APRESENTAÇÃO

Segurança da Informação

Esteganografia

Prof. MSc. Luis Gonzaga
luis.gonzaga@pucpr.br

Consegue identificar algo diferente na imagem?

O que é Esteganografia?

O que é Esteganografia?

- Estudo e prática da utilização de técnicas para ocultar a existência de uma mensagem dentro de outra.

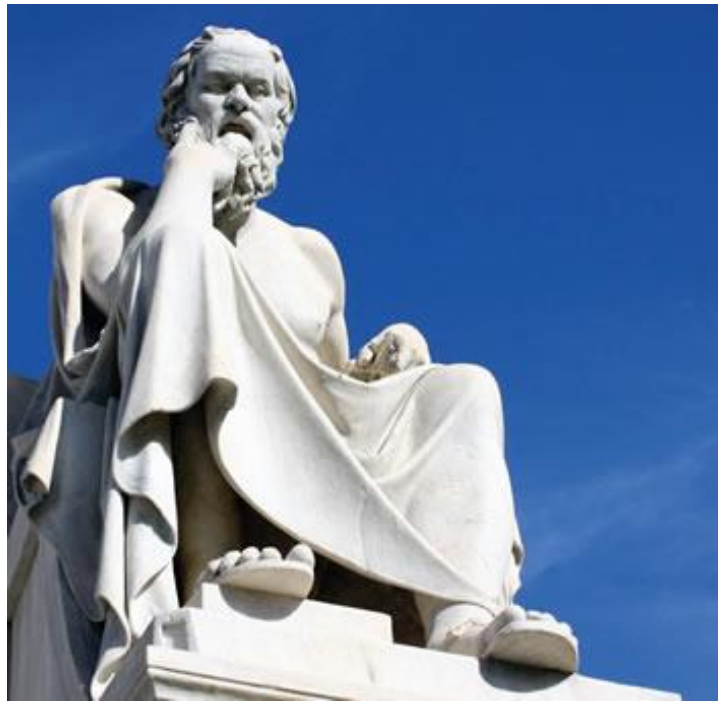
Terminologia Esteganografia

Radicais de origem grega:

Steganos + Graphos

Steganos: Encobrir, coberta

Graphos: Escrita



Objetivo da Esteganografia

- Objetivo principal: ocultar os dados para que estes não sejam descobertos;
- No ramo da segurança da informação, obter segurança por obscurantismo.

Definição de Esteganografia

- Método de esconder uma mensagem secreta dentro de outra mensagem/informação/arquivo.
- **Sinônimo de criptografia**?
  - Não! Ambos visam proteger uma informação, porém a esteganografia tem o objetivo de deixar a mensagem **oculta**, enquanto a criptografia visa deixar a mensagem **ininteligível**.

Criptografia x Esteganografia

Criptografia

Ocultar o **significado**

da mensagem

Esteganografia

Ocultar a **existência**

da mensagem

Na criptografia os receptores sabem da existência das mensagens, porém não conseguem, a princípio, entendê-las.

A esteganografia tenta fazer com que não se perceba que há uma mensagem naquele meio [WAYNER 2002].

História - Grécia

- A origem remete-nos a milhares de anos:
- Grécia Antiga:
  - Mensagens em tempos de guerra;
  - Tabuletas de madeira e cera;
  - General Histiaeus (raspar cabelo do escravo);
  - Astrogal (madeira com furos e barbante);
  - Grego Eneas - “O Tático”.

História – Chineses e egípcios

- Chineses:
  - Mensagens em folhas finas de papel de seda;
  - Enrolavam pequenas bolas que eram encobertas por cera;
- Hieróglifos (escrita egípcia):
  - Técnica comum utilizada para esconder as mensagens.

Johannes Trithemius

É considerado o pai da esteganografia.

O termo esteganografia só ficou em evidência nos meados do século XV, quando ele publicou um livro chamado *Steganographia*.

Tintas invisíveis

Idade Média

- Giovanni Porta (cientista italiano);
- Diversos livros contendo receitas de tintas secretas;
- Utilizadas em diferentes superfícies;
- Chave para comunicação secreta;

Idade Moderna

- Primeira e Segunda Guerra Mundial;
  - Reagentes químicos para cada tipo de tinta;
  - Espionagem
  - Leitura do papel aquecido
  - Mensagem particionada
    - Cortar, separar e juntar.

Cifradores Nulos

Qual foi o “protocolo” definido ?

“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”

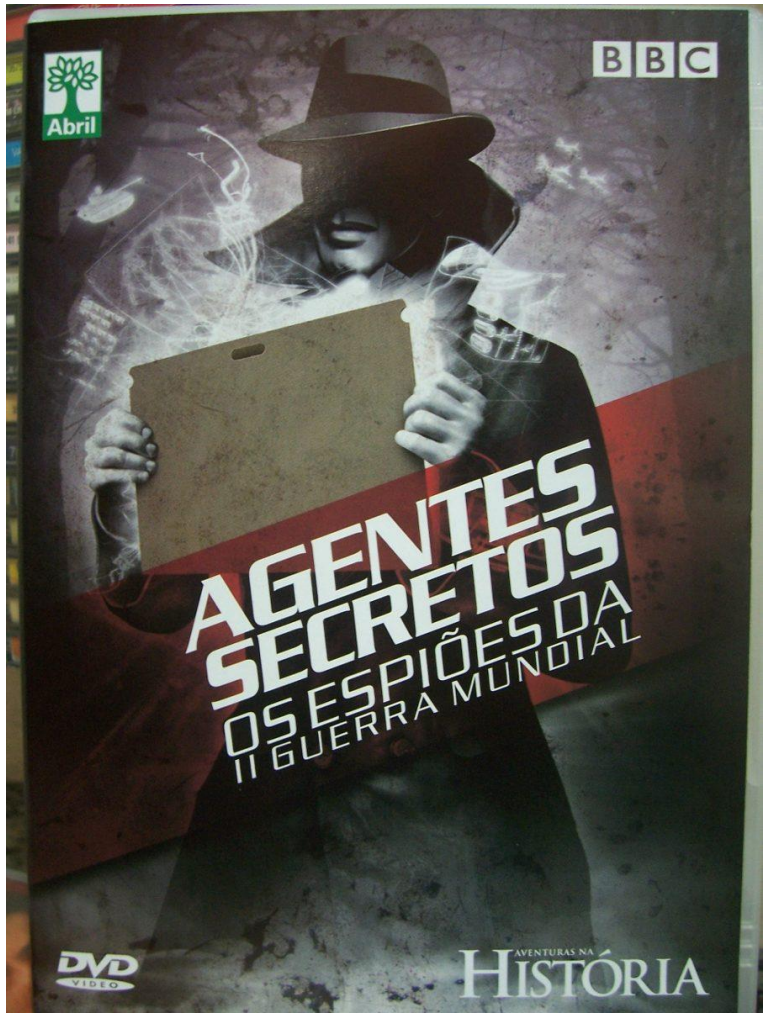
Mensagem subliminar:

“Newt is upset because he thinks he is president”

Exemplo apresentado por [JOHNSON 1998].

Micro pontos

- Segunda Guerra Mundial;
- Introduzido com chegada da fotografia;
- Mensagens:
  - Fotografadas e reduzidas;
  - Fotografia circular de 0,05 polegadas;
  - Cerca de 0,125 cm de diâmetro;
  - Adicionada no lugar de sinal de pontuação.



Utilização

- Copyright (marca d’água);
- Comentários em Imagens (raio x);
- Comunicação privada P2P;
- Publicar mensagens secretas na internet.

Motivação na atualidade

Introdução no meio digital

Comunicações privadas e sigilosas abrangem desde práticas comerciais até aplicações com fins militares

Técnica da “escrita escondida”

Aplicações no âmbito comercial

- Inserir informações ocultas de direitos autorais (*copyright*) ;
- Adicionar códigos contendo seriais únicos a cada produto
  - Impressão digital ou *finger printing*;
  - Combate à Pirataria;
- Existe o interesse ou necessidade de manter o sigilo:
  - Produtos novos, planos estratégicos e abordagens inovadoras;
  - Movimentações financeiras.

Aplicações no âmbito militar

- Fins militares e de inteligência:
  - Meios discretos para se comunicar;
  - Principalmente em tempos e áreas de conflito;
  - Só a criptografia pode não ser suficiente;
    - Emissor do sinal pode ser facilmente localizado e atacado;
  - Técnicas de esteganografia reforçam a segurança;
  - Exemplo: Modulação por espalhamento de espectro (salto de frequência);
    - Dificulta a detecção da transmissão pelo inimigo.

Aplicações no âmbito político

- Eleições:
  - Suporte no processo de comunicação;
  - Técnicas para comunicação anônima: um fator importante para garantir a integridade da votação.

Técnicas de Esteganografia

- Ruído: Substituir o ruído de uma imagem ou arquivo de áudio pela informação que se deseja transmitir;
- Espalhamento: Mecanismos que espalham a informação nos pixels de uma imagem ou em partes do arquivo de áudio;
- Ordenação: Transmitir a informação por meio da ordem em que os elementos de uma determinada lista estão dispostos;
- Divisão: Dividir a mensagem em partes que seguem caminhos diferentes.

Técnica do Ruído - LSB

- LSB - *Least Significant Bits* ou bits menos significativos.
- Usa os bits menos significativos para guardar os dados que se deseja esconder;
- As mídias digitais, tais como fotografias, filmes e música, possuem uma quantidade significativa de ruído, gerada no processo de digitalização da informação;
  - Exemplo: Imagens no formato JPEG;
- Alterar a intensidade de um pixel no máximo em 1%;
- Imagem fica praticamente inalterada;
  - Percepção visual do ser humano é incapaz de detectar.

Técnica do Ruído - BPCS

- BPCS - *Bit-Plane Complexity Segmentation* ou Segmentação de complexidade de plano de bits
- Utiliza o critério do ruído nos planos de bits;
- Qualidade da imagem não é prejudicada
- Baseada na visão humana
  - Não consegue perceber um rastro de informação em um padrão binário complicado e complexo;
  - O que é característico de um ruído;
- Princípio: dividir os planos de bits de uma imagem BMP, PNG ou JPG em regiões com ruídos e sem ruídos;

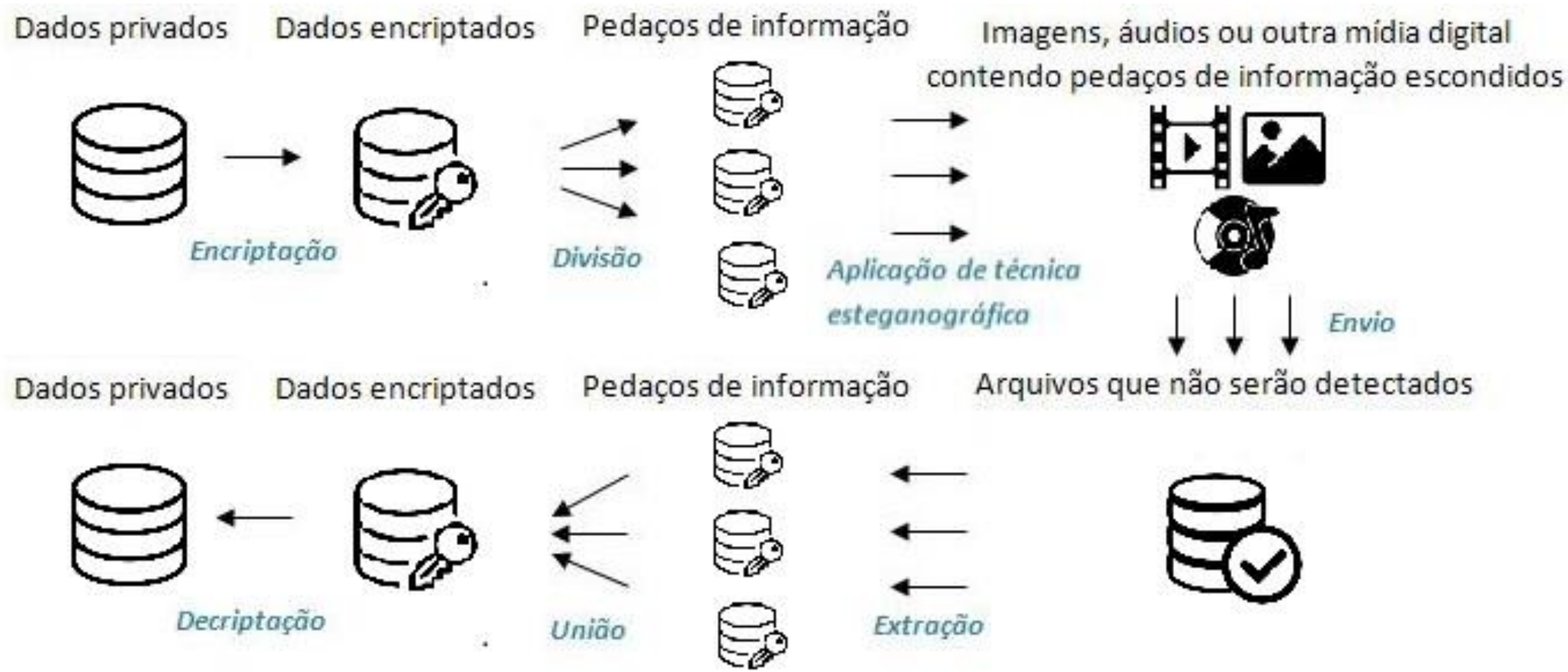
Técnica Espalhamento da Informação

- Informação é separada em partes e alocada em quantidades fracionadas;
- Baseiam-se nas técnicas desenvolvidas por engenheiros de rádio;
  - Utilização do espectro de frequências das ondas de rádio, por onde toda a energia é distribuída;
  - Sinal a ser transmitido é codificado em um sinal similar a um ruído de rádio;
  - Transmitido pelo espectro de frequências;
  - Cada frequência transmite um pedaço da informação;
  - Mensagem é obtida através da combinação das informações.

Técnica de Ordenação

- Ordenar dados que as vezes não necessitam ser ordenados.
- Mapear cada permutação de um conjunto de objetos (inteiro positivo);
- O mapeamento é usado para transmitir o conteúdo escondido;
- Alteração na ordenação dos objetos
  - O meio de transmissão não apresentam uma ordenação específica
- Não altera a qualidade da informação transmitida;
  - A informação pode ser perdida facilmente caso o meio seja codificado novamente.

Técnica de Dividir a Informação



Técnica de Filtragem e Mascaramento

- Mais robustas que a LSB;
- Imunes a compressão e recorte;
- Mais propensas a detecção;
- Trabalham com as modificações dos bits mais significativos das imagens;
- Apenas para escala de tons de cinza.

Técnicas Baseadas: Algoritmos de Transformações

- Explora o problema de compressão do LSB;
- Embutir os dados no domínio das transformações;
- Dados escondidos residem em áreas mais robustas;
  - Espalhadas na imagem inteira;
  - Fornecem melhor resistência contra processamento de sinal;
- Transformações mais utilizadas:
  - Transformada de Fourier Discreta;
  - Transformada de Cosseno Discreta (DCT);
  - Transformada Z ;
- Técnicas de mascaramento de informações mais sofisticas já conhecidas;
- Não apresenta maior robustez contra ataques de esteganálise.

Técnicas de Esteganografia em Vídeo

- Informações escondidas dentro do formato de vídeos (Avi, MP4, Mpeg);
- Geralmente é utilizado o método da Transformada de Cosseno Discreto (DCT) ;
- Similar a esteganografia realizada em imagens;
- Informações são escondidas em cada um dos frames do vídeo;
- Quanto maior for a quantidade de informação a ser ocultada, maior será possibilidade de percepção.

E se for um vídeo FULL HD?

- Resolução: **1920x1080** pixels;
- Quantidade de bits por frame: 1920x1080x3(RGB)x8(bits) = **49.766.400**;
- Assim pode-se ocultar 6.220.800 bits (777 KB) de informação por frame (**12%**);
- Como normalmente são 30 frames por segundo, é possível ocultar **140 MB** por minuto;
- Em um filme de 90 minutos, é possível esconder **12.5GB** de informação.

Técnicas de Esteganografia em Áudio

- Camuflar imagens em sinais de áudio;
- Sistema auditivo humano (SAH):
  - Tende a trabalhar em uma faixa de frequências muito grande;
    - 1 Bilhão de potências diferentes de sinais ;
    - Até mil frequências de sinais distintas;
  - O SAH é poderoso para captar sinais e frequências;
    - Entretanto não consegue fazer distinção de tudo que recebe;
    - Sons mais altos tendem a mascarar sons mais baixos;
- Técnicas de esteganografia em áudio exploram muitas das vulnerabilidades do ouvido humano.

Esteganálise

"Esteganálise é a área de estudo que visa detectar a presença de métodos de esteganografia."

Principais Objetivos da Esteganálise

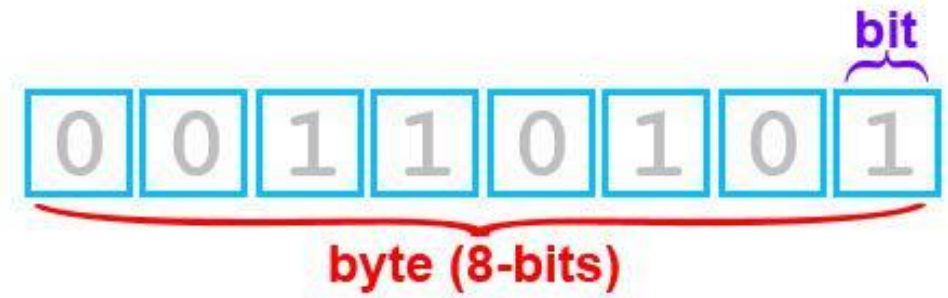
- Destruindo tudo: Muitas pessoas argumentam que a esteganografia não é tão útil, a informação pode ser totalmente destruída em um ataque;
- Adicionando novas informações: Usar o mesmo programa para codificar novas informações, o que pode sobrescrever a mensagem original;
- Alterando o formato do arquivo: Alterar o formato do arquivo, os arquivos armazenam informações de diversas maneiras conforme o seu formato;
- Comprimindo o arquivo: Comprimir um arquivo, baseando-se no fato de que os algoritmos de compressão tentam remover as informações extras do arquivo, onde geralmente é escondida a informação.

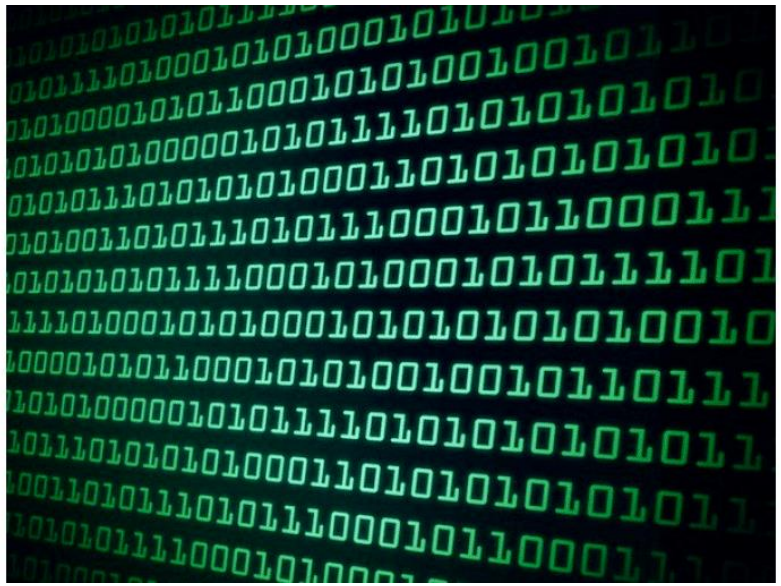
Classificação dos ataques de Esteganálise

- Ataques visuais: Inspecionar o arquivo visualmente, tentando localizar falhas nesse arquivo;
- Ataques estruturais: Identificar mudanças na estrutura dos arquivos, o que sugere que o mesmo foi manipulado;
- Ataques estatísticos: Aplicar Testes estatísticos afim de verificar a existência de informações escondidas.

Bit e Byte

- O bit (*Binary Digit*) é a unidade básica da informação digital;
  - É a menor unidade de informação que pode ser armazenada ou transmitida;
  - Pode assumir apenas dois valores: **0** ou **1;**
- Um **byte** é uma sequência de 8 bits.





Sistema de Numeração Binário

- Os computadores só compreendem 0 e 1;
- Informação é convertida para **código binário:**
  - Permite que o processador entenda as instruções;
  - Cálculos aritméticos e operações lógicas;
  - Linguagem de máquina.

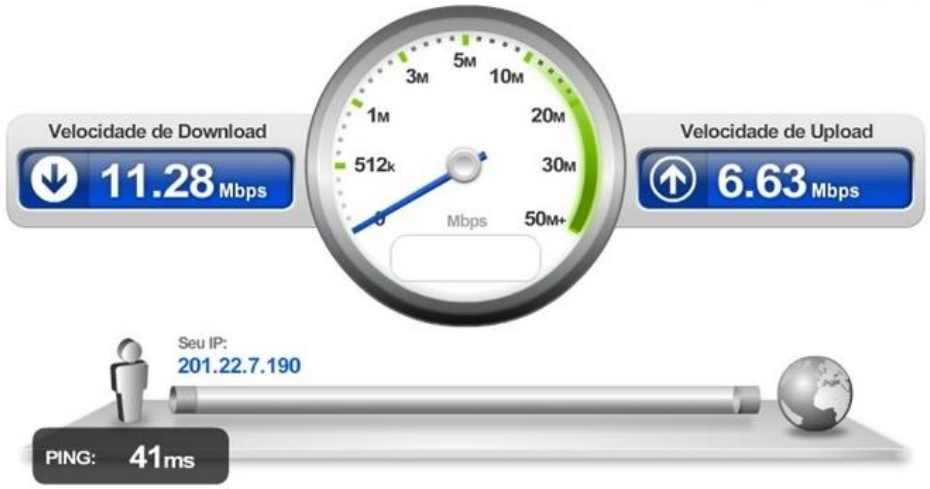
Decimal Base 10	Binário Base 2
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000

Unidades de Armazenamento

- As unidades de grandezas são importantes para representar alguma quantidade e a capacidade de armazenamento de um computador;
  - 1 byte = 8 bits
  - 1 KB (Quilobyte) = 1.024 bytes
  - 1 MB (Megabyte) = 1.024 Kb = 1.048.576 bytes
  - 1 GB (Gigabyte) = 1.024 Mb = 1.073.741.824 bytes
  - 1 TB (Terabyte) = 1.024 GB = 1.099.511.627.776 bytes
  - 1 ZB (Zettabyte) = 1.180.591.620.717.411.303.424 bytes

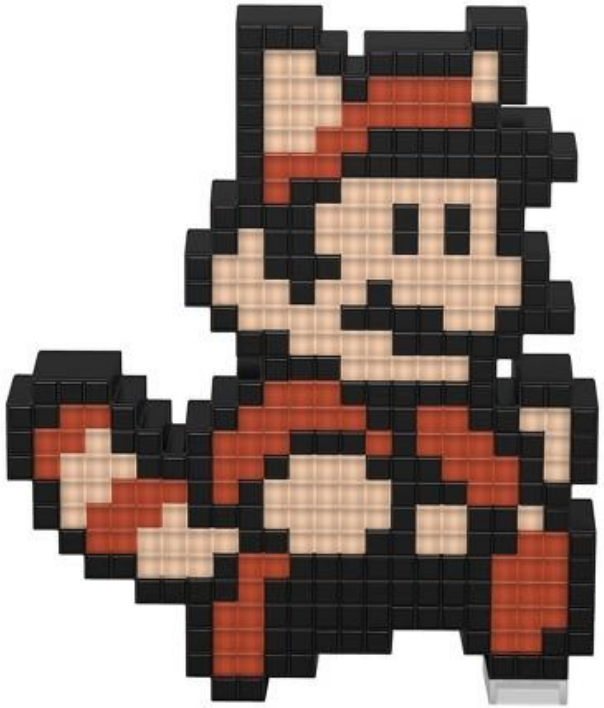
A medida da velocidade da internet

- As operadoras usam os bits na propaganda - Marketing;
  - MB (Megabyte) ≠ Mbps - Megabits
  - KB (Quilobyte) ≠ Kbps (Quilobits)
- Megabyte é 8 vezes maior do que o Megabit
- Quilobyte é 8 vezes maior do que o Kilobit



Técnica do bit menos significativo

- Uma imagem é composta por pixels.



Técnica do bit menos significativo

- Uma forma de representar uma imagem é através do formato RGB, no qual cada pixel de uma imagem é composto por três valores (bytes) que definem a cor.

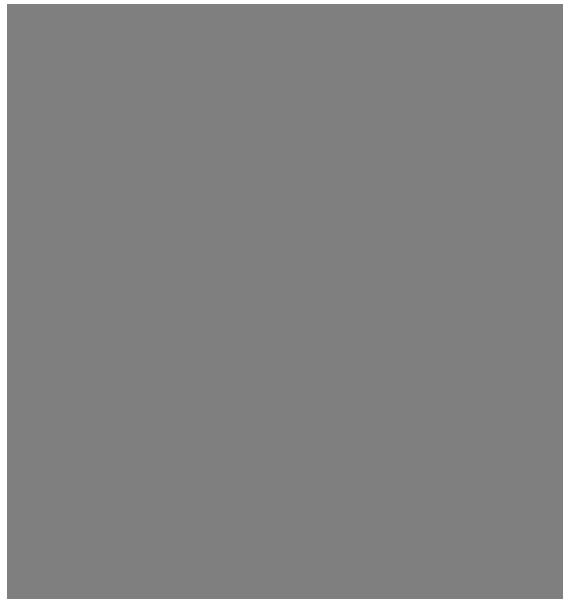
Técnica do bit menos significativo

- A combinação dos três valores de RGB definem a cor do pixel.
- Exemplo:

R = 126 (01111110)

G = 126 (01111110)

B = 126 (01111110)



Técnica do bit menos significativo

- A mudança do último bit RGB não influência a representação visual do pixel na imagem.

R = 126 (01111110)

G = 126 (01111110)

B = 126 (01111110)

R = 126 (01111111)

G = 126 (01111111)

B = 126 (01111111)

Técnica do bit menos significativo

- Ou seja, é possível inserir um conteúdo no último bit de cada cor do RGB, sem influenciar a visualização para os seres humanos.

R = 126 ou 127 (0111111**?**)

G = 126 ou 127 (0111111**?**)

B = 126 ou 127 (0111111**?**)

Conclusão

- A esteganografia digital têm sido cada vez mais explorada e utilizada atualmente;
- Existe uma diversidade de aplicações;
  - Foco na segurança da informação;
  - Diversas técnicas existentes;
- Muitas dessas técnicas podem ser facilmente integradas com métodos de criptografia, o que permite uma maior segurança nos dados em trânsito;
- As técnicas de esteganográficas não são perfeitas, a esteganálise entra em ação e vem atuando sobre essas falhas;
- Esteganografia ainda tem se mostrado muito eficaz em esconder informações.

Obrigado!

Luis Gonzaga
luis.gonzaga@pucpr.br

Referências

- KAHN, D. The history of steganography. In: Proceedings of the First International Workshop. Cambridge, UK: [s.n.], 1996.
- KAWAGUCHI, E; EASON, R. O. Principle and applications of BPCS-Steganography. SPIE Proceedings Series, Boston, vol. 3528, p. 464-473, 1999.
- KESSLER, G. C. An Overview of Steganography for the Computer Forensics Examiner. Computer and Digital Forensics Program, Champlain College, Burlington, julho 2004.
- MORRIS, S. The future of netcrime now (1) - threats and challenges. Home Office Crime and Policing Group, USA, 2004. Technical Report 62.
- ÖZER, H.; AVCIBAS, I.; SANKUR, B.; MEMON, N. Steganalysis of Audio Based on Audio Quality Metrics. Security and Watermarking of Multimedia Contents V, Proceedings of the SPIE, v. 5020, p. 55-66, 2003.
- PETITCOLAS, F. A. P.; ANDERSON, R. J.; KUHN, M. G. Information Hiding - A Survey. Proceedings of the IEEE special issue on protection of multimedia content, 87(7): 1062-1078, julho 1999.

Referências

- PETRI, M. Esteganografia. Trabalho de conclusão de curso enviado ao Instituto Superior Tupy, Joinville, 2004.
- POPA, R. An analysis of steganography techniques. Dissertação (Mestrado) - The Polytechnic University of Timisoara, Timisoara, Romênia, 1998.
- PROVOS, N.; HONEYMAN, P. Detecting Steganographic Content on the Internet. CITI Technical Report 01-11, agosto 2001.
- ROCHA, A. R.; COSTA, H. A. X.; CHAVES, L. M. Camaleão: Um Software para Segurança Digital Utilizando Esteganografia. Monografia (Ciência da Computação), Departamento de Ciências da Computação, Universidade Federal de Lavras, Lavras, Minas Gerais, 2003.
- WAYNER, P. Disappearing Cryptography - Information Hiding: Steganography and Watermarking. Morgan Kaufmann Publisher, 2ª Edição, maio 2002.