mínimo e Máximo.

Pronto, após adicionar a música que será utilizada como máscara, o arquivo que será escondido, a senha e a confirmação de senha e selecionar a taxa de bits, a opção "Hide" será habilitada. É só clicar no botão "Hide" e pronto, a esteganografia será realizada, o programa vai apenas solicitar que você selecione o local onde será salvo o novo arquivo que possuirá o mesmo nome e tamanho da música original, porém estará agora com o arquivo selecionado escondido dentro de si. Você pode testar o música, ela toca normalmente e ninguem vai perceber que existe um arquivo dentro.

No vídeo abaixo eu mostro todo o processo para esconder o arquivo na música e depois o processo inverso, extraír o arquivo dentro de uma música esteganografada.

Postado por Doug às 23:05



Recomende isto no Google

Marcadores: [Esteganografia](#), [Programas](#), [Tecnologia](#), [Tutoriais](#), [Áudio](#)

● Como esconder informações vitais em uma imagem?

3.05.2011

Steganografia é o plano de pesquisa, que permite ocultar os dados das demais de tal forma, aparentemente, não percebendo que um, Existem vários tipos de informação no arquivo. Por exemplo, você pode se esconder texto em imagens ou documentos. É recursos fácil e gratuito que pode ser feito.

* Por que é necessário?

Ainda assim, depois de todos os dados, você não gostaria de deixar o mundo inteiro laokile, seja senhas, Os primeiros testes, ou poesia, e dados comprometidos ülisalajased.

Mas não só isso, por exemplo, é muito conveniente para armazenar os arquivos de imagem em uma pequena descrição do, onde, O que ou quem está na foto. Isso pode ser feito de outra maneira, steganografia mas é sem dúvida uma forma muito mais frio para armazenar dados, como fazer isso através do meta-.

Além disso, fóruns públicos pode ser como o outro para transmitir mensagens secretas. Postando uma foto, que é uma mensagem gravada, e amigo, quem sabe a senha, Você pode lê-lo para fora, e todos os outros usuários nem sequer suspeitavam de nada!

* Para o usuário avançado é OpenPuff.

Se as restrições de serviço acima web será assediando você também, Você pode usar o programa OpenPuff, que oferece muitas oportunidades para um conjunto mais amplo. O programa está disponível em members.fortunecity.it/blackvisionit/PUFFV200.HTM ou em outro lugar na Internet, se o site deve ser aterrado. OpenPuff não precisa instalar, simplesmente pressionando uma pasta de programa em algum lugar e fugir.

* Você pode usar qualquer arquivo.

OpenPuff feito pelo programador, usuário que não tem nada, Portanto, a janela do programa suspeito como um espartano. Não pague a deixar-se dissuadido, porque o programa é ülivöimekas e permite que você esconda, não só os dados da imagem, mas também o som- ou arquivos de vídeo e, em alguns casos, também. exe. Então você pode optar por ocultar alguns desses arquivos de dados, que não atrai suspeitas.

Clique no botão Ocultar na tela inicial do programa. Caixa de diálogo é aberta, que tem quatro seções. Primeiro, Superior esquerdo é a senha para o. Você pode proteger com senha os dados ocultáveis, mas não é obrigatório. Selecione a seção de arquivo de dados no canto superior direito, O que você quer esconder. Você não pode escrever diretamente para o texto, o programa já foram feitas para mostrar o arquivo.

Em 3, Seleção de Prestadora, Clique no botão Adicionar e mais arquivo ou arquivos, que você deseja ocultar os seus documentos secretos. Razões de segurança OpenPuff, você pode compartilhar arquivos entre vários dados (portador) e para restaurar os dados mais tarde, você precisa de todos esses mesmos arquivos de interrupção.

Essa complexidade de dados do, mas uma segurança verdadeiramente bom, decodificar corretamente os arquivos porque eles ainda não foram estabelecidas a fim. Em seguida, selecione a seção 4, Seleção de Opções pouco, nível de criptografia utilizado na. Ele pode ser configurado separadamente para cada formato de arquivo.

Vale a pena lembrar, no entanto,, a recuperação bem sucedida dos dados ocultos com informações para descriptografar um arquivo depois de ter escolhido exatamente o mesmo para. Quanto menor o recipiente maior o arquivo e arquivo oculto, quanto maior o nível deve ser selecionado. O nível máximo de um arquivo, transferir os dados como uma interferência muito barulho, No entanto, o nível mínimo para cada um dos andmebiti 7 mura é mais. Quanto maior o nível de, ele pode conter mais ficheiros de dados.

* Peida!

Se todos os dados são adequadamente selecionados e os tamanhos dos arquivos são suficientes, um arquivo para outro a fim de esconder, Ocultar botão será ativo. Quando o botão não é visível, então você precisa se quer aumentar o tipo de arquivo ou um recipiente maior bitataset arquivos. Se tudo for feito corretamente, clique no botão Ocultar! Primeiro, o programa pede que você selecione uma pasta, você salvar um novo arquivo, e depois, se tudo tem ido, o relatório também mostra que as pequenas, Quantos arquivos foram processados, e informação de acompanhamento técnico.

* O processo de restauração é simples.

Arquivo ou arquivos para os dados ocultos também é fácil de ler. Inicie o programa novamente, a tela inicial, mas para agora escolher o comando Reexibir em vez da Ocultar. Digite a senha exatamente a mesma e exatamente a mesma opções do painel Opções de Seleção Bit. Escolhas incorretas da mensagem de erro que você pode, não revela, se a senha estava incorreta, O fim algfailide (Lembrar, dados também pode ser escondido em um arquivo em) ou algo mais.

* Manter arquivos com cuidado.

Arquivos, em cujos dados você está se escondendo, deve ser preservada exatamente como tal, como um programa para gravar. Sob nenhuma circunstância você deve abrir o arquivo e salve-se mais do que qualquer outro programa. Se o fizer, pode ficar corrompido estruturas de dados e os dados ocultos serão perdidos para sempre.

ШИФРОВАНИЕ

Теория

Любые данные, которые, как вам кажется, обладают определенной ценностью, имеет смысл спрятать и зашифровать. А лучше и то, и другое.

Простейший трюк — скрытие на компьютере одного из разделов диска, после чего он перестанет быть видным случайным людям (попасть на него можно будет только через командную строку). Откройте консоль Windows ("Пуск" > "Выполнить" > cmd.exe), наберите фразу diskpart и выполните команду list volume, чтобы получить информацию о каждом томе на компьютере. Запомните номер диска и букву, которую хотите скрыть, закрепите выбор командой select volume [номер диска] и введите remove letter [буква диска].

Однако помните: любая информация при желании может быть найдена, расшифрована и восстановлена даже после ее полного (как вам кажется) удаления. Поэтому самый надежный способ уничтожить данные — это перемолоть свой жесткий диск в блендере. Компания Blendtec вот уже много лет доказывает, что их техника за минуту превращает в труху не только еду, но также iPad, видеокамеру и даже шарики для гольфа. Посмотреть на блендеры в действии можно по адресу willitblend.com.

Практика

Информация может быть спрятана внутри файлов-изображений — это называется стеганографией (кстати, данный метод и использовали выдворенные недавно из США российские шпионы). Опробовать технологию в действии помогут программы вроде Invisible Secrets (invisiblesecrets.com) или OpenPuff: они помогают сохранить логин / пароль от интернет-банка в недрах семейной фотографии, а затем извлечь его оттуда.

Отдельное удовольствие — маскировка сообщений под спам. По адресу spammimic.com располагается сервис, превращающий любое короткое сообщение в бессмысленный спам-текст. Так что полученное вами сообщение про роботизированные японские унитазы на самом деле может быть скрытым приглашением в тайное масонское общество.



Written by

Monday, 01 August 2011 08:57

Новое приложение к журналу "ХАКЕР" за август 2011 года - одному из самых популярных изданий, посвященному искусству хакерства, интересным своими статьями для самообразования, информацией о том, что необходимо знать каждому пользователю компьютера. Главное отличие от других изданий - манера подачи материалов. Журналисты "Хакера" объясняют сложные вещи простым языком, с юмором и молодежным сленгом.

Единственным исключением является рубрика ВЗЛОМ, которая рассчитана на более серьезных специалистов, материалы в этой рубрике подаются более углубленно с множеством технических подробностей и терминов. [Все программы, помещенные на диске, проверены антивирусным ПО.](#) [Содержание диска](#) **Fedora 15**

OpenPuff v3.30 - профессиональный инструмент для стеганографии

La steganografia in pratica

 Crittografia, Open Source, Privacy, Segretezza, Steganografia

Ottobre 19, 2011

Sicurezza, Software



Se vi siete interessati alle problematiche connesse alla segretezza dei dati avrete sicuramente acquisito informazioni relative alle due principali tecniche utilizzate allo scopo, vale a dire la crittografia e la steganografia. Esse raggiungono lo stesso obiettivo partendo da due diversi approcci, mirando rispettivamente a proteggere ed a nascondere il messaggio scambiato tra due parti e per questo si prestano nella pratica a diversi casi d'uso.

Ma che cosa significa esattamente “nascondere il messaggio”? Se avete visto “A Beautiful Mind”, il film dedicato alla vita del matematico e premio Nobel John Forbes Nash Jr., ricorderete che ad un certo punto il protagonista passa la quasi totalità del proprio tempo ad ispezionare giornali e riviste alla ricerca di messaggi segreti inviati dai traditori comunisti ai propri agenti negli Stati Uniti. Ovviamente non sarebbe stato possibile pubblicare messaggi palesemente crittografati su un quotidiano, perché i lettori e le autorità si sarebbero ben presto insospettiti e ne avrebbero bloccata la diffusione. L'intuizione del personaggio impersonato dall'attore Russell Crowe era invece che i destinatari a conoscenza della chiave di interpretazione (la prima lettera della seconda parola di ogni frase, per fare un esempio banale) potessero leggere, da quello che a tutti appariva essere un normalissimo articolo giornalistico, il messaggio a loro indirizzato. Intuizione fondamentalmente corretta, ma difficile da provare con i mezzi dell'epoca.

Ora torniamo al periodo attuale e pensiamo ad una fotografia memorizzata in formato digitale, nella quale ciascun singolo pixel è codificato nelle proprie componenti RGB. Se per alcuni pixels si modifica il bit meno significativo di una componente (facendo passare il valore R da 00001111 a 00001110 ad esempio), si ottiene una foto indistinguibile dall'originale ma che può recare (utilizzando più bits in più pixels) un messaggio se mittente e destinatario si sono preventivamente accordati su posizione ed ordine dei bits modificati. E' l'algoritmo noto come steganografia LSB (acronimo di Least Significant Bit) ed è applicabile ad ogni contenuto rappresentato in maniera digitale (audio e video).

Per fare qualche prova con questa tecnica possiamo utilizzare [Steganography Studio](#), un tool open source esplicitamente sviluppato (in Java, quindi portatile su più ambienti) allo scopo di fornire uno strumento per lo studio degli algoritmi steganografici. All'interno dell'immagine che accompagna questo articolo ho inserito, mediante la funzione "Encode" di tale software, il logo del sito (il messaggio scambiato non è quindi necessariamente in forma testuale) utilizzando l'algoritmo SLSB (una variante di LSB che secondo l'autore possiede un maggior grado di immunità rispetto alle tecniche di steganalisi, con le quali un attaccante potrebbe essere in grado di dimostrare l'esistenza di dati nascosti all'interno di un contenuto multimediale). Il logo potrebbe essere ora estratto dall'immagine contenitore selezionando lo stesso algoritmo e la funzione "Decode" del software citato.

Steganography Studio è solo un tool didattico ma se abbiamo necessità concreta di utilizzare le tecniche di steganografia esiste un altro prodotto, ancora open source, veramente affidabile e completo. Mi riferisco ad [OpenPuff](#), che è oltretutto in grado di utilizzare come contenitori multimediali non solo le immagini ma anche i files audio e video.

Nascondi files con un programma professionale di steganografia: OpenPuff

By Carlo on 10/04/2011

In cosa si distingue la steganografia con la crittografia?

La steganografia è una tecnica molto antica che consiste nel nascondere messaggi e dati mediante un codice che mittente e destinatario concordano mentre la crittografia serve per proteggere files da accessi non autorizzati rendendoli inaccessibili a chi non conosce la chiave. Un classico esempio di steganografia è un messaggio o informazione nascosta all'interno di una immagine.

OpenPuff è un programma professionale, portatile, gratuito di steganografia adatto per la trasmissione nascosta di files all'interno di altri files detti carrier.

Dall'interfaccia dell'applicazione selezioneremo i files che vogliamo nascondere, quindi selezionare uno o più file che farà da carrier che possono essere file immagine, file audio, file video ed anche file flash. Il numero di bytes dei carrier deve essere almeno pari al numero di bytes del file nascosto. Sarà da specificare una password, la dimensione massima dei files da nascondere non può superare i 256 MB.

Per poter decifrare il messaggio sarà da utilizzare questo programma, conoscere la password, i carrier scelti e nel giusto ordine. Si tratta di una **soluzione estremamente sicura** con parecchi livelli di protezione adatto per invio con sicurezza di dati estremamente sensibili.

Per altre inforamzioni nel sito troviamo una guida completa in italiano ed un video.

OpenPuff Steganography & Watermarking 3.30



سایز : KB 407

سیستم عامل : XP/Vista/98/2000

:

سازنده

[/OpenPuff Steganography Home.html](#)

بف نهان نگاری و کوتاه نویسی راه حل نرم افزاری مورد استفاده برای مخفی کردن اطلاعات است و ساده تر نوشته‌ن.

این با پشتیبانی از فرمت های پیش فرض برای فایل تصویری مانند BMP ، فعلی می آید ، JPG ، PCX و JPEG و همچنین برای فرمت های زیر فایل های صوتی : AIFF ، بعد / خورشید ، MP3 و پل های ال. TGA ، و همچنین برای فرمت های زیر فایل های صوتی : VOB ، 3GP ، MP4 ، محورها ، FLV و SWF . انواع فایل های ویدئویی پشتیبانی شده عبارتند از EXE ، ال ال) • چند حامل زنجیر (تا 512MB بنهان جریان) امکانات افزوده شده : • ویندوز پشتیبانی اجرایی (EXE ، ال ال) • چند حامل زنجیر (تا 512bit) • رمزنگاری قوی (512 bit) کلید و رمز فرمت هگز) • تصادفی در زنجیره - رمزنگاری (8 منبع آزاد الگوریتم) • اطلاعات تغلا و سفید کردن • تطبیقی LSB و اندیشه سطح انتخاب • رابط کاربری ساده دنبال لینک و دانلود رایگان OpenPuff Steganography و نهان نگاری در حال حاضر.





ประเภท : [โปรแกรมด้านความปลอดภัย](#)

ผู้พัฒนา : [Cosimo Oliboni](#) | View : 415 (freeware) | File size : 407KB

โพสท์เมื่อ : 18 กรกฎาคม 2554, 23:21

ดาวน์โหลด : 127 ครั้ง

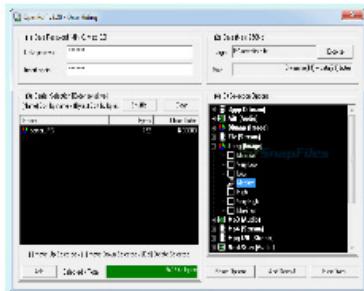
Rating : ★★★★★ 5 คะแนน , 1 ผู้ร่วมโหวต



[Like](#) [Sign Up](#) to see what your friends like.



Screen Shot



ข้อมูลทั่วไปของโปรแกรม

File Size : 407KB

File Author : [Cosimo Oliboni](#)

File Type : freeware

Category : [utilities-software](#)

OpenPuff เป็นโปรแกรมที่มีความน่าสนใจเป็นอย่างยิ่ง โดยโปรแกรมนี้จะสามารถทำให้คุณสามารถซ่อนข้อความลับของคุณเข้าไปในไฟล์ประเภทเสียง หรือซ่อนข้อความไว้ในรูปภาพ หรือซ่อนข้อความไว้ในไฟล์วิดีโอ หรือซ่อนข้อความไว้ในแฟ้มชี้ไฟล์ได้เพื่อป้องกันความลับร้าวไหลซึ่งนับว่าเป็นไอเดียที่น่าสนใจมาก ใจจะไปรู้ว่าเราจะส่งข้อความถึงกันผ่านไฟล์Mp3 โปรแกรมมีการเข้ารหัสสกิง 512 Bit และใช้รูปแบบการเข้ารหัสแบบ SHA512 คุณสามารถนำข้อมูลของคุณแยกไปเก็บซ่อนไว้ในไฟล์หลายๆ แบบเป็นกันเพื่อความปลอดภัยและลับสุดยอด นอกจากนั้นคุณยังสามารถที่จะประยุกต์ใช้โปรแกรมนี้ในการป้องกันการลักเมิดลิขสิทธิ์ผลงานของคุณได้อีกด้วย เช่น แอบใส่ข้อความลับไว้ในเพลงที่คุณแต่งขึ้นมาเองที่นี้เวลาใครคัดลอกไปเราก็สามารถตรวจสอบไฟล์ของเราได้แล้วครับนั่นว่าเป็น

برنامج لإخفاء البيانات داخل الملفات والتشفير بكلمة مرور OpenPuff 3.40

برنامج لـ إخفاء البيانات داخل الملفات والتشفير بكلمة مرور OpenPuff 3.40 في منتدى برامج الإنشاج بتاريخ 19 نوفمبر 2011.

[مشاركة هذه الصفحة](#)



تحميل

تطبيق لإخفاء البيانات ووضع العلامات .

برنامج Puff هو برنامج لإخفاء المعلومات والتلقيف . ومن الواضح أن إخفاء المعلومات ليست فكرة جديدة ولكنك يمكن أن تتعرف على واجهة البرنامج فهو مصمم للأشخاص الذين يعرفون ما يحتاجون إليه .

(إخفاء المعلومات Steganography) هو فن وعلم لكتابية الرسائل المخفية وهو طريقة لكي لا يعرف أى من المرسل أو المستقبل للرسالة بوجود محتواها وهو شكل من أشكال الأمان من خلال عدم الوضوح)

مستوى تحديد البت :

يمكنك معالجة كل نوع من أنواع النوافل بسبع طرق مختلفة : النمو المعقد لإزالة الإخفاء مضروباً في سبعة لكل نوع من النوافل المستخدمة .

خوارزمية التشفير :

16 خوارزمية تشفير مختلفة مع 16 متغير فرعى والذى تضع 256 . وهى تساماً كل قيمة ممكنة للبيت ! وعلاوة على ذلك ، يتم تكوين التسلسل الخوارزمي بعشوانية .

تشفيير كلمة المرور :

خوارزمية تشفير كلمة المرور تم تصميمها لإنتاج كمية كبيرة من القيم الثابتة الغزيره والزائدة . ومن الوضوح أن هذه الزيادات تعقد من محاولات إزالة الإخفاء الغير مسموح بها .

سلسلة الناقلين :

إخفاء البيانات يقسم بين نوافل كثيرة . التسلسل الصحيح للناقل فقط هو الذى يتتيح عملية إزالة الإخفاء : النمو المعقد لإزالة الإخفاء مضروباً في n حيث n عدد النوافل .

علاوة على ذلك ، يمكن إخفاء حتى حجم بيانات 256 ميجابايت ، إذا كان لديك ما يكفي من النوافل Carriers . آخر ناقل سيملىء بـ بت عشوائى حتى يتم التمييز بينه وبين الآخرين .

عمليات مرتبه أبجدياً :

عند الإخفاء ، يتم ترتيب النوافل أبجدياً . بدون أي علامات مادية منخفضة المستوى للترتيب المنطقي وبالتالي سوف تكون متاحة .

ملخص :

أى شخص قادر على تصحيح هذا البرنامج وإكتشاف خوارزميه التشفير (سيكون عملاً ضخماً ، ليس مستحيلاً ولكن هائل) وحتى في هذه الحالة سيحتاج إلى سلسلة من 20 ناقل مع 3 أنواع مختلفة من النوافل قد يحتاج إلى 4×10^19 محاولة لإزالة الإخفاء عن طريق الأفراد الإبرى مسموح لهم برؤية البيانات . ناهيك عن عدد مرات محاولة رفع الحساية عن كلمة المرور ! بالأداء المرتفع يمكن أن تنجذب ذلك فقط مع الفهم الكامل لجميع الخيارات الصعبة المقدمة لك .

التأليف :

الإصدار المبسط لعملية الإخفاء متوفراً لعملية التأليف . لديك فرصة أخرى لتسجيل عملك ! كل ناقل سوف يعمل كسلسلة نوافل مفردة .

سيتم ملء بـ الناقل بعلامة حقوق النسخ والنشر © الخاصة بك .

لن يكون هناك أى حساية بكلمة مرور أو تشفير أو ضغط .

سيعمل برنامج Puff كواجهة عامة لفحص سلامة حقوق النسخ والنشر .

الإعدادات المطلوبة فقط هي تحديد مستوى البت المستخدم في وقت التأليف .

. يدعم برنامج WinPE BMP, JPG, PCX, PNG, TGA, AIFF, MP3, NEXT/ SUN, WAV ووحدات

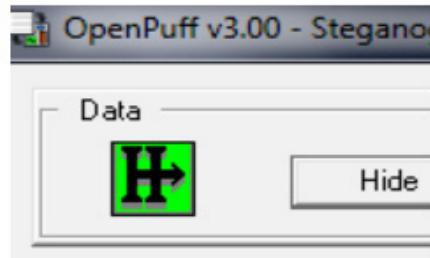
صور البرامج



برنامج لاخفاء ملفاتك ومعلوماتك الهامة وتشفيرها

OpenPuff 3.40

MB 3.6 :	حجم
Windows All :	نظام التشغيل
Freeware :	ترخيص
73 :	التحميل
★★★★★ :	التقييم



المقدمة وطريقة إخفاء بالماء

OpenPuff هو إخفاء المعلومات بديهية وتطبيق التأليف. ومن الواضح أن إخفاء المعلومات ليست فكرة جديدة ، ولكن يمكنك الاختيار من واجهة وإخفاء المعلومات التي **OpenPuff** ، مصممة للأشخاص الذين لا يعرفون ما يحتاجون إليه.

وصف عالمية رفيعة المستوى للهندسة المعمارية والنفخة :

• يتم تقسيم البيانات بين الناقلات

* هل يرتبط كل ناقل للعشوانية ولدت 128bit متوجه تهيئة (IV)

• يرتبط المستخدم كلمة السر (32 حرفا = 256bit) على تمديد كلمة عشرى

• يتم تشفير البيانات لأول مرة مع مفتاح 512bit ، وذلك باستخدام " مجرد " التشفير تيار المرك

• بيانات المشفرة ثم تدافعت (16 طلقة) لكسر أي نمط تيار المتبقية

• تدافعت البيانات ثم تبييض (= مختلطة مع ضريح عشوائي) لخداع الهجمات cryptanalytic

• تعديل ناقلات تلقى الدفق معالجتها

وهنا بعض الملامح الرئيسية : "OpenPuff"

- الصورة / الصوت / الفيديو (ترميز مستقل) / أدبوي / دعم فلاش

- متعددة ناقلات السلسل (إلى تيار 256MB المخففة)

- عشوائي لكل كتلة – 512bit التشفير – algorhythms

- بيانات تبييض

- LSB التكيفية اختيار القطع + المستوى

- من أداة لإخفاء المعلومات المهنية ، وأيضاً مناسبة للمبتدئين!

- الهدف منه فقط هو أن تكون على نطاق واسع بين المستخدمين المهتمين

ما هو الجديد في هذا الإصدار : []

- محرك التشویش ، والعمارة ، تصحيح خطأ

OpenPuff Steganography: jak zmást zloděje dat

Potřebujete-li uchránit cenná data před zraky nepovolaných osob, bez šifrování se nejspíš neobejdete. Co když ale nechcete, aby někdo o existenci vašich citlivých dat vůbec věděl? Jednoduše předstírejte, že jde o data jiná – OpenPuff vám z nich udělá třeba sadu skladeb ve formátu mp3.

11. 4. 2011

Jan Váňa

 poslat e-mailem

 verze pro tisk

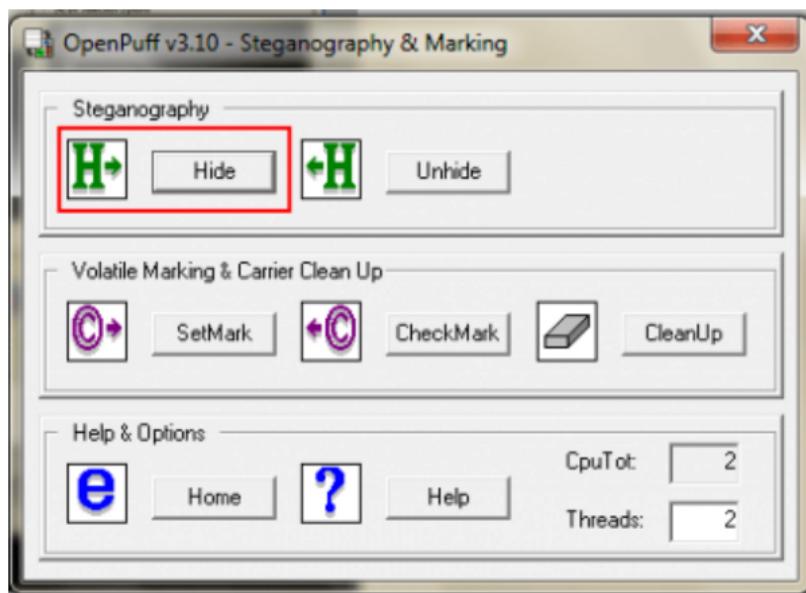
S aplikací OpenPuff Steganography snadno přeměníte dokument s citlivými daty např. na video z dovolené nebo poslední hit Metallicy. To se může hodit, pokud nejen že chcete mít data chráněna, ale máte zájem i na tom, aby nikdo nevěděl, že nějaká citlivá data vůbec jsou. Využity jsou přitom k zašifrování „military-strength“ (jak tvrdí na svých stránkách autorů) algoritmy a postupy jako například 512bitové kryptování algoritmem SHA512 a generátor pseudonáhodných čísel CSPRNG.

Zamaskujte data ve čtyřech krocích

OpenPuff Steganography najdete na [této adrese](#). Jedná se o aplikaci přenositelnou – tudíž ji netřeba instalovat. Několik okamžiků po spuštění zabere inicializace zmíněného pseudonáhodného generátoru CSPRNG.



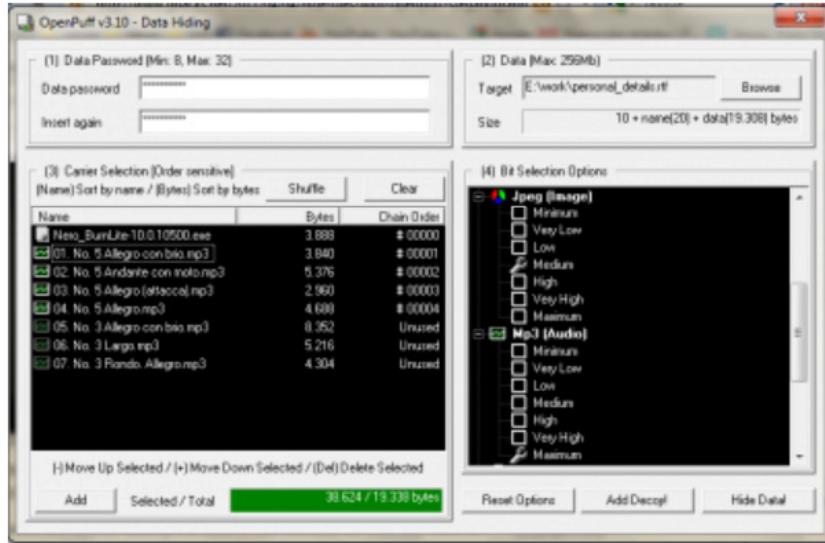
Úvodní obrazovka umožňuje přístup do dvou hlavních funkcí aplikace – tj. steganografie (maskování za jiná data) a přidání vodoznaku (watermark). Tlačítka **Help** a **Home** vás nasměrují na informace obsažené na domovských stránkách vývojářů.



Oheň, v němž se nachází příslovečné želízko OpenPuffu (tedy výše zmíněná steganografie), rozdmýcháte kliknutím na tlačítko **Hide**. Rozhraní pro zašifrování a skrytí požadovaných dat je přehledně rozděleno do čtyř sekcí, které logicky odpovídají čtyřem nutným krokům.

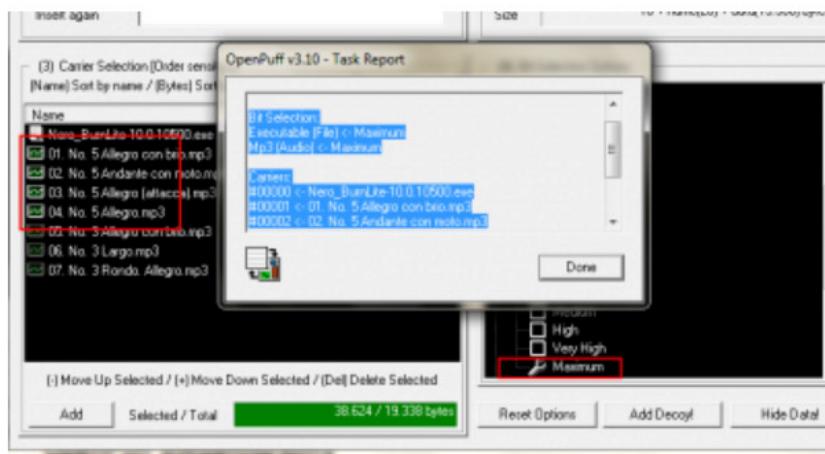
Vlevo nahoře se nachází dvě textová pole pro zadání vlastního hesla – toto se musí vejít do intervalu 8 až 32 znaků. Vpravo nahoře pak vložíte (tlačítko **Browse**) soubor, který má být uchráněn před záškodníky. Jeho velikost nesmí přesáhnout 256 MB.

*TIP: Celý proces skrytí a šifrování můžete aplikovat pouze na jeden soubor. To lze obejít použitím archivátorů – vložit můžete např. celou složku citlivých dat **zazipovaných** do jednoho souboru.*



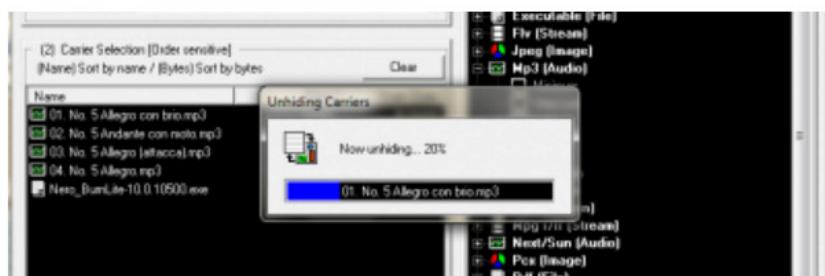
Pod bodem (3) **Carrier Selection** najdete seznam nosičů, na které bude šifrování navázáno. Seznam je nejprve třeba zaplnit – to provedete kliknutím na tlačítko **Add** v levém dolním rohu okna – přičemž podporovány jsou soubory obrázků (např. BMP, JPG, PNG a další), audio soubory (MP3, WAV, AIFF), některé video formáty a spustitelné soubory (přípona EXE) a další (seznam podporovaných souborů najdete na stránkách aplikace).

U použitých nosičů jsou důležité dvě věci: jednak počet použitých bajtů (sloupeček **Bytes**), jednak pořadí ve frontě nosičů (sloupeček **Chain Order**). Celkový počet použitých bajtů u nosičů musí být větší nebo roven délce šifrovaného souboru. K nastavení míry využití jednotlivých nosičů slouží čtvrté podokno, kde u každého z možných typů nosičů nastavíte, zda má být k maskování využit hodně nebo málo (sedmistupňová škála). Změny se u daného typu ihned projeví ve sloupci **Bytes**. Dostatečnou délku nosičů si ověříte v dolní části v poli **Selected / Total** (je-li hodnota před lomítkem – nosič – větší než hodnota za lomítkem – šifrovaný soubor – pole zezelená). Akci pak spusťte kliknutím na tlačítko **Hide Data!**.



Dešifrování je analogické, ale pozor na detaily

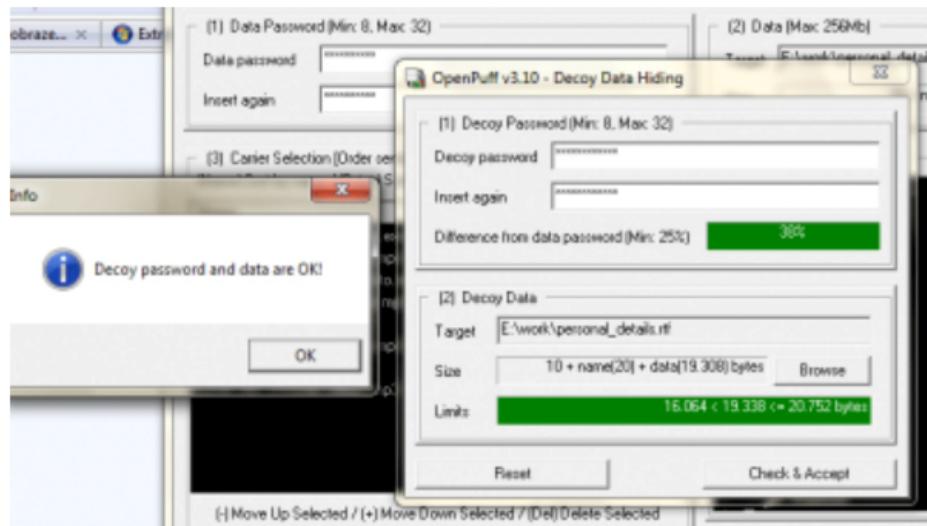
Výstup operace „Hide“ je sada souborů, které byly použity jako nosiče. Tyto ovšem obsahují i části šifrovaných dat – pokud chcete maskovaná data opět odkrýt, je důležité mít k dispozici kompletní a neporušenou sadu nosičů. Odmaskování pak provedete jednoduše tak, že v úvodním okně kliknete na **Unhide** a následně provedete analogicky kroky jako při maskování.



Na co je však třeba při demaskování myslet, je nutnost zachování **zcela totožných podmínek jako při maskování**. Zadání shodného hesla je samozřejmostí, u nosičů je však třeba dodržet jak **pořadí**, tak míru využití v okně **Bit Selection Options**. Jakákoliv drobná změna povede k neúspěchu.

Dvojitá maska – past na zasvěcené

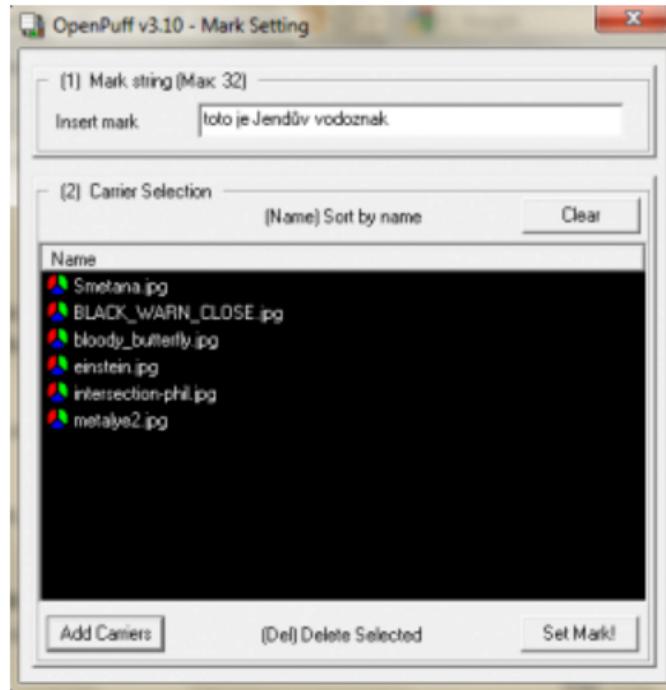
Pakliže by se třetí strana, která by měla zájem na vašich datech, nějakým způsobem dostala k informacím o počtu použitých nosičů, hesle apod., pořad ještě nemá vyhráno. V okně **Data Hiding** můžete využít dvojitého maskování pomocí tlačítka **Add Decoy!** (doslova „přidat návnadu“).



Přidáním druhého hesla a krycího souboru (**Decoy Data**) docílíte toho, že pokud záškodník znalý celé procedury demaskuje data, odhalí se mu pouze onen krycí soubor a nikoliv původní šifrovaná data.

Vodoznak potvrzuje autorství

V hlavním okně najdete ještě tlačítka **SetMark** a **CheckMark**. Pomocí nich označíte svá data digitálním vodoznakem (něco jako digitální podpis), který můžete následně kdykoliv ověřit a dokázat tak svoje autorství.



Kliknutím na tlačítko **Set Mark!** se řetězec v poli **Mark string** použije jako podpis pro skupinu souborů v seznamu **Carrier Selection**.



OpenPuff: Skrývání tajností v nevinných souborech

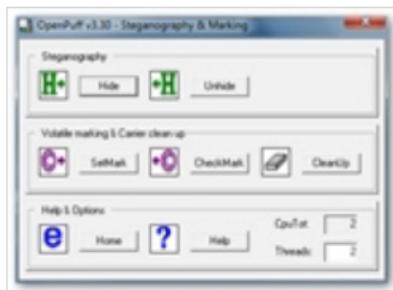
[Vytisknout](#) | [textová verze](#) | [velikost písma](#) **Velké písmo? Nastavte si menší**Autor: [Josef Kraus](#)

Vytváření, přechovávání i posílání zašifrovaných dat může už samo o sobě představovat riziko odhalení. Alternativou je uchování v tajnosti i fakt, že se snažíte něco skrýt.

OpenPuff je malá, jednoduchá a velice účinná aplikace, která se zabývá tzv. steganografií. Jedná se o způsob šifrování informací, kdy data jsou skryta do dat jiných tak, aby nebylo na pohled vůbec poznat, že zde jsou nějaké informace ukryty. Jedná se typicky o zakomponování údajů do obrázků, fotek či dokumentů, které nevypadají podezřele, když samy o sobě leží na disku počítače nebo se posílají jako příloha e-mailu.

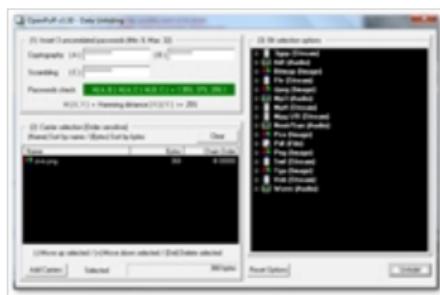
Ukrývání dat

OpenPuff nabízí ve svém minimalismu hned dva způsoby tajného skrývání údajů do běžných souborů. Tím první je výše uvedený postup zakomponování jedných dat do jiných. V malém okně aplikace, kterou není třeba instalovat a běží i z přenosného zařízení, zvolíte tlačítko pro skrytí pomocí steganografie. Rázem se otevře druhé a větší okno, v němž celou operaci provedete v několika krocích.



Základní rozcestník.

Na prvním místě je třeba zadat tři různá a dlouhá hesla, které slouží jako přístupový klíč ke skrytým informacím. V druhém kroku zvolíte soubor, který chcete ukrýt. V třetím pak soubor nebo soubory, do kterých tajná data hodláte vložit. Podmínkou je, že musí být objemově větší, než zdrojový soubor. K vyvážení těchto dvou poměrů pak poslouží možnost nastavení kvality (bitrate, hloubky atd.) formátů, v nichž chcete informace uchovávat.



Zašifrování.

Na rozdíl od jiných podobných programů, které pracují pouze s grafickými soubory, OpenPuff nabízí celou škálu výstupních formátů. Zařadit sem lze krom grafiky i audio, video a také PDF. Jedná se celkově o 16 různých druhů výstupu.



Dešifrování.

Skrytá značka

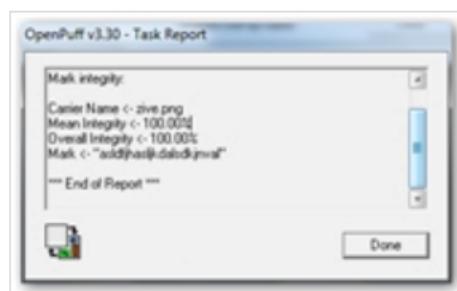
Celý proces nakonec vyhodí do zvolené složky nové soubory obsahující skryté informace. K těm se můžete zpět dostat opět pomocí OpenPuffu, pokud zvolíte tlačítko „odkryt“ a zadáte správně hesla. Druhou dovedností, kterou aplikace obsahuje, se týká skrytého

značkování, takže si potvrďte pravost onoho souboru, popř. autenticitu jeho odesílatele. Postup je podobný. Na úvod v základním okně je třeba zvolit tlačítko pro umístění značky.



Vkládání znaků.

Poté v novém okénku zadáte až 32 znaků, které se pak skrytě do následně vybraného souboru vloží. Že se jedná o takto označený soubor, poznáte, pokud si v programu zvolíte možnost pro kontrolu značky. Po provedeném procesu se zobrazí ony skryté informace. Pokud chcete onu značku odebrat, učiníte tak opět jednoduchou volbou přímo v aplikaci. OpenPuff je tedy zajímavým pomocníkem i pro málo zkušené uživatele, kteří jeho ovládání pochopí během pár minut. Většimu rozšíření aplikace navíc nahrává i fakt, že je možné ji užívat zcela zdarma.



Zpráva o přítomnosti značky.

OpenPuff

Stahnout

Verze 3.30 - 407,4 kB



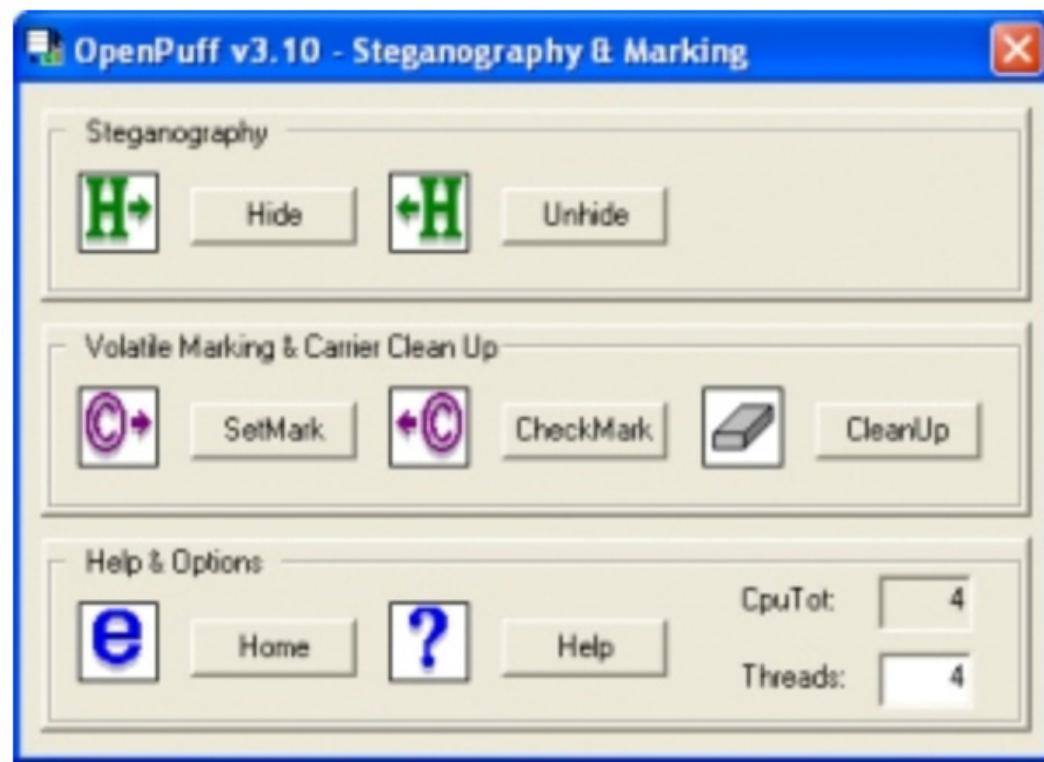
Licence: Freeware

Autor: [oliboni](#)



Verstecken und markieren

2 April 2011



Bei uns klingt der Name dieses Programms für Windows etwas ungewöhnlich; aber es kommt ja aus Italien. [OpenPuff 3.10](#) ist eine Software zur Steganographie, also zum Verstecken von Daten innerhalb von anderen Daten. Und da das Markieren von Dateien damit eng

verwandt ist, kann das Programm auch dafür verwendet werden. Interessant ist OpenPuff deshalb, weil eine sehr grosse Zahl an Träger-Formaten verwendet werden kann: Bilder (BMP, JPG, PCX, PNG, TGA), Audio-Dateien (AIFF, MP3, NEXT/SUN, WAV), Videos (3GP, MP4, MPG, VOB), Adobe-Formate (FLV, SWF, PDF) und sogar Windows-Formate (EXE, DLL). Ein weiterer Vorteil ist, dass das Programm nicht installiert werden muss (weil portabel) und deshalb niemand aus seiner Anwesenheit den Schluss ziehen kann, dass es evtl. verwendet worden sein könnte.



Startseite > Heft-DVD



Heft-DVD

AUSGABE 12/10

Top Software für Ihren PC: Auf der CHIP Heft-DVD finden Sie ausgesuchte Vollversionen sowie brandaktuelle Tools, Videos, Spiele, Tutorials und eBooks. Thema der DVD: Die große CHIP Privacy Suite *

[Empfehlen](#)

CHIP-CODE: GBTOOLS

Angry IP Scanner 3.0 Beta

Hooker 2.65 Beta

LicenseCrawler 0.0.42

OpenPuff 2.0

SmartSniff 1.72

Spy Screen

Switch Off 3.3.2

System Control Manager

WirelessKeyView 1.34

So blenden Sie Daten in JPEGs

Steganographie ist der Prozess des Versteckens Daten in einer solchen Weise, dass ihre Existenz nicht nachweisbar ist. Steganographie ist sicherer als die Verschlüsselung, weil ein Dritter, fängt eine verschlüsselte Nachricht, die Informationen kennt Wesen verborgen ist, und mindestens eine Chance hat, das Entschlüsseln der Nachricht. Hide Daten in ein JPEG-Bild mit Hilfe der Steganografie-Software, andere von der Annahme, dass alle Daten auf allen verborgen ist zu verhindern, die JPEG-Datei noch verhalten wird und erscheinen in der Regel bei Diebstahl oder abgefangen werden.

OpenPuff

- 1** Herunterladen und entpacken Cosimo Oliboni ist OpenPuff Software
- 2** Führen Sie das Programm "OpenPuffv340.exe." Nach einer Be-Sequenz, erscheint die Oberfläche des Programms.
- 3** Klicken Sie auf den Button "Hide" in die "Steganographie" Abschnitt. Eine neue Schnittstelle angezeigt.
- 4** Geben Sie drei einzigartige Passwörter in die drei Textfelder in der oberen linken Bereich der Benutzeroberfläche. Jeder muss mindestens acht Zeichen lang sein. Wenn Sie möchten, können Sie nur zwei oder ein Passwort, indem Sie die "B" und / oder "C" Kontrollkästchen nutzen, aber das macht Ihren versteckten Daten nicht so sicher. Die "Passwörter überprüfen"-Feld wird grün, wenn Sie das Passwort Anforderungen erfüllt haben.
- 5** Klicken Sie auf die Schaltfläche "Durchsuchen" in der oberen rechten Ecke der Benutzeroberfläche. Im daraufhin angezeigten Dialogfenster finden und wählen Sie die Datendatei, die Sie ausblenden möchten, und klicken Sie auf "Öffnen".
- 6** Klicken Sie auf "Hinzufügen" in der linken unteren Ecke der Benutzeroberfläche. Im daraufhin angezeigten Dialogfenster finden und wählen Sie die JPEG-Datei Sie möchten die Daten darin zu verstecken, und klicken Sie auf "Öffnen". Wenn das JPEG zu klein ist, erscheint ein Dialog. Klicken Sie auf "OK" und finden Sie eine größere JPEG oder verwenden Sie eine kleinere Datei. Wenn die JPEG ist groß genug, um die Daten zu verstecken, wird sie in der "Carrier Selection"-Liste und die "Selected / Total"-Anzeige leuchtet grün.
- 7** Klicken Sie auf die "Hide Data!" -Taste. In dem Dialog, der erscheint, finden und wählen Sie ein Verzeichnis in das neue JPEG-Datei speichern und klicken Sie auf "OK". Eine "Task completed" Dialog und ein Bericht angezeigt, wenn der Vorgang abgeschlossen ist. Ihr neues JPEG-Datei wird in das angegebene Verzeichnis. Kehrt man den Prozess, um Ihre Daten aus der JPEG-Datei, indem Sie auf "Einblenden"-Taste in zunächst für das Programm-Interface abrufen.



OpenPuff 3.3.0

Nachrichten in Bildern verstecken

Downloads: 429

Oberflächensprache: Englisch

Einschränkungen:

Hersteller: Cosimo Oliboni

【Beschreibung】

OpenPuff ist ein interessantes Tool, mit dem Sie Nachrichten in sämtlichen Bildern auf Ihrer Festplatte verstecken können.

Auch wenn OpenPuff hauptsächlich dazu gedacht ist, Nachrichten in Bildern zu verstecken, lassen sie sich auch in Video- und Bilddateien verstecken, wenn sie in den Formaten MP3, MPG, 3GP, WAV oder auch FLV vorliegen.

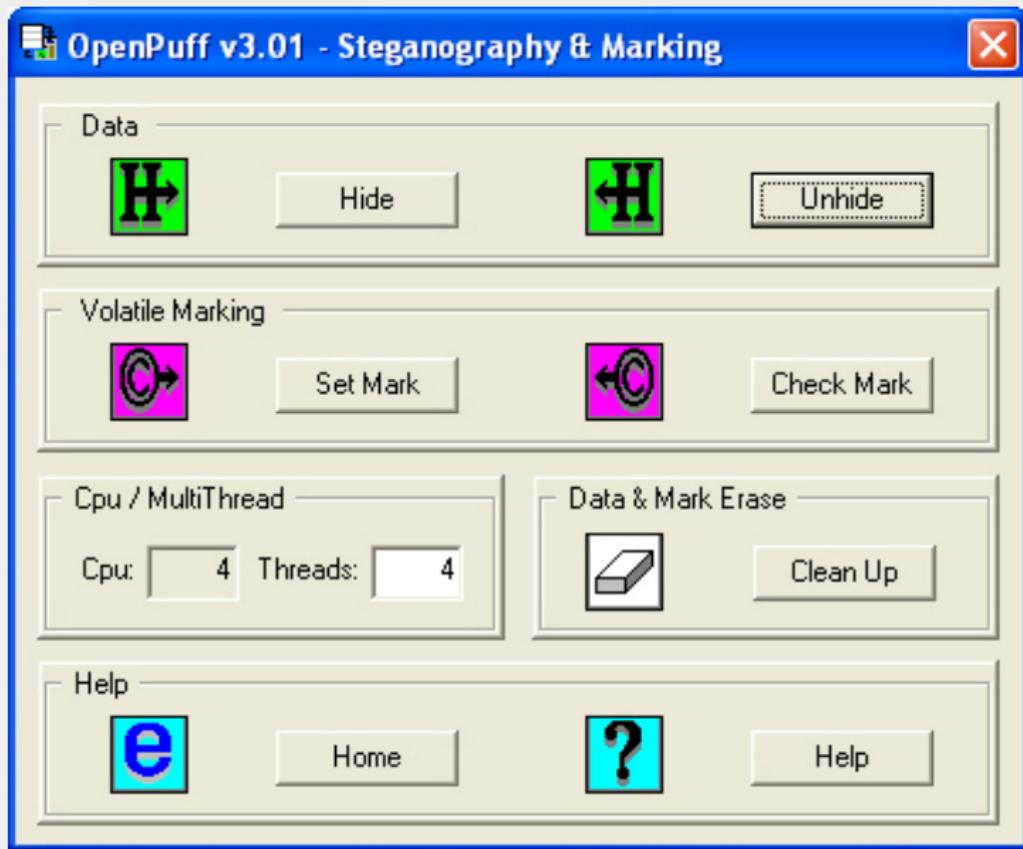
OpenPuff ist ein interessanter und effektiver Weg, um wichtige Informationen auf Ihrer Festplatte zu schützen. Anfangs verursacht man damit einiges an Chaos, sobald man sich jedoch an den Umgang gewöhnt, ist es eine großartige Anwendung.

【Bildschirmfoto】



→ OpenPuff 3.40

von **adminus Pro** @ 18. Jul 2011 - 09:32:52



OpenPuff ist ein Steganografie-Programm. Damit kann eine geheime Datei verschlüsselt versteckt werden in einer unverdächtigen Wirtsdatei, die nach wie vor funktionsfähig ist und auch öffentlich zugänglich sein kann. Als Wirtsdateien kommen eine ganze Reihe von Typen in Frage, z.B. exe, jpg, bmp, mp3, wav, pdf, flv und viele andere mehr. Außerdem kann man damit ein unsichtbares Wasserzeichen in einer Datei unterbringen, z.B. um eigene Urheberrechte zu sichern.

Das Programm eignet sich nicht, um massenhaft verschlüsselte Daten zu speichern, wie es z.B. von TrueCrypt praktiziert wird. Statt dessen versteckt man hier ein von der Anzahl der Bytes her relativ kleines Geheimnis in einer größeren, völlig harmlos erscheinenden äußeren Hülle.



OPENPUFF

OpenPuff is een geavanceerde Steganographische tool waarmee je data kunt verbergen in bestanden.

OpenPuff is een gratis programma waarmee je data kunt verbergen met behulp van steganografie. Zo kun je bijvoorbeeld teksten verbergen in grafische bestanden die er op het eerste gezicht uitzien als een normale foto. Openpuff verbergt je boodschap in deze drager en beveilt het met zeer sterke wachtwoorden en encryptie.

Het bewerkte bestand sla je veilig op, of je kunt het versturen. Met openpuff, en de juiste gegevens, is het mogelijk om daarna de verborgen gegevens weer te extraheren.

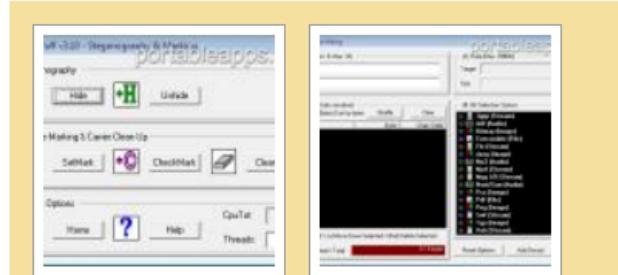
Met deze software is het ook mogelijk een onzichtbaar watermerk in je afbeeldingen te verstopen.

OpenPuff maakt gebruik van professionele steganografische technieken:

- Deniable steganography
- moderne multi-cryptography (16 parallele algorithmes)
- 512bit key cryptography met SHA512 wachtwoord
- HW seeded willekeurig nummer generator (CSPRNG)
- Data scrambling (CSPRNG-based shuffling)
- Data whitening (CSPRNG-based noise mixing)
- Adaptive LSB + Bits selection level

OpenPuff ondersteund verschillende dragers

- afbeeldingen (BMP, JPG, PCX, PNG, TGA)
- audio (AIFF, MP3, NEXT/SUN, WAV)
- video (3GP, MP4, MPG, VOB)
- flash (FLV, SWF, PDF)
- windows Executable(EXE, DLL)



actuele versie

3.40

website maker

[EmbeddedSw](#)

website project

[embeddedsw.net/](#)

tags

[openpuff](#) [steganografie](#) [encryptie](#)
[coderen](#) [data](#) [wachtwoord](#)



DOWNLOAD

(3.64 Mb)