Esteganografia - Conceito e prática

O termo **esteganografia** deriva do grego, em que estegano significa “esconder ou mascarar”, e grafia, “escrita”. Desta forma, **esse termo pode ser definido como a arte de esconder informações, tornando-as ocultas**. Existem muitas técnicas esteganográficas que escondem dados dentro de arquivos. Seu principal objetivo é que esses dados não sejam percebidos por terceiros, ou seja, a presença de mensagens escondidas dentro de arquivos é simplesmente desconhecida. Somente o receptor da mensagem tem conhecimento de sua existência, assim como da maneira como extraí-la.

Muitos são os meios utilizados para a aplicação da **esteganografia**. Mensagens podem ser escondidas em imagens, utilizando-se de algumas técnicas específicas, como a do bit menos significativo. Além de imagens, arquivos de áudio também podem ser usados para ocultar mensagens, de maneira que estas não sejam percebidas por quem estiver ouvindo o som. Outros métodos usam também arquivos de texto, arquivos HTML e pacotes TCP para esconder informações.

A **esteganografia** possui inúmeras aplicações. No entanto, é relevante notar que as técnicas também possuem algumas restrições. Por exemplo, o tamanho das informações a serem escondidas é limitado pelo tamanho do próprio meio que será utilizado. Quanto menos essas informações degradarem a aparência dos arquivos, maior é o potencial das técnicas esteganográficas. Geralmente, mensagens muito grandes acabam ferindo a integridade do meio, o que facilita uma fácil detecção de que uma possível mensagem foi escondida no arquivo.

Esteganografia x Criptografia

Ao contrário do que pode parecer, esteganografia e criptografia são duas áreas com objetivos diferentes.

Enquanto a **criptografia** tem o propósito de impedir que as pessoas saibam o conteúdo de uma mensagem, a **esteganografia** se baseia em evitar que as pessoas saibam que a mensagem existe. Ou seja, na **criptografia**, os receptores sabem da existência das mensagens, porém não conseguem lê-las; já a **esteganografia** tenta fazer com que os receptores não percebam que há uma mensagem naquele meio (imagem, música, etc).

Quando se trata de segurança da informação, a **criptografia** é mais comumente usada. Porém, quando uma mensagem está **criptografada**, ela fica destacada por potencialmente possuir uma informação secreta e interessante. A vantagem da **esteganografia** está relacionada ao não-conhecimento da mensagem, o que evita que muitos ataques sejam realizados.

Para que a comunicação seja a mais privada possível, muitos combinam a **esteganografia** com a **criptografia**. Dessa forma, caso seja descoberto que a mensagem está camuflada, ainda existirá um novo obstáculo a ser superado para que ela possa ser lida.

Aplicações da esteganografia

A **esteganografia** teve sua origem diretamente relacionada a aplicações: o termo, como dito anteriormente, deriva de "**escrita escondida**", sendo relacionado com comunicações sigilosas ou privadas. No meio digital, o uso da esteganografia é amplo: abrange desde práticas comerciais a aplicações com fins militares.

Um autor de um documento, por exemplo, pode inserir mensagens escondidas de direitos autorais (*copyright*) de modo que, quando reveladas, demonstrem que a propriedade intelectual do documento lhe pertence. Se outra pessoa possuir acesso ao documento e clamar que ele é seu, o autor pode provar o contrário, já que só ele tem conhecimento de como readquirir a mensagem escondida. Este tipo de aplicação é conhecido como marca d'água digital ou *watermarking*.

Ainda sob escopo comercial, deve-se lembrar que é de interesse das empresas manterem segredo sobre produtos novos, planos estratégicos ou abordagens inovadoras sobre tecnologias recentes. Com base nisto, a **esteganografia** cumpre bem o papel de ocultar a existência de informações, inserindo dados escondidos em meios de comunicação diversos. É possível, por exemplo, usar técnicas para ocultar um documento de texto em uma figura qualquer (como o logotipo da empresa), de modo que apenas os receptores que souberem de sua existência poderão recuperá-lo e efetivamente lê-lo.

Agências militares e de inteligência precisam de meios discretos para se comunicar, sobretudo em áreas de conflito. A transmissão de conteúdo **criptografado** não é muito eficiente neste quesito, dado que o emissor do sinal pode ser facilmente localizado e possivelmente atacado. Por este motivo, técnicas de **esteganografia** são largamente usadas em comunicações militares, como a modulação por espalhamento de espectro, dificultando a detecção da transmissão pelo inimigo.

Também é possível citar aplicações ilegais para a **esteganografia**, como registros ocultos de atividades fraudulentas ou de dados relacionados a espionagem industrial. Além de esconder dados sigilosos ilegalmente, criminosos também podem se comunicar usando métodos **esteganográficos**, de modo que suas mensagens dificilmente sejam detectadas ou interceptadas.

Técnicas de esteganografia digital

Este artigo está focado nas técnicas de **esteganografia digital**, que se baseiam em algum meio digital para que a informação seja camuflada. Estas técnicas podem ser divididas de acordo com o critério utilizado para esconder o conteúdo que se deseja transmitir. Abaixo, são expostos alguns desses critérios..

- Ruído: é uma técnica simples que consiste em substituir o ruído em uma imagem ou em um arquivo de áudio pela informação que se deseja transmitir;

- Espalhando a Informação: mecanismos mais sofisticados espalham a informação nos pixels de uma imagem ou em partes de arquivos de áudio;

- Ordenação: consiste em transmitir a informação através da ordem em que os elementos de uma lista são dispostos;

- Dividindo a Informação: divide a mensagem em partes que seguem caminhos diferentes até o destino; algumas técnicas mais sofisticadas possibilitam, inclusive, que a informação seja reconstruída a partir de

uma fração do total de pacotes em que a mensagem foi dividida.

A combinação das técnicas expostas acima permitem diferentes níveis de segurança, gerando informações ocultas difíceis de serem decifradas. Uma imagem digital que se deseja transmitir secretamente, por exemplo, pode ser escondida em uma lista, que, por sua vez, pode ser armazenada no ruído de um segundo arquivo, o qual pode ser transmitido de forma a ocultar a fonte da informação.

Sempre é possível detectar uma técnica **esteganográfica**, pois ela altera propriedades estatísticas do meio original. Todavia, tendo em vista que os melhores ataques (tentativa de descobrir os dados ocultos e/ou de removê-los) são aqueles específicos para a técnica, se a técnica é mais difícil de ser detectada, ela será mais eficiente na tentativa de proteger a mensagem, pois o atacante terá que usar um método mais geral e, portanto, menos eficaz.

Softwares que podem ser utilizados

Existem diversos aplicações que podem ser utilizadas para ocultar informações dentro de outros arquivos, embora eu apresente apenas duas, sendo uma para ambiente Windows e outra para o GNU/Linux.

OPENPUFF (Windows)

Esse aplicativo pode esconder informações dentre de imagens, músicas, arquivos PDF, dentre outros.

Como usar o OpenPuff

Clicando na opção "**Hide**" (para esconder os arquivos), uma nova janela é aberta e você precisa fazer o seguinte:

- Colocar ao menos uma senha para a proteção. Podem ser três senhas diferentes, o que aumenta segurança;

- Adicionar o arquivo que irá "hospedar" o documento confidencial. Pode ser uma imagem, por exemplo. Assim, insira o arquivo no quadro preto esquerdo da janela;

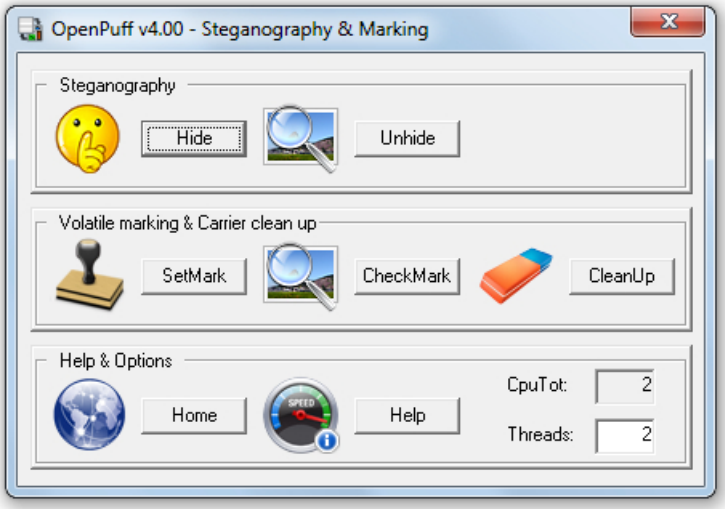
- Procure o arquivo confidencial através do botão “Browse”, que está no canto direito superior da tela.

É preciso dizer que o arquivo receptor da informação precisa ser maior em bytes que o confidencial. Com tudo pronto, apenas clique em “Hide Data!”, que o programa abrirá uma nova janela para que você selecione uma pasta para salvar o novo documento que contém as informações secretas escondidas.

Recuperando o arquivo oculto

Agora você deve clicar na opção “**Unhide**” na tela inicial do aplicativo.

Depois, forneça a senha que você inseriu quando ocultou o documento e procure o arquivo receptor através da opção “Add Carriers”. Feito isso, apenas clique em “Unhide!” e salve o arquivo confidencial em uma pasta de sua preferência.



O download do OpenPuff pode ser realizado no seguinte endereço:

OpenPuff - Steganography & Watermarking - EmbeddedSW

https://embeddedsw.net/OpenPuff_Steganography_Home.html

Conclusões

A **esteganografia digital**, ou seja, a arte de esconder informações em meios digitais, vem sendo cada vez mais pesquisada e utilizada nos dias de hoje. Ela possui uma infinidade de aplicações, e talvez a mais importante delas seja a segurança da informação, já que, com a **esteganografia**, as mensagens ficam escondidas nos meios usados, e a informação passa despercebida por terceiros.

A quantidade de técnicas existente é grande. Elas podem se basear na presença de ruídos em imagens, em uma ordenação de elementos, nas características auditivas dos seres humanos, entre outras. Algumas delas espalham a informação em imagens e arquivos de áudio; outras, dividem-na em várias partes. Muitas dessas técnicas podem ser facilmente integradas com métodos de **criptografia** para que a segurança dos dados que estão sendo transmitidos seja maior.

Ao mesmo tempo que o número de técnicas tem aumentado, a **esteganálise**, isto é, a área responsável por descobrir a existência de mensagens em arquivos, vem tentando decifrar todos esses métodos. Os diversos ataques possíveis, ou seja, os ataques visuais, os estruturais e os estatísticos, são usados de forma a saber sobre a existência ou não de alguma mensagem secreta. Uma vez que essa existência é descoberta, o **esteganalista** pode querer ler a mensagem, torná-la inconsistente ou simplesmente destruí-la.

As técnicas **esteganográficas** não são perfeitas; a **esteganálise** está sempre buscando suas falhas, a fim de descobrir os algoritmos usados. Porém, mesmo assim, a **esteganografia** mostrou-se muito eficaz em esconder informações que não podem cair acidentalmente nas mãos de terceiros. Uma grande quantidade de pesquisas e estudos está em andamento, evidenciando a importância dessa área atualmente.