Esteganografia, a segurança através da obscuridade, com análise dos aplicativos OpenPuff e Quick Stego

Mariela Alves Rodrigues
mrl.ti2018@gmail.com
Computação Forense e Perícia Digital
Instituto de Pós-Graduação - IPOG
Palmas, TO, 12/09/2020

Resumo

O crescimento acelerado das trocas de informações sigilosas na internet levou à necessidade de ampliação da segurança das mesmas, já que ataques maliciosos estão cada vez mais iminentes. Dado isso, a esteganografia é de vital importância no auxilio da proteção digital, assim como na observação dos impactos causados pelo mau uso dela. Ela inclui um amplo conjunto de métodos de camuflagens secretas desde os tempos mais antigos, tal como o uso de tintas “invisíveis”, micro pontos, tabletes de cera, até o uso de canais escondidos (técnica do LSB), marcas d’água, assinaturas digitais dentre outras. O presente artigo se propõe a expor a história, significado, técnicas e aplicações da esteganografia, diferenciando-a da criptografia, e dando ênfase em dois aplicativos gratuitos, OpenPuff e Quick Stego, com a discussão das formas de uso deles.

Palavras-chave: Esteganografia. Criptografia. Segurança da Informação. OpenPuff. Quick Stego.

1. Introdução e História

A expansão da internet tornou mais fácil o compartilhamento das informações, levando ao aprendizado de ferramentas diversas, as quais em muitos casos são usadas para práticas indevidas e maliciosas, feitas quase sempre no anonimato. Dentre essas ferramentas discutiremos sobre as técnicas de esteganografia, juntamente com análise dos aplicativos OpenPuff e Quick Stego.

A esteganografia é uma palavra que vem do grego e significa “escrita oculta” (stegano= escondido ou secreto e grafia= escrita ou desenho). Trata-se do estudo de técnicas que permitam camuflar informações dentro de outros arquivos sejam eles imagens, músicas, vídeos ou mesmo textos (ATTABY, 2017). A menção histórica mais antiga e confirmada dessa técnica advém do célebre livro “As Histórias”, de Heródoto, data de cerca de 440 a.C onde é relatado o caso de certo grego que precisava fazer contato com o seu superior(um tirano de nome Aristágoras de Mileto), de uma forma oculta. Sendo assim, ele escolheu um escravo que lhe era muito fiel, e raspou-lhe a cabeça, escrevendo em seu couro cabeludo a tal mensagem. Em seguida aguardou que os cabelos do mesmo crescessem, e só então o enviou ao encontro de Aristágoras. O serviçal recebera a instrução de raspar novamente a sua cabeça perante o tal tirano, com o intuito de que ele pudesse ler o aviso secreto. A partir desse tempo, a esteganografia passou a ser utilizada de

várias formas com o objetivo de que as mensagens não fossem interceptadas por pessoas não autorizadas. Sabe-se ainda de narrativas sobre recados impressos em tabletes(KUMAR, 2010), os quais eram recobertos por cera (escondendo a verdadeira mensagem), ou ainda gravados em seda fina (típicos da China), das quais eram feitas bolinhas envoltas por cera, que deveriam ser engolidas por mensageiros e enfim regurgitadas no local de destino (tudo isso em tempo suficiente para que o organismo não a digerisse).

> O termo “esteganografia” só ficou conhecido no século XV, quando o monge Johannes Trithemius (Figura 01) publicou o livro *Steganographia*, escrito em três volumes. Na época em que foi publicado, acreditava-se que esse livro tinha como assunto principal magias, espíritos, entre outros. Porém, mais tarde, a “chave” para a decodificação do livro foi identificada, e descobriu-se que, na verdade, o livro falava sobre esteganografia e criptografia, detalhando várias técnicas destinadas a enviar mensagens sem que elas fossem percebidas (GIL et al., 2008).

Figura 01: Johannes Trithemius, considerado o pai da esteganografia
Fonte: https://www.nndb.com/people/790/000115445/

Durante a segunda guerra mundial, devido ao aumento na qualidade das câmeras, lentes e filmes, tornou-se possível aos espiões nazistas, a criação de uma das formas mais interessantes e engenhosas de comunicação secreta. As mensagens nazistas eram fotografadas e, posteriormente, reduzidas ao tamanho de pontos finais (**.**) em uma sentença. Assim, uma nova mensagem totalmente inocente era escrita contendo o filme ultrarreduzido como final das sentenças. A mensagem gerada era enviada sem levantar maiores suspeitas. Esta engenhosidade ficou conhecida como tecnologia do micro ponto (SINGH, 2001). Estas histórias (JOHNSON et al., 1998) mostram uma esteganografia primitiva. Hoje as mensagens são embutidas em imagens, som, protocolos como TCP/IP (AHSAN et al., 2002); em geral meios digitais.

A esteganografia está presente em nossas vidas de uma forma bem constante, tal qual nas cédulas monetárias (figuras 02,03 e 04), ou ainda nos documentos de identificação (RG, CPF, etc.), onde podemos verificar a existência de inúmeras

mensagens escondidas, através do auxílio de equipamentos como lentes, reagentes químicos, foto reagente, luz, tato, etc.
É importante diferenciar esteganografia de marca d´água, apesar de muitas vezes os métodos serem tratados juntos. No primeiro, o foco está em esconder uma mensagem, não se preocupando se o método é robusto e busca a maior quantidade possível de espaço para a mensagem. No segundo, a marca d´água não deve necessariamente estar escondida, o método deve ser robusto e não majora o espaço.

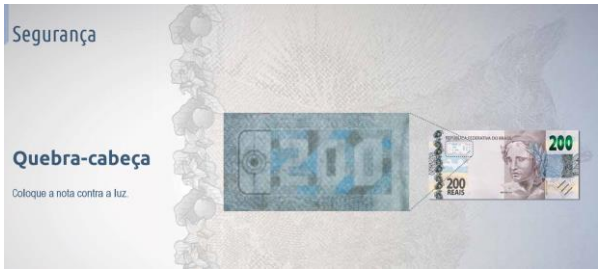

Figura 02, 03 e 04: Na cédula de R$200,00, existe uma marca d'água que vista contra a luz, mostra a imagem do lobo-guará e um quebra cabeça, juntamente com elementos em relevo para sentir com os dedos
Fonte: https://cultura.uol.com.br/noticias/12523_nota-de-r-200-entre-elementos-de-seguranca-marca-d-agua-e-textura-em-alto-relevo.html

2. Esteganografia e Criptografia

A esteganografia é um ramo da criptografia, e ambas devem ser usadas conjuntamente, a fim de oferecer uma forma robusta e altamente eficiente para manter os dados íntegros e protegidos. Dessa forma, caso seja descoberto que a mensagem está camuflada, ainda existirá um novo obstáculo a ser superado para que ela possa ser lida. Sabe-se que é difícil localizar uma mensagem escondida em qualquer lugar, porém ao se ter uma suspeita, ficaria mais fácil determinar se existe ou não esteganografia, do que quebrar a criptografia. Embora transmitam equivalência, elas não podem ser confundidas, enquanto a criptografia tem a função de ocultar o significado de uma mensagem (torna-o ilegível/incompreensível), a esteganografia tem o objetivo de camuflar a existência da informação na mensagem. Esta última não pode ser detectada, ao contrário do que acontece com os arquivos cifrados. É justamente por isso que as técnicas para ocultar informações em outros arquivos possuem diversas aplicações, inclusive para o terrorismo. Em termos práticos, uma pode ser utilizada dentro da outra. Podemos ter uma mensagem criptografada que pode ser escondida em um lugar específico (arquivo de imagens,

músicas etc.), aumentando assim seu grau de segurança. A esteganografia é uma das técnicas utilizadas para garantir a autenticidade e verificar direitos autorais em imagens e outras mídias. De acordo com Oliveira (2007), mesmo que existisse uma esteganografia perfeita, certamente ela teria um custo muito elevado e inviável para ser usada em grande escala. Logo, poderia ser usada somente para troca de chaves simétricas, ao invés de ser usada para transmitir a mensagem. A esteganografia consegue fornecer uma segurança a mais que a criptografia e com ela a mensagem não é interrompida, se não for detectada.

3. Objetivos

Com o acelerado crescimento da tecnologia no mundo e do tráfego de dados, os especialistas acreditam que muitas informações veiculadas na web podem esconder instruções com planos de atentados e outras mensagens de cunho delituoso, fato este que abriu novas oportunidades para as técnicas de ocultação de informações. O termo esteganografia é um vocábulo desconhecido para quem não está diretamente envolvido com a segurança de dados e pessoas nos meios eletrônicos (MARTINS,2010). Mesmo em filmes policiais e investigativos, famosos por abordarem técnicas e soluções mirabolantes, deixam um pouco de lado essa complicada palavra e tudo o que a envolve. Dado isso o manejo das ferramentas pelo profissional da computação forense é de vital importância, devendo o mesmo estar atento ao descarte de imagens aparentemente inofensivas, pois poderão estar perdendo informações valiosas em um trabalho pericial.

Este artigo propõe-se a mostrar as técnicas de esteganografia, 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 (WAYNER, 2002).

4. Técnicas Esteganográficas

Para que a mensagem esteganográfica seja transmitida é necessário um meio ou objeto de transporte, de modo que se obtenha a segurança desejada. Este pode ser um texto (verificação do número de guias, espaços em branco, letras maiúsculas, etc.), imagem (intensidade dos pixels para esconder a informação, dado que as mais usadas são as de 8 e 24 bits, onde o tamanho da imagem é grande podendo ocultar as informações, sendo que imagens maiores podem exigir compressão para evitar detecção, e as técnicas de inserção de LSB, mascaramento e filtragem), um arquivo de áudio (meio muito importante devido a voz sobre IP(VOIP) ser muito popular, sendo usado nos formatos WAVE,MIDI, AVI e MPEG para esteganografia) ou outro meio qualquer aceitável. Mesmo sem ter um arquivo, pode-se usar a esteganografia, por exemplo, em um protocolo de rede ou meio não eletrônico (ou seja, TCP, UDP, IP, etc., dado que as mensagens são escondidas nos pacotes de dados aparentemente corrompidos que são, por padrão, ignorados pelo receptor e, portanto, também pelo interceptor). Tais técnicas podem ser classificadas nas categorias de domínio espacial e de frequência.

Sabendo-se que uma das formas mais comuns de esteganografia consiste em esconder uma mensagem dentro de uma **imagem**, neste artigo abordaremos as técnicas mais utilizadas aplicadas sobre elas apenas, não focando em outros meios/objetos de transporte. Os tipos de imagens mais usados são: BMP, GIF, JPEG e TIFF. Esses arquivos possuem características que podem ser exploradas, tal como sua resolução, altura e largura. Ao escondermos uma mensagem é necessária a presença de dois arquivos: um contendo a imagem na qual ela será inserida, e outro contendo a mensagem em si. Após a obtenção dos mesmos, opta-se pelo melhor método a ser utilizado na inclusão da mensagem. As técnicas mais triviais são:

• inserção no *bit* menos significativo (LSB – Least Significant Bit): alteração de alguns bits nos pixels que formam a imagem.
• técnicas de filtragem e mascaramento: uso de marcas d´água digitais nas imagens.
• algoritmos e transformações: funções matemáticas em algoritmos de compressão.

4.1 Inserção do *Bit* Menos Significativo (LSB)

Mídias digitais, como fotografias, filmes e música, possuem uma quantidade significativa de ruído (variação aleatória do brilho ou cor) gerada de sua conversão em sinal digital. Esconder a informação que se deseja transmitir nesse ruído é, provavelmente, a técnica esteganográfica mais utilizada (WAYNER, 2002).

A alteração de *bits* de informação de arquivos grandes é a forma mais empregada na esteganografia digital, nela usamos os bits menos significativos para guardar os dados que se deseja camuflar. Ela funciona da seguinte forma: obtemos uma foto, e a cada 100 pixels um *bit* de informação é alterado, mudando levemente a cor dele; em seguida o receptor, ao usar um software específico, abrirá a imagem e extrairá os *bits* modificados que formarão outra mensagem, e que poderá ser um simples texto ou até um vídeo. Isto faz com que a técnica seja uma ótima solução esteganográfica, uma vez que a imagem fica praticamente inalterada, principalmente no que diz respeito à percepção visual do ser humano (WAYNER, 2002). Esta técnica constitui a forma de mascaramento em imagens mais difícil de ser detectada, pois podem inserir dados em pixels não sequenciais, tornando complexa a detecção (POPA, 1998) (PETITCOLAS et al., 1999) .É uma técnica de domínio espacial, difícil de ser notada, mas são muito vulneráveis à manipulação de imagens, principalmente as que envolvem a compressão (KAUR, 2016). Converter uma estego-imagem de um formato que utiliza compressão sem perdas, como o BMP, para outro que utiliza compressão com perdas, como o JPEG, pode destruir a informação escondida.

Principais características da técnica LSB:

● Fácil compressão;
● Fácil implementação;
● Sem limitações quanto ao tipo de imagem;
● Alta capacidade de armazenamento;
● Baixa segurança (facilmente detectável a presença de informações ocultas);
● Baixa robustez (dados perdidos com qualquer alteração na estego-imagem).

A seguir pode-se verificar o método sendo aplicado, onde os *bits* modificados encontram-se na cor preta. Neste exemplo apenas 4 dos 9 *bits* menos significativos foram remodelados. Em média, 50% dos *byte*s são alterados após a aplicação das técnicas LSB.

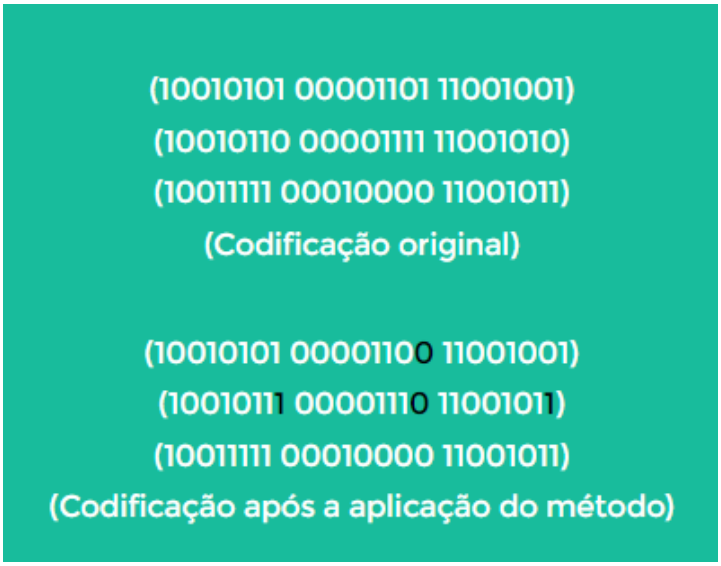

Figura 05 – método para esconder o dado “101101101” em três pixels codificados com 24 bits cada
Fonte: https://www.gta.ufrj.br/ensino/eel878/redes1-2016-1/16_1/esteganografia/#tecnicas

4.2 Filtragem e Mascaramento

As técnicas de filtragem e mascaramento são extremamente semelhantes as do LSB, porém tentam contornar a maior fraqueza delas: sua falta de robustez. Se parece muito com marcas d’água visíveis, pois os pixels camuflados são iluminados ou escurecidos por um dado fator, porém este fator deve ser tal que a modificação seja invisível. Nenhuma informação é gravada neste método, pois é usado para criar uma marca d’água digital que prove a autenticidade de uma imagem.

> São restritas às imagens em tons de cinza (grayscale). Têm a função de esconder a informação através da criação de uma imagem semelhante às marcações de copyright em papel. Isto acontece devido às técnicas de watermarking, que garantem que, mesmo se a imagem for modificada por métodos de compressão, a marcação não será removida. São técnicas mais robustas que a inserção LSB no sentido de gerarem estego-imagens imunes a técnicas de compressão e recorte. Trabalham com modificações nos bits mais significativos das imagens. As imagens de cobertura devem ser em tons de cinza porque estas técnicas não são eficientes em imagens coloridas. Modificações em bits mais significativos de imagens em cores geram alta quantidade de “ruído”, tornando as informações detectáveis (JULIO, 2007).

Principais características da técnica de filtragem e mascaramento:
- Fácil compressão;
- Fácil implementação;
- Restrita apenas às imagens em tons de cinza;
- Alta capacidade de armazenamento;
- Baixa segurança (facilmente detectável a presença de informações ocultas);
- Boa robustez

4.3 Algoritmos e Transformações

De acordo com Trassante (2009), as técnicas até agora descritas são mais rápidas e simples de serem efetuadas, porém todas possuem alguma forte limitação, como o

escopo reduzido das imagens em tons de cinza e a sensibilidade a alterações de brilho ou compressão das técnicas de manipulação do LSB.
Os algoritmos de transformação geralmente trabalham com brilho, saturação e compressão das imagens. Essa técnica consegue tirar proveito de um dos principais problemas da inserção no canal LSB que é a compressão. Para isso são utilizadas: a transformada de Fourier discreta, a transformada de cosseno discreta e a transformada Z (GONZALEZ et al., 2002).
Principais características da técnica de algoritmos e transformações:
● Difícil compressão;
● Difícil implementação;
● Sem limitações quanto ao tipo de imagem;
● Boa capacidade de armazenamento;
● Alta segurança;
● Alta robustez (Os dados são embutidos no domínio de transformação, sendo escondidos em áreas mais robustas, espalhadas através da imagem inteira).

5. Ferramentas Gratuitas: OpenPuff e Quick Stego

A seguir realizaremos uma discussão de como essas ferramentas podem ser utilizadas, ressaltando seus principais particularidades.

5.1 OpenPuff

O OpenPuff é uma ferramenta profissional de esteganografia e marcas d´água, gratuita e portátil, para Microsoft Windows criada por Cosimo Oliboni e ainda mantida como software independente. Esse programa permite ocultar qualquer tipo de arquivo dentro de outros, com uma variedade muito maior de formatos de saída, possibilidade de usar múltiplos arquivos, e principalmente: maior segurança (MOTTA, 2019).Uma característica especial do OpenPuff é a “Esteganografia negável”, que permite que dois conjuntos separados de dados sejam ocultados em um arquivo de transporte. Isso permite que alguém esconda informações confidenciais e também de engodo. Se forçado a divulgar as senhas que protegem os dados ocultos, um usuário pode desistir das senhas falsas, revelando informações não incriminatórias, enquanto as informações confidenciais ainda permanecem ocultas e protegidas por um conjunto separado de senhas secretas. Tal programa também permite inserir uma sequência oculta de até 32 caracteres em um arquivo portador. Este é um tipo de marca d”água digital, a qual pode ser revelada, sem a necessidade de uma senha, usando a função CheckMark no OpenPuff. Essa característica pode ser usada para identificar e rastrear arquivos postados em formulários públicos ou compartilhados com grupos selecionados de pessoas.

A marca d'água é a ação de assinar um arquivo com uma identificação ou marca de copyright. O OpenPuff faz isso de uma forma esteganográfica invisível, aplicada a qualquer portador compatível. A marca oculta, não sendo protegida por senha, é acessível a todos (usando o programa).

A última versão suporta vários formatos tais como:

- Imagens Bmp , Jpg , Png , Tga, Gif;
- Áudios Aiff , Mp3 , Wav;

- Vídeos 3gp , Mp4 , Mpeg I , Mpeg II , Vob.

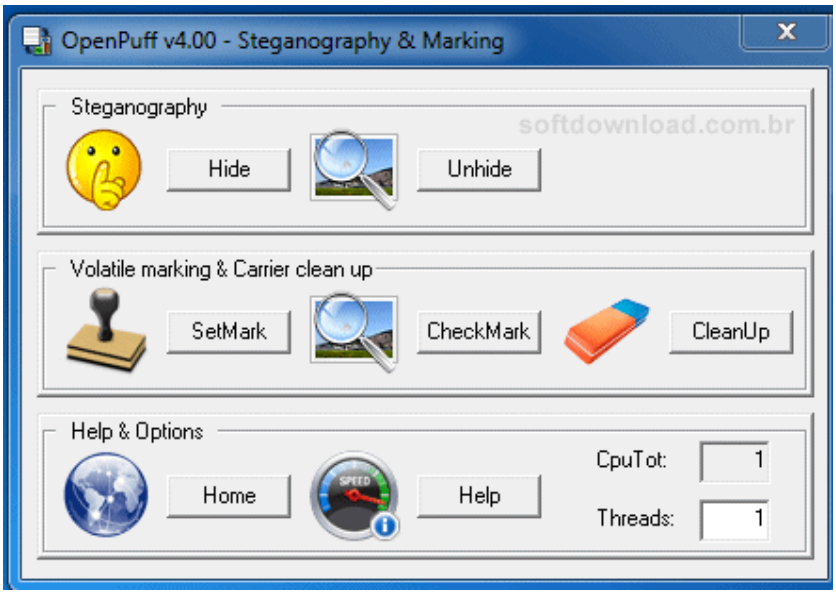

Figura 06 – Interface inicial da ferramenta OpenPuff
Fonte: https://www.softdownload.com.br/esconda-arquivos-fotos-musicas-videos-openpuff.html

Ao abrir o programa, nota-se uma interface bem simples dividida em três seções: Steganography (Esteganografia, onde pode-se esconder e revelar dados ocultos), Volatile marking & Carrier Clean Up (Marca d´água e limpeza do arquivo portador, local em que se cria marcas d'água para comprovar a autoria sobre algum conteúdo), e Help & Options (Ajuda e Opções). Se o objetivo for esconder arquivos confidenciais dentro de arquivos de imagem, música ou vídeo basta clicar no botão "Hide" (conforme figura 06).
Para testá-lo, o primeiro passo consiste em criar uma mensagem de teste, a qual pode ser feita, por exemplo, no bloco de notas. Abrimos então o editor de textos, e digitamos um texto qualquer. Logo em seguida, salvamos esse arquivo e saimos do bloco de notas. É necessário escolher uma imagem para ser a portadora da mensagem. Sendo assim, abrimos o OpenPuff e clicamos no botão "Hide" (na seção *Steganography*), e então realizaremos a inserção do texto arquivo criado anteriormente para teste na imagem escolhida (uma nova interface aparece-figura 07).

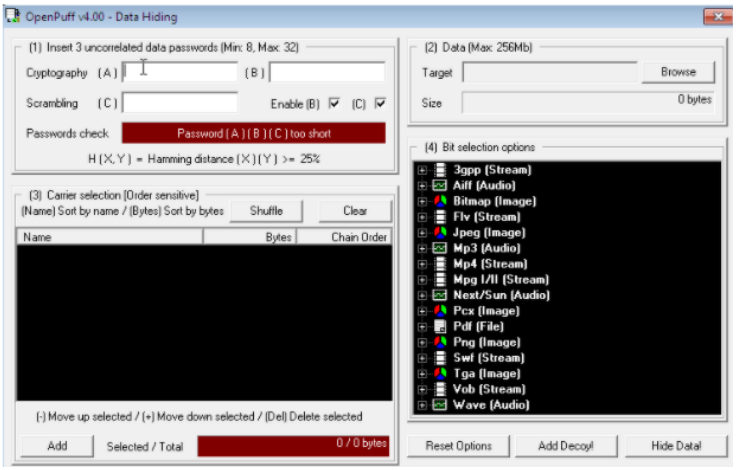

Figura 07 – Interface ao clicar em "Hide" da ferramenta OpenPuff
Fonte: https://www.softdownload.com.br/esconda-arquivos-fotos-musicas-videos-openpuff.html

A partir desse ponto, é preciso definir três senhas (podendo usar apenas uma, visto que ao desmarcar o botão “enable”, desabilitam-se as senhas adicionais.). Nos campos (A), (B) e (C) colocamos as senhas desejadas, guardando-as para posterior extração. Em seguida, escolhe-se o arquivo original, clicando em “browse”, observando quantos bytes ele ocupa, tendo um máximo de 256Mb. Após tal seleção, vamos inserir os arquivos falsos, clicando no botão “add” da seção 3, com intuito de escolher uma imagem em formato e tamanhos adequados. Os arquivos devem ser adicionados até a caixa inferior ficar verde (figura 8). Note que não há problema em extrapolar a quantidade necessária.

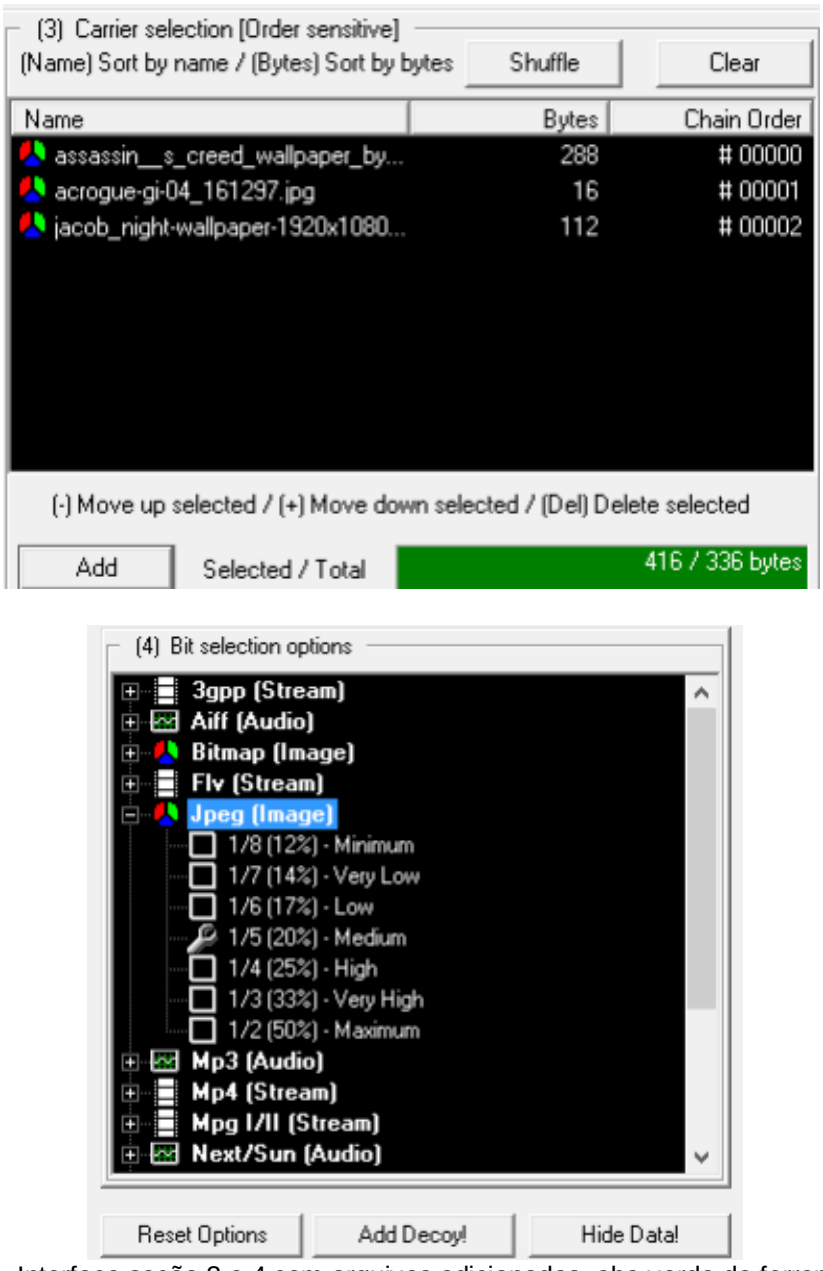

Figura 08 e 09 – Interface seção 3 e 4 com arquivos adicionados, aba verde da ferramenta OpenPuff e nível de segurança a ser selecionado
Fonte: https://embeddedsw.net/doc/Openpuff_lecture_Esteganografia_utilizando_o_openPuff.pdf

A próxima etapa consiste em definir o nível de segurança. Na caixa preta, temos os tipos de arquivos e seus respectivos níveis de seleção. Na prática, não há muita

diferença entre eles. Vale observar que, quanto mais alta for a porcentagem, maior espaço livre estará disponível nos arquivos, e portanto menor a segurança. Após isso, clicamos no botão “Hide Data!” no canto inferior direito para realizar a operação esteganográfica, e escolher um local para salvar a imagem contendo sua mensagem oculta. Em alguns instantes, receberemos a mensagem “1/1 carrier processed”, indicando que os dados foram processados com êxito. Clique em “OK” , verificando o relatório e então se fecha a caixa de diálogo, clicando no botão “Done”. Com isso a imagem contendo sua mensagem secreta será salva no computador. Ao abri-la perceberemos que não há rastros visíveis da mensagem ocultada na imagem, mas ela estará presente.
Através do OpenPuff também podemos recuperar os arquivos escondidos, através do botão “Unride” na interface inicial do programa, utilizando as senhas digitadas no início do processo, de modo a realizar o processo inverso de decodificação.

5.2 Quick Stego

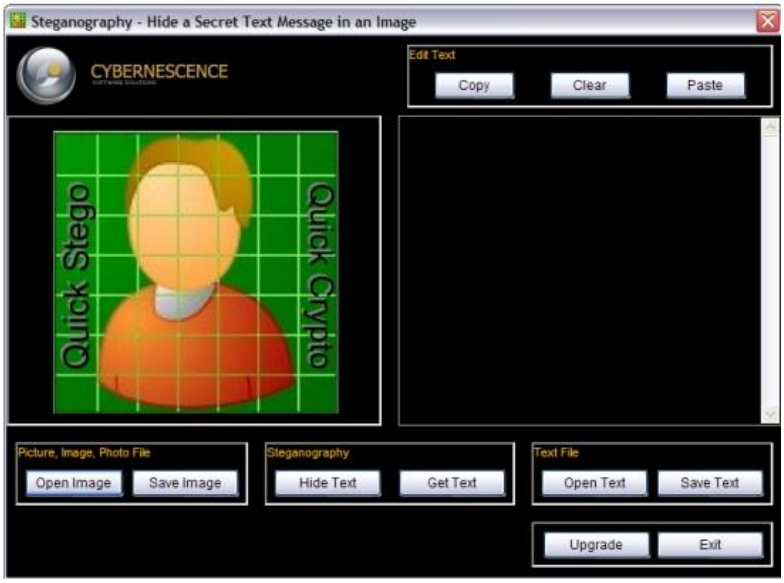

Figura 10 – Interface inicial Quick Stego
Fonte: https://www.cyberpratibha.com/blog/steganography-tools-for-windows-10/

O Quick Stego é um software gratuito, prático e fácil de usar que permite ocultar texto dentro de imagens (não trabalha com arquivos de áudio ou vídeo) somente do tipo JPEG (bem restrito), onde apenas outros usuários de Quick Stego possam recuperar e ler as mensagens secretas que estão ocultas (GHETTI, 2012). Depois que o texto estiver oculto em uma imagem, mesmo ela já salva ainda é uma “imagem”, e será carregada como qualquer outra, aparecendo visualmente como antes (praticamente idêntica aos olhos humanos). A imagem pode ser salva, enviada por e-mail ou pela web, normalmente, a única diferença é que portará um texto oculto.
Não é um método seguro, uma vez que não envolve nenhuma senha e que qualquer pessoa de posse do programa poderá facilmente ter acesso ao texto escondido como antes. Ele trabalha alterando imperceptivelmente os pixels (elementos individuais da imagem) da ilustração, codificando o conteúdo secreto e adicionando pequenas variações de cor a ela.

Após ser instalado, sua operação é bem intuitiva. Basta clicarmos em “Open Image” e selecionarmos algum arquivo do tipo JPEG (o qual guardará o texto oculto). Na caixa da direita, digite o texto a ser ocultado. Deve ficar da seguinte forma:

Figura 11 – Interface do Quick Stego ao digitar o texto que será ocultado
Fonte: https://www.docdroid.net/01pqh5P/esteganografia-utilizando-o-quickstego-pdf#page=2

Em sequência clique em “Hide Text” para ocultar. Por fim, para exportar a imagem com o texto oculto, clique em Save Image (selecione o diretório e salve).
Para recuperar os dados, é necessário reiniciar o Quick Stego, clicar em Open Image, selecionar a imagem desejada, então o texto irá automaticamente aparecer na caixa da direita, de uma forma bem simples e “insegura”.

6. Aplicações da Esteganografia

Além das aplicações militares ou de inteligência, as técnicas esteganográficas permitem diversos usos, mais ou menos óbvios, e que estão evoluindo com o decorrer dos anos, de acordo com a criatividade humana. De um lado, elementos que discordam dos regimes autoritários, onde a censura ou a perseguição política é praticada podem usar a esteganografia para estabelecer comunicações secretas, evitando assim a investigação por parte dos órgãos responsáveis. De outra forma, para fins menos honrosos, a esteganografia também está relacionada ao uso criminoso ou mesmo terrorista. Comunicar-se quando estamos sob vigilância é um desafio muito difícil. As autoridades dispõem de recursos e ferramentas jurídicas para intervir nas comunicações, seja por telefone, correio ou telemática. Quando um grupo de delinquentes sabe que estão sendo observados, a esteganografia é apresentada como uma alternativa altamente desejável para proteger suas comunicações mais sensíveis. O caso mais famoso relatado pelas mídias (jornal folha de São Paulo, de 10 de março de 2008) foi o do traficante colombiano Juan Carlos Ramirez Abadia, o qual intrigou os delegados da Polícia Federal, pela quantidade de imagens da gatinha *Hello Kitty* que ele guardava em seus computadores. Eram em torno de 200 imagens, quase todas enviadas por e-mail, onde descobriram que elas não eram inócuas (figura 12), uma vez que continham mensagens de voz (áudio) e texto embutida (local em que emitiam ordens para movimentação de cocaína entre países, e também desaparecer com pessoas na Colômbia).

Figura 12 – Ilustração de como Juan Carlos Ramirez Abadia traficava dando ordens através de mensagens ocultadas em imagens
Fonte: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/11338/1/CP_COENC_2015_2_08.pdf

Dentre os bons exemplos do uso da arte de esconder mensagens, podemos citar as marcas d'água em imagens, por razões tais como a proteção dos direitos autorais, evitando falsificações. Marcas d'água digitais (também conhecido como impressões digitais) são semelhantes às da esteganografia que estão encobertas em arquivos, que parecem ser parte do arquivo original e, portanto não são facilmente detectáveis por uma pessoa normal. Além disso, a esteganografia pode ser usada para adicionar recados em imagens online (como post- its anexos aos arquivos). Empresas fabricantes de impressoras, tal como HP e a Xerox também a utilizam, adicionando minúsculos pontos amarelos em cada página, os quais são pouco visíveis e contêm codificados nele os números de série, data e hora da impressão.

A esteganografia de áudio também é empregada, uma vez que o ouvido humano, devido à sua anatomia, pode captar as vibrações de uma membrana entre a faixa de frequência de 20 Hz e 20 kHz. Desta forma, inferimos que um dos modelos de esteganografar um conteúdo em um áudio seria inserir sons em frequências baixas (infrassons) e/ou altas (ultrassons). Um caso interessante, que já fora utilizado, é o do aparelho chamado “The Mosquito” (LYALL, 2005), que é um dispositivo eletrônico usado em alguns países para impedir que os jovens se reúnam, principalmente fora

de lojas e mercados, e espera reduzir o comportamento antissocial, como vadiagem e vandalismo (controle social). Funciona com base no princípio simples de que o alcance da audição para os humanos se deteriora com a idade. Assim, os ultrassons que o “The Mosquito” produz só podem ser ouvidos pelos jovens. Para causar um leve desconforto, essas ondas de áudio também podem ser transmitidas em níveis mais altos de pressão sonora. Outra abordagem da técnica de “esconder” áudio fora relatada no início de 2018, onde a Amazon anunciou que havia tomado medidas para garantir que os dispositivos do Amazon Echo na casa dos espectadores não fossem ativados inadvertidamente durante o anúncio do “Super Bowl” para dispositivos Alexa. Especula-se que a Amazon fez uso inteligente da faixa de frequência acústica para conseguir isso. Com isso observa-se que o mesmo conceito pode ser estendido a ondas de áudio inaudíveis de fontes aparentemente inócuas, como a televisão, que podem interagir com dispositivos domésticos inteligentes sem o conhecimento dos proprietários do dispositivo.

7. Conclusão

Sabendo-se que a segurança é uma questão crucial quando da transferência de informações através do uso da internet, ocultá-las com métodos de esteganografia ameniza as chances de a mensagem ser captada, dado que qualquer pessoa não autorizada pode hackear os dados e torná-los inúteis ou obter informações não destinadas a ele.Por si só, a esteganografia não é uma boa solução para o sigilo, mas seus recursos devem estar aliados aos da criptografia, sendo assim teremos uma segurança mais forte. Observamos que as técnicas existentes para esteganografia são frágeis de certo modo, principalmente no quesito integridade, já que uma simples compressão pode destruir a informação oculta, mas também ditas fortes quanto à segurança da informação, uma vez que a complexidade e o alto custo computacional tornaria inviável o desenvolvimento de algoritmos de esteganálise (a arte de detectar informação escondida em um objeto, ou seja, analisar um arquivo, procurar por informação oculta e destruí-la se este for o interesse) que conseguisse extrair a mensagem oculta, e não somente, identificar sua existência.

Após a análise de dois programas gratuitos de esteganografia, observamos que a capacidade do OpenPuff em ocultar dados de vários tipos diferentes de formatos, dividindo-os em vários arquivos e de fornecer ocultação de dados falsos na ajuda e proteção contra coerção (ou seja, forçando alguém a divulgar senhas usadas para proteger informações ocultas) nos leva a crer que o mesmo é uma boa ferramenta gratuita do ramo disponível atualmente. O Quick Stego apesar de ser mais simples no tópico utilização, é muito restrito, visto que só trabalha com imagens do tipo JPEG, e ainda não apresenta muita segurança, justamente pelo fato de não requer nenhum tipo de senha, e qualquer pessoa de posse desse programa pode ter acesso ao texto escondido.

Infelizmente a esteganografia pode funcionar com uma ferramenta de grande valor para objetivos ilícitos, justamente pela sua característica de esconder a existência de uma informação, tal qual relatado no caso do traficante Juan Carlos Ramirez. O progresso da tecnologia nos levará ao uso cada vez mais frequente dessa ideia, sejam na utilização de marcas d’água, ferramentas de controle social (“The Mosquito”), impressoras modernas, ou no que a e criatividade humana fora capaz de concretizar.

8. Referências Bibliográficas

AHSAN, Kamram; KUNDUR, Deepa. **Practical data hiding in TCP/IP**. Toronto: 2002.

ATTABY, Abdelhamid Awad; AHMED, Mona F.M.Mursi; ALSAMMAK, Abdelwahab. **Data hiding inside JPEG images with high resistance to steganalysis using a novel technique DCT-M3.** Cairo: 2017.

GHETTI, Hudson. **Quick Stego: ocultando textos em arquivos de imagem.** Clube do Hardware: 2012.

GIL, Fernando O.; MALANDRIN, L. J. A. A.; MORIGAKI, R. H.; BARRETO, P. S. L. M. **SEA- Sistema Esteganográfico de Arquivos**. Gramado: 2008.

GONZALEZ, Rafael C.; WOODS, Richard E. **Digital Image Processing**. Boston: 2002.

JOHNSON, Neil F.; JAJODIA, Sushil. **Exploring steganography: Seeing the Unseen**. Fairfax: 1998.

JULIO, Eduardo P.; BRAZIL, Wagner Gaspar; ALBURQUERQUE, Célio V. Neves. **Esteganografia e suas Aplicações**. Niterói: 2007.

KAUR, Harpreet; RANI, Jyoti. **A Survey on different techniques of steganography.** Punjab: 2016.

KUMAR, Arvind; POOJA, Km.**Steganography- A Data Hiding Technique**. Meerut: 2010.

LYALL, Sarah. **This Mosquito makes unruly teenagers buzz off**. The New York Times: 2005.

MARTINS, Elaine. **O que é esteganografia**. Tecmundo (revista digital): 2010.

MOTTA, Sérgio. **OpenPuff- Esconda arquivos dentro de outros arquivos**. Softdowload: 2019.

OLIVEIRA, Fábio Borges**. Análise da segurança de criptografia e esteganografia em sequências de imagens.** Petrópolis: 2007.

PETITCOLAS, F. A. P.; ANDERSON, R. J.; KUHN, M. G. **Information hiding — A survey**. Cambridge: 1999.

POPA, R. **An analysis of steganography techniques**.Timisoara: 1998.

SINGH, S. **O livro dos códigos.** Rio de Janeiro: 2001.

TRASSANTE, Bruno Nunes. **Esteganografia em imagens digitais**. Porto Alegre: 2009.

WAYNER, P. **Disappearing Cryptography – Information Hiding: Steganography and Watermarking**. Morgan Kaufmann Publisher, 2ª Edição:2002.