Técnica anti-forense: esteganografia em imagens

Leonardo G. Carvalho[1], **Matheus S. Redecker**[1]

[1]Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS
Porto Alegre, RS - Brasil

{leonardo.gubert}{matheus.redecker}@acad.pucrs.br

Abstract. *The steganography in images is the art of hiding information inside images. The steganography in images can be used to exchange confidential messages, or hide information from others. This work shows a description of the techniques used in the creation and detection of steganography.*

Resumo. *A esteganografia em imagens é a arte de ocultar informações dentro de imagens. A esteganografia em imagens pode ser usada para troca de mensagens sigilosas, ou ainda esconder informações de terceiros. Este trabalho mostra uma descrição das técnicas usadas na criação e na detecção da esteganografia.*

1. Introdução

No passado, as pessoas usavam tintas invisíveis ou tatuagens escondidas para trocar informações sigilosas. Hoje em dia com os computadores e a internet, existem maneiras melhores de conseguir isso. Uma dessas maneiras é a esteganografia [Provos and Honeyman 2003]. Esteganografia é uma palavra que vem do grego e significa "escrita oculta" e consiste na arte ou ciência de se escrever mensagens ocultas de tal forma que ninguém saiba que essa mensagem exista. É diferente da criptografia em que a mensagem tem sua existência conhecida, mas não se sabe como decifrá-la [Braga]. A esteganografia vem se destacando muito no decorrer dos tempos e está ganhando popularidade com a Internet, para comunicação em segredo e para atender a atual demanda da indústria por marca d'água digital e impressão digital para áudio e vídeo [PETRI 2004]. Arquivos como os de imagem e som possuem áreas de dados que não são usadas ou são pouco significativas. A esteganografia tira proveito disso, trocando essas áreas por outra informação [Kunz].

A esteganografia em imagens é obtida sabendo explorar as limitações do sistema visual humano (SVH). Ela evoluiu muito com o desenvolvimento de computadores gráficos rápidos e poderosos, além de que os softwares esteganográficos estão disponíveis para usuários diários da Internet [PETRI 2004]. Uma imagem colorida é normalmente formada por um conjunto de pixels, nos quais suas cores são armazenadas em 3 ou 4 canais, sendo eles RGB (vermelho, verde e azul) ou RGBA (vermelho, verde, azul e alpha) respectivamente, cada canal contendo 8 bits (1 byte). Alterando-se o bit menos significativo de qualquer um dos canais não ocasiona-se mudanças perceptíveis na imagem. Desta forma, podemos trocar estes bits por uma outra sequencia (arquivo ou texto) usando apenas o bit menos significativo de um ou todos canais de cada pixel [Kunz , PETRI 2004].

2. Técnicas

As técnicas mais comuns para fazer estas alterações envolvem o uso de *least-significant bit* (LSB), *filtering*, *masking* e *transformations*. Estas técnicas podem ser usadas com variados graus de sucesso em diferentes tipos de arquivos de imagem [Hariri et al. 2011]. A distribuição das técnicas na imagem pode ser feita de forma sequencial, ou seja, do inicio da imagem para o final, linha por linha, de trás para frente, coluna por coluna.

2.1. Least Significant Bits

As fotografias possuem uma quantidade significativa de ruído e esconder a informação que se deseja transmitir nesse ruído é, provavelmente, a técnica esteganográfica mais utilizada. Uma imagem pode utilizar diversas formas de armazenar a informação de cada pixel dependendo do formato com que foram exportadas. Uma imagem BMP por exemplo pode utilizar o formato RGB24 (24 bits/pixel, 8 bits para cada canal) ou até mesmo RGBA32 (32 bits/pixel, 8 bits para cada canal). Além do RGB, também existem imagens que trabalham com apenas 1 canal (*grayscale*) ou com o formato CMYK (ciano, magenta, amarelo e preto, cada canal com 8 bits), normalmente utilizado para imagens que serão impressas. A técnica dos *Least Significant Bits* pode ser considerada a técnica mais simples, pois apenas utiliza o bit menos significativo de cada pixel da imagem, podendo usar o ultimo bit de cada canal para esconder as informações [Hariri et al. 2011].

As mudanças que ocorrem na imagem com essa técnica são quase imperceptíveis pelo fato de que a alteração da tonalidade da cor é pequena demais para que o olho humano detecte a diferença. Além disso, em média apenas metade dos bits são alterados, o que deixa algumas cores totalmente inalteradas [Hariri et al. 2011].

Para uma melhor eficacia é recomendado usar essa técnica em imagens com formatos em que não sejam comprimidas, pois os algoritmos de comprimir imagens como o JPEG se aproveitam dos ruídos para eliminar algumas informações [Hariri et al. 2011, Duarte].

A figura 1 mostra duas imagens, a original a esquerda e a com esteganografia a direita, e nela pode ser visto que não há uma difereça perceptível.

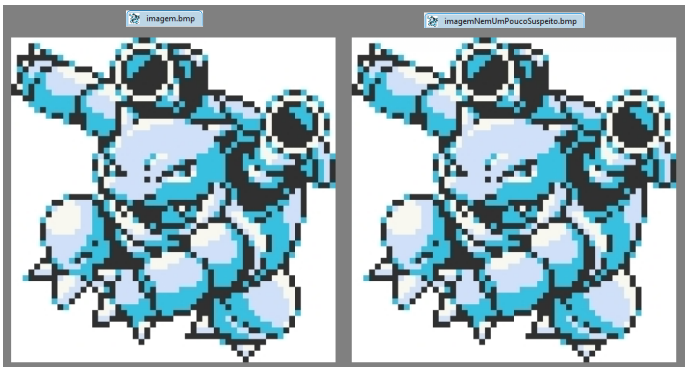

Figura 1. Informação escondida com esteganografia dentro da imagem

2.2. Masking and filtering

As técnicas de *masking* e *filtering* geralmente são utilizadas em imagens em tons de cinza (*grayscale*). Estes métodos são semelhantes a marcas dágua, pois criam marcações na

imagem alterando a luminância de algumas partes. As alterações são feitas sem que o olho humano consiga notar a diferença. *Masking* utiliza aspectos visíveis da imagem, por esse motivo ela é mais robusta que a LSB e como a parte modificada não está nos ruídos, este tipo de técnica pode ser melhor empregado nas imagens de formato comprimidos, como JPEG [Hariri et al. 2011]. A Imagem 2[Wu and Tsai 2003] mostra um exemplo dessa conversão.

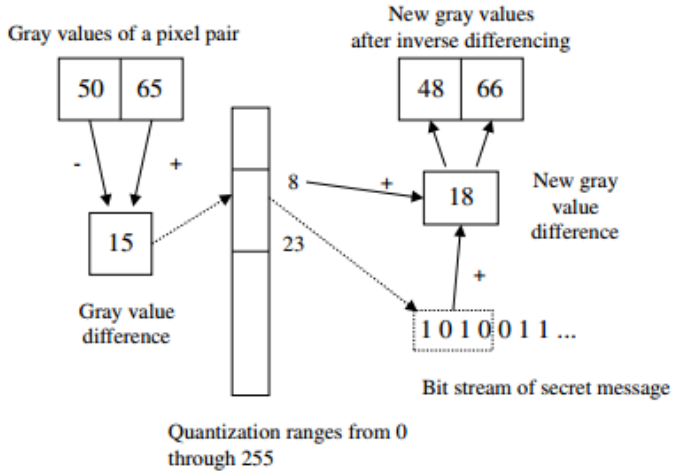

Figura 2. Masking and filtering

2.3. Transformations

Uma forma mais complexa de esconder informação dentro das imagens vem de transformações discretas de cosseno. *Discrete cosine transformations* (DCT) é usada para transformar blocos de 8x8 de uma imagem em 64 coeficientes de DCT. Cada coeficiente DCT F(u,v) de um bloco 8x8 de uma imagem com pixels f(x,y) é dado por [Hariri et al. 2011]:

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * \cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right], \quad C(x) = \begin{cases} \frac{1}{\sqrt{2}} & x = 0 \\ 1 & else. \end{cases}$$

3. Esteganálise

As técnicas de esteganografia não são totalmente perfeitas. Nenhuma delas garante que as informações escondidas não serão detectadas ou interceptadas por terceiros. A esteganálise busca utilizar métodos para detectar a esteganografia. A esteganálise pode buscar apenas verificar a existência de informações escondidas, sem estar preocupada em saber o conteúdo da mensagem, ou ainda recuperar os dados escondidos. Recuperar os dados adiciona um nível maior de complexidade ao processo de esteganálise, pois é necessário conhecer previamente o algoritmo de esteganografia utilizado. Além disso, a mensagem pode estar criptografada. As técnicas de esteganálise possuem algumas limitações. Muitas delas, por exemplo, foram feitas especialmente para determinados algoritmos e softwares de esteganografia que já são previamente conhecidos, e com isso

se o algoritmo ou o software for diferente essa analise tem grande probabilidade de falhar [Duarte].

Após a descoberta de que há informação na imagem, pode-se ter diferentes objetivos em relação aos arquivos que ela contém. Os principais objetivos são:

- Destruir a informação - Com o intuito de destruir a informação que está contida na imagem, pode-se destruir a imagem, ou para não danificar a imagem, pode-se adicionar novas informações com a ambição de colocar dados em cima dos dados anteriores, ou ainda, alterar o formato da imagem ou comprimi-la pode também destruir os dados que estão presentes.
- Obter a informação - Com o intuito de obter a informação que está contida na imagem, pode-se tentar utilizar algoritmos conhecidos para remontar a imagem. O problema vem do fato de que se a informação está criptografada, mesmo após descobrir o arquivo, tem o esforço para abrir-lo se for possível.

4. Conclusão

A partir da pesquisa desse trabalho podemos concluir que a esteganografia sempre altera a imagem original, e com isso é possível detectar a presença de esteganografia nas imagens. A diferença da imagem esteganografada para a original é tão pequena que não é perceptível ao olho humano.

A esteganografia se torna uma aplicação interessante para troca de mensagens de forma sigilosa, pois quem abre a imagem de imediato não detecta nada de diferente. Para descobrir a informação escondida não é uma tarefa trivial, pelo fato das diversas técnicas existentes, e para extrair as informações é preciso saber qual a técnica foi usada para esconder a informação. Se além da esteganografia, a informação escondida estiver criptografada, é praticamente impossível descobrir a informação, o máximo que um interceptador consegue fazer é destruir a informação.

Essa técnica é de fácil acesso e uma pesquisa rápida na internet já é possível conseguir um software pronto para usar. Um exemplo de software é o *Hide & Reveal*[1] e o software desenvolvido por nós para a demonstração do trabalho OEscondedor[2].

Referências

Braga, N. C. Esteganografia (a arte de escrever mensagens ocultas) *url:* http://www.newtoncbraga.com.br/index.php/eletronica/52-artigos-diversos/7049-esteganografia-a-arte-de-escrever-mensagens-ocultas-art1175.

Duarte, O. C. M. B. Esteganografia *url:* http://www.gta.ufrj.br/grad/09_1/versao-final/stegano/index.html.

Hariri, M., Karimi, R., and Nosrati, M. (2011). An introduction to steganography methods. *World Applied Programming*, 1(3):191–195.

Kunz, L. Esteganografia em imagens usando codificação de huffman *url:* http://www.inf.ufrgs.br/ lkunz/cpd/.

[1] http://hidereveal.ncottin.net/

[2] https://github.com/Redecker/OEscondedor

PETRI, M. (2004). Esteganografia. *Instituto Superior Tupy, SC, 62p*.

Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to steganography. *Security & Privacy, IEEE*, 1(3):32–44.

Wu, D.-C. and Tsai, W.-H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 24(9):1613–1626.