Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Aplicação de Técnicas de Esteganografia em Arquivos de Áudio

Renato A. Nobre - 15/0146698

Monografia apresentada como requisito parcial
para conclusão da matéria de Segurança Computacional

Brasília
2019

Sumário

Capítulo 1

Introdução

Um dos ramos da criptografia é a esteganografia. De origem grega, a palavra significa a arte da escrita escondida (estegano = esconder; grafia = escrita)

A esteganografia é um mecanismo que permite a transmissão de uma mensagem secreta dentro de uma mensagem inócua. Ao invés de chave e/ou algoritmo, o próprio uso da criptografia é ocultado pelos principais [1].

Esquemas de assinatura digital via de regra permitem a introdução de canais subliminares na assinatura lavrada em mensagens inócuas, onde a mensagem secreta é ocultada através da escolha da chave pública de verificação, ou na preparação do autenticador [1].

Este trabalho tem como objetivo fazer uma breve análise dos diversos tipos de esteganografia existentes e entrar mais afundo no estudo dos mecanismos esteganográficos de áudio.

Capítulo 2

Fundamentação Teórica

2.1 Esteganografia

Um dos ramos da criptografia é a esteganografia. De origem grega, a palavra significa a arte da escrita escondida (estegano = esconder; grafia = escrita) [2].

As aplicações de esteganografia incluem identificação de componentes dentro de um subconjunto de dados, legendagem, rastreamento de documentos e certificação digital, e demonstração de que um conteúdo original não foi alterado [2].

O uso deste método não é recente, seu primeiro registro é perto de 440 A.C. Esse método envolveu Demerstus, que escreveu uma mensagem aos espartanos alertando sobre invasões eminentes de Xerxes. A mensagem foi esculpida na madeira da tabuleta de cera e depois coberta com uma nova camada de cera. Esta tábua aparentemente vazia foi entregue com sua mensagem oculta com sucesso [3].

A esteganografia continuou ao longo do tempo para se desenvolver em novos níveis. Durante tempos de guerra, a esteganografia é usada extensivamente. Durante a Guerra Revolucionária Americana, as forças britânicas e americanas usaram várias formas de tintas invisíveis. A tinta invisível envolvia materiais comuns, incluindo leite, vinagre, suco de frutas e urina, para o texto oculto. Decifrar essas mensagens ocultas exigia luz ou calor. Durante a Segunda Guerra Mundial, os alemães introduziram micropontos. Os micropontos eram documentos completos, imagens e planos reduzidos ao tamanho de um ponto e anexados a documentos comuns [3].

A arte de detectar mensagens escondidas nos mais diversos meios de comunicação por sua vez é denominada esteganálise.

Premissas

Para os métodos esteganográficos esconderem um conteúdo com uma probabilidade satisfatória do mesmo não ser encontrado, este precisa seguir uma série de premissas.

- **Segurança -** A fim de não levantar suspeita, enquanto tenta criar uma blindagem contra um algoritmo de descoberta, o conteúdo escondido deve ser invisível tanto perceptivelmente quanto por meios estatísticos. Além disso, a complexidade computacional de qualquer ferramenta de esteganografia útil não pode ser infinitamente grande. Em termos de praticidade, um sistema pode ser considerado seguro, ou esteganograficamente forte, se não for possível descobrir a presença de estego-conteúdo usando qualquer meio acessível;
- **Carga Útil -** Diferentemente de marca d'água, que precisa embutir somente uma quantia pequena de informações de direitos autorais, a esteganografia é direcionada à comunicação escondida e portanto normalmente exige capacidade de inclusão suficientemente grande. Os requisitos para capacidade significativa de dados e segurança são frequentemente contraditórios. Dependendo dos argumentos de aplicação específica, um compromisso deve ser buscado;
- **Robustez -** Embora robustez contra ataques não seja uma prioridade importante, ter a capacidade de resistir a compressão é certamente desejável, pois a maioria das imagens JPEG coloridas são comprimidas antes de serem colocadas on-line [3].

2.2 Técnicas Comuns de Esteganografia

2.2.1 Esteganografia em Texto

Muitas técnicas envolvem a modificação do layout de um texto, regras como o uso de cada n-ésimo caractere ou a alteração da quantidade de espaço em branco após as linhas ou entre as palavras. A última técnica foi usada com sucesso na prática e, mesmo depois de um texto ter sido impresso e copiado no papel por dez vezes, a mensagem secreta ainda pode ser recuperada. Outra maneira possível de armazenar um segredo dentro de um texto é usar uma fonte de capa publicamente disponível, um livro ou um jornal e usar um código que consiste, por exemplo, na combinação de um número de página, um número de linha e um número de caractere. Dessa forma, nenhuma informação armazenada dentro da fonte de cobertura levará à mensagem oculta. Descobrir isso depende unicamente de obter conhecimento da chave secreta [4].

2.2.2 Esteganografia em Imagem

Para ocultar informações, a inserção direta de mensagens pode codificar cada bit de informação na imagem ou incorporar seletivamente a mensagem em áreas "barulhentas" que atraem menos atenção - aquelas áreas onde há uma grande variação de cor natural. A mensagem também pode ser espalhada aleatoriamente por toda a imagem. Existem várias maneiras de ocultar informações em mídia digital. Abordagens comuns incluem:

- Inserção de Bit Menos Significativa
- Mascaramento e Filtragem
- Codificação de Padrão Redundante
- Criptografar e Dispersar
- Algoritmos e Transformações

Cada uma dessas técnicas pode ser aplicada, com vários graus de sucesso [4].

2.2.3 Esteganografia em Áudio

Em um sistema de esteganografia de áudio baseado em computador, as mensagens secretas são incorporadas ao som digital. A mensagem secreta é incorporada alterando ligeiramente a sequência binária de um arquivo de som. O software de esteganografia de áudio existente pode incorporar mensagens em arquivos de som WAV, e até MP3. Incorporar mensagens secretas em som digital geralmente é um processo mais difícil do que incorporar mensagens em outras mídias. A fim de ocultar mensagens secretas com sucesso, uma variedade de métodos para incorporar informações em áudio digital foi introduzida. Esses métodos variam de algoritmos bastante simples que inserem informações na forma de ruído de sinal para métodos mais poderosos que exploram sofisticadas técnicas de processamento de sinal para ocultar informações. A lista de métodos que são comumente usados para esteganografia de áudio são listados e serão discutidos posteriormente no trabalho [4].

- codificação LSB
- codificação de paridade
- codificação de fase
- Espalhamento de espalhamento
- esconder eco

2.2.4 Esteganografia em Vídeo

Os arquivos de vídeo geralmente são uma coleção de imagens e sons, portanto, a maioria das técnicas apresentadas em imagens e áudio também pode ser aplicada a arquivos de vídeo. As grandes vantagens do vídeo são a grande quantidade de dados que podem ser escondidos no interior e o fato de ser um fluxo de imagens e sons em movimento. Portanto, qualquer distorção pequena, mas de outra forma perceptível, pode passar despercebida pelos seres humanos por causa do fluxo contínuo de informações [4].

2.2.5 Esteganografia em Protocolos

O termo esteganografia de protocolo refere-se à técnica de incorporação de informações em mensagens e protocolos de controle de rede usados na transmissão da rede. Nas camadas do modelo de rede OSI, existem canais secretos onde a esteganografia pode ser usada. Um exemplo de onde a informação pode estar oculta está no cabeçalho de um pacote TCP/IP em alguns campos que são opcionais ou nunca são usados [4].

2.2.6 Estado da Arte

As imagens são a mídia de cobertura mais popular para esteganografia e podem ser armazenadas em um formato bitmap direto (como BMP) ou em um formato comprimido (como JPEG). Imagens de palheta de cores estão normalmente no formato GIF. O ocultamento de informações é realizado ou no domínio espacial ou no domínio de frequência. Em termos de esquemas de inserção, vários métodos (como substituição, adição e ajuste) podem ser usados. Uma abordagem de ajuste é a QIM, que usa diferentes quantizadores para transportar diferentes bits dos dados secretos.

As abordagens mais comuns de inserção de mensagens em imagens incluem técnicas de inserção no bit menos significativo, técnicas de filtragem e mascaramento e algoritmos e transformações. Cada uma destas técnicas pode ser aplicada à imagens, com graus variados de sucesso. O método de inserção no bit menos significativo é provavelmente uma das melhores técnicas de esteganografia em imagem [3].

2.3 Trabalhos Relacionados

Uma breve análise da literatura existente na área é o suficiente para notar que existe um vazio na área de esteganografia em áudio, diversos trabalhos discutem formas de esteganografia em imagem. Alguns trabalhos mais relevantes podem ser considerados aqui.

Gupta e Chaudhary discutem a implementação de ocultar um arquivo de som em uma imagem digital. Este som pode ser voz, dados de VoIP ou uma música. Nesta abordagem, um arquivo MP3 foi usado com imagem JPEG para implementação. O k-LSB de pixeis mais à direita foi utilizado para incorporar bits de MP3 em um pixel. Os pixeis são escolhidos de tal forma que a distorção na imagem seria minimizada devido à incorporação. Isso é implementado de tal forma que torna difícil concluir sobre a existência dos dados ocultos dentro da imagem. Uma técnica de meta-heurística *Cuckoo Search* foi usada para encontrar as soluções mais adequadas para a minimização [5].

Djaziri-Larbi, Zaien e Sevestre-Ghalila propuseram usar imagens GIF como um "canal de transmissão" para transmitir bits de som "ocultos" com menor distorção perceptual da imagem e sem alterar a portabilidade do formato GIF, por meio da ocultação de dados. Os bits inseridos não são nem secretos nem destinados a problemas de segurança. Eles devem ser reproduzidos por um reprodutor de áudio em sincronia com o reprodutor GIF para adicionar som à animação GIF. O processo de incorporação é um algoritmo de esteganografia baseado em luminância de baixa complexidade, que modifica ligeiramente as cores dos pixeis das imagens GIF para inserir os bits de som. A extração do áudio inserido é completamente cega: o áudio é extraído diretamente dos pixeis de cada imagem da capa. [6]

Rocha, Goldenstein, Costa e Chaves realizaram pesquisar das principais técnicas de esteganografia em imagens digitais da atualidade e desenvolver um software capaz de permitir a comunicação segura pela internet. [7]

Tendo isso em mente é necessário realizar um maior estudo da esteganografia em áudio.

2.4 Esteganografia em Arquivos de Áudio

Na esteganografia de áudio, o arquivo de áudio é usado como arquivo de capa para ocultar a mensagem secreta. O processo de esteganografia pode incorporar dados secretos em arquivos WAV, AU e MP3. Na esteganografia de áudio, podemos inserir informações em arquivos de som com a ajuda do Sistema Auditivo Humano (HAS). O HAS percebe o ruído aleatório aditivo e também as perturbações em um arquivo de som também podem ser detectadas. O processo de ocultação consiste em 2 etapas: Em primeiro lugar, os bits redundantes no arquivo de áudio são identificados. Em segundo lugar, dados secretos são incorporados substituindo esses bits redundantes com bits das mensagens. [8]

2.4.1 Tipos de Codificação

Codificação de Bit Menos Significativo

Neste método, os bits de mensagem secreta substituem o LSB de sequências binárias de cada amostra de arquivo de áudio digitalizado. Na codificação LSB, grande quantidade de dados pode ser codificada. É um método simples, rápido e popular para incorporar informações em arquivos de áudio. Mas a desvantagem desse método é que ele é vulnerável a ataques.

Codificação de Fase

Neste método, a fase de referência que representa os dados secretos substitui a fase do segmento de áudio inicial, ou seja, o sinal de áudio é criptografado usando Transformada Discreta de Fourier. A codificação de fase explora o fato de que o Sistema Auditivo Humano (HAS) não consegue reconhecer a mudança de fase no sinal de áudio, pois ele reconhece o ruído

Assim, nesta técnica, os bits de mensagem são codificados quando a fase se desloca no espectro de fase de um sinal digital, alcançando uma codificação inaudível em termos de relação de ruído sinal-para-percepção (SPNR). Como a codificação de fase codifica dados secretos apenas no primeiro segmento de sinal, a desvantagem desse método é que ele fornece baixa transmissão de dados. Assim, a codificação de fase é usada somente quando uma pequena quantidade de dados precisa ser ocultada como marca d'água.

Codificação de Dados em Eco

Nesse método, um eco é introduzido no sinal original e os dados secretos são incorporados no arquivo de áudio. Este método fornece alta taxa de transmissão de dados e alta robustez em comparação com outros métodos. Três parâmetros do sinal original são manipulados quando os dados são ocultados usando este método - amplitude inicial, offset e taxa de decaimento para que o eco não seja audível. Esse método não é tão popular por causa da baixa taxa de dados e segurança.

Codificação de Paridade

Neste método, um sinal é dividido em amostras separadas e cada bit de mensagem secreta é incorporado a partir do bit de paridade, evitando assim a quebra de um sinal em amostras individuais. O bit secreto a ser codificado é comparado com o bit de paridade de uma região selecionada, se eles não corresponderem, o processo inverte o LSB de uma das

amostras na região. Assim, o remetente tem mais opções na codificação do bit secreto. É a técnica robusta de ocultação de dados usando esteganografia de áudio.

Codificação em Espectro de Espelhamento

Este método espalha a informação secreta sobre o espectro de frequência do arquivo de som usando um código que é independente do sinal real. Assim, a largura de banda do sinal real é mais do que é realmente necessário para a transmissão. A vantagem deste método reside no fato de que fornece taxa de transmissão de dados moderada e alto nível de robustez, mas introduz ruído no arquivo de som.

2.5 Utilidades

A flexibilidade da esteganografia de áudio é o que a torna potencialmente poderosa. Os cinco métodos discutidos fornecem aos usuários uma grande quantidade de opções e tornam a tecnologia mais acessível a todos. Uma parte que deseja se comunicar pode classificar a importância de fatores como taxa de transmissão de dados, largura de banda, robustez e audibilidade de ruído e, em seguida, selecionar o método que melhor se adapta às suas especificações. Por exemplo, dois indivíduos que apenas querem enviar uma mensagem secreta ocasional para frente e para trás podem usar o método de codificação LSB que é facilmente implementado. Por outro lado, uma grande corporação que deseja proteger sua propriedade intelectual de "piratas digitais" pode considerar um método mais sofisticado, como codificação de fase, SS ou ocultação de eco. [4]

O método de análise estatística também pode ser usado em arquivos de áudio, já que a técnica de modificação do LSB também pode ser usada em sons. Exceto por isso, existem várias outras coisas que podem ser detectadas. Frequências altas e inaudíveis podem ser verificadas em busca de informações, e distorções ou padrões estranhos nos sons podem indicar a existência de uma mensagem secreta. Além disso, diferenças no eco do tom ou no ruído de fundo podem levantar suspeitas. [4]

Referências

[1] Rezende, Pedro A. D.: *Criptografia e segurança na informática*. 2017. 1

[2] Julio, Eduardo Pagani, Wagner Gaspar Brazil e Célio Albuquerque: *Esteganografia e suas aplicações*. Livro de Minicursos do SBSEG. Rio de Janeiro: Sociedade Brasileira de Computação, 7:54–102, 2007. 2

[3] Siper, Alan, Roger Farley e Craig Lombardo: *The rise of steganography*. Proceedings of Student/Faculty Research Day, CSIS, Pace University, 2005. 2, 3, 5

[4] Bandyopadhyay, Samir K, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee e Poulami Das: *A tutorial review on steganography*. Em *International conference on contemporary computing*, volume 101, páginas 105–114. Citeseer, 2008. 3, 4, 5, 8

[5] Gupta, Ankur e Ankit Chaudhary: *A metaheuristic method to hide mp3 sound in jpeg image*. Neural Computing and Applications, 30(5):1611–1618, 2018. 6

[6] Djaziri-Larbi, Sonia, Awatef Zaien e Sylvie Sevestre-Ghalila: *Voicing of animated gif by data hiding*. Multimedia Tools and Applications, 75(8):4559–4575, 2016. 6

[7] Rocha, Anderson, Siome Goldenstein, Heitor Costa e Lucas M Chaves: *Segurança e privacidade na internet por esteganografia em imagens*. Em *Webmedia & LA-Web–Joint Conference 2004*, 2004. 6

[8] Chugh, Gunjan e Priyanka Gaba: *Review on audio and video steganography techniques*. 2018. 6