Esteganografia

Steganography

Eduardo Azevedo[a]*; João Gabriel Faveri[a]; Sergio Eduardo Nunes[a]

[a]Faculdade Anhanguera de Limeira, SP, Brasil

*E-mail: eduardo971@gmail.com

Resumo

O assunto segurança é uma preocupação constante entre os profissionais de tecnologia da informação, usuários comuns e empresas de diversos seguimentos. Este artigo dispõe a respeito do conceito e funcionamento da tecnologia conhecida como Esteganografia, que pode ser definida como a arte da ciência da comunicação, na qual o objetivo é esconder dentro de outro arquivo aparentemente inofensivo alguma mensagem. Dessa forma, se a mensagem for interceptada, não será possível detectá-la.

Palavras-chave: Segurança da Informação. Esteganografia. Criptografia.

Abstract

The issue security is a constant concern among information technology professionals, common users and companies from several segments. This article provides with the concept and operation of the technology known as steganography. It can be defined as the art of Communication Science, where the goal is to hide some message inside another apparently harmless file. Thus, if the message is intercepted, you cannot detect it. To prove the efficiency of steganography technique, testing for security analysis on e-mail providers was done.

Keywords: *Information Security. Steganography. Cryptography.*

1 Introdução

Com a crescente dependência de pessoas e organizações perante as tecnologias, cuidar do bem mais precioso é vital para garantir o sucesso de uma organização ou a correta utilização de informações pessoais do indivíduo. É por isso que a cada dia mais, pessoas e organizações se preocupam com a segurança da informação.

Aspectos que sempre serão fundamentais em qualquer situação são: garantia da disponibilidade de recursos e informações, integridade da informação e confidencialidade da mesma (HOLANDA, 2005).

Todos os recursos da informação, tais como banco de dados, servidores, estações de trabalho, aplicações e afins devem estar devidamente cadastrados e protegidos a fim de se garantir a qualidade de serviço.

A integridade dos dados visa garantir que a informação será disponibilizada sempre na sua última versão. As ferramentas devem controlar as versões, alterações e assim monitorar, garantindo a veracidade da informação para a organização.

O termo mais importante neste trabalho é a confidencialidade da informação. Isso implica que a mesma somente deverá ser disponibilizada a quem de direito, minimizando ataques, vazamento de informações, acesso a informações desnecessárias, assegurando, assim, que as informações estratégicas da empresa estarão a salvo.

> A segurança da informação é adotar controles físicos, tecnológicos e humanos personalizados, que viabilizem a redução e administração dos riscos, levando a empresa a atingir o nível de segurança adequado ao seu negócio (SÊMOLA, 2003, p.35).

Com isso posto, a escrita secreta visa esconder um texto, a fim de que outra pessoa não saiba de sua existência (CARVALHO, 2008). Esta técnica pode fornecer uma poderosa ferramenta para a transmissão segura das informações.

Basicamente a escrita secreta se divide em duas partes: a criptografia e a esteganografia. A diferença entre elas está no fundamento, pois a criptografia deixa evidente que existe um dado e que o mesmo está cifrado. Por sua vez a esteganografia visa ocultar essa informação, e a mensagem é embutida em outro tipo de mídia, fazendo-se pensar que não há nada oculto (CARVALHO, 2008).

Este artigo demonstra o processo de ocultar mensagens em arquivos de imagem e, posteriormente, como fazer o processo inverso para revelar a mensagem oculta. Para isso foi utilizado o sistema operacional Linux via *Shell*, sendo feito o processo pelo próprio *kernel* do sistema operacional.

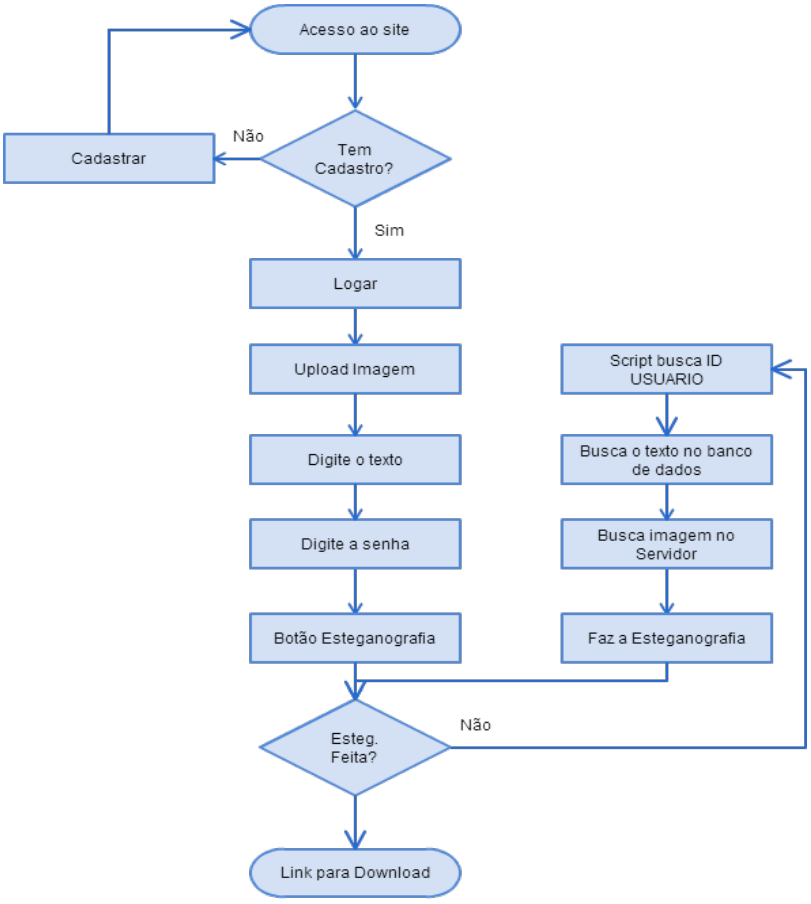
Após as mensagens esteganografadas foi proposto um teste nos provedores de e-mail mais utilizados, a fim de se provar a eficácia da técnica de esteganografia em "driblar" as políticas de segurança com mensagens ocultas.

2 Material e Métodos

Para realizar a esteganografia e a esteganografia reversa, foi desenvolvido um *site*. Esta aplicação permite

o carregamento da imagem e da mensagem de forma simplificada, a fim de facilitar os processos. O fluxograma da Figura 1 descreve os passos a serem realizados pela aplicação.

Figura 1: Fluxograma da esteganografia



Fonte: O autor.

A primeira parte do processo é carregar a imagem. Para assegurar seu funcionamento, a imagem foi limitada a três *megabytes*, para não sobrecarregar o servidor e o funcionamento do Steghide.

A segunda etapa consiste em embutir a mensagem na imagem carregada. Esta mensagem foi limitada em 225 caracteres, para não ocorrer distorções na imagem pelo fato do Steghide utilizar os *pixels* para esconder a mensagem.

Após a imagem selecionada e a mensagem definida o processo de esteganografia se inicia. Quando a mensagem estiver embutida na imagem, o *site* fornece a opção de fazer *download* da imagem esteganografada.

Na esteganografia reversa (processo para retirar a mensagem no interior da imagem), a imagem com o texto embutido é carregada; assim que o processo termina é possível fazer *download* do arquivo de texto.

Para o desenvolvimento da aplicação, foram utilizadas as ferramentas descritas a seguir:

- ✓ Sistema Operacional: Linux Mint, que possui interface de fácil usabilidade. A distribuição Linux garante a segurança, pois o processo de esteganografia é realizado inteiramente no Shell.
- ✓ GIT: é um sistema de gerenciamento de código fonte e controlador de versões de código aberto, independente de *internet* para sua utilização (CHACON, 2009).
- ✓ *Bitbucket*: é um *site* destinado a salvar repositórios com os códigos-fontes na nuvem. Os projetos só podem ser acessados pelo administrador. Possui ainda a opção de visualizar o código-fonte antigo, controlar as versões e ter um histórico de todas as etapas do desenvolvimento.
- ✓ *Brackets*: editor *Open-Source* (livre de licença) voltado para a edição de códigos HTML (*Hyper Text Markup Language)*, JavaScript e CSS (*Cascading Style Sheets*). Concorrente direto do mais famoso editor de código (Sublime), permitiu utilizar as ferramentas como o *plugin* de indentação automática que garantiu uma melhor visualização do código.
- ✓ *Bootstrap*: possibilita que o desenvolvimento *front-end* do *site* seja responsivo na *web*, permitindo assim que a aplicação possa ser utilizada em qualquer dispositivo, sem alteração do seu *layout*.
- ✓ L.A.M.P: para comunicação do *site* com o servidor foi

utilizado o L.A.M.P. (Linux + apache + MySql + Php, Pear e Python), no qual o Linux é o sistema operacional, o Apache é o servidor *Web*, o MySql é o *software* de banco de dados e o PHP é a linguagem de programação.

2.1 Testes e análise experimental

A fim de se medir a eficácia da técnica, os parâmetros observados foram: formato da figura; qualidade da figura; tamanho da figura (cm e pixels); cor da figura e tamanho do arquivo.

3 Resultados e Discussão

O termo Esteganografia é derivado de duas palravas do grego, "*steganos*" - coberto e "*graphein*" - escrita, ou seja, "escrita oculta" (PETITCOLAS; ANDERSON; KHUN, 1999). Essa poderosa tecnologia pode auxiliar na proteção e privacidade. A técnica de funcionamento pode ser exemplificada como: uma imagem de 1024 por 768 *pixels* totaliza um arquivo de 786,432 *pixels*. Como cada *pixel* tem quatro *bytes*, pode-se esconder cerca de 390 *kbytes* de informação nessa imagem, isto é, mais ou menos sete linhas de um arquivo de bloco de notas (ROCHA, 2003). Essa técnica visa à alteração do *bit* menos significativo de cada *byte* de cada *pixel,* para ocultar as partes da mensagem. Não alterando assim as características do arquivo, somente o seu tamanho.

Em esteganografia, existem duas opções de compressão de arquivos ou dois tipos de algoritmos usados para tal, chamados de *Lossy* e *Lossless*. Na opção *Lossy* ocorre perda de dados, ou seja, reduz-se a quantidade de espaço que um arquivo consome. Esse tipo de algoritmo pode produzir um arquivo remontado diferente do arquivo original, sem compressão.

Já a compressão *Lossless*, que é o objeto de estudo e experimentos utilizados neste artigo, consiste em reduzir o espaço de armazenamento exigido para informação digital. O algoritmo de compressão *Lossless* trabalha sem perda de dados, ou seja, se um arquivo compactado for descompactado, ele volta com o mesmo formato original.

Outra parte desse tipo de compressão usada na esteganografia em imagens é a que o algoritmo trabalha com o *Least Significant Bit* - LSB. A partir da reorganização dos dados na matriz da imagem, são inseridos dados embutidos, não alterando o formato original da imagem. Isso é muito importante para ficheiros executáveis e outros que incluem um código- fonte (CARVALHO, 2008).

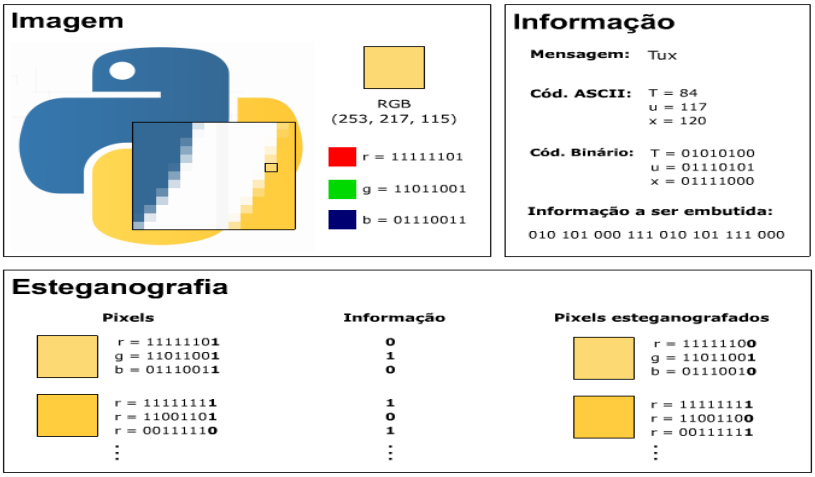
Steghide é um programa de esteganografia capaz de esconder dados em vários tipos de arquivos de áudio e de imagem. As frequências de som e de cor, respectivamente, não são alteradas tornando o arquivo resistente contra testes estatísticos de primeira ordem (DEMACDOLINCOLN, 2013).

O algoritmo de criptografia padrão é o *Rijndael* com uma chave de 128 *bits* de comprimento, no qual os "dados secretos" são compactados e criptografados. Em seguida, uma sequência de posições de *pixels* no arquivo que servirá de "esconderijo" é criada com base em um gerador de números aleatórios inicializado com a senha (os "dados secretos" serão incorporados nos *pixels* destas posições). Posteriormente, um algoritmo de correspondência grafo-teórico encontra pares de posições tais que troquem seus valores. Isso tem o efeito de incorporar a parte correspondente dos "dados secretos". Se o algoritmo não consegue encontrar mais pares, todas as trocas são efetivamente realizadas (HETZL, 2002).

O *steghide* usa o método LSB, ou seja, substitui o *bit* menos significativo dos *pixels* que formam as cores das imagens do tipo *Bitmap* – BMP – em imagens deste tipo, as cores nos *pixels* são formados da seguinte maneira: imagens como "*jpg*" possuem blocos sucessivos de 8 *bits*, o que permite que se tenha 2^{24} cores diferentes (uns 16 milhões de tonalidades), com 24 *bits* por *pixel* (DEMACDOLINCOLN, 2013).

O método de esteganografia LSB vai substituir o *bit* menos significativo de cada uma das três cores que formam um *pixel* (RGB – *Red* (Vermelho)*, Green* (Verde) *e Blue (*Azul)), assim cada *pixel* aceita até 3 *bits* de informação; desse modo, cada imagem consegue armazenar até 3 vezes o número de *pixels* que possui (DEMACDOLINCOLN, 2013), assim como demonstrado na Figura 2.

Figura 2: Detalhes do processo de esteganografia



Fonte: vivaolinux.com

Esteganálise consiste na ideia de detectar uma mensagem oculta via esteganografia. Este tipo de processo atua de duas formas: a primeira tem como objetivo identificar a presença de mensagens ocultas na imagem; a outra, extrair da imagem a mensagem oculta.

De acordo com Albuquerque (2007), os tipos de esteganálise são:

- ✓ Ataques Aurais: retiram partes significativas do objeto de cobertura como um meio de facilitar a busca por ruídos adicionados via esteganografia;
- ✓ Ataques Estruturais: visam procurar alterações no padrão do arquivo do objeto de cobertura;
- ✓ Ataques Estatísticos: procuram encontrar padrões de comportamento do conteúdo do arquivo.

Nos dias de hoje dificilmente são encontradas aplicações e técnicas de ataques para mídias continuam, ou seja, áudio e vídeo. O foco principal refere-se à esteganálise em imagens.

3.1 Discussão

Neste estudo, como o sistema desenvolvido para estaganografar aceita "*gif*", "*jpeg*", "*jpg*" e "*png*", foram feitos testes com cada uma das extensões. Após isso, por meio do terminal Linux, comparou-se o tamanho do arquivo original e o estaganografado.

Como exemplo, foi embutida na Figura 3 a frase:

> Definições, assim como perguntas e metáforas, são instrumentos para fazer pensar. Sua autoridade reside inteiramente na sua utilidade, não na sua correção. Usamos definições a fim de delinear problema que desejamos investigar, ou favorecer interesses que queremos promover. Em outras palavras, inventamos definições e as descartamos na medida em que servem aos nossos propósitos (POSTMAN, 1980, p.25).

Figura 3: Arquivo Rossi.jpg sem esteganografia

Fonte: motogp.com

Após o processo, podem-se comparar as Figuras 3 e 4, notando-se que não há nenhuma diferença, em nenhum dos cinco parâmetros analisados. Isso ocorre por causa do método LSB, que "esconde" a mensagem, possibilitando o envio da mesma de forma mais segura.

No experimento, foram esteganografadas 10 figuras de cada uma das extensões (quatro tipos). As amostras possibilitaram obter um comparativo com os arquivos originais. Os critérios como formato da figura, qualidade e cor foram analisados visualmente. Já o tamanho dos pixels e do arquivo foi observado por meio do terminal Linux e foram consultados as suas propriedades.

A Figura 4 demonstra a imagem esteganografada, permitindo assim observar que, apesar de possuir uma mensagem em seu interior, não houve alterações visuais perceptíveis.

Figura 4: Imagem do arquivo Rossi.jpg com esteganografia

Fonte: O autor.

Observou-se o mesmo comportamento em todas as extensões. Nenhuma das extensões apresentou qualquer tipo de alteração na figura que permitisse algum interceptador encontrar a mensagem embutida.

4 Conclusão

Devido ao aumento de dispositivos conectados na rede mundial, por meio dos mais diversos dispositivos, ataques e invasões de privacidade ocorrem com maior frequência, comprometendo, assim, o sigilo nas informações pessoais e profissionais.

A técnica de esteganografia é uma ferramenta que possibilita contornar esse problema, fazendo com que, ao contrário da criptografia, computadores que realizam um escaneamento na rede não saibam que uma mensagem está sendo transmitida.

O método aplicado garantiu a privacidade por meio da confidencialidade, como também a integridade por meio da utilização de cifras do tipo *HASH* para verificação da diferença de conteúdo de arquivos esteganografados.

Diante dos resultados apresentados, observou-se que não há privacidade em meios eletrônicos. Entretanto é possível transmitir mensagens, de forma oculta, garantindo que, em caso de interceptação, o seu conteúdo não será lido ou alterado.

A maior contribuição da ferramenta em questão está na sua utilização para comunicações confidenciais por canais ou ambientes não seguros. O processo de embutir e retirar a mensagem na figura é feita de forma simples, possibilitando que usuários com pouco conhecimento possam garantir a integridade das informações.

Referências

ALBUQUERQUE, C.N. *et. al*. Esteganografia e suas aplicações. *In:* PROCEEDINGS DO SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO – SBSEG, 2007. Rio de Janeiro, 2007, p.199

CARVALHO, D.F. Esteganografia digital para transmissão oculta de mensagens. Disponível em: <http://stoa.usp.br/diegofdc/files/-1/4188/EsteganografiaDigitalPalestra.pdf>. Acesso em: 11 set. 2014.

DEMACDOLINCOLN. Esteganografando com o steghide. 2013. Disponível em:<http://e17aeternus.wordpress.com/2013/08/04/steghide/>. Acesso: 1 jun. 2014.

HETZL, S. Steghide: manual. Disponível em: <http://steghide.sourceforge.net/documentation/manpage.php>. Acesso: 8 maio 2014.

HOLANDA, R. O estado da arte em sistemas de gestão da segurança da informação: norma ISO/IEC 27001: 2005. Módulo Security Magazine, 2005. Disponível em: <http://www. modulo. com. br/index. jsp>. Acesso em: 23 ago. 2014.

PETITCOLAS, F.A.P.; ANDERSON, R.J.; KUHN, M.G. *Ocultação de informações*: a survey. 1999.

POSTMAN, N. Language education in a knowledge context. *Rev. General Semantics*, v.37, n.1, p.25-37, 1980.

ROCHA, A.R. Monografia: camaleão: um software digital utilizando esteganografia. 2013. Disponível em: http://www.ic.unicamp.br/~rocha/sci/stego/src/monografia.pdf. Acesso em: 27 ago. 2014.

SÊMOLA, M. *Gestão da segurança da informação*: visão executiva da segurança da informação aplicada ao Security Officer. Rio de Janeiro: Elsevier, 2003.