Universidade Estadual de Campinas - UNICAMP
Instituto de Computação - IC

Análise e Implementação de Técnicas de Detecção de Mensagens Escondidas em Imagens Digitais[1]

Anderson Rocha Siome Goldenstein (Orientador)

Campinas, 16 de abril de 2005

[1] Projeto financiado pela CAPES (Março / Agosto de 2004) e FAPESP (Setembro 2004 / Fevereiro de 2006)

Roteiro

1. Objetivos da tese
2. Introdução ao assunto
   - O que é uma imagem
   - Mascaramento de informações
   - Mascaramento de informações em imagens
3. Esteganálise
   - Definições
   - Importância
   - Principais técnicas
4. Cronograma
5. Conclusões

Objetivos da tese

1. Estudar técnicas de detecção de mensagens escondidas em imagens digitais;
2. Levantar pontos fortes e fracos;
3. Desenvolver um *software* de detecção;
4. Validar as técnicas em um banco de imagens;
5. Propor melhorias (se possível);

O que é uma imagem

- Uma imagem monocromática é uma função de intensidade de luz bidimensional $f(x, y)$;

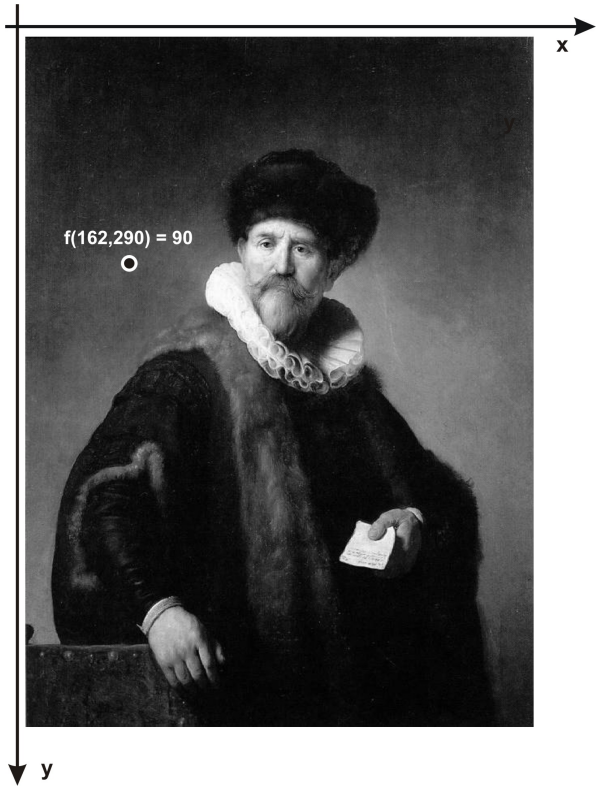

Figura: Tela *Nicolaes Ruts* - Rembrandt

- Uma imagem colorida é uma imagem multibanda, onde a cor em cada ponto (x, y) é definida através de três grandezas: *luminância*, *matiz* e *saturação*;

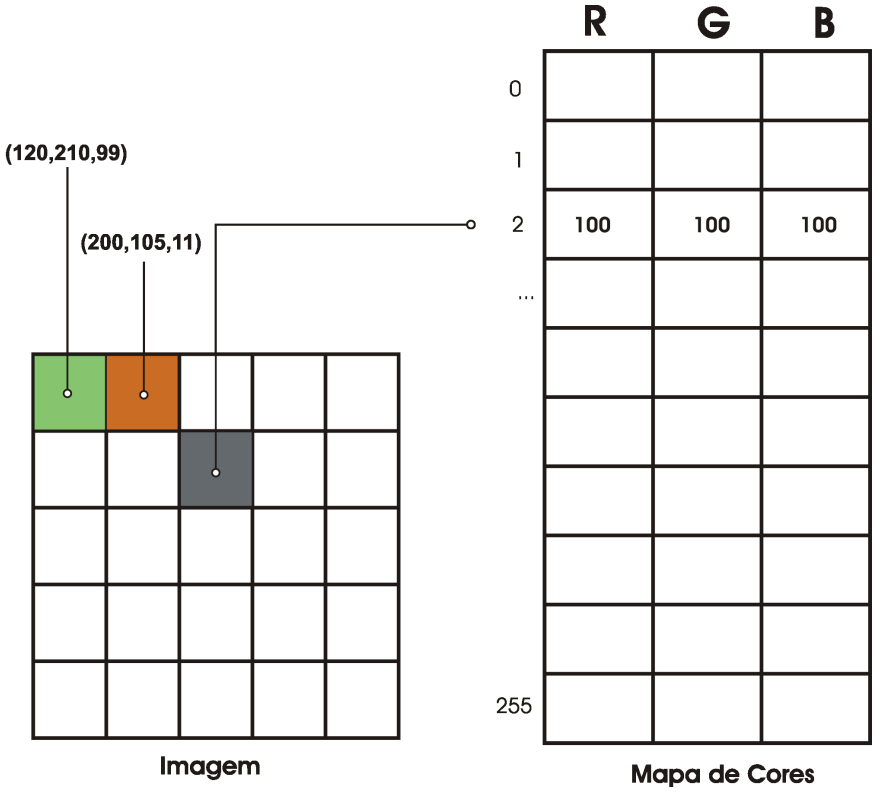

Figura: Possíveis representações de uma imagem colorida

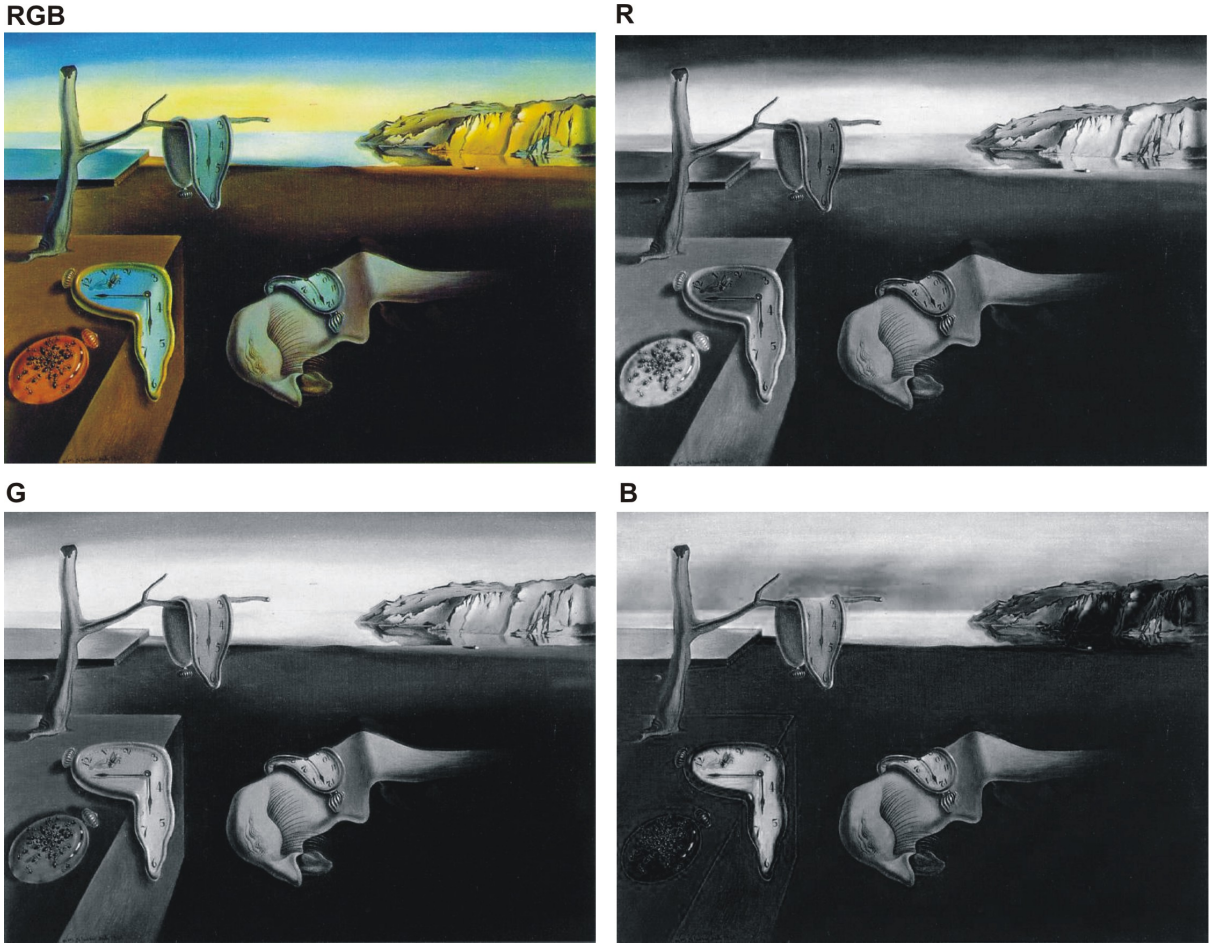

Figura: Tela *Persistence* - Salvador Dali

Mascaramento de informações

1. Definições
   - Esteganografia;
   - Objeto de cobertura;
   - Dado embutido;
   - Estego-objeto;
   - Chave de deslocamento;

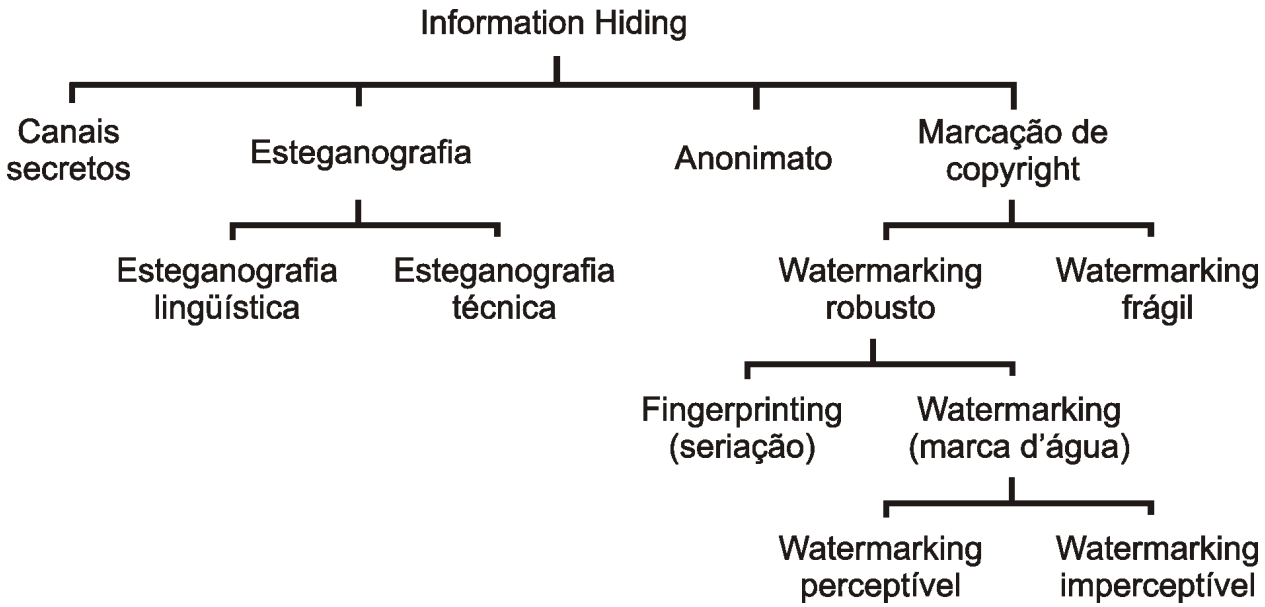

Figura: Hierarquia do mascaramento de informações

Mascaramento de informações em imagens

1. Consiste em substituir componentes de ruído por uma mensagem secreta pseudo-randômica;
2. Três abordagens básicas:
   - Inserção no *bit* menos significativo (LSB);
   - Técnicas de filtragem e mascaramento;
   - Algoritmos e transformações;

- Inserção no *bit* menos significativo (LSB)

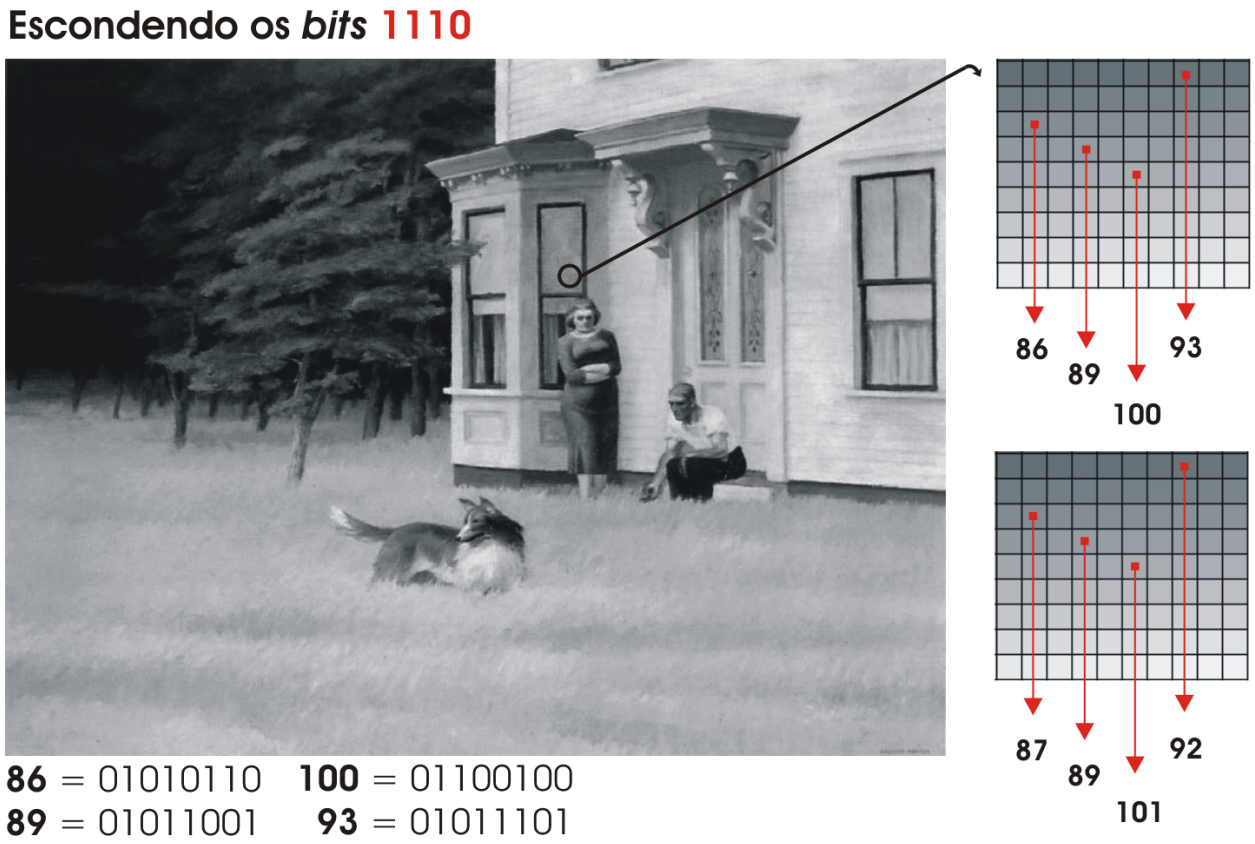

Figura: Como esconder os *bits* **1110** na tela *Cape Evening* - Hopper

Esteganálise – Definições

- Campo de pesquisas relacionado às tentativas de descobrir mensagens secretas;
- Técnicas de esteganografia possuem falhas e/ou inserem artefatos detectáveis nos objetos de cobertura;
- Pesquisas concentradas na detecção das mensagens;

Esteganálise – Importância

1. Técnicas de *copyright* eficientes e eficazes;
2. Computação forense;
3. Coleção de evidências para investigações;
4. Rastreamento de atividades criminais
   - Jogos e pornografia;
   - Pedofilia;
   - Tráfico de pessoas;

Esteganálise – Tipos de ataques

1. Aurais;
2. Estruturais;
3. Estatísticos
   - Teste do χ^2;
   - Análise RS;
   - Análise das cores únicas no cubo RGB;
   - Taxa de inversão da energia do gradiente;
   - Análise de estatísticas de alta ordem;
   - Métricas de qualidade de imagem;
   - Métricas de tons contínuos e pares de amostragem;

Análise RS

1. Simulação artificial de um novo mascaramento;
2. Análise da capacidade de mascaramento *sem perdas*;
3. A randomização do plano LSB diminui a capacidade de mascaramento *sem perdas*;
4. Criação de funções F_1, F_{-1} e F_0 para simular o mascaramento;
5. Função de discriminação f para capturar suavidade de um subconjunto de *pixels*

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \tag{1}$$

Análise RS

1. Definição de uma máscara M cujos elementos $k \in \{-1, 0, 1\}$;
2. Divisão da imagem em grupos
   - regulares: $G \in R_M \Leftrightarrow f(F_M(G)) > f(G)$;
   - singulares: $G \in S_M \Leftrightarrow f(F_M(G)) < f(G)$;
   - não usáveis: $G \in U_M \Leftrightarrow f(F_M(G)) = f(G)$;
3. Em imagens naturais $|R_M| \cong |R_{-M}|$ e $|S_M| \cong |S_{-M}|$;

Análise das cores únicas no cubo RGB

1. Número de cores únicas é tipicamente baixo;
2. Aumento no número de cores próximas após o mascaramento;
3. O algoritmo geral consiste em
   - Calcular a razão R entre as cores verdadeiras e as cores próximas ($d \leq 3$);
   - Mascarar uma pequena mensagem pseudo-aleatoriamente na imagem de teste;
   - Calcular a nova razão R' na imagem de teste modificada;
4. Se a imagem é uma estego-imagem $R \cong R'$;

Análise de estatísticas de alta ordem

1. Criação de modelos estatísticos de alta ordem para imagens naturais;
2. Busca de desvios nestes modelos;
3. Classificação
   - *Support Vector Machines*;
   - Discriminantes de Fisher;
4. Decomposição da imagem através de filtros de *passa-baixas* e *passa-altas*;

Análise de estatísticas de alta ordem

1. Cálculo de *média*, *variância*, *assimetria* e *curtose* dos coeficientes de cada sub-banda;
2. Segundo conjunto de estatísticas a partir dos erros de um PLOCM[2];
3. Total de $24(n-1)$ estatísticas para o vetor característico;

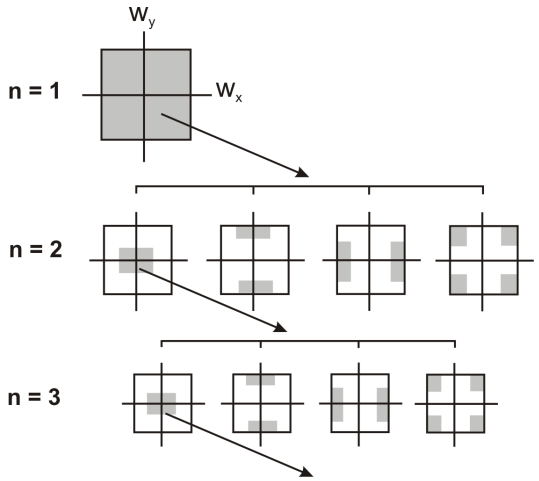

Figura: Decomposição da imagem em múltiplas escalas e orientações

[2] Preditor Linear Ótimo dos Coeficientes de Magnitude

Cronograma de atividades

1. Levantamento bibliográfico;
2. Estudo sobre os impactos da esteganografia;
3. Estudo das principais técnicas de detecção;
4. Construção de um banco de imagens;
5. Implementação;
6. Validação;
7. Documentação;
8. Artigos, tese e relatórios FAPESP;

Conclusões

1. Limitações;
2. Importância;
3. Constante evolução;

Conclusões

De artificio sine secreti latentis suspicione scribendi!
(David Kahn)

Pode-se desenvolver um software que seja capaz de enganar todos os computadores uma vez, ou mesmo pode-se enganar alguns computadores todas as vezes. No entanto, nunca se poderá desenvolver um software capaz de enganar todos os computadores todas as vezes.
(Anônimo)

Dúvidas?

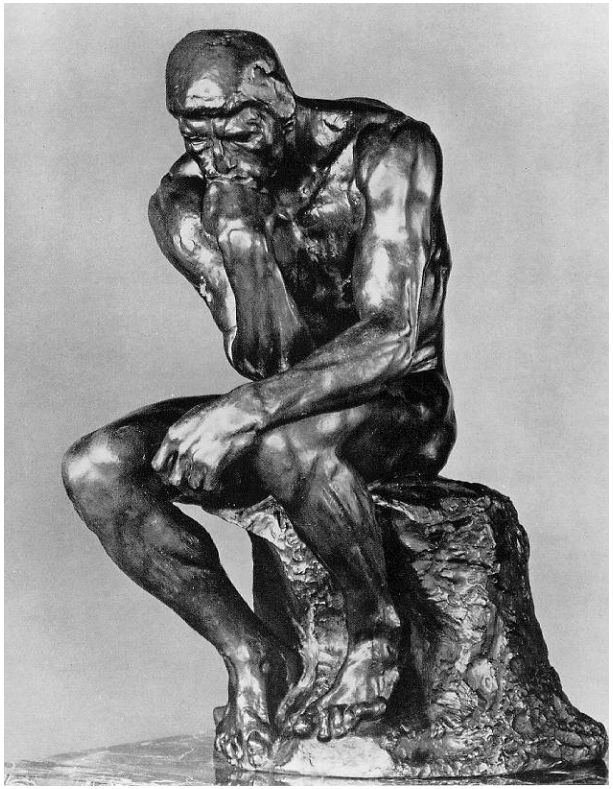

Figura: *O pensador* - Rodin