

# O que é Esteganografia

Postado Em 25/08/2015 [data do post] por [Fábio dos Reis](#) [autor do post] em [Segurança](#) [categoria do post]

## Esteganografia

Esteganografia é a prática de esconder mensagens, arquivos ou imagens / vídeos dentro de outras mensagens, arquivos ou imagens / vídeos. O termo Esteganografia deriva da combinação das palavras em grego steganos (protegido, oculto) e graphein (escrever). É, portanto uma espécie de “escrita oculta”

Usando técnicas de esteganografia podemos esconder mensagens dentro de uma imagem, por exemplo, de modo que as pessoas que olharem para essa imagem não terão nenhuma idéia de que ali há informações ocultas.

A esteganografia é uma arte antiga. Essa técnica já era citada no século 15 em tratados de criptografia como o Steganographia de Johannes Trithemius. Naquela época já se ocultavam mensagens com o uso de tintas invisíveis no meio de textos visíveis em cartas, por exemplo.

Hoje podemos esconder informações em arquivos de computador. Por exemplo, podemos incluir em uma fotografia digital uma mensagem oculta, fazendo alterações em alguns bits específicos da imagem, sem que isso altere de forma perceptível a imagem em si.

Uma das formas mais comuns de esteganografia consiste em esconder uma mensagem dentro de uma imagem. Os tipos de imagens mais usadas para esse fim são:

- BMP
- GIF
- JPEG
- TIFF

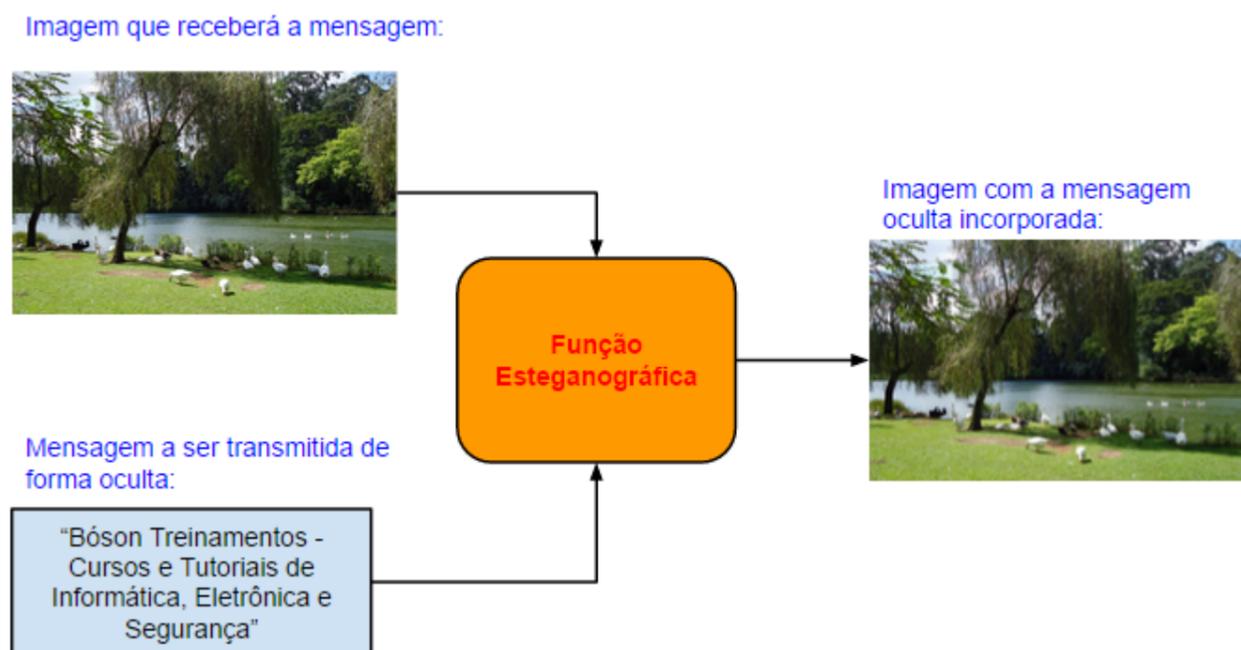
Os arquivos de imagem possuem características que podem ser exploradas, como sua resolução, altura e largura. Para que seja possível esconder uma mensagem em um arquivo de imagem são necessários dois arquivos:

- O arquivo contendo a imagem na qual a mensagem será inserida
- O arquivo contendo a mensagem em si

De posse desses arquivos, podemos escolher o método que será utilizado para inserir a mensagem na imagem. Os métodos mais comuns incluem:

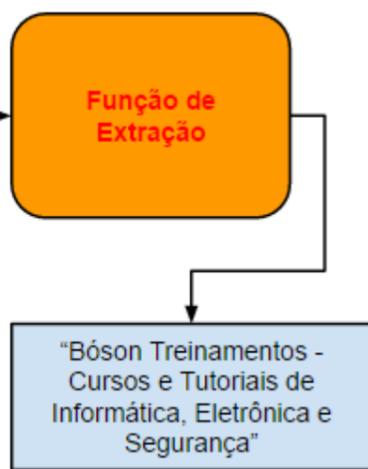
- Bit menos significativo (LSB – Least Significant Bit) – Alteração de alguns bits nos pixels que formam a imagem.
- Filtragem e mascaramento – uso de marcas d’água digitais nas imagens
- Algoritmos e Transformação – funções matemáticas em algoritmos de compressão

O processo funciona conforme ilustra a imagem a seguir:



O destinatário, ao receber a imagem, executará o processo inverso para extrair dela a mensagem oculta, conforme podemos ver na figura abaixo:

Imagem com a mensagem oculta incorporada:



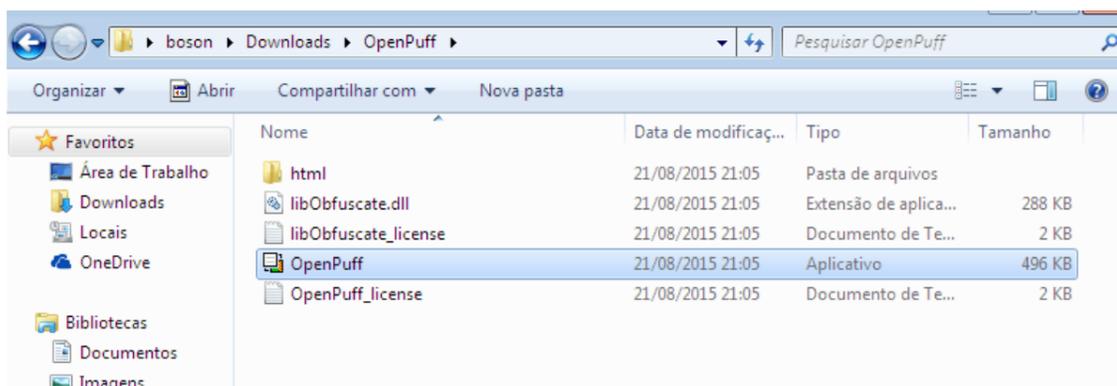
Mensagem oculta recuperada:

## Exemplo de Ferramenta de Esteganografia

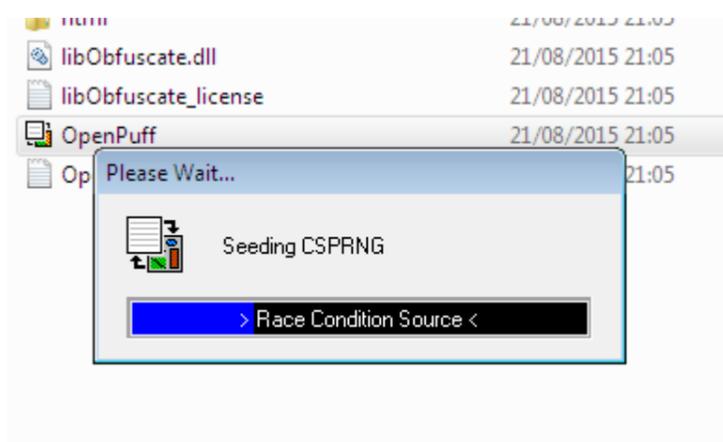
Vamos ver alguns exemplos de como esconder mensagens em arquivos digitais, com o uso de ferramentas específicas. Vamos trabalhar com a ferramenta freeware **OpenPuff**, que é uma ferramenta profissional de esteganografia e marcas d'água que suporta vários formatos de arquivos portadores (arquivos que carregam as mensagens ocultas), como por exemplo:

- Imagens BMP, JPG, PNG, TGA
- Áudio em MP3, AIFF, WAV
- Vídeo MP4, MPG, VOB
- Adobe FLV, PDF, SWF

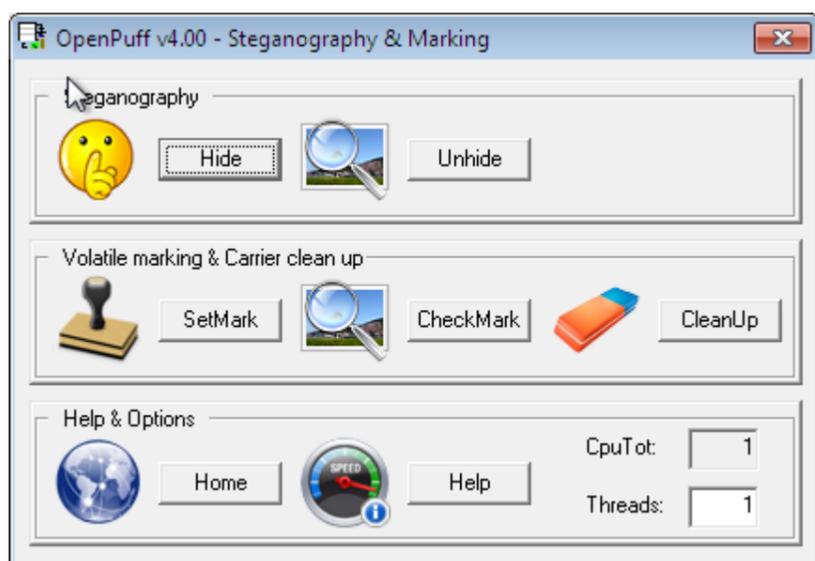
Baixe o [OpenPuff clicando neste link](#), e logo após descompacte o arquivo zipado em uma pasta do seu computador (versão para Windows). Após descompactar o arquivo, entre na pasta do OpenPuff e abra o programa executando o arquivo OpenPuff.exe:



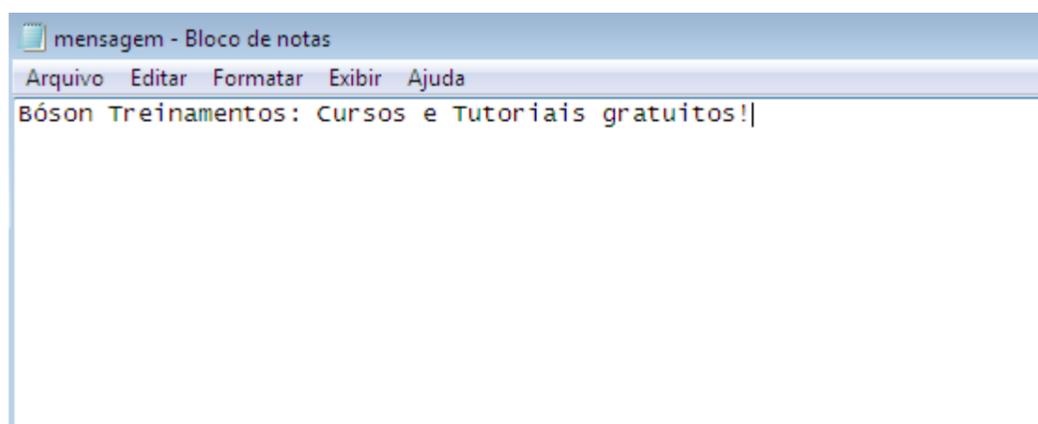
Aguarde enquanto o Gerador de Números Pseudo-Aleatório Criptograficamente Seguro (CSPRNG) é alimentado:



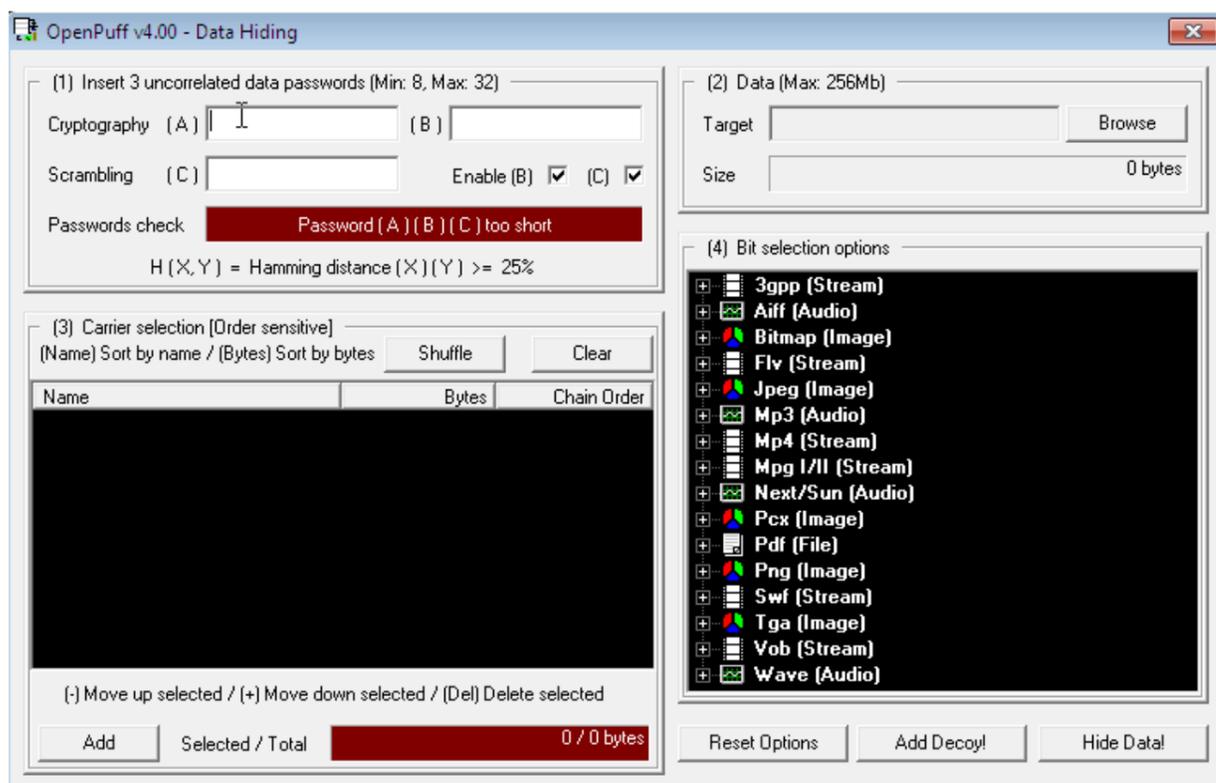
Em alguns segundos aparecerá a interface do OpenPuff, que é dividida em três seções: Steganography (Esteganografia), Volatile marking & Carrier Clean Up (Marca d'água e limpeza do arquivo portador), e Help & Options (Ajuda e Opções):



Vamos esconder uma mensagem em um arquivo de imagem agora. Primeiramente, vamos criar a mensagem de teste. Abra um editor de textos, como o Bloco de Notas, e digite qualquer texto desejado nele. Salve e saia do programa (batizarei meu arquivo de texto de “mensagem.txt” para maior clareza):

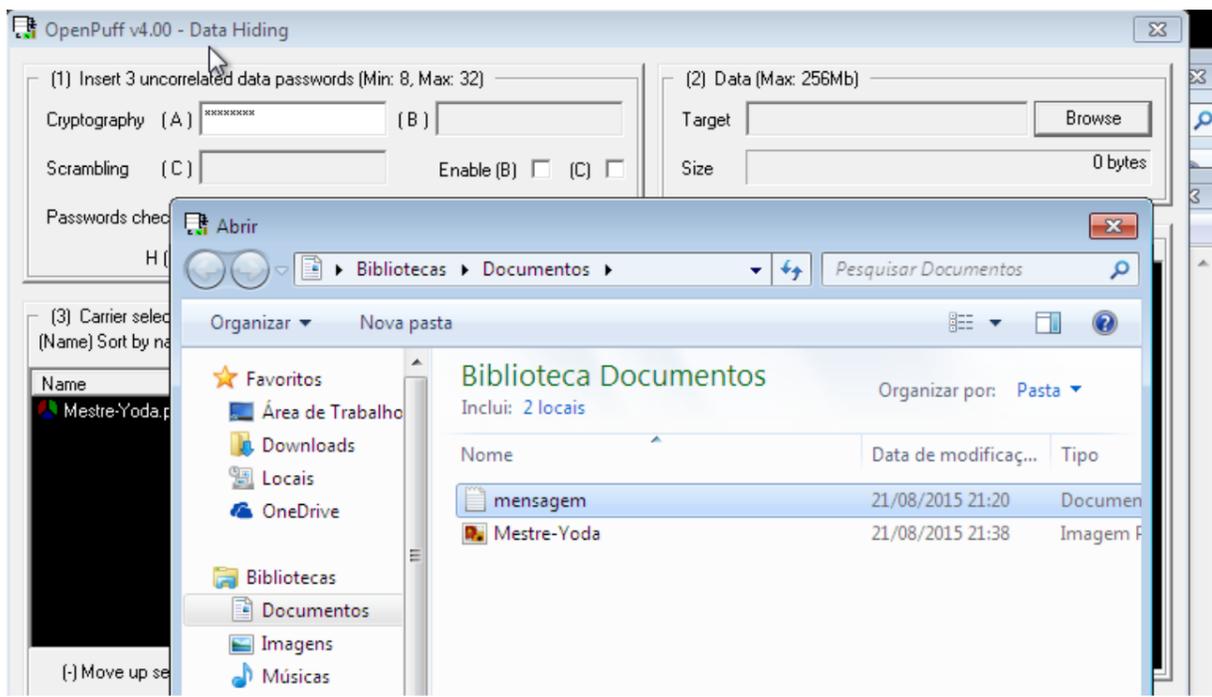


Excelente. Escolha também uma imagem (ou várias) para ser a portadora da mensagem. Agora, volte ao OpenPuff e clique no botão “**Hide**” na seção “**Steganography**” para que possamos inserir o texto do arquivo mensagem.txt na imagem escolhida. Será aberta a janela a seguir:

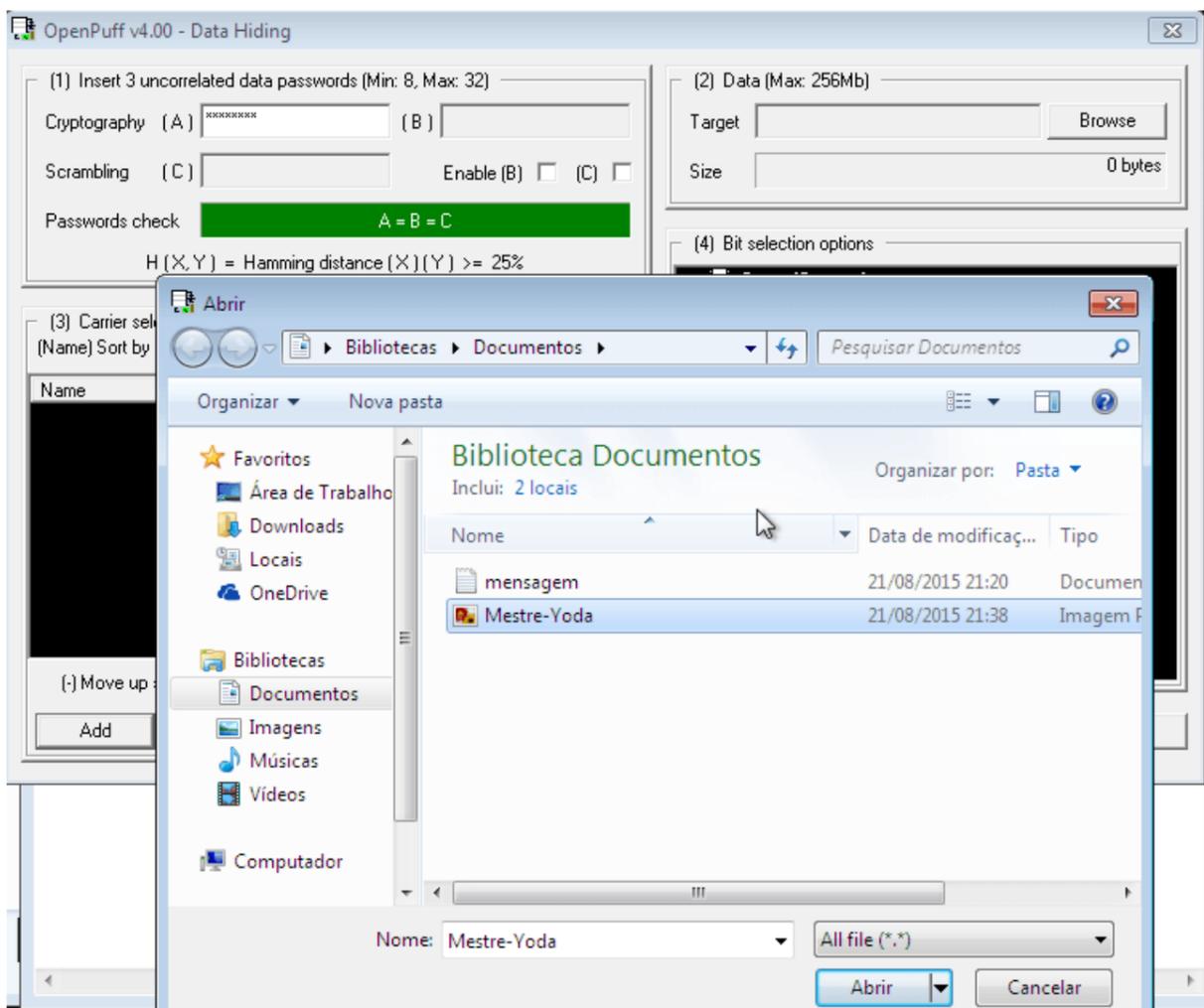


Vamos configurar alguns parâmetros agora para que possamos ocultar nossa mensagem na imagem escolhida. Você precisa, primeiramente, inserir no mínimo uma senha, clicando na caixa de texto “Cryptotgraphy (A)” e digitando-a. Essa senha será usada para proteger os dados ocultos no arquivo, e também para alimentar (seed) a criptografia e codificação da mensagem. Escolha a senha de sua preferência. Opcionalmente, você pode escolher mais duas senhas, que devem ser digitadas em “(B)” e “Scrambling (C)”. Vou usar apenas o padrão da senha (A) – desmarque os checkboxes “Enable (B) e (C)” neste caso.

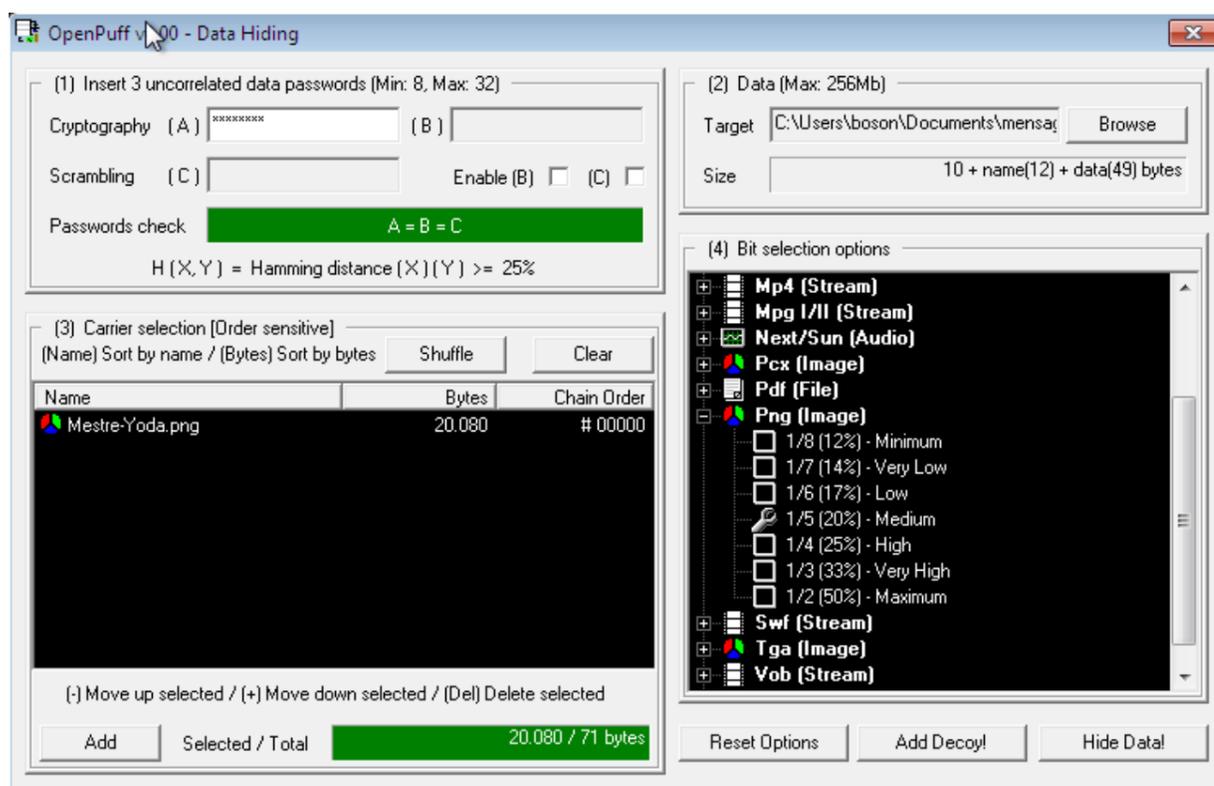
Vamos adicionar a mensagem ao OpenPuff agora. Clique no botão “Browse”, na caixa “Target”, seção (2) Data (no canto superior direito da tela), para escolher a mensagem-alvo, que será incorporada à imagem escolhida (no caso, meu arquivo mensagem.txt), e clique em “Abrir”. Note que os dados a serem ocultados podem ter no máximo 256MB de tamanho no OpenPuff. Você pode compactar e comprimir os arquivos de dados se desejar, ANTES de ocultá-los com o OpenPuff:



Após entrar com a mensagem, clique no botão “Add”, no canto inferior esquerdo, e escolha a imagem que será a portadora dessa mensagem. Clique em **Abrir** para adicionar a imagem:

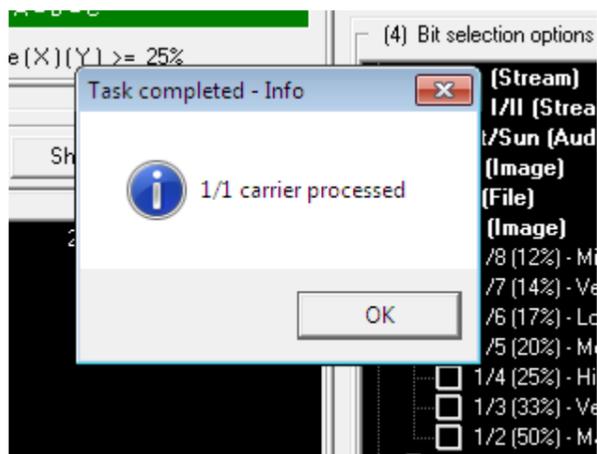


Escolhi a imagem “Mestre-Yoda.png” que estava em meu computador. Você pode adicionar quantas imagens quiser – adicione-as até a barra inferior ficar verde:

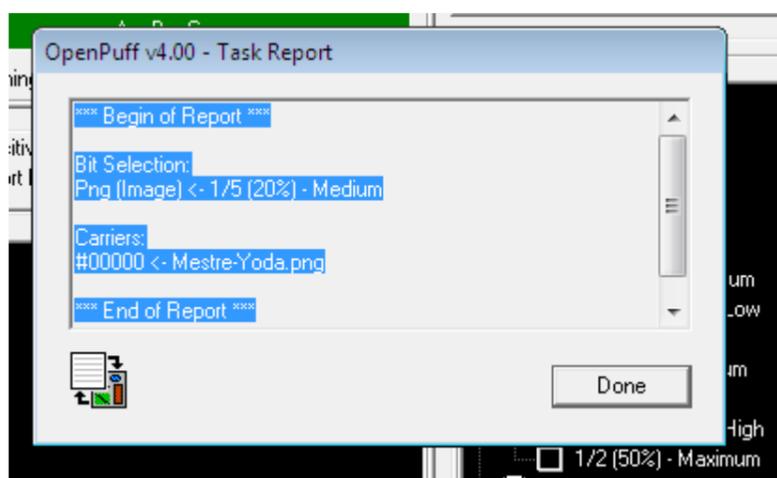


Excelente!. Já temos tudo o que precisamos para esconder a mensagem dentro da imagem do Mestre Yoda. Na caixa “(4) Bit selection options” podemos fazer ajustes como a razão entre dados e ruído, sendo esses ajustes úteis por exemplo quando queremos espalhar os dados secretos entre vários arquivos portadores, bastando para isso expandir a seleção do formato de arquivo portador selecionado e escolher o valor desejado. Não vou mudar nada neste exemplo.

Agora clique no botão Hide Data! no canto inferior direito para realizar a operação esteganográfica, e escolha um local para salvar a imagem contendo sua mensagem oculta. Em alguns instantes, você deve receber a mensagem “1/1 carrier processed”, indicando que os dados foram processados com êxito:



Clique em “OK”, verifique o relatório e então feche a caixa de diálogo clicando no botão “Done”:



Pronto! A imagem contendo sua mensagem secreta foi salva no computador. Abra-a e verifique-a minuciosamente – você perceberá que não há rastros visíveis da mensagem ocultada na imagem – mas a mensagem está lá:

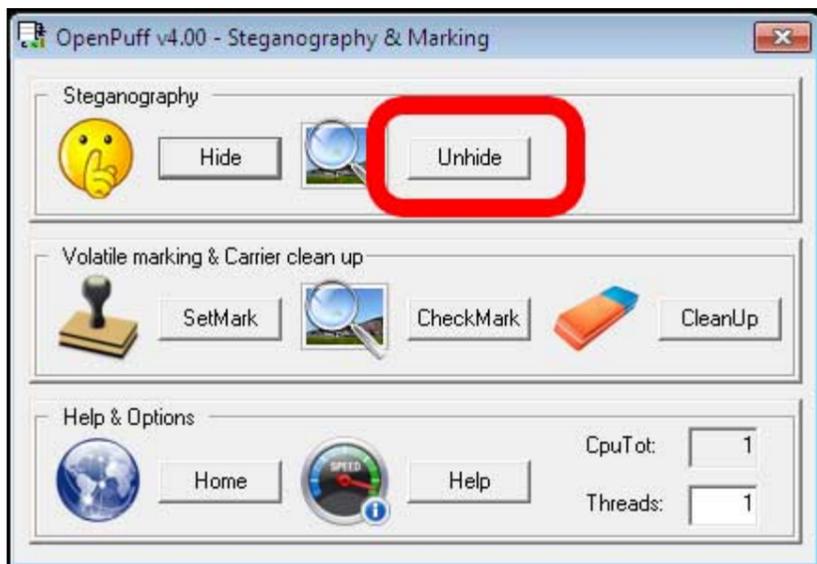


## Extraindo uma mensagem de um arquivo esteganografado

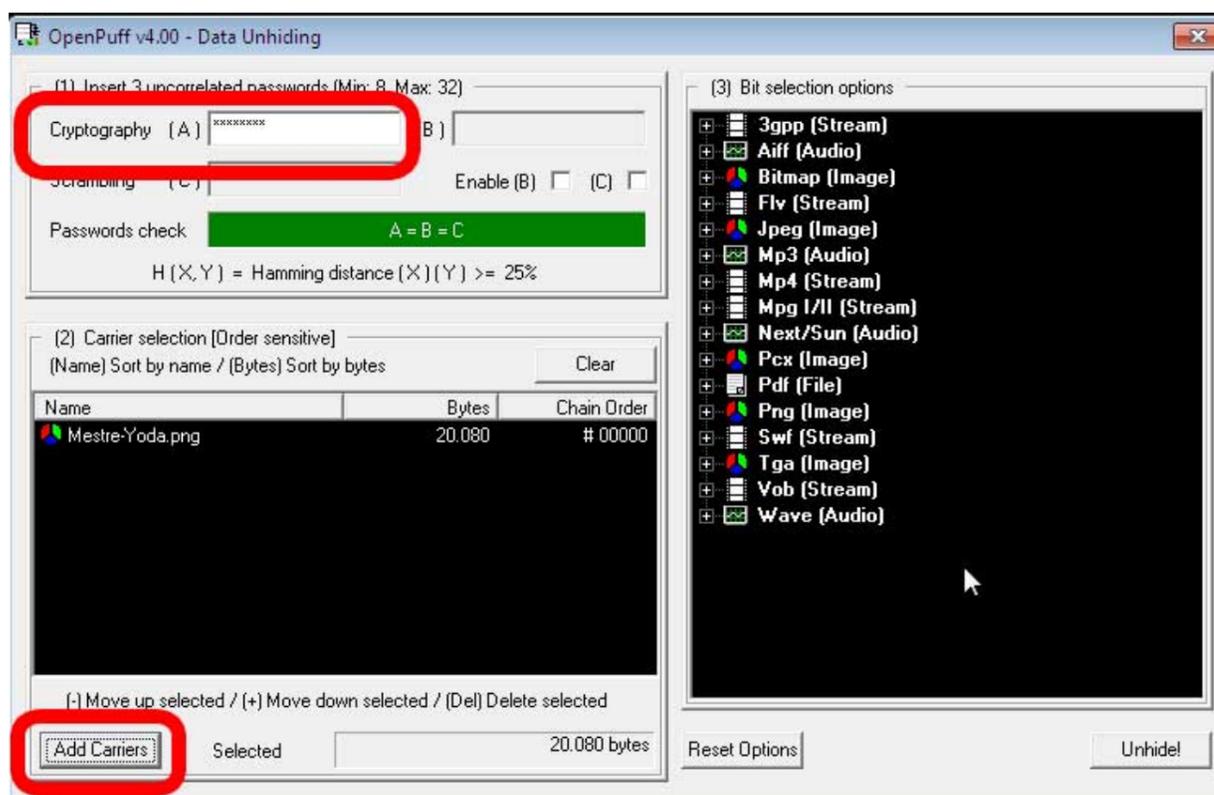
Vamos agora realizar o processo de extração da mensagem oculta por esteganografia em outro arquivo – no caso, no arquivo de imagem do Mestre Yoda que usamos anteriormente. Usaremos novamente o software OpenPuff, pois foi com ele que ocultamos nossa mensagem na foto.

Para isso, siga os passos a seguir:

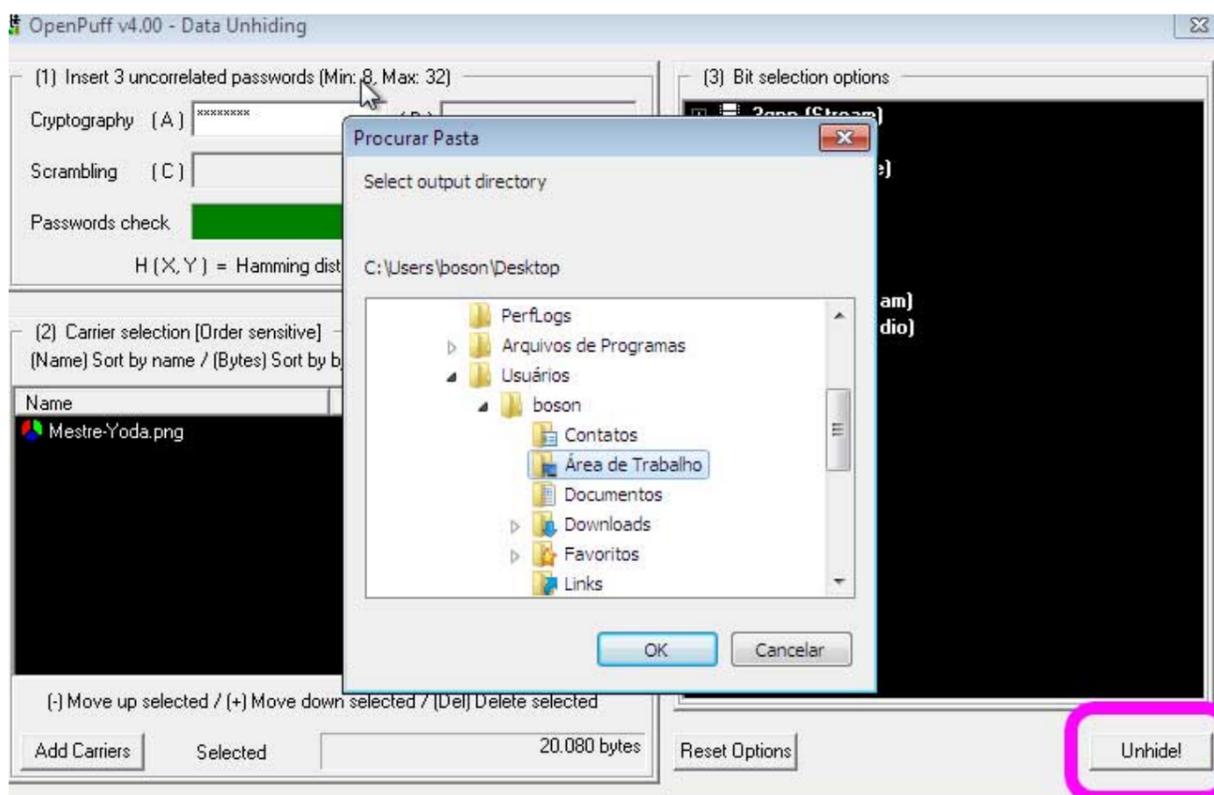
1. Abra o OpenPuff e, na tela inicial do programa, clique no botão “**Unhide**”, na seção Steganography:



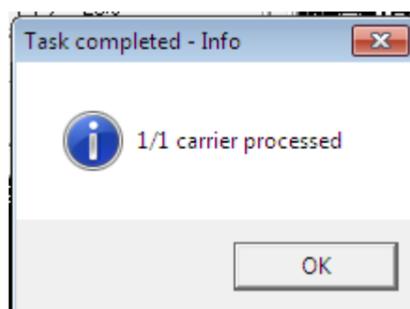
2. Entre com as senhas nos campos correspondentes da seção (1). Em nosso exemplo, usei apenas a senha “Cryptography (A)”, e por isso desmarquei os checkboxes “Enable (B)” e “(C)”. Em seguida, clique no botão Add Carriers na seção (2) Carrier Selection para selecionar a imagem que contém a mensagem oculta:



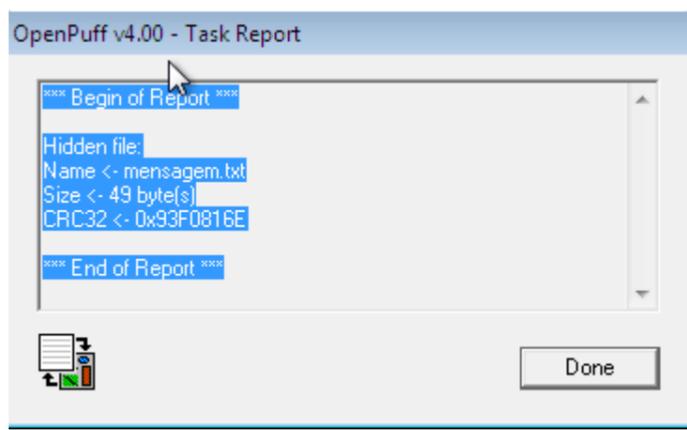
3. Após selecionar a imagem, clique no botão “Unhide!” na seção (3), na parte inferior do lado direito da janela, e selecione o diretório de destino da mensagem. Clique em OK logo após.



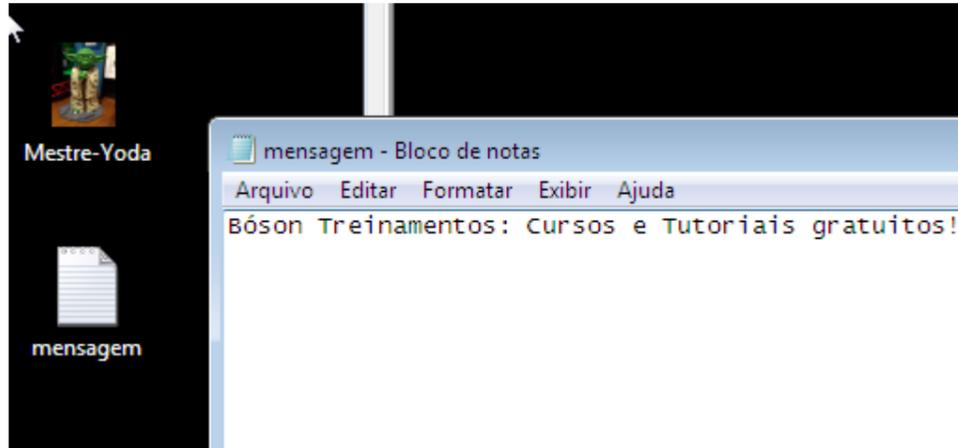
4. Clique em OK novamente para finalizar a tarefa:



5. E então clique em Done para fechar o relatório da tarefa. Abra o diretório escolhido e encontre a mensagem, que deve estar lá. Abra-a para verificar seu conteúdo:



Veja a mensagem recuperada a seguir:



Procedimento finalizado com sucesso! Ocultamos uma mensagem por esteganografia em um arquivo de imagem usando o software OpenPuff, e logo após conseguimos recuperar a mensagem oculta.