Fatec Sebrae

REVISTA FATEC SEBRAE EM DEBATE:
Gestão, Tecnologias e Negócios
Volume 05 | Número 09 | JUL - DEZ. 2018 | ISSN: 2358-9817

CRIMES CIBERNÉTICOS: UM COMPARATIVO DE TÉCNICAS DE ESTEGANOGRAFIA.

Camila Pellizon Floret
Universidade Sagrado Coração

Prof. Me. Henrique Pachioni Martins
Universidade Sagrado Coração

Profa. Dra. Simone Cristina Mussio
Faculdade de Tecnologia de Jahu

Profa. Dra. Valéria Cristiane Validório
Faculdade de Tecnologia de Jahu

Resumo:

A segurança da informação está relacionada com as variedades de ameaças as quais os dados são expostos nas redes. A perícia forense computacional tem como objetivo localizar informações registradas ou transmitidas em forma binária, as quais podem ser utilizadas como prova em processos penais, civis e administrativos. Existem diversos tipos de técnicas antiforenses, entre as quais vale ressaltar a criptografia, que permite a alteração da informação, tornando-a compreensível a terceiros, e esteganografia, que é a escrita cifrada de textos com caracteres convencionais, sendo letras, números ou símbolos, podendo ser camuflados em áudios, imagens e vídeos.

FATEC Sebrae – Faculdade de Tecnologia Sebrae - CEETEPS – Centro Estadual de Educação Tecnológica Paula Souza – São Paulo, Brasil.

REVISTA FATEC SEBRAE EM DEBATE: gestão, tecnologias e negócios

Editor Geral
Prof. Dr. Mário Pereira Roque Filho

Organização e Gestão
Prof. Ms. Clayton Pedro Capellari

Correspondência
Alameda Nothmann, nº 598 Campos Elíseos, CEP 01216-000 São Paulo – SP, Brasil.
+55 (11) 3224.0889 ramal: 218
E-mail: f272dir@cps.sp.gov.br

Os principais objetivos deste trabalho incidem em efetuar uma análise bibliográfica sobre os conceitos de esteganografia, pesquisar os softwares de perícia forense digital que possibilitam a verificação dos arquivos, assim como comparar e relatar as diferenças dos arquivos originais dos modificados. A metodologia utilizada consiste em analisar as imagens em diversas extensões, como JPEG, PNG e BMP, e dimensões, de 256, 512, e 1024 pixels, através dos softwares Backtrack ou Kali Linux, Computer Aided Ambiente Investigative (Caine), Helix3, e Forense Digital Toolkit (FDTK).

Palavras-chave: Segurança da informação. Perícia forense computacional. Esteganografia.

Abstract:

Information security is related to the threat variables to which the data are exposed on the networks. Computer forensics aims at locating information recorded or transmitted in binary form, which can be used as evidence in criminal, civil and administrative proceedings. There are several types of anti-forensic techniques, among which it is worth emphasizing cryptography, that allows information alteration, making it comprehensible to third parties, and steganography, that is an encrypted writing of texts with conventional characters, such as letters, numbers or symbols, that can be hidden in audios, images and videos. The main objectives of this work are based on a bibliographic analysis of steganography concepts, and also on a research for digital expertise software that allows the verification of files, as well as in relating the differences between the original files and the modified ones. The methodology used consists in analyzing images such as JPEG, PNG and BMP, dimensions, of 256, 512, and 1024 pixels, by means of the software Backtrack or Kali Linux, Computer Aided Ambiente Investigative (Caine), Helix3, and Digital Toolkit Forensics (FDTK).

Keywords: Information security. Computational forensics. Steganography.

Introdução

Com os recursos oferecidos pelos serviços de *World Wide Web*[1] (WWW), as redes de computadores, interligadas no mundo inteiro, facilitaram a troca de dados e informações entre usuários, empresas privadas, públicas, instituições acadêmicas e governamentais em poucos milissegundos.

Os grandes números de informações circuladas indevidamente podem influenciar no desenvolvimento moral e social das pessoas. Logo, essa disseminação de conteúdos contribui para que usuários tenham acesso a eles, beneficiando-os ou prejudicando-os.

No Brasil, segundo Gonzaga (2012), em uma pesquisa realizada pela Norton/Symantec, o custo anual dos crimes realizados foi de R$ 16 bilhões, que correspondem a sete por cento de prejuízo global. Em 2013, houve uma perda entre R$ 7 a 8 bilhões.

A maioria dos usuários que possuem conhecimento em informática avançada sabe que parte das conexões é criptografada, ou seja, são dados originais transformados em dados ilegíveis, permitindo que sejam apenas conhecidas pelos seus destinatários.

A criptografia é a arte do texto escrito ou dado em um código secreto. Trata-se de dados em um simples formato ilegível chamado de texto cifrado (COUNCIL, 2009). A esteganografia é o ramo particular da criptologia que consiste em fazer com que uma forma escrita seja camuflada com o propósito de encapotar sua verdadeira essência (PINOCHET, 2014).

Por se referir a um conteúdo muito abrangente, é fundamental estar diante das investigações e pesquisas de novos meios tecnológicos para atividades criminosas. Com base nesse contexto, o presente trabalho tem como intuito colaborar com atividades futuras, envolvendo os comparativos de ferramentas de esteganografia, que têm por princípio manter a integridade e segurança da informação, principalmente, contribu-

[1] *World wide web:* rede mundial de computadores.

ir com interessados na área de segurança, como, por exemplo, peritos forenses ou até mesmo estudantes das áreas de tecnologia da informação.

Deste modo, este trabalho tem como objetivo explorar técnicas de esteganografia digital por meio de comparativo de *softwares open-source*[2], a fim de comprovar as vantagens e desvantagens da utilização de cada uma das técnicas estudadas. Além disso, é importante também realizar uma análise bibliográfica sobre os conceitos de esteganografia; analisar e selecionar softwares de perícia forense digital que possibilitem na verificação dos arquivos de tamanhos e extensões específicas; comparar e relatar as diferenças encontradas dos arquivos originais dos modificados; e identificar as vantagens e desvantagens da utilização das ferramentas.

Segurança da informação

O conceito de segurança da informação está padronizado pela NBR ISO/IEC 17799:2005, que hoje é a norma ISO 27002. Esse código de prática de gestão de segurança da informação está relacionado com o aumento do número de pessoas e as variedades de ameaças que os dados são expostos na rede.

A informação está em toda a parte, assim, pode ser armazenada em papéis impressos, eletronicamente, imagens. Seja qual for o método apresentado, podemos considerar que é um recurso estratégico, sendo um mecanismo importante usado para proteger o conjunto de informações e preservar ao máximo os valores que possuem (SANTO, 2010).

Política de segurança da informação

A política tem como alvo proporcionar um apoio e uma orientação, logo é analisado de tempos em tempos, de acordo com os requisitos e as possíveis variações das regulamentações relevantes.

Conforme Marciano (2006), os ambientes organizacionais estão sujeitos a diversos eventos e potencialidades, divididos em três categorias: ameaças, vulnerabilidade e incidentes, compondo e caracterizando os riscos à segurança.

[2] *Open-source:* programas de código aberto.

- Ameaças: “Ameaças são condições ou agentes causadores de incidentes que comprometam as informações e seus ativos através da exploração de alguma vulnerabilidade” (MELO DE ARAÚJO, 2015, p. 8). Pode-se definir que ameaças são eventos ou atitudes indesejáveis, que potencialmente remove, desabilita, danifica ou destrói um recurso. Nestes casos, podem vir os agentes maliciosos, conhecidos como crackers.

- Vulnerabilidade: De acordo com Stallings e Brown (2014), vulnerabilidade é o defeito ou fraqueza no projeto que pode gerar a operação e o gerenciamento do sistema, sendo explorada para violar a política de segurança. Os exemplos de vulnerabilidades são as falhas no projeto, na implementação ou na configuração de um software ou sistema operacional, serviços ou equipamentos de rede.

- Incidentes: “Um incidente de segurança é a ocorrência de um evento que pode causar nos processos de negócio, uma consequência da violação de alguns aspectos” (LYRA, 2008, p. 4). Alguns exemplos de incidentes de segurança são as tentativas de uso ou acesso não autorizado a sistemas ou dados, tentativa de tornar serviços indisponíveis, modificação em sistemas (sem o conhecimento ou consentimento prévio dos donos) e o desrespeito à política de segurança ou à política de uso aceitável de uma instituição.

Arquitetura de segurança

É necessário medir as obrigações de segurança de uma organização, avaliar e escolher inúmeros produtos e políticas de segurança, pois os responsáveis precisam de algum meio sistemático de delimitar as condições de segurança e caracterizar as técnicas para satisfazer os requisitos.

De acordo com Stallings (2008), o foco desta estrutura são os ataques ativos e passivos, mecanismos e serviços.

Fundamentado no Somasundaram e Shrivastava (2009), há dois tipos de ataques que estão relacionados à segurança da informação: os ataques ativos e ataques passivos.

- Ataques ativos: São alterações não autorizadas de informações que podem ameaçar a integridade e disponibilidade dos dados. Dentro deste ataque temos a ame-

aça de interceptação é a parte não autorizada ganha o acesso ao recurso (viola a confidencialidade).

- Ataques passivos: São tentativas de obter um acesso não autorizado às informações sem alterá-las, mas que podem ameaçar a confidencialidade dos dados. Dentro deste ataque, temos a ameaça de interrupção, quando um recurso do sistema se torna indisponível ou inútil (viola a disponibilidade). Ameaça de modificação já e quando a transformação não autorizada do recurso (viola a integridade) e a sua fabricação criam uma determinada informação ao se passar por outra pessoa (viola a autenticidade).

Mecanismos

Mecanismos de segurança são recursos destinados a detectar, prevenir ou recuperar de um ataque à segurança. Há três mecanismos importantes: assinatura digital, criptografia e controle de acesso.

- Assinatura digital: Conforme Silva e Santos (2012), a assinatura digital é um conjunto de dados criptografados, associados a um documento, o qual garante a sua integridade e autenticidade, protegendo-o contra falsificação. Baseia-se no fato de que apenas o dono conhece a chave privada. Se ela foi utilizada para codificar um dado, só o dono poderia ter praticado tal ação. A verificação da assinatura é feita com o uso da chave pública, pois somente ela pode decodificá-lo, caso o texto tenha sido codificado com chave privada.

- Criptografia: É a arte de codificação que permite a transformação reversível da informação de forma a torná-la compreensível a terceiros. Há dois tipos de criptografia, os quais serão vistos na sequência deste trabalho.

- Controle de acesso: São restrições de uso não autorizado de um ativo, isto é, esse serviço controla quem pode ter acesso, sob quais condições pode ocorrer e os que são permitidos para aqueles que ingressam.

Criptografia

É empregada em determinados algoritmos numa chave secreta, para que, a partir do conjunto de dados não criptografados, possa produzir uma sequência de dados criptografados.

De acordo com Oliveira (2006), há dois tipos de criptografia: criptografia assimétrica e criptografia simétrica.

- Criptografia assimétrica ou chave pública: São protocolos baseados em algoritmos que requerem duas chaves, uma delas é a privada e a outra pública. A chave pública pode ficar disponível para qualquer usuário que queira se comunicar com outro de modo seguro, mas a chave privada deverá ficar em poder apenas de cada titular. Exemplos de métodos criptográficos que usam chaves assimétricas: curvas elípticas, *Diffie-Hellman*[3]*, ElGamal e Rivest*[4]*, Shamir and Adleman*[5] (RSA).

A Figura 1 ilustra que a chave pública e privada depende do emissor para criptografar e emissor para decodificar.

Figura 1 – Criptografia assimétrica

Fonte: Pereira (2009).

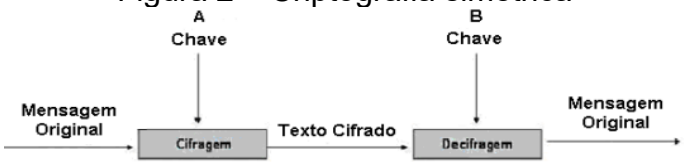
Conforme Pereira (2009), se A deseja enviar uma mensagem de forma segura para B, ambos têm que concordar com um sistema de criptografia de chave pública em comum. Em seguida, B fornece para A sua chave pública, podendo enviá-la ou disponibilizá-la em qualquer meio de comunicação, não sendo necessário um meio seguro. A chave A cifra a mensagem que deseja enviar com a chave do B e a envia para o mesmo. O B, ao receber a mensagem, decifra A utilizando sua chave privada e obtém a mensagem original enviada pelo próprio A.

[3] *Diffie-Hellman.*

- Criptografia simétrica ou chave privada: A chave é o elemento que dá acesso à mensagem oculta trocada entre duas partes, ou seja, é igual para ambas e deve permanecer em segredo. Exemplos de métodos criptográficos que usam chave simétrica: 3DES (*Triple Data Encryption Standard*[6]), *Advanced Encryption Standard*[7] (AES), *Blowfish*[8] e *Rivest Ciphers*[9] (RC4).

A Figura 2 mostra que a chave idêntica depende do emissor para criptografar e receptor para decodificar.

Figura 2 – Criptografia simétrica



Fonte: Pereira (2009).

De acordo com Pereira (2009), se A enviar uma mensagem para B, A deverá empregar a mensagem a um algoritmo e alimentá-lo com uma chave secreta. Assim, a informação vai ser encriptada e um atacante externo não pode visualizá-la. Em seguida, A envia a mensagem para B e este executará processo reverso: emprega a mensagem cifrada ao algoritmo e o alimenta com a mesma chave secreta para poder decriptá-la.

Segurança em sistemas computacionais

De acordo com Stallings (2008), os serviços de segurança têm a finalidade de reforçar a segurança dos sistemas de processamento de dados e transferências de dados de uma organização. Eles definem que um serviço prestado por uma camada de protocolo de comunicação de sistemas abertos garanta a segurança adequada dos sistemas ou das transferências de dados.

---

[4] *ElGamal e Rivest.*
[5] *Shamir and Adleman.*
[6] *Triple Data Encryption Standard.*
[7] *Advanced Encryption Standard.*
[8] *Blowfish.*
[9] *Rivest Ciphers.*

De acordo com Almeida et al. (2015), há três princípios: confidencialidade, integridade e disponibilidade. A explicação resumida é que somente pessoas autorizadas devem ter acesso à informação, a qual não deverá ter alterações. Somente as informações autorizadas serão salvas pelo proprietário e este é único responsável por disponibilizá-las. Se um ou mais desses princípios forem desobedecidos, temos um incidente de segurança em sistemas computacionais.

As técnicas usadas em roubo de informação, geralmente, estão ligadas à descoberta e à exploração de vulnerabilidades, características que o torna um sistema sensível a ataques.

Um ataque é um conjunto de passos executados, no âmbito da exploração de vulnerabilidades, que permite concretizar uma ação ilícita. Uma ameaça é o dano resultante da execução de um ataque.

A defesa consiste na união das políticas e mecanismos implantados para diminuir as vulnerabilidades, para detectar e anular ataques passados ou atuais, assim como para minimizar os riscos decorrentes de outros ataques futuros. Geralmente, quando um sistema computacional está sendo atacado, este começa a perder desempenho.

Perícia forense computacional

A perícia computacional é um ramo da ciência forense que se concentra na lei de processo penal e nas evidências aplicadas a computadores e dispositivos relacionados. Não se limita apenas a computadores, mas também inclui telefones móveis, assistente digital pessoal e redes.

Segundo Eleutério e Machado (2011), informática forense é informação armazenada ou transmitida de forma binária, podendo ser usada como prova em processos penais, civis e administrativos. Esses dados podem ser encontrados a partir de dispositivos eletrônicos. Dessa maneira, há diversos tipos de crimes, como: crimes cometidos utilizando equipamentos computacionais como ferramenta de apoio à prática do delito e crimes cometidos utilizando equipamentos computacionais como meio para a realização do delito.

- Crimes cometidos utilizando equipamentos computacionais como ferramenta de apoio à prática do delito: Segundo Amadio et al. (2012), no ato criminoso,

o computador é utilizado como uma ferramenta de apoio para efetuar o crime. Várias práticas criminosas podem ser realizadas, tais como: falsificação de documentos, venda de produtos proibidos, sonegação fiscal, compra de votos em caso de eleições e vários outros.

- Crimes cometidos utilizando equipamentos computacionais como meio para a realização do delito: Segundo Amadio et al. (2012), a peça central é o computador, pois se tal dispositivo não existisse, esse crime virtual não seria praticado. Várias práticas criminosas podem ser realizadas tais como: ataques a sites, roubos de informações confidenciais, programas maliciosos para roubo de senhas, entre outros.

De acordo com Romeiro (2002), os crimes de informática devem ser classificados quanto ao seu objetivo material, podendo ser descritos como: crimes de informática comum, crimes informática misto e crimes informática puro.

- Crimes de informática comum: O objetivo é utilizar o sistema de informática como mera ferramenta a praticar o crime, não sendo essencial para o delito.

- Crimes de informática misto: O alvo é apenas o bem juridicamente protegido da informática, o sistema de informática é ferramenta imprescindível a sua consumação.

- Crimes de informática puro: A finalidade é apenas o sistema de informática, logo, tais crimes se compõem de softwares, hardwares, dados e sistemas contidos no computador e meios de armazenamento.

Os locais de crime envolvendo os equipamentos computacionais são onde as supostas infrações penais ocorreram. Podemos encontrar evidências muito úteis à investigação, com o propósito de esclarecer a autoria (quem), a dinâmica (como) e a materialidade do delito (o que aconteceu). (ELEUTÉRIO; MACHADO, 2011).

Conforme Eleutério e Machado (2011), os peritos e suas equipes devem realizar um reconhecimento na área do crime, identificando os equipamentos computacionais. Os profissionais capacitados devem ter o conhecimento em equipamentos e técnicas forenses para verificar o conteúdo armazenado nos dispositivos, permitindo que ne-

nhuma informação seja modificada, garantindo, assim, a preservação das evidências digitais.

Técnicas de ataques

Os ataques são métodos de remoção, ocultação e subversão de evidências com o objetivo de suavizar os resultados de análises forenses computacionais, a fim de dificultar o trabalho dos peritos. Existem vários tipos de técnicas antiforenses, como: destruição de dados, limpeza de registros, modificação de dados, ocultação de dados, digital *watermarking*[10] e esteganografia.

- Destruição de dados: As ferramentas conhecidas como *wiping tools*[11] são utilizadas para dificultar ou impedir a recuperação dos dados, ou seja, destruir os dados que ficam armazenados no HD. Além desta destruição lógica, em alguns casos, os criminosos podem danificar fisicamente as mídias, dificultando e até impossibilitando a recuperação dos dados (FAGUNDES, 2007; KONRATH, 2007; LUDWIG, 2007; NEUKAMP, 2007; PEREIRA, 2007).

- Limpeza de registros: Segundo Fagundes et al. (2007), os registros são bancos de dados que armazenam as configurações e opções de todos os hardwares. Os softwares de limpeza de registros são capazes de zerar e sobrescrever arquivos de dados, qualquer tipo de recuperação se torna impraticável ou até impossível de ser realizada.

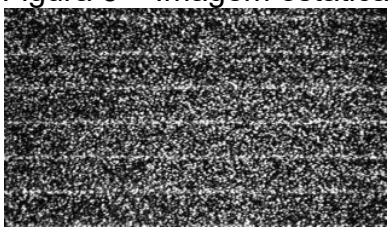
- Modificação de dados: Conforme Fagundes et al. (2007), há dois tipos comuns para realizar a modificação dos dados: alteração da extensão dos arquivos e modificação do conteúdo do cabeçalho dos arquivos.

- Ocultação de dados: Segundo Albuquerque et al. (2007), os dados podem ser escondidos de duas formas: digital *watermarking* e esteganografia. Apesar de aparecerem quase sempre em conjunto com a esteganografia, o sistema digital *watermarking* não pertence ao mesmo ramo da esteganografia.

[10] *Digital watermarking:* marca de água digital.
[11] *Wiping tools: ferramenta de limpeza.*

- Digital *watermarking*: Este método de técnica digital é conhecido como marca d'água e se refere a um sinal portador de informações, visivelmente imperceptível, introduzido em uma imagem digital. A imagem que contém a marca é considerada como imagem hospedeira ou marcada. A Figura 3 mostra a técnica digital *watermarking* mais utilizada: a imagem estática.

Figura 3 – Imagem estática



Fonte: Rosa (2013).

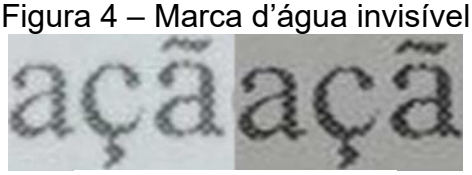
A representação não possui nenhum movimento, por isso são chamadas de imagens estáticas.

Cabe aqui lembrar que há quatro propriedades básicas referentes à marca d'água: marca d'água invisível, marca d'água invisível frágil, marca d'água invisível robusta e marca d'água visível.

- Marca d'água invisível: De acordo com Barcelos et al. (2015), é baseada na alteração dos pixels das imagens. Essa modificação dos pixels é imperceptível ao sistema visual humano. As alterações feitas podem ser feitas tanto no domínio do espaço como no domínio da frequência, a escolha deve estar de acordo com a característica que queira dar ao sistema. Para detectar a marca d'água deve-se utilizar um algoritmo de extração ou um detector de presença. Geralmente quem usa este tipo de digital *watermarking* as propriedades de direitos autorais e autenticação de imagens.

A Figura 4 apresenta a marca d'água invisível.

Figura 4 – Marca d'água invisível



Fonte: Ferreira (2015).

As características identificadoras da marca d'água invisível foram preservadas, permitindo a ampliação das imagens, mantendo os elementos identificadores dos caracteres, e obtendo resultados melhores que os textos digitalizados.

- Marca d’água invisível frágil: Serve para garantir a autenticidade da imagem. A digital *watermarking* fornece uma segurança de que a imagem marcada não seja editada ou adulterada, cobrindo a origem declarada ou assumida. É possível construir marcas d’águas cuja remoção pode ser detectada (BARRETO, 2003).

- Marca d’água invisível robusta: De acordo com Barreto (2003) serve para assegurá-la os direitos de propriedades intelectuais. Esse sistema deteriora a qualidade de imagem resultante a ponto de destruir seu conteúdo visual. Os ataques mais comuns são processamento comum dos de sinais, distorções geométricas comuns, realce de contraste e brilho, inserção de ruído, filtragem linear e não linear, impressão e escaneamento, compressão com perda, ataques de colisão e falsificação e remarcar mídias marcadas.

A Figura 5 ilustra um ataque comum que é o realce de contraste e brilho.

Figura 5 – Realce de contraste e brilho

Fonte: Ferreira (2015).

A manipulação de brilho e contraste de imagens podem acentuar as características das letras, aos quais foram submetidas a tratamento.

- Marca d’água visível: É pouco utilizada, pois é sensível a ataques, e pode ser facilmente removida com uma simples operação de recorte. Este sistema serve apenas como um sinal de advertência para indicar que tem a mídia digital é de certo proprietário. Este tipo de digital *watermarking* geralmente é utilizado pelas emissoras de televi-

são que inserem seus logotipos nas transmissões, como segue a Figura 6 (BARCELOS, 2015; BATISTA, 2015; FIENO, 2015; LOPES, 2015).

Figura 6 – Marca d'água visível

Fonte: IFTV (2012).

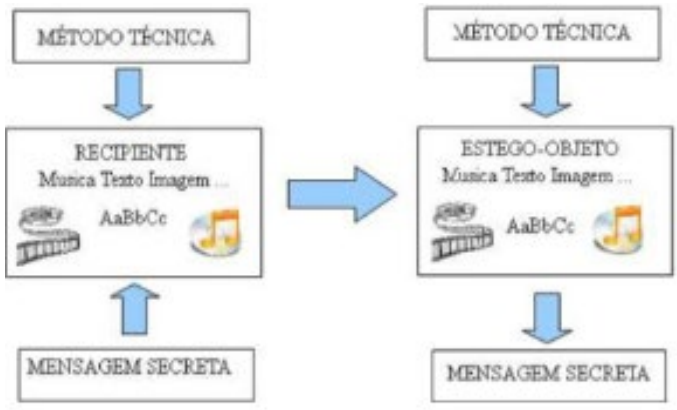
Esta imagem exibe a marca d'água no canto inferior do Sistema Brasileiro de Televisão (SBT).

Esteganografia

Esteganografia é a arte de camuflar informações para que estas não sejam percebidas. Segundo Alencar (2015), é a escrita cifrada de textos com caracteres convencionais, podendo ser letras, números ou símbolos.

A Figura 7 ilustra de forma resumida o processo da esteganografia.

Figura 7 – Resumo da esteganografia

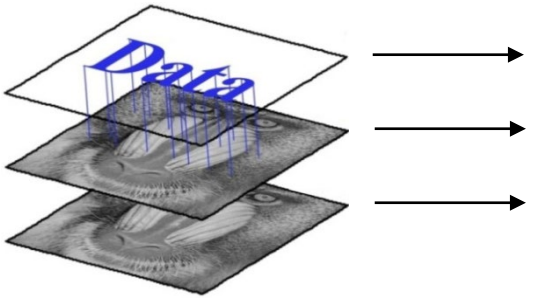


Fonte: Teixeira (2011).

O resumo do processo de esteganografia baseia-se na mensagem secreta enviada ao recipiente, podendo ser camuflada por vários tipos de arquivos. O *stego-object*[12] é a união dos dois componentes: a mensagem secreta e o recipiente.

A Figura 8 mostra como os dados são embutidos na imagem.

Figura 8 – Funcionamento da esteganografia.



I – Dados a serem embutidos.

II – Dados são embutidos na imagem com uso de uma chave (*stego-key*[13]).

III – O *stego-object* é criado contendo a informação escondida.

Fonte: Li (2015).

Nota: Adaptada pelos autores.

Os dados embutidos são inseridos em algum arquivo de maneira confidencial. A mensagem protegida é o arquivo que servirá de esconderijo para o dado que será embutido. A chave (*stego-key*) poderá ser usada ao inserir dados na mensagem coberta. O resultado final (*stego-object*) da mensagem coberta possuirá as informações que foram inseridas ocultamente. Há uma diferença de criptografia e esteganografia, conforme apresenta a Tabela I.

Tabela I – Diferenças entre criptografia e esteganografia

Criptografia	Esteganografia
A mensagem visível, mas cifrada, torna-se uma mistura de caracteres sem qualquer significado.	Oculta a mensagem em outro objeto de aparência inocente, como imagens, vídeos, áudios ou arquivos.
A coleção de caracteres aleatórios gera muita suspeita e curiosidade.	Uma coleção de imagens, vídeos ou áudios que não gera suspeita.
Requer cuidado ao reutilizar chaves.	Requer cuidado quando reutilizar arquivos

[12] *Stego-object:* estego-objeto.
[13] *Stego-key:* estego-chave.

	de áudio ou imagem.
Existem leis que, inclusive, proíbem seu uso.	Não existem leis regulamentando ou proibindo o uso.

Fonte: Honda (2011).

Nota: Adaptada pelos autores.

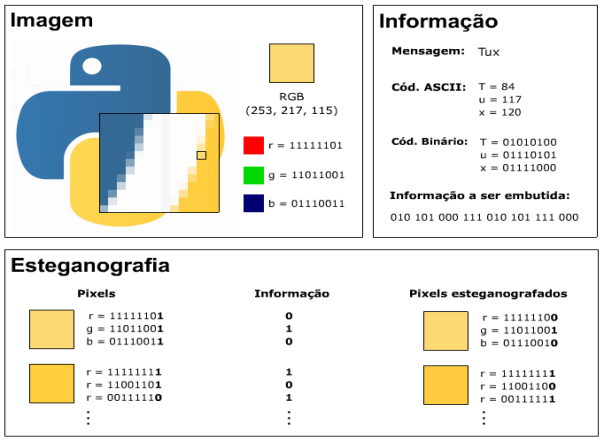
A criptografia tem como alvo tornar a mensagem ilegível para um agente fora da comunicação. Sendo assim, ela se preocupa em ocultar a existência das mensagens através de diversas técnicas clássicas e/ou computacionais, podendo ser ocultadas em áudios, imagens e vídeos.

- Esteganografia em áudios: As técnicas de esteganografia em áudios exploram a vulnerabilidade do sistema auditivo humano podendo captar até um bilhão de potências diferentes e até mil frequências de sinais distintas. A intenção é que os sons mais altos prevalecem do que os sons mais baixos, além que existem algumas distorções dos ambientes que simplesmente são ignoradas pelo ouvido.

- Esteganografia em imagens: Existem diversas técnicas indicadas a seguir que manuseiam com imagens, que são a técnica de inserção do *least significant bit*[14], as técnicas de filtragem e mascaramento, e as técnicas de algoritmos e transformações.

A Figura 9 apresenta os detalhes da esteganografia no LSB.

Figura 9 – Detalhes da esteganografia



[14] *Least significant bit:* bit menos significativo.

Fonte: Almeida (2011).

A mensagem TUX deve estar representada na forma de bits para ser embutida na imagem. Por isso, o código ASCII de cada letra é convertido em números binários, e cada pixel RGB tem seus três bits menos significativos trocados por outros três bits da mensagem.

- Esteganografia em vídeos: Segundo Fiori de Carvalho (2005), a esteganografia de imagem é similar à esteganografia de vídeos, exceto pelo fato das informações estarem ocultas em diversões quadros ou frames dos arquivos, criando uma grande complexidade nas buscas destes dados.

Metodologia

Na primeira etapa deste trabalho, foi elaborado o referencial teórico, por meio de pesquisas em livros, artigos científicos e outros trabalhos focados na área de segurança da informação, na perícia forense computacional e nos softwares utilizados no decorrer do trabalho. Na segunda fase, foi elaborada a parte prática, utilizando-se dos softwares de esteganografia, tais como: Backtrack ou Kali Linux, Caine, Helix e FDTK.

A aplicação das análises de esteganografia foi realizada em um notebook particular do fabricante Acer, modelo Aspire 5750, plataforma Windows 7, sistema operacional de 64 bits, processador Intel Core i3-2330 CPU @ 2.20 GHz e 4 GB de memória RAM. Os softwares escolhidos são funcionais em apenas plataforma Linux. Para isso, foi feita a instalação de uma máquina virtual Oracle VM VirtualBox, versão 5.1.4, lançada em 16 de agosto de 2016, a qual foi escolhida pela compatibilidade com qualquer sistema operacional.

O Backtrack ou Kali Linux, versão 1.1.0, foi selecionado por ter características de interface gráfica de fácil manuseio e por incluir um scanner de portas, um analisador de pacotes, um cracker de senhas e uma suíte de software para redes sem fio de teste de penetração; além disso, possui uma flexibilidade na distribuição.

O Caine, versão 7.0, foi escolhido por ser uma interface gráfica de fácil manuseio, de inicialização rápida e por bloquear todos os dispositivos de bloco frequente-

mente utilizados em dispositivos de comunicação paralela, como discos rígidos e drives de CDs, em modo de somente leitura.

O FDTK, versão 3.0, foi selecionado por ter suas vantagens de uma interface gráfica de fácil manuseio, em idioma português e por possuir etapas, como: coleta, exame, análise de dados e toolkits.

O Helix3, versão ISO2008R1, foi escolhido por ter suas vantagens de não inicializar o disco rígido, bem como por possuir um kit básico que inclui antivírus, análises de redes, recuperadores de senhas, examinador de arquivos binários, etc.

Após a instalação dos softwares *open-source*, foram executadas as imagens de dimensões: 256, 512, e 1024 pixels e as extensões: BMP, JPEG e PNG, que suportam milhões de cores e conserva os detalhes.

A escolha das imagens coloridas levará à identificação da modificação do pixel, analisando o que cada ferramenta suporta. Os testes foram feitos no Binwalk do Backtrack ou Kali Linux, Okteta do Caine, Outguess e Hexdump do FDTK, e Bless Hex Editor do Helix3.

Posteriormente, as imagens inseridas foram comparadas aos resultados obtidos, acessando os valores hexadecimais do arquivo original e do arquivo modificado. O alvo foi encontrar os valores que não correspondem ao arquivo original.

Resultados

Com a atualização na plataforma Windows 7 Home Basic para Windows 10 Home e do Virtual Oracle, versão 5.0.20, para 5.1.4, disponível no dia 16 de agosto de 2016, foram efetuados os downloads dos softwares Backtrack ou Kali Linux, versão 2016.1; Caine, versão 7.0; FDTK, versão 3.0; e Helix, versão ISO2008R1.

O arquivo com o nome de “Mensagem” foi elaborado em formato TXT, tamanho 1 KB, o qual inseriu a seguinte frase sem acentos, “Uma perícia bem-feita é capaz de fazer dos vestígios deixados na cena do crime a única testemunha capaz de expressar a verdade absoluta e, portanto, a justiça que sempre se busca”.

No Backtrack ou Kali Linux, foi usado o Binwalk, versão 2.1.1, pois é uma ferramenta de fácil manuseio e as características mais importantes para o desenvolvimento do trabalho são a localização e extração dos arquivos binários.

O Caine apresenta uma ferramenta chamada Okteta, versão 0.13.3. Esta foi empregada por ser um editor de dados de arquivos e usada para comparar as imagens em diversos tamanhos e extensões, podendo ser codificada em binário, decimal, octal e hexadecimal.

No FDTK, foi utilizado o Hexdump. Este é um comando que obtém a entrada a partir de um arquivo ou de uma entrada padrão, fornecendo muitas opções para extrair e depurar o conteúdo do arquivo escrito por qualquer programa de aplicação.

No Helix3, a ferramenta Bless Hex Editor é um editor binário que permite modificar arquivos como sequência de byte.

Considerações finais

Neste trabalho, foram apresentados os conceitos de segurança da informação, perícia forense computacional, técnicas de ataque, com foco em esteganografia, e crimes informáticos. Além disso, na parte prática, foram apresentados quatros softwares de esteganografia que utilizam diferentes ferramentas para ocultação e comparação de dados das imagens digitais.

As técnicas de esteganografia têm seu uso legal e ilegal. Como uso legal no presente e no futuro, esteganografia tem sido usada e será cada vez mais utilizada na proteção de direitos, principalmente quando se considera as novas formas de comercialização utilizando a mídia digital.

As escolhas dos softwares ocorreram por serem ferramentas open-source, de plataforma Linux, e por diferenciarem o método como foi obtido no resultado.

O Backtrack ou Kali Linux fornece uma interface mais complexa, uma vez que é necessário compreender cada linha de comando da ferramenta Binwalk e, consequentemente, qual a melhor opção para aplicar. Para aqueles que não conhecem a língua inglesa, esta ferramenta não é considerada com boa opção de uso.

O software Caine é de interface amigável ao usuário. A ferramenta Okteta é um editor simples para os dados brutos dos arquivos. Para aqueles que desejam uma comparação rápida e eficiente, esta ferramenta é considerada como uma ótima opção de escolha.

O FDTK é fácil de manusear, visto que é necessário abranger cada linha de comando das ferramentas Hexdump, as quais obtêm a entrada a partir de um arquivo ou de uma entrada padrão, fornecendo muitas opções para extrair e depurar. Já o Outguess é que realiza a análise da imagem e utiliza a técnica de substituição dos bits menos significativos para ocultar as mensagens inseridas na imagem original. Para aqueles que não têm conhecimento da língua inglesa, esta ferramenta não é apropriada para o seu uso.

O software Helix3 fornece uma interface simples na execução. A ferramenta Bless Hex Editor é um editor binário que permite editar arquivos como sequência de byte. Para aqueles que desejam uma comparação ligeira e eficiente, esta ferramenta é considerada uma excelente opção.

Por fim, todos os softwares apresentaram vantagens e desvantagens, no entanto tiveram um desempenho excelente na execução e obtiveram resultados positivos, ou seja, mensagens ocultas no arquivo modificado foram localizadas.

Referências

ALBUQUERQUE, Célio V. N.; JULIO, Eduardo P.; BRAZIL, Wagner G.. **Esteganografia e suas aplicações.** 2007. 49 f. Trabalho de Conclusão de Curso (Doutorado em Computação) - Universidade Federal Fluminense, Niterói, 2007.

ALENCAR, Marcelo S.. **Informação, codificação e segurança de redes.** Rio de Janeiro: Elsevier, 2015. Disponível em: <https://books.google.com.br/books?id=jpbpCgAAQBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false>. Acesso em: 29 abr. 2016.

ALMEIDA, Daniela; AMARAL, Érico; PINHO, Leonardo; ROTONDO, Gustavo; FREITAS, Mariana Pompeo; JACOBSEN, Wilson. **Da computação forense a técnica de esteganografia. Um ensaio sobre a ocultação de informações em sistemas computacionais.** 2015. 10 f. Trabalho de Conclusão de Curso (Graduação em Engenharia da Computação) – Universidade Federal do Pampa, Bagé, 2015.

ALMEIDA, Rafael José de Alencar. **Viva o Linux.** 2011. Disponível em: <https://www.vivaolinux.com.br/artigo/Esteganografia-e-Esteganalise-transmissao-e-deteccao-de-informacoes-ocultas-em-imagens-digitais>. Acesso em: 13 abr. 2016.

AMADIO, Renato A.; GALVIAN, Julio César; GONÇALVES, Márcio; WUILLES DOS SANTOS, Herlones. **Perícia forense computacional: metodologias, técnicas e ferramentas.** 2012. 17 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) – Faculdade de Ciências Sociais Aplicadas do Vale do São Lourenço, Jaciara, 2012.

BARCELOS, Célia A. Z.; BATISTA, Marcos Aurélio; FIENO, Alexandre; LOPES, Ivan O.. **Introdução à marca d'água digital.** 2006. 9 f. Trabalho de Conclusão de Curso (Mestrado em Banco de Dados e Computação Gráfica) – Universidade Federal de Uberlândia, Uberlândia, 2015.

BARRETO, Paulo Sérgio L. M.. **Criptografia robusta e marcas d'água frágeis: construção e análise de algoritmos para localizar alterações em imagens digitais.** 2003. 150 f. Trabalho de Conclusão de Curso (Doutorado em Engenharia) – Escola Politécnica da Universidade de São Paulo, São Paulo, 2003.

BROWN, Lawrie; STALLINGS, William. **Segurança de computadores.** São Paulo: Elsevier, 2014. Disponível em: <https://books.google.com.br/books?id=y2DcAwAAQBAJ&printsec=frontcover&hl=ptBR#v=onepage&q&f=false>. Acesso em: 15 abr. 2016.

COUNCIL, E-C. **Computer forensics: investigating network intrusions and cybercrime.** Clifton Park: Course Technology, 2009. Disponível em: <https://books.google.com.br/books?id=FfoFAAAAQBAJ&printsec=frontcover&hl=ptBR#v=onepage&q&f=false>. Acesso em: 30 abr. 2016.

ELEUTÉRIO, Pedro M. da S.; MACHADO, Marcio P.. **Desvendando a computação forense.** 1 ed. São Paulo: Novatec, 2011.

FAGUNDES, Leonardo L.; KONRATH, Marlom; LUDWIG, Glauco; NEUKAMP, Paulo; PEREIRA, Evandro D. V.. **Forense computacional: fundamentos, tecnologias e desafios atuais.** 2007. 51 f. Trabalho de Conclusão de Curso (Mestrado em Ciência da Computação) – Universidade do Vale do Rio dos Sinos, São Leopoldo, 2007.

FERREIRA, Felippe P. **Proteção da prova documental impressa e digitalizada com a utilização de watermarking.** 2015. 8 f. Trabalho de Conclusão de Curso (Graduação em Engenharia) – Universidade de Brasília, Brasília, 2015.

FIORI DE CARVALHO, Diego. **Exploração tecnológica para esteganografia em vídeos digitais.** 2005. 211 f. Teste (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2005.

GONZAGA, Yuri. **Custo anual do cibercrime no Brasil é de R$ 16 bilhões, diz estudo.** Folha de São Paulo, São Paulo, 04 out. 2012.

HONDA, Raphael R.. **Análise e implementação de algoritmos para manipulação de esteganografia em imagens.** 2011. 58 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Fundação de Ensino “Eurípides Soares da Rocha”, Marília, 2011.

LYRA, Mauricio. **Segurança e auditoria em sistemas de informação.** 1 ed. Rio de Janeiro: Ciência Moderna, 2008.

MARCIANO, João Luiz P.. **Segurança da informação – Uma abordagem social.** 2006. 211 f. Teste (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2006.

MELO DE ARAÚJO, Victor. **Segurança da informação: uma abordagem holística com foco na implantação de um GSI.** 2015. 100 f. Trabalho de Conclusão de Curso (Graduação em Redes e Telecomunicação) – Universidade Salvador Laureate, Salvador, 2015.

OLIVEIRA, Ronielton R.. **Criptografia tradicional simétrica de chave privada e criptografia assimétrica de chave pública: análise das vantagens e desvantagens.** 2006. 20 f. Trabalho de Conclusão de Curso (Pós-Graduação e Criptografia e Segurança em Redes) – Universidade Federal Fluminense, Niterói, 2006.

PEREIRA, Aparecido José. **Esteganografia – Implementação de um software para ocultar mensagens criptografadas em imagens.** 2009. 43 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Centro Universitário Eurípides de Marília, Marília, 2009.

PINOCHET, Luis H. C.. **Tecnologia da informação e comunicação.** Rio de Janeiro: Elsevier, 2014. Disponível em: <https://books.google.com.br/books?id=plgaBQAAQBAJ&pg=PT233&dq=esteganografia&hl=pt-BR&sa=X&ved=0ahUKEwjC7oy-

9IzNAhXCSSYKHRkqCUgQ6AEIHDAA#v=onepage&q=esteganografia&f=false>. Acesso em: 10 abr. 2016.

ROMEIRO, Leandro K.. **Crimes de informática.** 2002. 43 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Ciências Jurídicas, Universidade Tuiuti do Paraná, Curitiba, 2002.

SANTO, Adrielle F. S. do E.. **Segurança da informação.** 2010. 11 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Instituto Cuiabano de Educação, Cuiabá, 2010.

SANTOS, Diana L. R.; SILVA, Rita M. S.. **Segurança da informação: a norma ISO/IEC 27000 e ISO/IEC 27001.** 2012. 25 f. Trabalho de Conclusão de Curso (Mestrado em Ciência da Informação) – Faculdade de Engenharia da Universidade do Porto, Porto, 2012.

SOMASUNDARAM, G.; SHRIVASTAVA, Alok. **Armazenamento e gerenciamento de informações.** Indianápolis: Techbooks, 2009. Disponível em: <https://books.google.com.br/books?id=d8uCfC46hwsC&printsec=frontcover&hl=ptBR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>. Acesso em: 13 abr. 2016.

STALLINGS, William. **Criptografia e segurança de redes – Princípios e práticas.** 4 ed. São Paulo: Prentice Hall Brasil, 2008.

TEIXEIRA, Márcio Ranieri. **Esteganografia em arquivos texto e técnicas de detecção.** 2011. 42 f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2011.