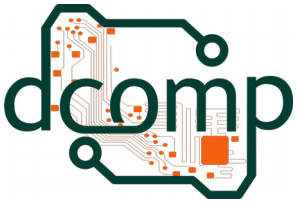
Universidade Federal do Espírito Santo
Centro de Ciências Agrárias – CCENS UFES
Departamento de Computação



Análise Forense
Esteganografia

Computação Forense
Site: http://jeiks.net
E-mail: jacsonrcsilva@gmail.com

Esteganografia

- A esteganografia é um dos ramos da criptografia;
- De origem grega, a palavra significa a arte da escrita escondida
  - estegano = esconder e
  - grafia = escrita
- A esteganálise é a arte de detectar mensagens escondidas nos mais diversos meios de comunicação.
- A esteganografia inclui um amplo conjunto de métodos e técnicas para prover comunicações secretas desenvolvidos ao longo da história.
- Dentre as técnicas se destacam:
  - tintas invisíveis, micropontos, arranjo de caracteres (*character arrangement*), assinaturas digitais e canais escondidos.

Esteganografia

- As aplicações de esteganografia incluem:
  - identificação de componentes dentro de um subconjunto de dados,
  - legendagem (*captioning*),
  - rastreamento de documentos e certificação digital (time-stamping) e
  - demonstração de que um conteúdo original não foi alterado (tamper-proofing).
- Entretanto, a esteganografia pode ser usada correta ou incorretamente.
- Há indícios recentes de que a esteganografia tem sido utilizada para divulgar imagens de pornografia infantil na Internet, além das mensagens de redes terroristas como a Al-Qaeda.

Terminologia

- Há três áreas de pesquisa:
  - no campo da esteganografia,
  - marcas dágua e
  - seriação digitais.

- Isso leva a uma certa confusão na terminologia.

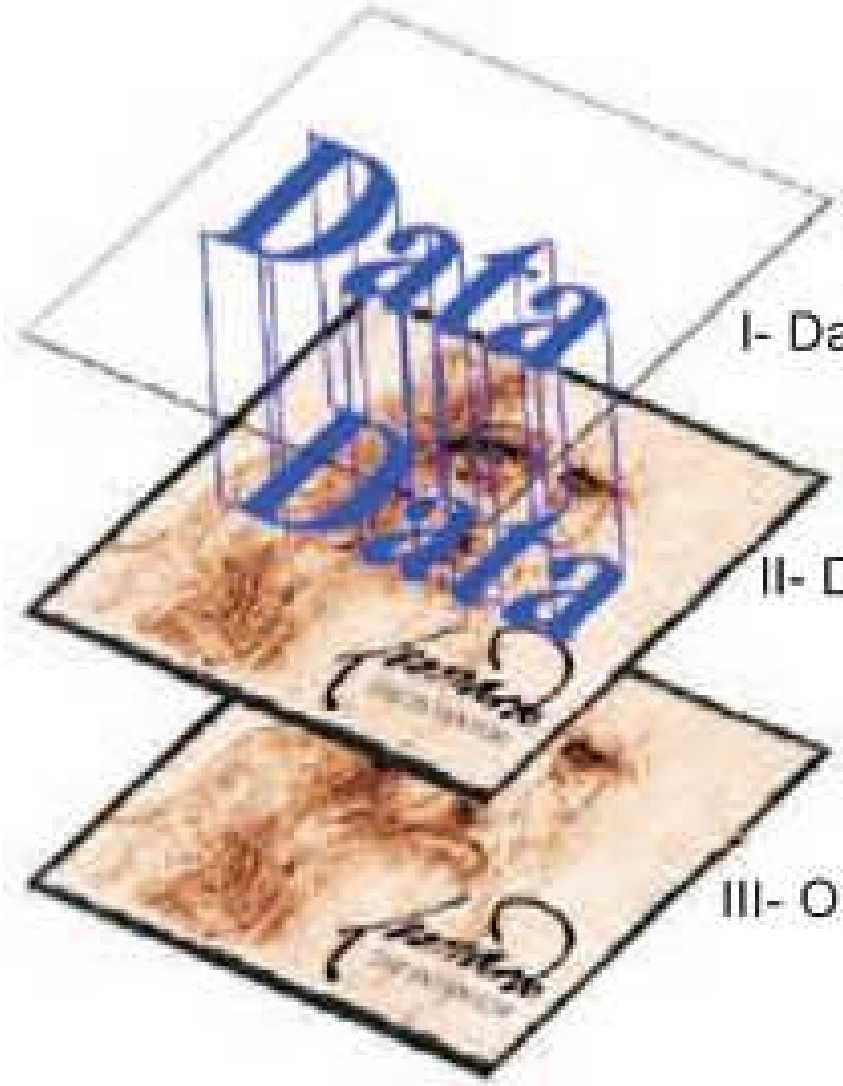
Terminologia

- principais termos utilizados nestas áreas:
  - dado embutido ou *embedded data*:
    - é o dado que será enviado de maneira secreta, normalmente em uma mensagem, texto ou figura;
  - mensagem de cobertura ou *cover-message*:
    - é a mensagem que servirá para mascarar o dado embutido. Esta mensagem de cobertura pode ser de áudio (*cover-audio*), de texto (*cover-text*) ou uma imagem (*cover-image*);
  - estego-objeto ou *stego-object*:
    - após a inserção do dado embutido na mensagem de cobertura se obtém o estego-objeto;

Terminologia

- principais termos utilizados nestas áreas:
  - estego-chave ou *stego-key*:
    - adicionalmente pode ser usada uma chave para se inserir os dados do dado embutido na mensagem de cobertura. A esta chave dá-se o nome de estego-chave;
  - número de série digital ou marca *fingerprinting*:
    - consiste em uma série de números embutidos no material que será protegido a fim de provar a autoria do documento.

Escondendo dados em uma imagem



I- Dado a ser escondido (dado embutido)

II- Dados são embutidos na imagem com uso de uma chave (estego-key)

III- O estego-objeto é criado contendo a informação escondida

Esteganografia

- A esteganografia pode ser dividida em dois tipos:
  - Técnica:
    - Se refere às técnicas utilizadas quando a mensagem é fisicamente escondida. Exemplo: escrever uma mensagem em uma tábua de madeira e cobri-la com cera, como faziam alguns povos na antiguidade.
  - Linguística:
    - Se refere ao conjunto de técnicas que se utilizam de propriedades linguísticas para esconder a informação, como por exemplo *spams* e imagens.

Sistemas de Marcação

- Os sistemas de marcação
  - visam proteger a propriedade intelectual sobre algum tipo de mídia (eletrônica ou não).
- São conhecidos também como *watermarking* (marca d'água).
- Os sistemas de marcação não pertencem ao ramo da esteganografia.
- Ambos pertencem a uma área de pesquisa conhecida como ocultamento da informação ou *information hiding*.

Sistemas de Marcação

- O sistema de marcação tipo marca d'água se refere a métodos que escondem informações em objetos que são robustos e resistentes a modificações.
- Assim, seria impossível remover uma marca d'água de um objeto sem alterar a qualidade visual do mesmo.
- Por outro lado a esteganografia se propõe a esconder uma informação em uma imagem de cobertura.
- Se a imagem for destruída ou afetada, a mensagem é perdida.
- Uma outra diferença clara entre esteganografia e técnicas de marca d'água é que enquanto o dado embutido da esteganografia nunca deve ficar aparente, a marca d'água pode ou não aparecer no objeto marcado, dependendo da aplicação que se queira atender.

Sistemas de Marcação

- Classificação dos Sistemas de Marcação:
  - Quanto a sua robustez:
    - Robustos: são aqueles em que mesmo após a tentativa de remoção a marca permanece intacta;
    - Frágeis: são os sistemas em que qualquer tentativa de modificação na mídia acarreta a perda da marcação. É muito útil para verificação de cópias ilegais.

      Quando se copia um objeto original, a cópia é feita sem a marca.
  - Quanto a sua aparência:
    - De marcação imperceptível: são os sistemas onde a marca encontra-se no objeto ou material, porém não é visível diretamente;
    - De marcação visível: neste sistema a marca do autor deve ficar visível para comprovar a autoria visualmente. Exemplo: marcas d ´água em cédulas de dinheiro e em selos.

Aspectos Históricos

- A esteganografia é uma arte antiga, com suas origens na antiguidade.
- Os gregos já a utilizavam para enviar mensagens em tempos de guerra.
- Uma das “Estórias de Herodotus”:
  - Um mensageiro se disfarçou de caçador para enviar uma mensagem ao rei escondendo-a dentro de uma lebre. Como o mensageiro estava disfarçado, passou despercebido pelos portões do palácio e o rei pôde receber a mensagem.

Aspectos Históricos

- Mensagens também foram enviadas através de escravos de confiança.
  - Alguns reis raspavam as cabeças de escravos e tatuavam as mensagens nelas. Depois que o cabelo crescesse, o rei mandava o escravo pessoalmente com a mensagem. Ninguém suspeitaria onde a mensagem se encontrava, a menos que soubesse exatamente onde procurar. Neste caso o segredo com a localização da mensagem deveria ser mantido.
- Outro exemplo de esteganografia na Grécia antiga:
  - Eram furados buracos em livros acima das letras que formavam a mensagem desejada. Quando o destinatário recebesse o livro poderia procurar pelos buracos sobre as letras para reconstruir as mensagens. Para quem não soubesse do código, o livro pareceria ter apenas seu conteúdo escrito pelo autor.

Aspectos Históricos

- Os chineses:
  - Escreviam mensagens em finas folhas de papel de seda que eram depois enroladas como uma bola e cobertos com cera. Esta bola era então escondida em algum lugar do corpo ou engolida para prevenir sua detecção.
- Os egípcios:
  - Usavam ilustrações para cobrir as mensagens escondidas. O método de escrita egípcio conhecido como hieróglifo era uma técnica comum para esconder mensagens. Quando um mensageiro egípcio era pego com um hieróglifo que continha algum código, o inimigo não suspeitava e a mensagem podia ser entregue sem problemas ao destinatário.

Aspectos Históricos

- Em 1499, um monge chamado Tritheimius escreveu uma série de livros chamados “Steganographia” nos quais ele descreveu várias técnicas diferentes.
- Uma delas, desenvolvida na idade média, foi a grelha de Cardano, criada por Girolamo Cardano

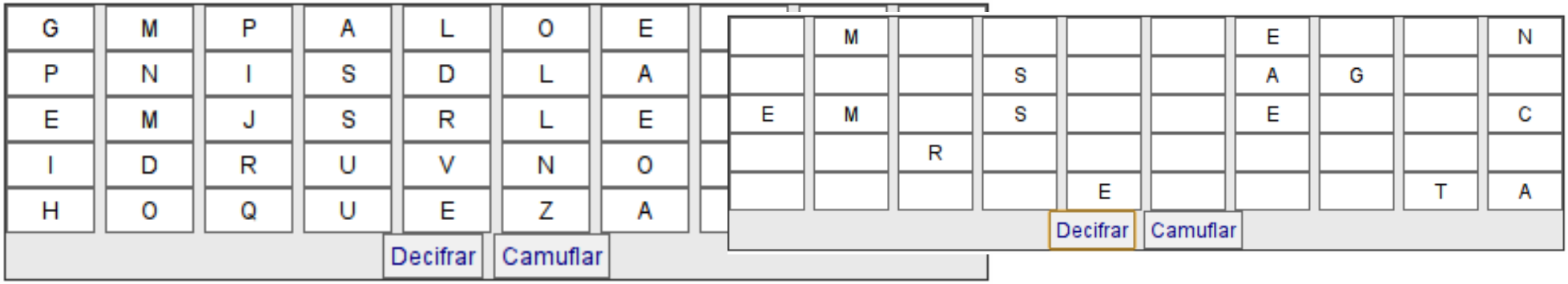
Steganographia

Tritheimius

Girolamo Cardano

Grelha de Cardano

- A grelha de Cardano:
  - folha de material rígido com aberturas retangulares da altura de uma linha de texto e de comprimento variável, colocadas em intervalos irregulares.
- O remetente coloca esta matriz sobre a folha de papel e escreve a mensagem secreta nas aberturas.
- Depois, retira a grelha e preenche os espaços vazios com letras quaisquer.
- O destinatário simplesmente coloca uma grelha igual sobre o texto recebido para fazer aparecer a mensagem recebida.



Tintas Invisíveis

- Os primeiros experimentos começaram na idade média.
- Giovanni Porta escreveu vários livros de história natural.
  - Dentro destes livros estavam receitas de tintas secretas que poderiam ser usadas para escrever sobre a pele humana e outras superfícies.
  - Este tipo de tinta foi desenvolvido e usado mais tarde no fim dos anos de 1700 e foi a chave para comunicações secretas.
- Tintas invisíveis também foram muito usadas em esteganografia nos tempos mais modernos e são utilizadas até hoje.
  - Utilizadas por espiões durante a primeira e a segunda grande guerra com o desenvolvimento de reagentes químicos específicos para cada tinta.
  - Textos eram escritos em jornais, revistas ou livros com tintas invisíveis para serem passados de forma segura até seus destinatários.
- Uma outra utilização era escrever a mensagem com tinta invisível sobre um papel, cortá-lo em alguns pedaços e depois rejuntá-los no destinatário.

Cifradores Nulos

- Cifradores nulos
  - são mensagens nas quais certas letras devem ser usadas para formar a mensagem e todas as outras palavras ou letras são consideradas nulas.
- Para ouso do cifrador nulo, ambos os lados da comunicação devem usar o mesmo protocolo de uso das letras que formam a mensagem.
- Um exemplo de um código utilizando cifrador nulo é mostrado abaixo:

  “News Eight Weather: tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The highways are knowingly slippery. Highway evacuation is suspected. Police report emergencies in downtown ending near Tuesday”.
- Usando as primeiras letras de cada palavra o texto que aparece é:

  “Newt is upset because he thinks he is president”.

Micro-pontos

- Um micro-ponto é
  - uma fotografia da mensagem secreta que deve ser entregue. Com a tecnologia avançando rapidamente, é possível tirar uma foto de uma mensagem e reduzi-la a uma fotografia circular de 0,05 polegadas ou 0,125 cm de diâmetro.
- Esta minúscula fotografia é então colada em um sinal de pontuação de uma frase ou no “pingo” de uma letra “i” de uma outra mensagem qualquer que será entregue.
- Somente aqueles que sabem onde procurar o micro-ponto poderão detectar sua presença.

Estado da Arte

- As imagens são os tipos de arquivos mais utilizados para esteganografia;
- Podem ser armazenadas:
  - em bitmap direto (como BMP),
  - em formato comprimido (como JPEG) ou
  - em palheta de cores: GIF;
- O ocultamento de informações é realizado:
  - Ou no domínio espacial: utilização de máscaras, que são pequenas matrizes bidimensionais. Os valores de seus coeficientes determinam o objetivo a ser alcançado durante o processamento.
  - Ou no domínio de frequência: tem suas técnicas fundamentadas no teorema da convolução, que é uma das propriedades da transformada de Fourier.

Estado da Arte

- Em termos de esquemas de inserção, vários métodos podem ser usados, como:
  - Inserção no bit menos significativo (LSB);
  - Técnicas de filtragem e mascaramento;
  - Algoritmos e transformações; e
  - outras técnicas de substituição, adição ou ajuste.
- Cada uma destas técnicas pode ser aplicada à imagens, com graus variados de sucesso.

Requisitos

- Três requisitos importantes para qualquer sistema esteganográfico:
  - Segurança:
    - Manter o conteúdo escondido tanto perceptivelmente quanto por meios estatísticos. Em outras palavras, tenta-se criar uma blindagem contra um algoritmo de suspeita para não levantar uma suspeita.
  - Carga útil:
    - Possuir capacidade suficiente para armazenar a informação escondida que deseja-se comunicar.
  - Robustez:
    - Embora não seja importante ser robusto contra ataques, 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.

Bit Menos Significativo

- Técnicas baseadas na modificação dos bits menos significativos dos valores de pixel no domínio espacial.
- Também chamadas de LSB (*Least Significant Bit*);
- A inclusão de LSB simples é suscetível a processamento de imagem, especialmente a compressão sem perda.
- Podem ser aplicadas a cada pixel de uma imagem codificada em 32bits por pixel.
  - Estas imagens possuem seus pixeis codificados em quatro bytes: canal alfa (*alpha transparency*); vermelho (*red*); verde (*green*); e azul (*blue*).
  - Seleciona-se um bit (o menos significativo) em cada byte do pixel para representar o bit a ser escondido sem causar alterações perceptíveis na imagem.
- Constituem a forma de mascaramento em imagens mais difícil de ser detectada, pois podem inserir dados em pixeis não sequenciais, tornando complexa a detecção.

Filtragem e Mascaramento

- As técnicas de filtragem e mascaramento:
  - são mais robustas que LSB;
  - Geram estego-imagens imunes a compressão e recorte;
  - São técnicas mais propensas a detecção.
  - Trabalham com modificações nos bits mais significativos das imagens.
  - Não são eficazes em imagens coloridas.
- Modificações em bits mais significativos de imagens em cores geram muitos artefatos tornando as informações mais propensas a detecção.
- Estas técnicas são semelhantes a marca d'água visível
  - Os valores de pixel em áreas mascaradas são aumentados ou diminuídos por um pouco de porcentagem.

Algoritmos e Transformações

- Essas técnicas conseguem 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.
- Os dados são embutidos no domínio de transformação, sendo escondidos em áreas mais robustas, espalhadas através da imagem inteira.
- Fornecem melhor resistência contra processamento de sinal.
- Configuram-se como as mais sofisticadas técnicas de mascaramento de informações conhecidas, embora sofisticação nem sempre implique em maior robustez aos ataques de esteganálise.

Espalhamento de Espectro

- Na técnica de espalhamento de espectro, os dados escondidos são espalhados ao longo da imagem de cobertura.
- Uma stego-chave é usada para selecionar randomicamente os canais de frequência.
- A *White Noise Storm* é uma ferramenta popular usando esta técnica.
- Uma forma de utilizar:
  - Os dados embutidos são primeiramente modulados com pseudo ruído e então a energia é espalhada sobre uma faixa de frequência larga, alcançando somente um nível muito baixo de força de inclusão. Isto é valioso para alcançar a imperceptibilidade.

Esteganografia em vídeo

- Quando informações são escondidas dentro de um vídeo, normalmente é usado o método da DCT (transformada cosseno direta).
- Muito similar a esteganografia em imagens,
  - exceto pelo fato de que as informações são escondidas em cada *frame* do arquivo de vídeo.
- Da mesma forma que nas imagens,
  - quanto maior for a quantidade de informação a ser escondida no vídeo,
  - maior será a possibilidade do método esteganográfico ser percebido.

Esteganografia em áudio

- Esconder imagens em sinais de áudio é algo desafiante,
  - O sistema auditivo humano (SAH) pode trabalhar em uma faixa muito grande de frequências.
  - O SAH pode captar até um bilhão de potências diferentes de sinais (altura) e até mil frequências de sinais distintas.
  - A sensitividade a ruído também é muito apurada. Uma perturbação em um arquivo de som pode ser detectada facilmente.
- Porém, o SAH não consegue:
  - Fazer diferenciação de tudo que recebe. Os sons mais altos tendem a mascarar sons mais baixos.
  - Perceber um sinal em fase absoluta, somente em fases relativas.
  - E algumas distorções do ambiente muito comuns que são simplesmente ignoradas pelo ouvido na maioria dos casos.
- As técnicas de esteganografia exploram muitas destas “vulnerabilidades” do ouvido humano.
- Porém, sempre têm que levar em conta a extrema sensibilidade do SAH.

Técnicas de Esteganálise

- Grande parte das técnicas de esteganografia possuem falhas ou inserem padrões que podem ser detectados.
- Algumas vezes, basta um agressor fazer um exame mais detalhado destes padrões gerados para descobrir que há mensagens escondidas.
- Outras vezes, o processo de mascaramento de informações é mais robusto e as tentativas de detectar ou mesmo recuperar ilicitamente as mensagens podem ser frustradas.
- A pesquisa de métodos para descobrir se há alguma mensagem escondida por esteganografia é chamada de **esteganálise**.

Técnicas de Esteganálise

- Existem diversas abordagens para se detectar a presença de conteúdo escondido em imagens digitais.
- Estas abordagens podem ser divididas em três tipos:
  - Ataques aurais,
  - Ataques estruturais e
  - Ataques estatísticos.

Técnicas de Esteganálise

- Ataques aurais:
  - Consistem em retirar as partes significativas da imagem como um meio de facilitar aos olhos humanos a busca por anomalias na imagem.
  - Um teste comum é mostrar os bits menos significativos da imagem.
  - Câmeras, scanners e outros dispositivos sempre deixam alguns padrões nos bits menos significativos.

Técnicas de Esteganálise

- Ataques estruturais:
  - A estrutura do arquivo de dados algumas vezes muda assim que outra mensagem é inserida.
  - Nesses casos, um sistema capaz de analisar padrões estruturais seria capaz de descobrir a mensagem escondida.
  - Exemplo:
    - Se mensagens são escondidas em imagens indexadas (baseadas em paletas de cores),
    - pode ser necessário usar diferentes versões de paletas.
    - Este tipo de atitude muda as características estruturais da imagem de cobertura.
    - Logo as chances de detecção da presença de uma mensagem escondida aumentam.

Técnicas de Esteganálise

- Ataques estatísticos:
  - os padrões dos pixeis e seus bits menos significativos frequentemente revelam a existência de uma mensagem secreta nos perfis estatísticos.
  - Os novos dados não têm os mesmos perfis esperados.
  - Muitos dos estudos de Matemática e Estatística têm por objetivo classificar se um dado fenômeno ocorre ao acaso.
  - Técnicas estatísticas também podem ser usadas para determinar seuma dada imagem e/ou som possui alguma mensagem escondida.
  - Na maioria das vezes, os dados escondidos são mais aleatórios que os dados que foram substituídos no processo de mascaramento.

Trabalhando com esteganografia...