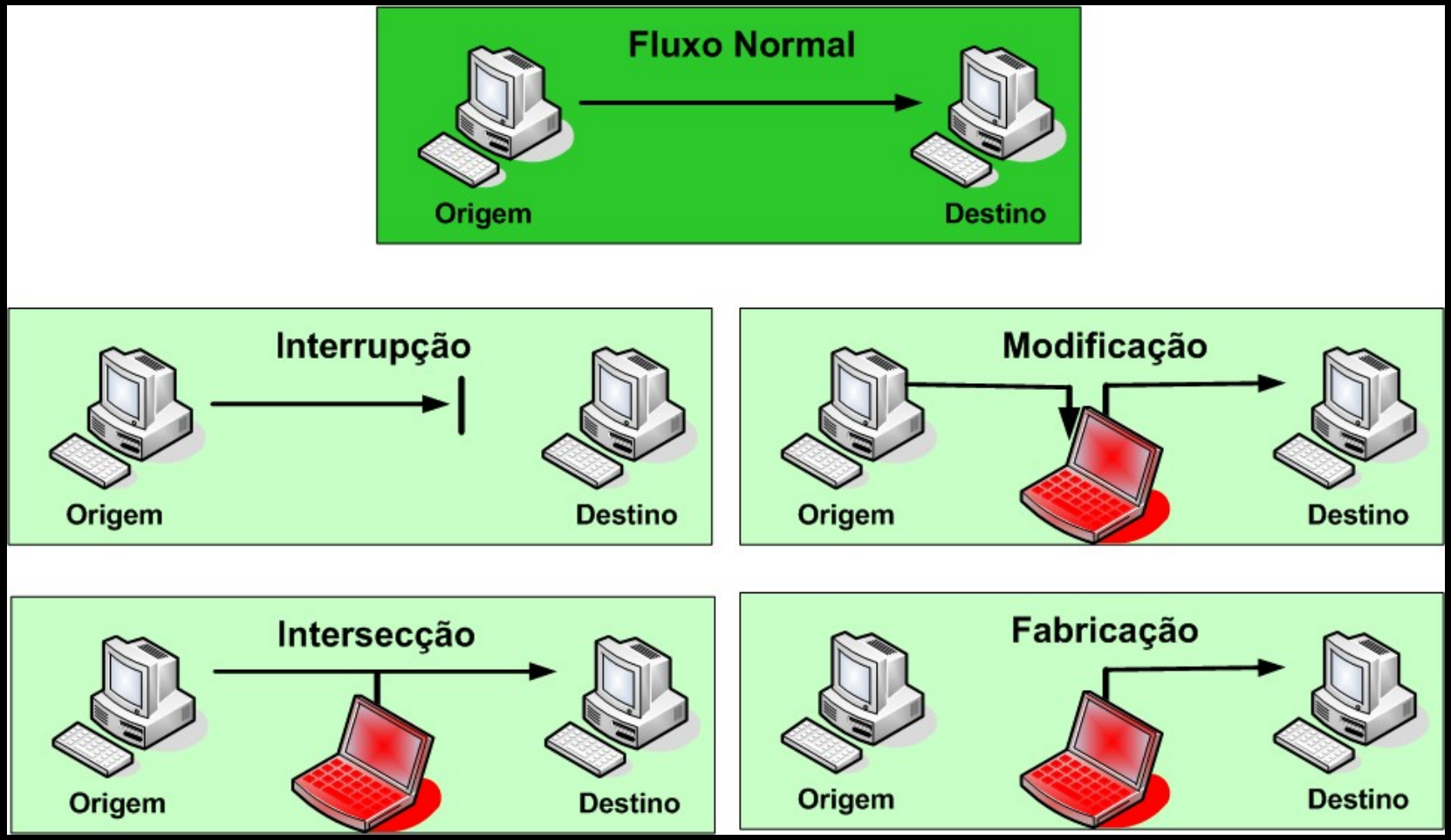
Esteganografia Digital para transmissão oculta de mensagens

Diego Fiori de Carvalho
dfiori@icmc.usp.br
stoa.usp.br/diegofdc

Sumário

- Motivação
- Histórico
- Definições
- Classificação
- Esteganografia Técnicas
- Imagens/Áudio/Vídeos
- Canais Ocultos
- Outras Aplicações
- Links

Comunicação



Projetos Invasão Privacidade

- *Echelon*
- *PATRIOT (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism)*
- *Carnivore (*Programa do FBI para vigiar o correio eletrônico*)*

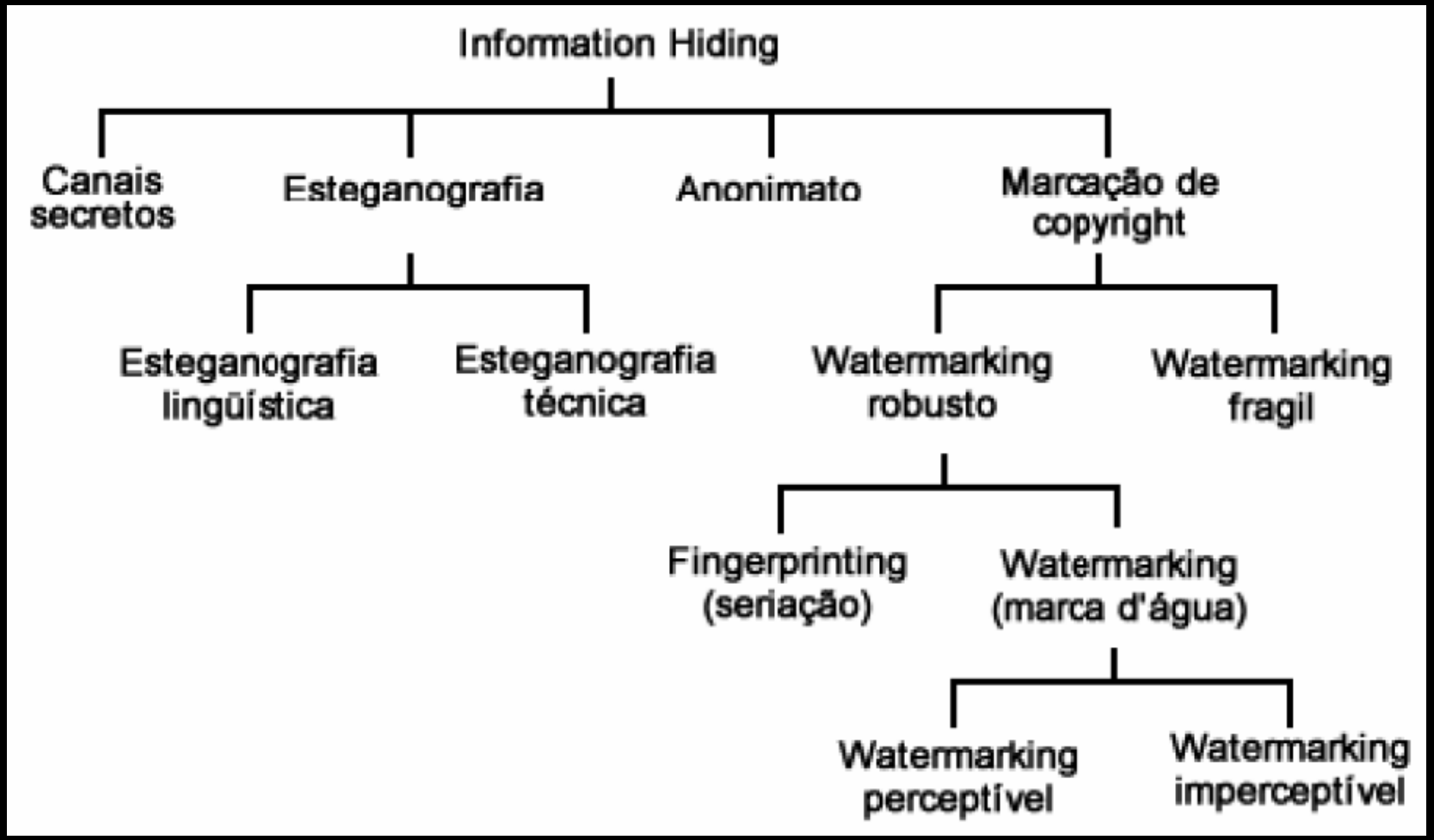
História

- Heródoto: “As histórias” Grécia X Persas 500 A.C
  - Atenas e Esparta contra Xerxes
  - Demerato : Jovem grego na Pérsia
- Desafio: Como comunicar a Grécia das intenções de Xerxes sem ser descoberto?
  - Tabuletas de madeira com mensagem secreta revestidas de cera.
- Outros exemplos: Uso de seda pelos chineses

Definições

- Esteganografia: É uma palavra de origem grega, onde *Stegano* significa escondido ou secreto e *Grafia*: escrita ou desenho.
- Criptografia X Esteganografia

Classificação



Esteganografia

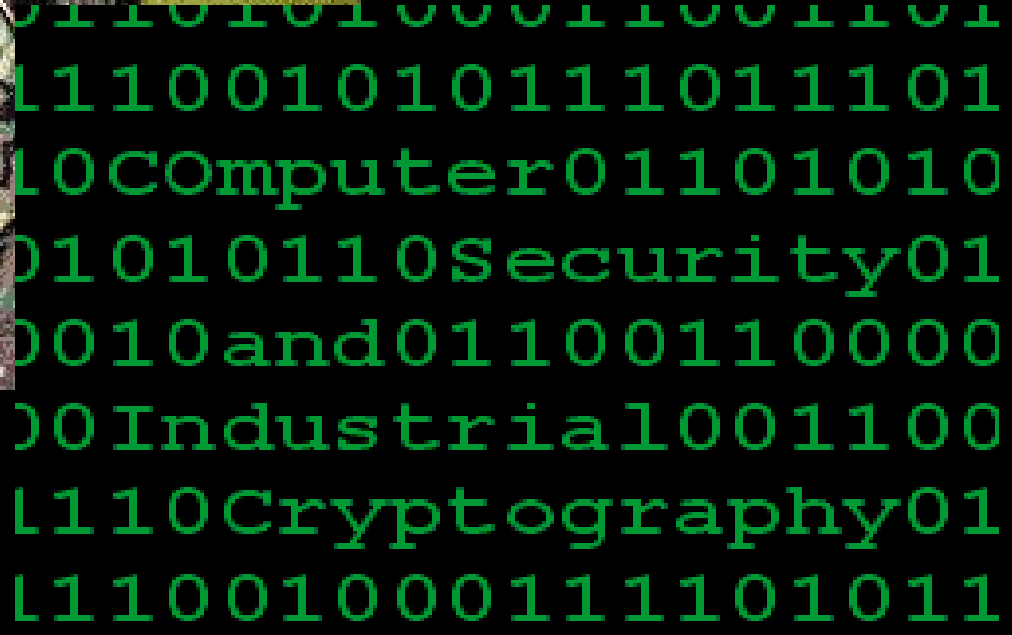
- A *esteganografia* apresenta-se como uma tecnologia apta a auxiliar as pessoas a aumentarem sua privacidade
- Juntamente com a criptografia, os cidadãos têm em mãos uma forma robusta e altamente eficiente para manter suas informações íntegras e protegidas

Stego Imagens

- Motivação

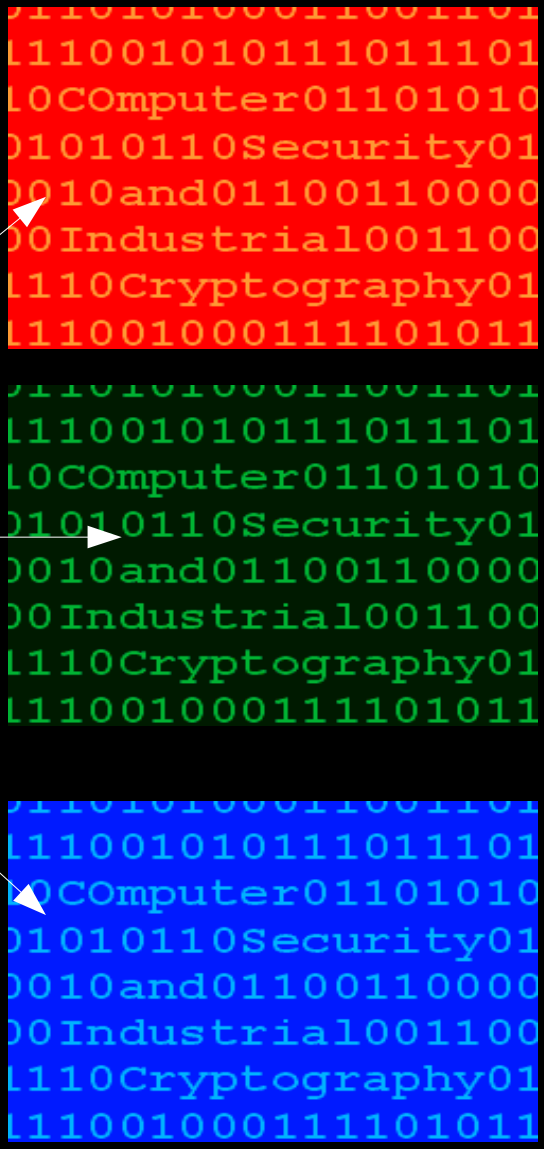
Stego Imagens

- Motivação



Stego Imagens

- Motivação



Stego Imagens

" Tenho também importante mensagem para nossos jovens, nesse período difícil que atravessamos. Vocês devem levantar bem alto a bandeira da Jihad contra os sionistas. Vocês são os legítimos sucessores de nossos valentes ancestrais. A propósito de nossos jovens, é bom saber que eles acreditam no paraíso após a morte. Eles sabem que tomar parte na luta contra os infiéis não abreviará seus dias. E que estar ausente dela não tornará seus dias mais longos. Nossos jovens sabem muito bem o significado dos versos: Se a morte é certa, então é uma vergonha morrer covardemente. Quem não morrer pela espada, morrerá por outra razão....."

Nomenclatura

- **Ocultamento de dados (*information hiding*)**
  - dado embutido (*embedded data*)
  - mensagem de cobertura (*cover-message*)

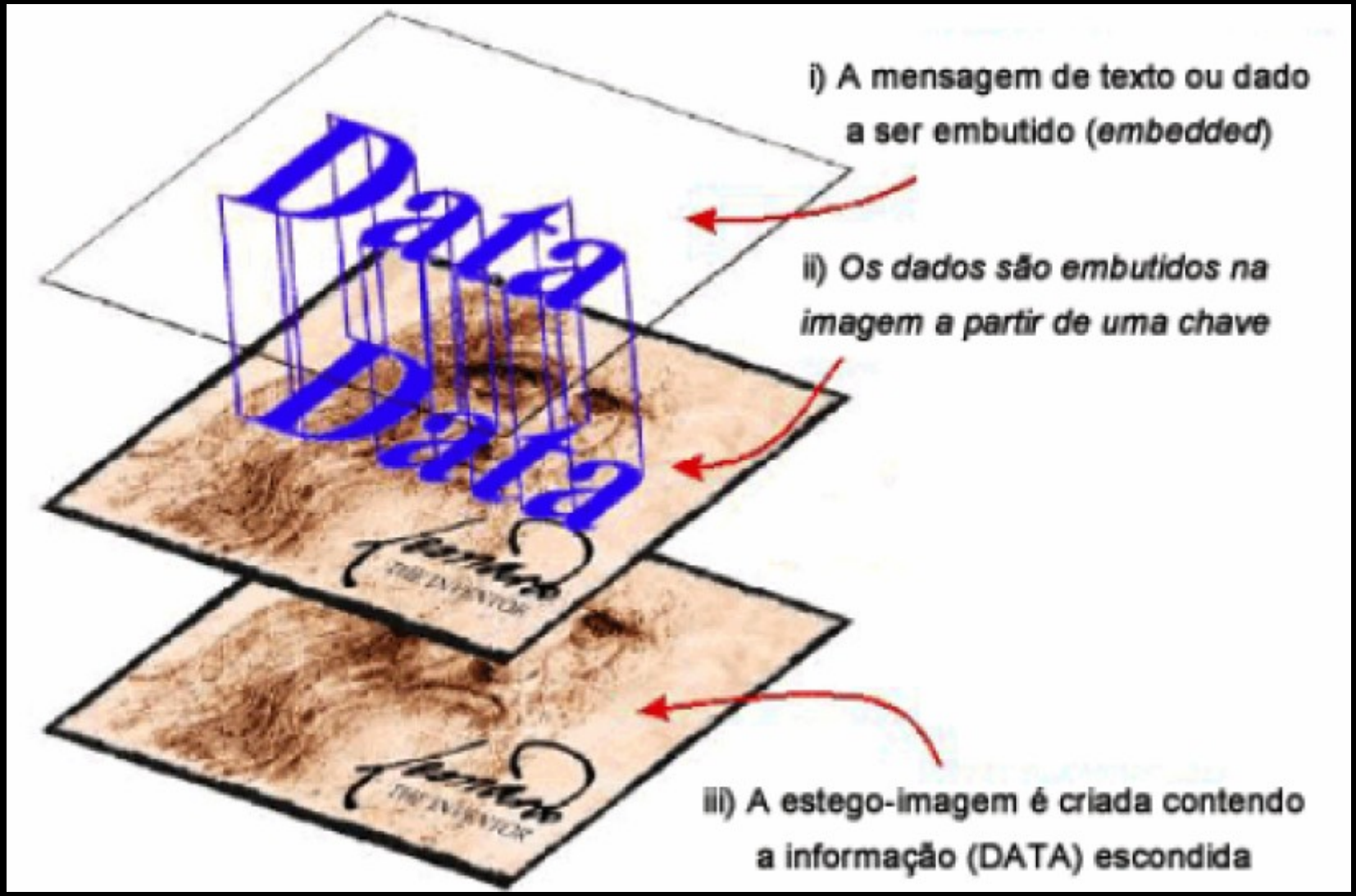
ou

  - imagem de cobertura (*cover-image*)

ou

  - áudio de cobertura (*cover-audio*)
  - texto de cobertura (*cover-text*)
  - estego-objeto (*stego-object*)
  - estego-imagem
  - estego-chave (*stego-key*)

Nomenclatura



Esteganografia Técnicas

- Principais algoritmos de esteganografia digital são baseados na substituição de componentes de ruído de um objeto digital por uma mensagem secreta pseudo-randômica
- O estego-objeto gerado pode ser dividido em:
  - *stream cover*

    Formado por um *stream* de dados contínuos como,por exemplo, uma transmissão telefônica
  - *random access cover*

    Pode ser um arquivo do formato “.WAV, .JPG”

Esteganografia Técnicas

- ***Stream covers***
  - Não se pode identificar os tamanhos dos dados escondidos nem onde estes começam ou terminam no objeto de cobertura
  - A sua geração é feita a partir de um *keystream generator*, algo como uma chave de criptografia que diz em que ordem os bits devem ser inseridos e recuperados
  - Técnica é conhecida como método do intervalo randômico

- ***Random access cover***
  - Permite ao emissor da mensagem colocar os dados em qualquer ordem no objeto de cobertura e também saber onde é o início e o fim da mensagem escondida
  - Freqüentemente, os bits de cobertura são os menos significativos do objeto de cobertura (LSB)

Esteganografia Técnicas

- Random Access Cover
  - Técnicas para Imagens
    - LSB (Least Significant Bit) Inserção no bit menos significativo
    - Técnicas de filtragem e mascaramento
    - Algoritmos e transformações

Esteganografia Técnicas

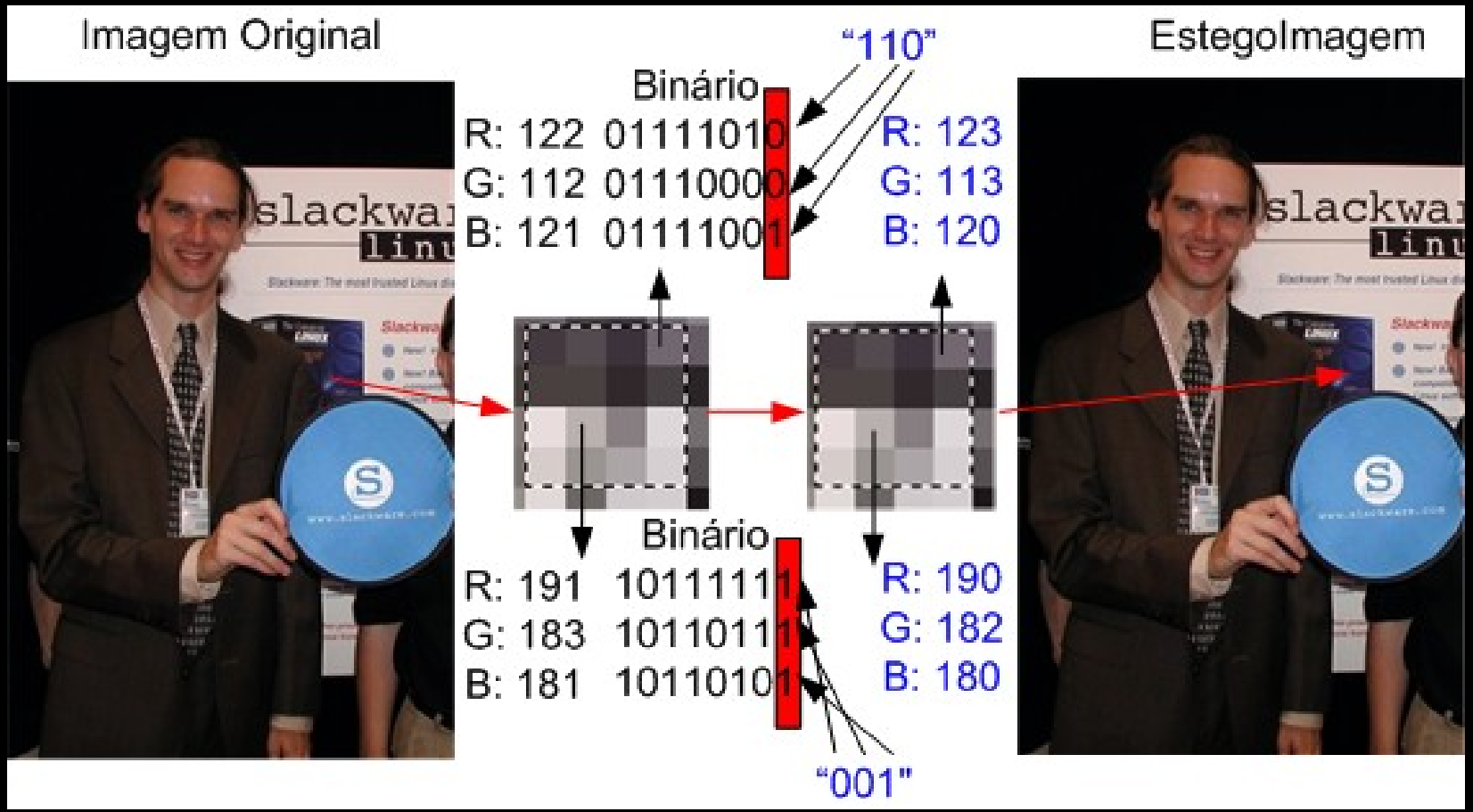
- Random Access Cover
  - Áudio
    - Apesar de ser tão poderoso SAH para captar sinais e freqüências, não consegue fazer diferenciação de tudo que recebe:
      - Sons mais altos tendem a mascarar sons mais baixos
  - Vídeo
    - Mais quadros para ocultamento de dados -> Maior qtde de informação AVI
    - Problemas com Compressão temporal: MPEG-1,MPEG-2, MPEG-4
    - MPEGLets em MPEG-4 via API MPEG-J

LSB

- Como exemplo da grande quantidade de dados que podem ser escondidos, suponha uma imagem com tamanho de 1024 por 768 pixels
- Total de 786.432 pixels
- Como cada pixel possui 4 bytes na sua codificação, têm-se 4 bits para o uso de técnicas baseadas em LSB
- Assim, existe uma possibilidade de esconder cerca de 390KB de dados neste objeto de cobertura

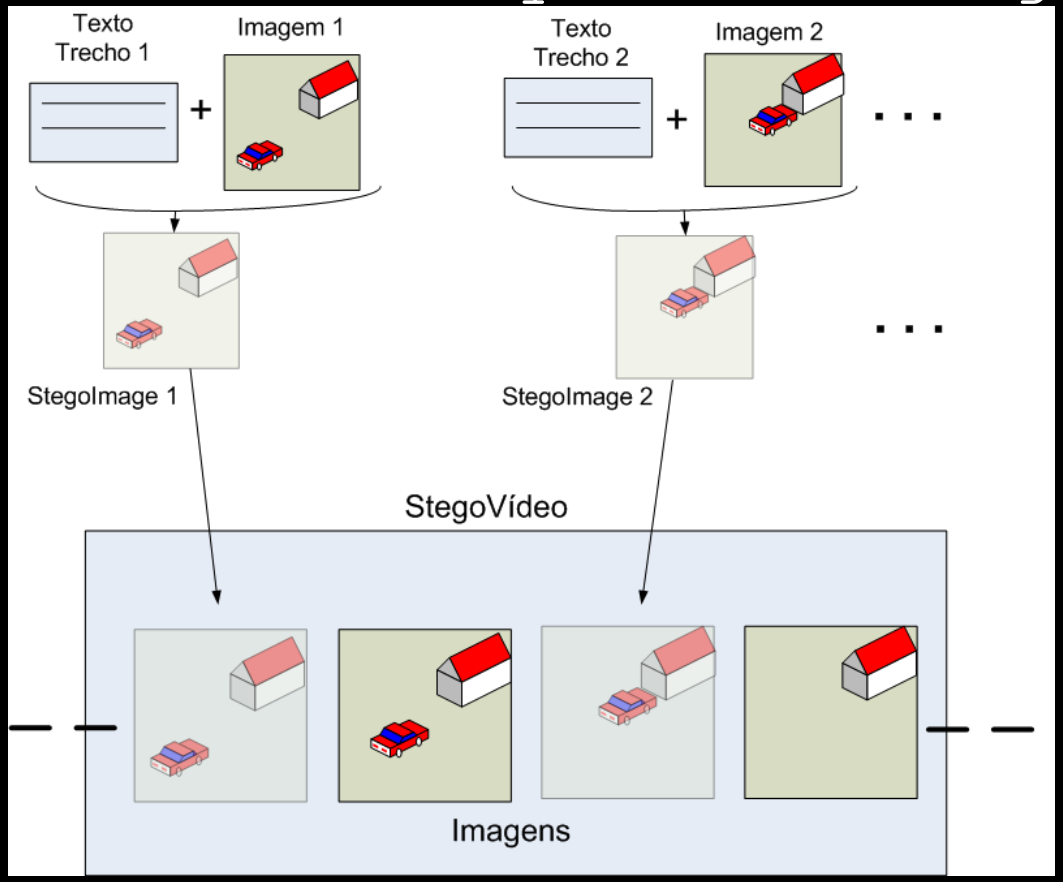
JPEG-JSTEG

- LSB: Least Significant Bit

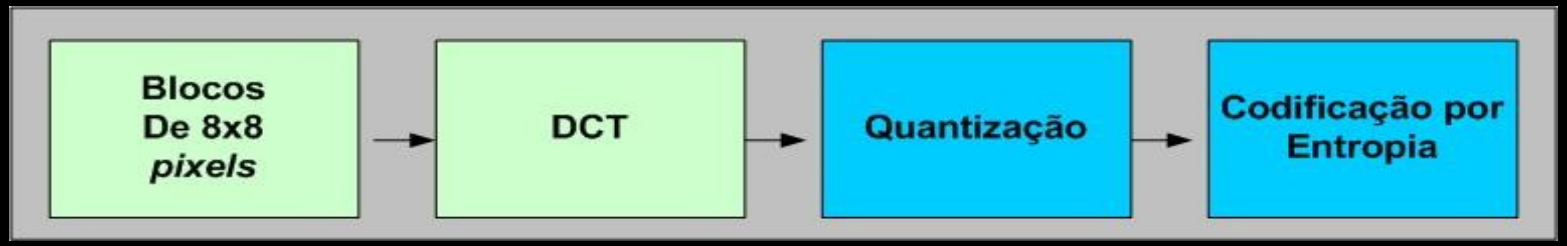


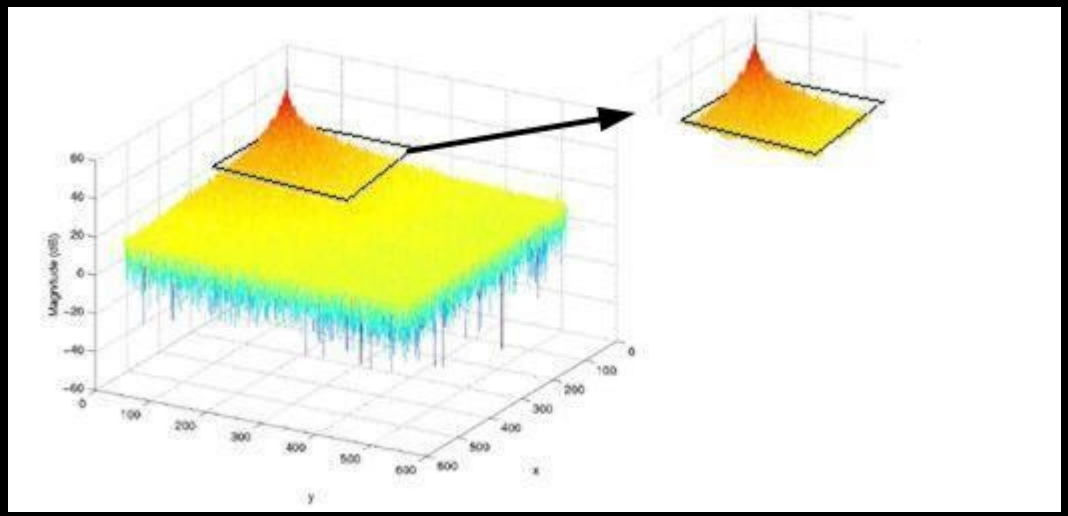
Esteganografia em Vídeos ?

- Vídeo: 24/30 quadros/segundo



Inserção LSB JPEG-JSTEG





Threshold das freqüências mais altas
Após a aplicação da DCT.

JPEG-JSTEG

Utilizando CJPEG e DJPEG para Esteganografia

Para esteganografar textos nas imagens utilizamos o comando CJPEG e para a recuperação do texto esteganografado é utilizado o comando DJPEG. Para efetuar tal operação basta usar e abusar da opção -steg, respeitando a seguinte sintaxe de execução:

```
# cjpeg -steg (arquivo txt) (imagem) > (stegoimagem)
```

Para testar, crie com seu editor de textos preferido (vim, pico, emacs) um arquivo txt, denominado teste.txt e aplique este comando sobre uma imagem .gif seguindo o exemplo abaixo:

```
# cjpeg -steg teste.txt imagem.gif > stegoimagem.jpg
```

Para realizar a desesteganografia, utilize o comando djpeg, como pode ser visualizado abaixo:

```
# djpeg -steg messagem stegoimagem.jpg > imagem.gif
```

Dependendo do tamanho da imagem, você facilmente poderá incluir folhas de texto no interior das mesmas.

Canais Ocultos

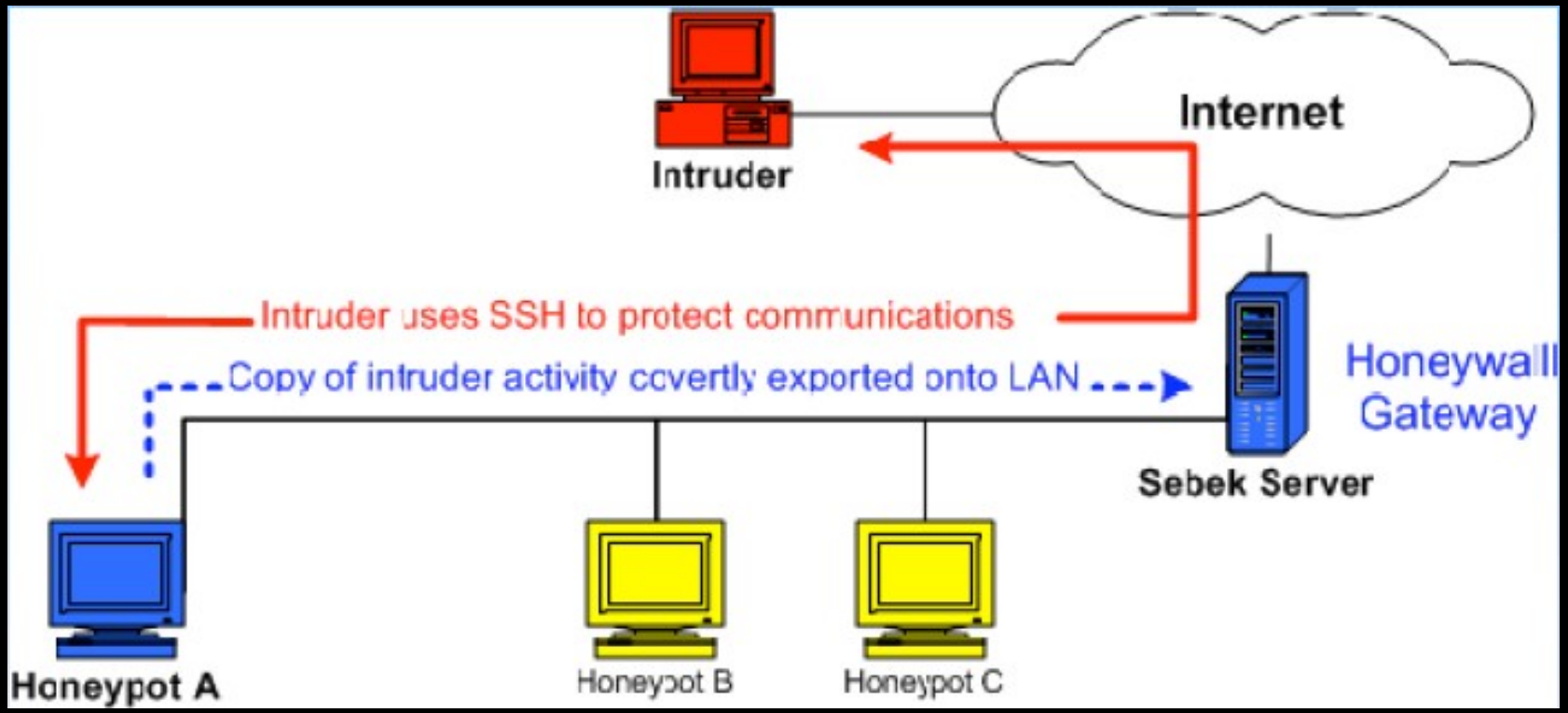
- Stream Covers
  - Um covert channel é um canal de comunicação que permite a um processo transmitir informação de uma forma que viola a política de segurança do sistema
  - Transferência de informação através de um canal escondido
    - Ocultar informação na rede

Canais Ocultos

- Exemplos
  - Túneis ICMP
  - Túneis DNS
  - Túneis HTTP
  - TCP/IP Headers

Canais Ocultos

- Know your enemy - Sebek



Túneis ICMP

- ICMPTX
- Itun
- PingTunnel
- Ptunnel

Túneis DNS

- Porque DNS?
  - Normalmente liberado em firewalls
- Funcionamento (OzymanDNS)
  - Envio de pacotes
  - Nome DNS comporta até 253 caracteres 63 caracteres entre os pontos (.)

Túneis DNS

- Codificação de informação usando base32
  - Um caracter para cada 5 bits (a-z, 0-6) 180 caracteres (3 grupos de 60) separados por pontos = 180 *5 = 900 bits = 112 bytes por consulta

Exemplo:

```
ajabdbcctvaojbz55mqwe224ceyeltkbhyaasncpljgc53pirtsmuz
ahcjrw.uujca7ytd3tifmmglrcsl65r3w3ba4mixix6nemd6eulfy2
as62xmff3zecv.ttivj2trx642zlrgpbwo2f2glnxk7yxyu3pfeiuvga
vc7mijpqn5sh4j.63034-0.id-1187.up.foo.com
```

Problemas

- Como o administrador de redes bloqueia este tipo de práticas?
  - Detectar e bloquear covert channels e comunicação via esteganografia é uma tarefa complexa. Normalmente é necessário saber o que se está procurando

Detecção

- Esteganografia
  - Bloquear anexos em e-mails > X MB?
  - Esteganálise
- Covert Channels
  - Verificar anomalias em cabeçalhos IP, TCP, ICMP
  - Verificar desvios de tráfego normal (EtherApe, IDS estatístico)
  - Verificar conteúdo de tráfego ICMP (Ex: ping)
    - Magic numbers (ex: 0xD5200880 - ptunnel)
  - Verificar conteúdo de cabeçalhos HTTP

Outras Aplicações
Esteganografia

- Comunicação Oculta
- Militares
- Economia de Banda
- Imagens Médicas: DICON
- Copyright
- Câmera fotográfica segura

Links

- MP3 Stego
  http://www.petitcolas.net/fabien/steganography/
- Dicas-L JPEG-JSTEG
  http://www.dicas-l.com.br/dicas-l/20061225.php
- Material sobre Esteganografia
  http://stoa.usp.br/diegofdc/
- Esteganálise - OutGuess
  http://www.outguess.org/detection.php
- Phrack - ICMP Tunneling

  http://www.phrack.org/issues.html?issue=49&id=15#article
- Covert Channels in SBSEG2007 - Ivo Peixinho
  http://sbseg2007.nce.ufrj.br/Minicurso-PDF.htm