How to hide data in images

By Ravi Sinha on *December 17, 2013, 10:59 IST*

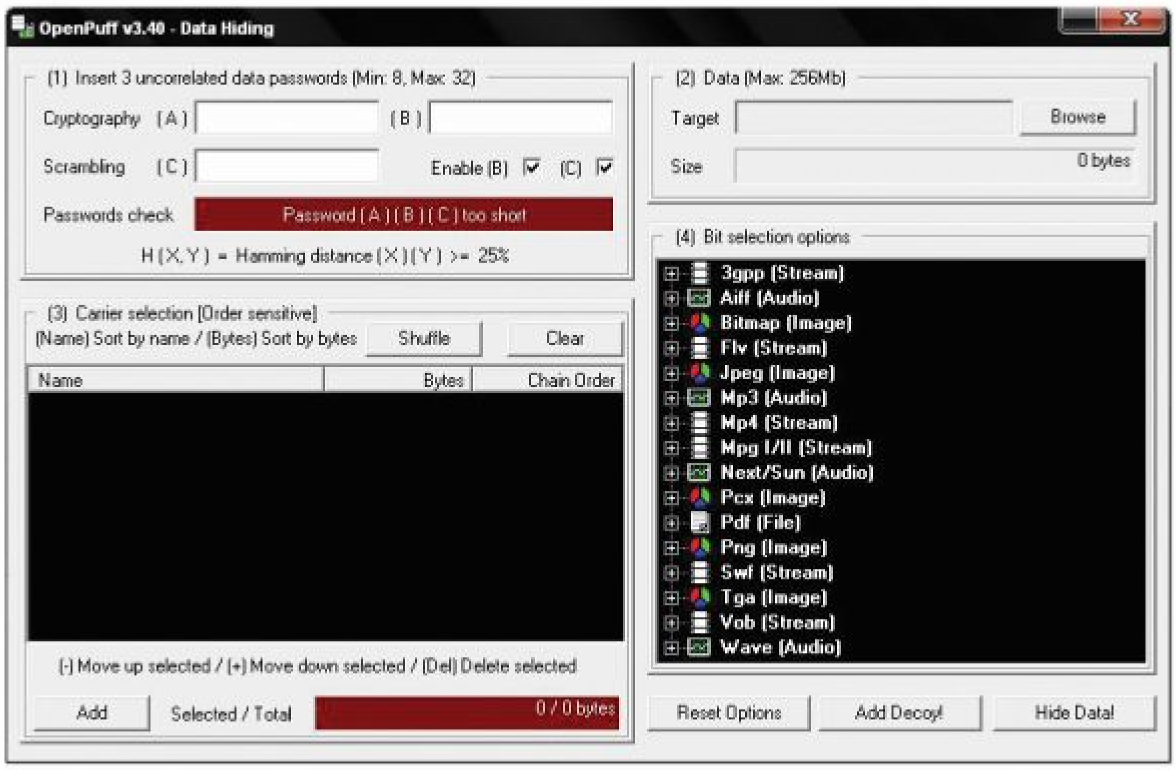
Learn how you can dabble in Steganography - the art of hiding data inside images

If there's one thing that history and popular culture has taught us about spies and secrets, it's that often, the best hiding spot is the one in plain sight. After all, if a nosy intruder is searching for valuable information, surely the last place he'd check is right under his own nose, right?

This logic forms the basis for steganography, itself an ancient historical practice of concealing information within images. This practice differs greatly in purpose from cryptography. The latter employs code to hide a message. This appears as jumbled letters and numbers, unless a cipher (or key) was used to decrypt the information back into its readable state. However, while cryptography is great for sending messages securely across unsafe channels, the very nature of the encrypted message will tip off anyone to its true form. In short, just because it's hard to break into, doesn't mean you want to leave it in plain sight. What if sending encrypting messages itself is against the law?

This is where steganography comes in. Using basic freeware tools like OpenPuff, it's possible to hide audio files, video, messages and images within a file (usually an image).

In steganography, the file or image used to deliver the hidden data is called the carrier. The hidden data is referred to as the payload. A carrier is usually required to hold up against different steganalysis methods, as well as common sense. Several digital artists use steganography to embed digital watermarks into their work. In case anyone else tries to lay claim to his or her property, the decrypted watermark can reveal the true owner.



OpenPuff v3.40 - Data Hiding

(1) Insert 3 uncorrelated data passwords (Min: 8, Max: 32)

Cryptography (A) (B)

Scrambling (C) Enable (B) ☑ (C) ☑

Passwords check: Password (A) (B) (C) too short

H(X,Y) = Hamming distance (X)(Y) >= 25%

(2) Data (Max: 256Mb)

Target

Size: 0 bytes

(3) Carrier selection [Order sensitive]

[Name] Sort by name / [Bytes] Sort by bytes

Name	Bytes	Chain Order

[-] Move up selected / [+] Move down selected / [Del] Delete selected

Selected / Total: 0 / 0 bytes

(4) Bit selection options

Use applications like OpenPuff to hide data in images

You can download OpenPuff from http://bitly.com/opuff1. After downloading and installing OpenPuff you'll see two primary options for steganography: Hide and Unhide.

Select Hide, and you'll be taken to a menu divided into four steps. The first step entails entering up to three different passwords to secure your data. You can choose to enter only one password as well, if keeping up with them all becomes tough. Next, you'll have to select your payload or target that you'll be transferring. Use the Browse button, and select the target to see it's overall size in a bar below the name.

In this third step, you'll have to choose a carrier. Keep in mind that the carrier can't be smaller than the target (since this will no doubt raise suspicions). You can attach multiple carrier bits if one file isn't big enough. Hit the Add button to navigate to files designated as the carriers and select them to see their space in relation to the target space. If the carrier space is greater, the red status bar will turn green.

The Bit Selection Option allows you to properly encode the carrier's size until it matches with the target. Keep in mind that some formats would be better suited than others. OpenPuff will alert you if the file type isn't supported for being a carrier.

After bit selection, hit "Hide Data!" and a new file will be created. On the outside, the carrier will look like a normal image file. Navigate to the Unhide option in the main menu and proceed to enter all the relevant details used for encrypting the file. Ensure that the passwords and bit selection option are exactly the same as those used before, or else the file won't open. Select your carrier file then, hit "Unhide!" and voila! The payload is now revealed.

You can also choose to fool any attackers by using the "Add Decoy" option. Simply head over the Hide menu, and after the previous four steps, select "Add Decoy". You can add a file, just like when adding the payload, and set multiple passwords for it. When you're done, hit "Hide Data". The decoy can be revealed in the same way as the payload, only you have to use the details entered for the decoy.

Selecting the SetMark option, and adding a mark to a specified carrier can add watermarks. Similarly, CheckMark allows you to verify the watermark by selecting the carrier in question. You can also use CleanUp to erase a watermark from an image.
Steganography obviously has its disadvantages and controversies but when used effectively, it becomes an invaluable tool for covert transmissions. Not to mention those times when you just want to claim right to your work.