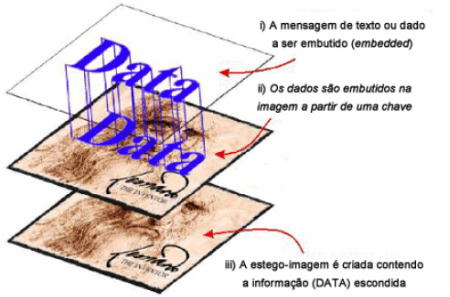
Esteganografia e suas Aplicações

Eduardo Julio, Wagner Brazil, Célio Albuquerque

{ejulio, wbrazil, celio}@ic.uff.br

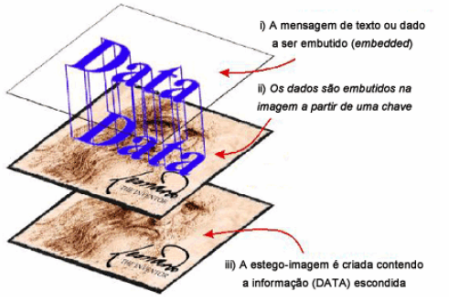
Instituto de Computação

Universidade Federal Fluminense



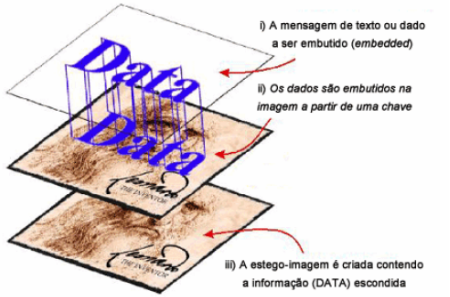
Agenda

- Introdução
  - Definições
  - História
  - Impactos Sociais
- Técnicas de Esteganografia
- Técnicas de Esteganálise
- Aplicações
- Considerações Finais



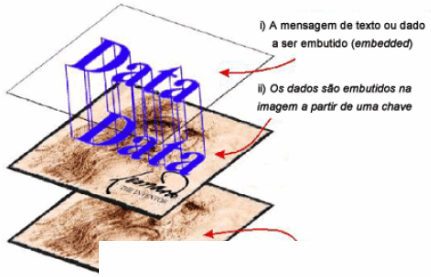
Introdução

- ***Esteganografia* é a**
  - arte de mascarar informações ou
  - arte da escrita escondida
  - *estegano = esconder, mascarar*
  - *grafia = escrita*
- **Diversos métodos utilizados:**
  - tintas “invisíveis”
  - micro-pontos
  - arranjo de caracteres
  - assinaturas digitais
  - canais escondidos (*covert channels*)



Definições

- **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*)

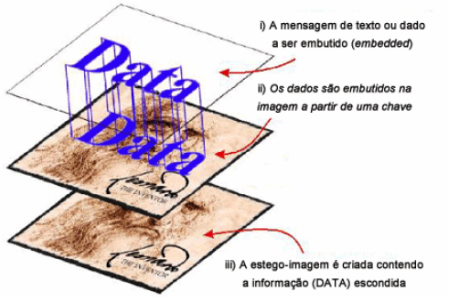


Exemplo

i) A mensagem de texto ou dado a ser embutido (*embedded*)

ii) *Os dados são embutidos na imagem a partir de uma chave*

iii) A estego-imagem é criada contendo a informação (DATA) escondida



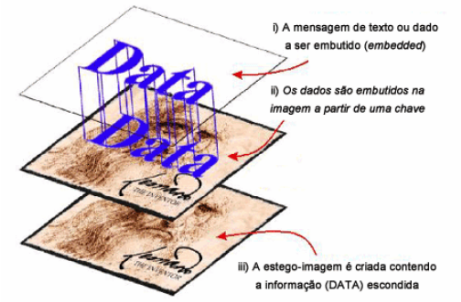
Exemplo

"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".

"Newt is upset because he thinks he is president".

Taxonomia

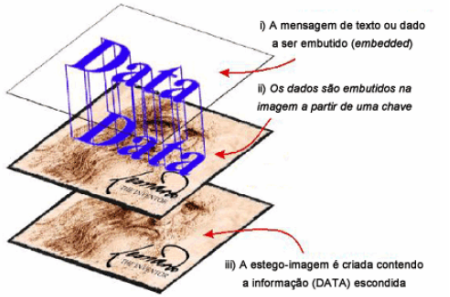
- Information Hiding
  - Canais secretos
  - Esteganografia
    - Esteganografia lingüística
    - Esteganografia técnica
  - Anonimato
  - Marcação de copyright
    - Watermarking robusto
      - Fingerprinting (seriação)
      - Watermarking (marca d'água)
        - Watermarking perceptível
        - Watermarking imperceptível
    - Watermarking fragil



Marcação Visível

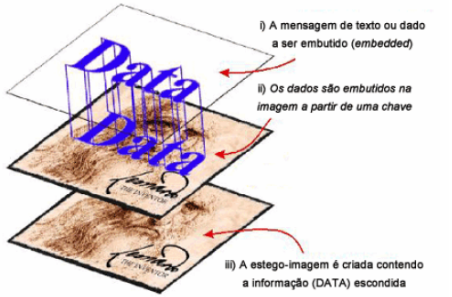

i) A mensagem de texto ou dado
a ser embutido (*embedded*)
ii) *Os dados são embutidos na*
imagem a partir de uma chave
iii) A estego-imagem é criada contendo
a informação (DATA) escondida

História



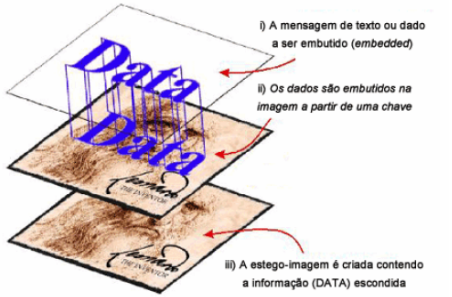
História

- Primeiros registros: **Heródoto**, pai da História, conta que um homem, de nome Harpagus, **matou uma lebre e escondeu uma mensagem em suas entranhas.** Em seguida, enviou a lebre através de seu **mensageiro** que **se passou por um caçador**



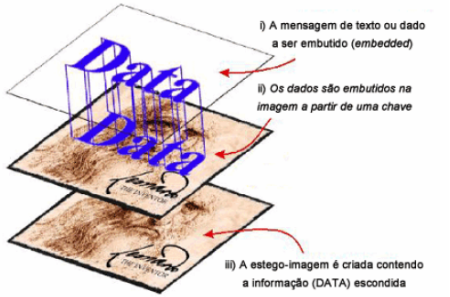
História

- Século V A.C., o grego Histaieus, para encorajar Aristágoras de Mileto e seus compatriotas a começar uma revolta contra Medes e os Persas, raspou a cabeça de um de seus escravos mais confiáveis e tatuou uma mensagem em sua cabeça. Assim que os seus cabelos cresceram, o escravo foi enviado à Grécia com instruções de raspar sua cabeça permitindo aos seus amigos receberem a mensagem



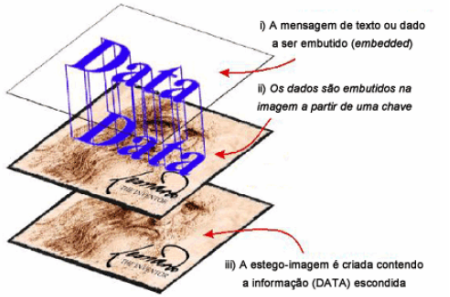
História

- Uso de tabletes de madeira cobertos de cera
  - serviam como meio de escrita para a Grécia Antiga
  - textos eram escritos sobre a cera e, quando se tornavam inúteis, a cera era derretida e uma nova camada de cera era colocada sobre a madeira



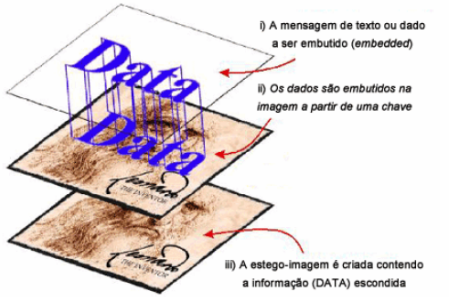
História

- Demeratus, um grego exilado na corte persa, ficara sabendo que o rei da Pérsia, Xerxes, estava planejando invadir
  - Resolveu encontrar um meio de avisar a corte grega sobre os planos audaciosos de Xerxes e utilizou os tabletes de cera.
  - Ao invés de escrever na cera, Demeratus derreteu a cera, escreveu a mensagem na própria madeira e depois a recobriu com cera novamente como se estivesse construindo um tablete de cera novo
  - Passaram sem problemas na fronteira persa e chegaram na Grécia
  - Como ninguém na Grécia sabia do procedimento do emissor da mensagem, os tabletes ficaram um bom tempo sem serem decifrados.
  - Até que uma mulher grega, Gorgo, derreteu a cera



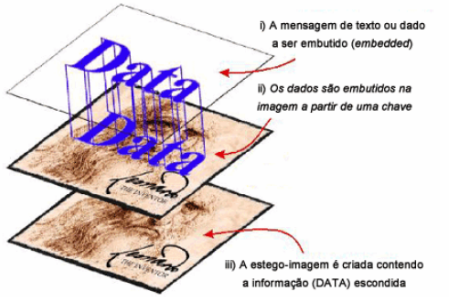
História

- Grego Enéas, o Tático inventou uma técnica esteganográfica intitulada astrogal
  - madeira com vários furos, cada qual representando uma letra
  - quando alguém desejasse enviar uma mensagem, este deveria passar um barbante pelos furos correspondentes às letras da mensagem a ser transmitida
  - cabia ao receptor da mensagem acompanhar as várias ligações de pontos feitas pelo barbante e, assim, decifrar a mensagem
  - quando era interceptado,era tido apenas como um brinquedo de criança



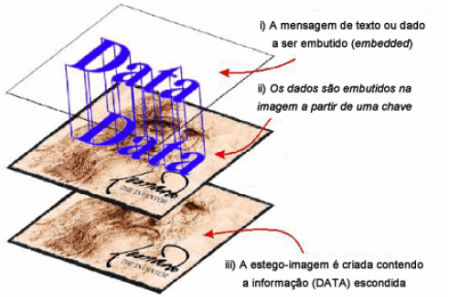
História

- Dois mil anos mais tarde, remetentes ingleses empregaram o mesmo método, não para garantir o segredo de suas cartas, mas para evitar o pagamento de taxas muito caras
  - antes da reforma do serviço postal em 1850, enviar uma carta custava cerca de um shilling para cada cem milhas de distância
  - os jornais, no entanto, eram isentos de taxas
  - Graças a furinhos de agulha, os espertos ingleses enviavam suas mensagens gratuitamente
  - Este procedimento foi utilizado também pelos alemães durante a Primeira Guerra Mundial



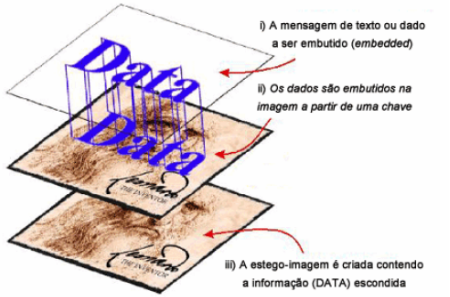
História

- Na Renascença, Giovanni Porta, um dos maiores criptoanalistas de seu tempo, “aperfeiçoou” a técnica da lebre de Harpagus
  - alimentar um cachorro com a mensagem e enviá-lo
  - o receptor ao recebê-lo, o mataria e recuperaria a mensagem



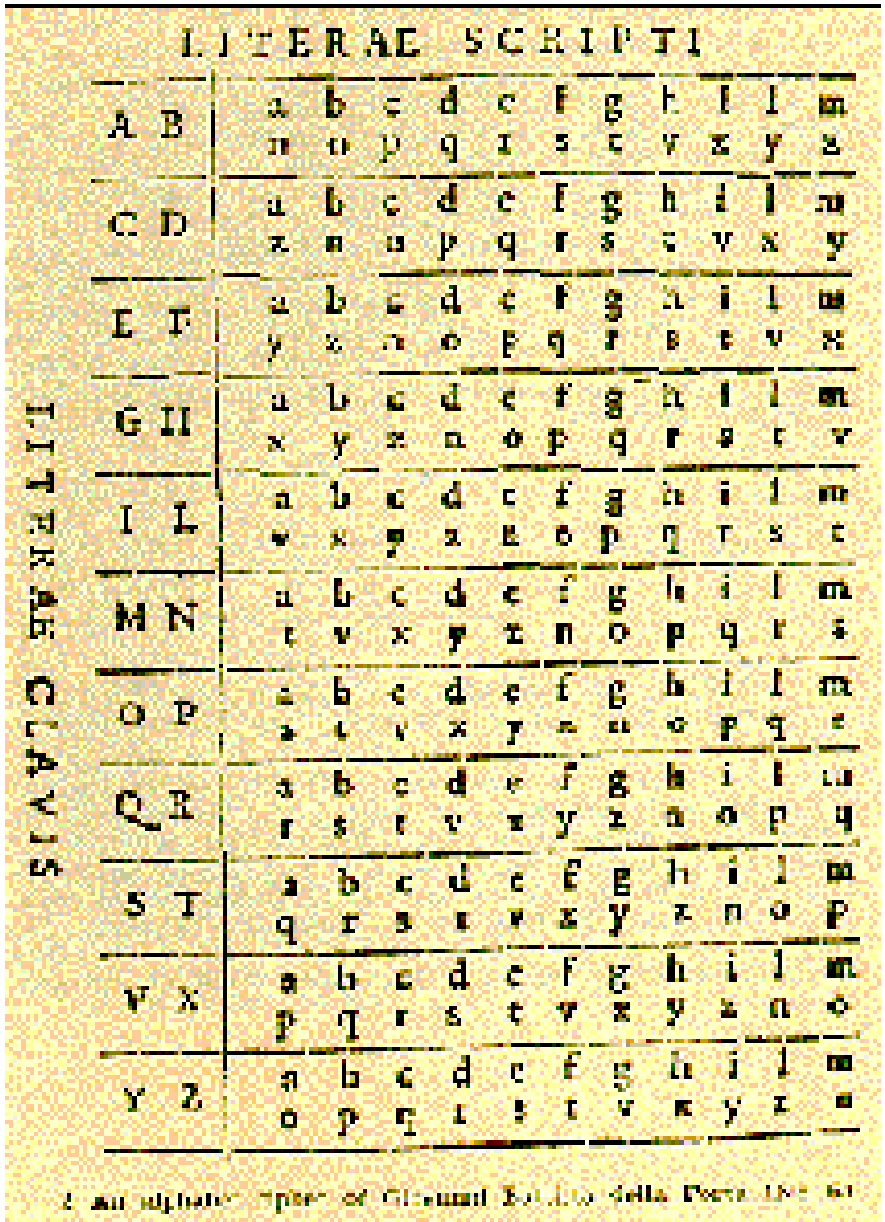
História

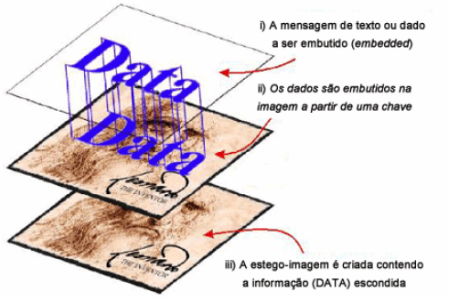
- Porta também descobriu como esconder uma mensagem em um ovo cozido
  - basta escrever sobre a casca com uma tinta contendo uma onça de alume (+- 29g) diluído em cerca de meio litro de vinagre.
  - a solução penetra a casca e se deposita sob esta
  - basta descascar o ovo para ler a mensagem



História

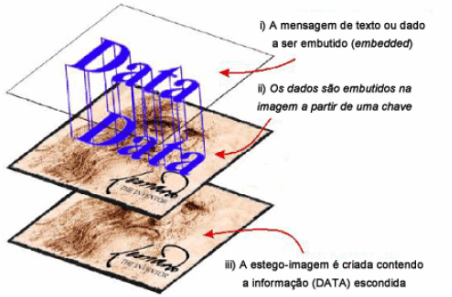
- Também é de Porta a criação da famosa ***cifra indecifrável*** (*Le chiffre indéchiffrable*), um dos primeiros sistemas de criptografia por substituição





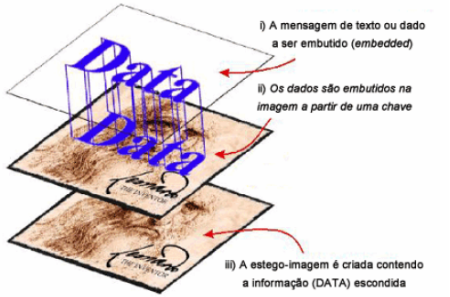
História

- Outra técnica interessante faz uso de inúmeras variações de tintas “invisíveis”
  - Já apareciam em relatos de Plínio, o Velho, e Ovídio no século I DC
  - Ovídio, em sua *Arte do amor*, propusera o uso do leite para escrita de textos “invisíveis”
    - Para decodificar a mensagem, o receptor deveria borrifar o papel com ferrugem ou carbono negro
    - Estas substâncias aderiam ao leite e a mensagem era revelada



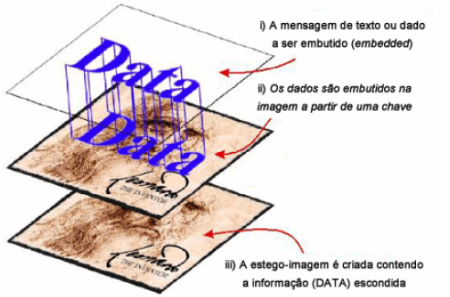
História

- As primeiras tintas eram simples fluidos orgânicos que não exigiam nenhuma técnica especial para serem reveladas
  - algumas vezes, bastava apenas aquecer o papel e a mensagem aparecia
  - pode ser confirmado com as tintas baseadas em fluidos de suco de limão
- Durante a primeira guerra mundial, espiões alemães colocavam pequenos “pontos” de tinta invisível sobre letras de revistas e jornais de grande circulação
  - as folhas de revistas “pontuadas”, quando aquecidas, revelavam a seqüência das letras e toda a mensagem ali escondida



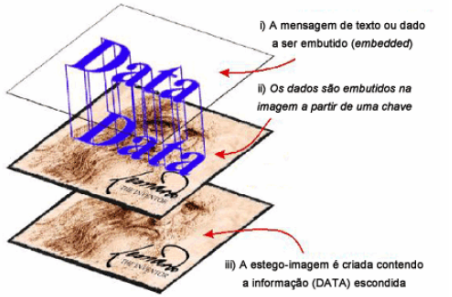
História

- Com o progresso global da ciência, outras formas mais poderosas de tintas invisíveis foram aparecendo através da história.
- De forma geral, as tintas invisíveis são químicas que, misturadas a outras químicas, tornam o resultado visível
  - ácido galotânico, feito a partir de nozes
    - se tornam visíveis apenas em contato com sulfato de cobre
    - espião
  - nazista George Dasch, na segunda guerra mundial
    - escreveu mensagens em seu lenço utilizando uma solução de sulfato de cobre
    - mensagem poderia ser decodificada utilizando vapor de amônia



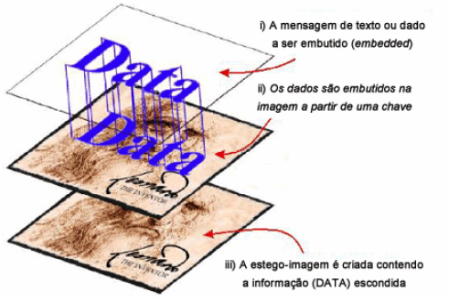
História

- Campo da fotografia
  - reduzir fotos de páginas inteiras de texto a tamanhos consideráveis.
    - aplicação na guerra franco-prussiana.
    - Paris estava sitiada pela Prússia
    - habitantes escreviam mensagens e fotografavam-nas, reduziam ao máximo os negativos e utilizando-se de pombos-correio, enviavam as mensagens para fora de Paris, conseguindo estabelecer um canal de comunicação com os arredores da cidade sitiada



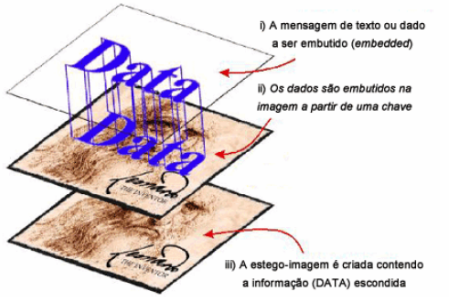
História

- Na segunda guerra mundial, com um aumento na qualidade das câmeras, lentes e filmes, tornou-se possível aos espiões nazistas, a criação de uma das formas mais interessantes e engenhosas de comunicação secreta
  - mensagens nazistas eram fotografadas e, posteriormente, reduzidas ao tamanho de pontos finais (.) em uma sentença
    - uma nova mensagem totalmente inocente era escrita contendo o filme ultra-reduzido como final das sentenças. A mensagem gerada era enviada sem levantar maiores suspeitas
    - ficou conhecida como ***tecnologia do micro-ponto***



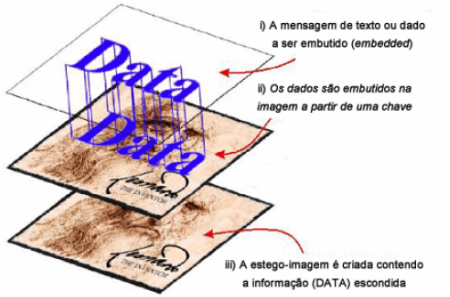
História

- *Semagramas* são formas de comunicação secreta que não estão na forma escrita
- A utilização também na segunda guerra mundial
  - censores americanos interceptaram um carregamento de relógios e mudaram toda a sua disposição na caixa, bem como a de seus ponteiros
  - havia o medo de que disposição dos ponteiros e dos relógios escondesse alguma mensagem secreta



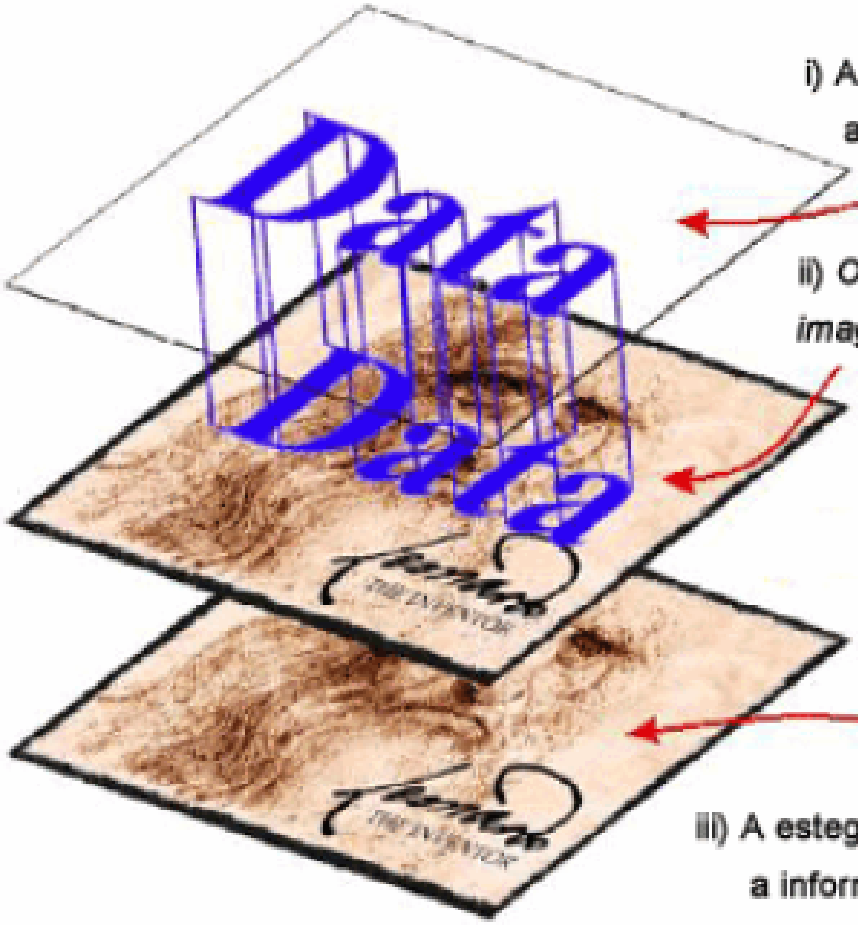
História

- Vallerie Dickinson, espiã a do Japão na segunda grande guerra, usava vestidos de bonecas para avisar aos japoneses sobre ações americanas
  - pequenos vestidos representavam *destroyers*
  - grandes vestidos poderiam representar *couraçados* ou *cruisers*

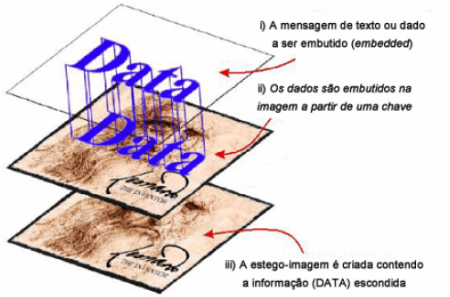


História

- Girolammo Cardano (grelha de cardano)
  - um papelão com furos em locais estratégicos
  - tanto o emissor quando o receptor, em posse de uma grelha dessas poderia se comunicar colocando-a sobre uma grande quantidade de texto e apenas apareceriam as palavras sob os furos da grelha

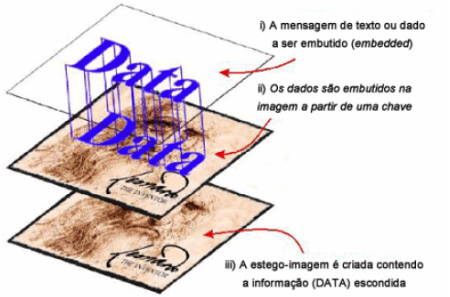


Impactos Sociais



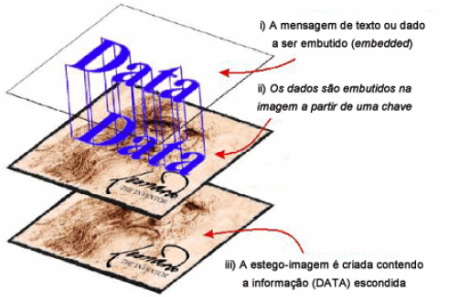
Impactos Sociais

- *World Trade Center* em 11 de setembro de 2001
  - *Al Qaeda* de Osama bin Laden, estaria se comunicando com suas células espalhadas pelo mundo através de mensagens escondidas em imagens digitais, distribuídas através de *chats*, grupos de discussão, *e-mails*, leilões eletrônicos entre outros meios



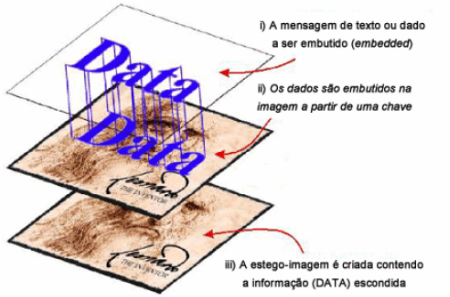
Impactos Sociais

- 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



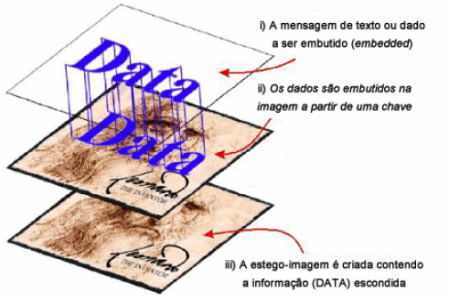
Impactos Sociais

- Propostas de controle de privacidade já existem ou estão em andamento:
  - *PATRIOT (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism)*
  - *Carnivore (*Programa do FBI para vigiar o correio eletrônico*)*
  - *DMCA (Digital Milenium Copyright Act)*
  - *CAPPS II (Computer Assisted Passenger Pre-Screening System)*



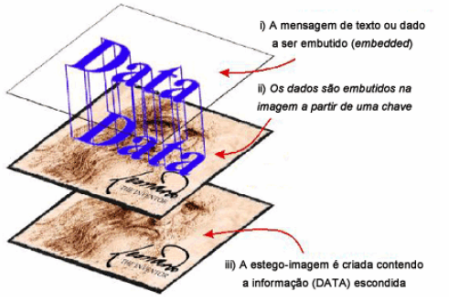
Impactos Sociais

- Uso legal:
  - estruturas de dados aprimoradas: informações podem ser escondidas de modo a funcionarem como estruturas de dados avançadas
    - armazenar informações médicas a respeito de um paciente em seu próprio raio X.
    - fotos de satélite poderiam armazenar dados geográficos sobre os locais observados



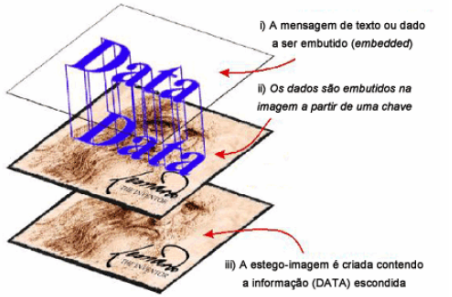
Impactos Sociais

- Uso legal:
  - marcas d'água resistentes: os criadores de conteúdo digital tais como livros, filmes e arquivos de áudio querem adicionar informações escondidas em suas criações de modo a garantir a sua propriedade
    - Vários tipos de marcações (watermarks) podem ser feitos, desde aquelas que permanecem no documento até que ele seja totalmente destruído às que desaparecem após qualquer tipo de modificação no meio em que se encontra



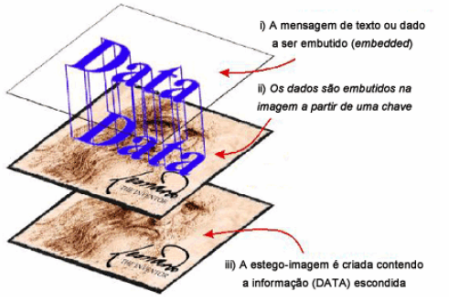
Impactos Sociais

– rastreamento de documentos: informações escondidas podem identificar os verdadeiros donos de um determinado conteúdo digital (*fingerprinting*)
  - um documento pode facilmente ser classificado como pirateado ou não



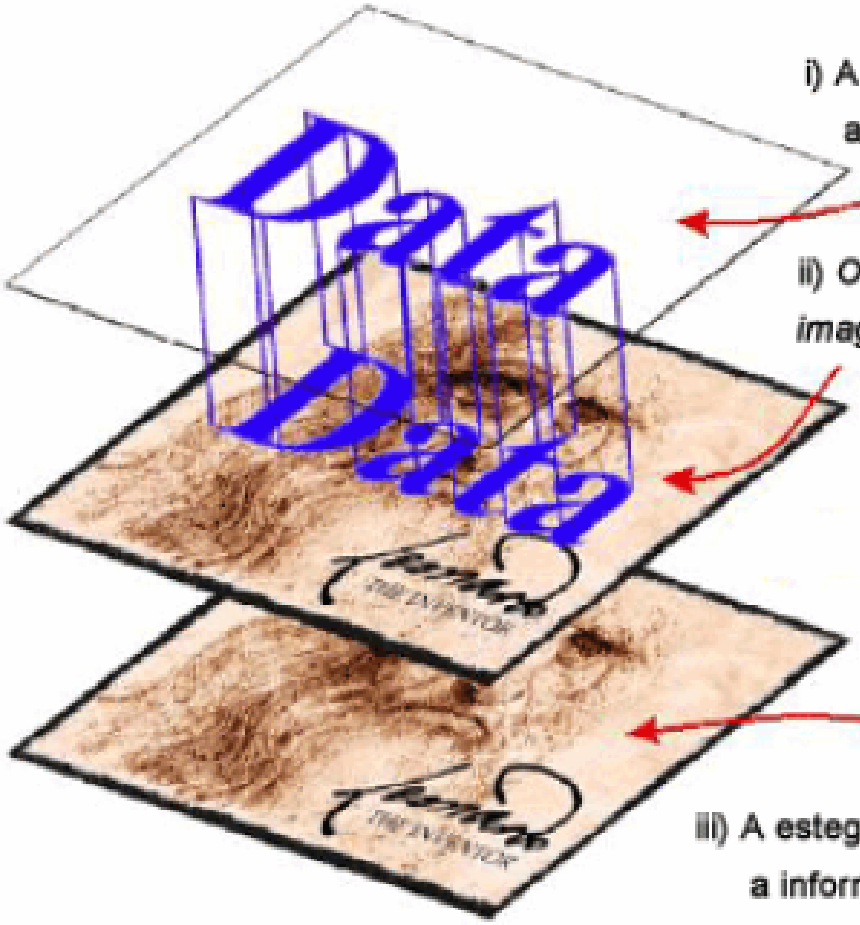
Impactos Sociais

- autenticação de documentos: pode-se inserir uma assinatura de autenticidade em documentos digitais.
  - um software apenas irá executar e/ou mostrar o conteúdo do documento caso ele seja autêntico
- comunicações privadas: o mascaramento de informações pode ser utilizado para estabelecer comunicações seguras entre os cidadãos através da rede mundial de computadores (internet)

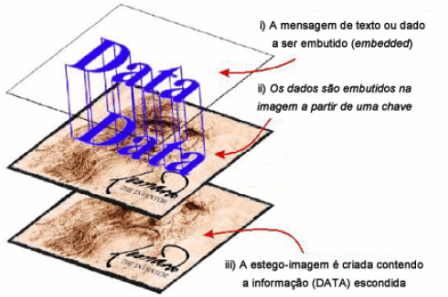


Impactos Sociais

- Uso ilegal:
  - fraudes e lavagem de dinheiro
  - comunicações criminais
  - roubo de propriedade intelectual
  - *hacking*
  - desvio de dinheiro
  - jogos e pornografia
  - assédio e extorsão
  - disseminação de vírus
  - pedofilia
  - tráfico de pessoas

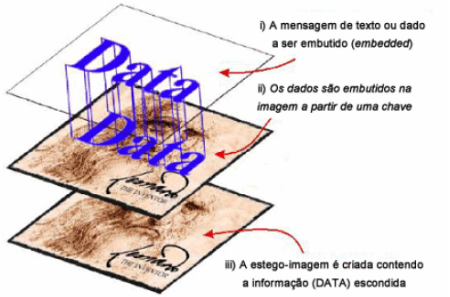


Técnicas de Esteganografia



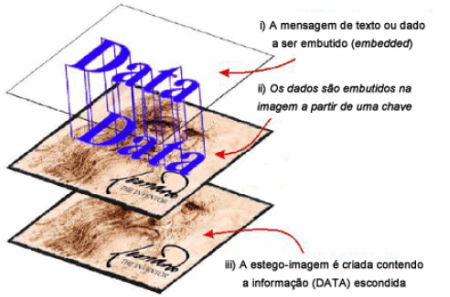
Técnicas de Esteganografia

- 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"



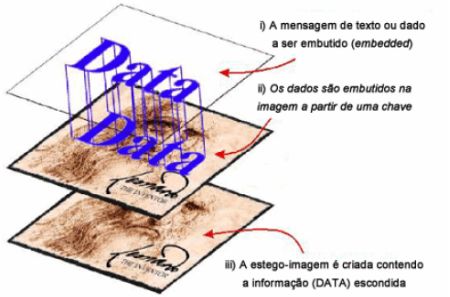
Técnicas de Esteganografia

- ***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)



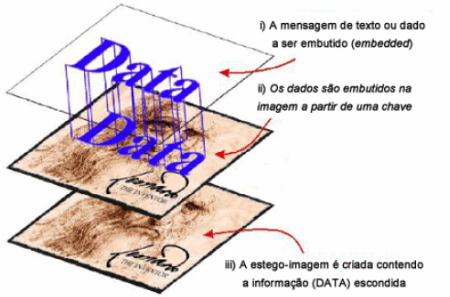
Técnicas de Esteganografia

- **Requisitos para sistemas esteganográficos**
  - Segurança
  - Robustez
  - Carga útil



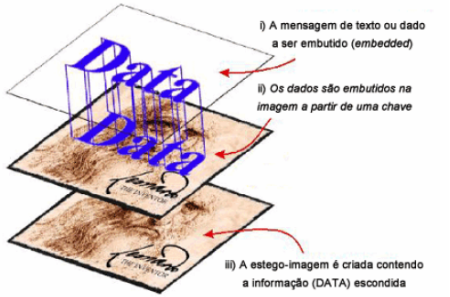
Técnicas de Esteganografia

- **Técnicas de codificação em imagem**
  - Inserção no bit menos significativo
  - Técnicas de filtragem e mascaramento
  - Algoritmos e transformações



Técnicas de Esteganografia

- **Inserção no bit menos significativo**
  - Técnicas baseadas em LSB podem ser aplicadas a cada byte de uma imagem de 32-bits (cada pixel codificado em quatro bytes)
    - Canal alfa (*alpha transparency*), canal vermelho (*red*), canal verde (*green*) e canal azul (*blue*)
  -
  - Seguramente, pode-se selecionar **um bit** (o menos significativo) em cada byte do pixel para representar o bit a ser escondido sem causar alterações perceptíveis na imagem



Técnicas de Esteganografia

Exemplo:

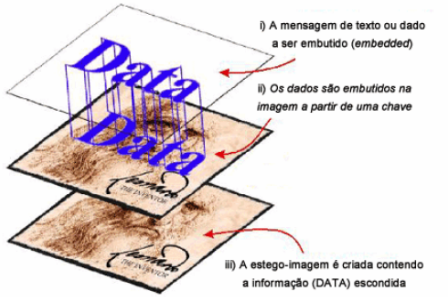
- Esconder a letra E dentro da porção de imagem
- Letra E pode ser escrita em forma binária segundo seu código ASCII como 10000011

(00100111 11101001 11001000 11101010) [a, R, G, B]
(10100111 11001000 11101001 11101000) [a, R, G, B]
(11001000 00100111 11101001 00100111) [a, R, G, B]

Porção de uma imagem de cobertura

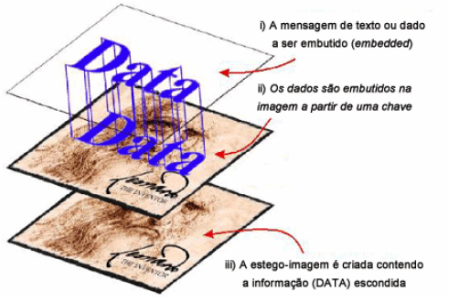
(00100111 11101000 11001000 11101010) [a, R, G, B]
(10100110 11001000 11101001 11101001) [a, R, G, B]
(11001000 00100111 11101001 00100111) [a, R, G, B]

Porção da estego-imagem gerada pela porção de imagem



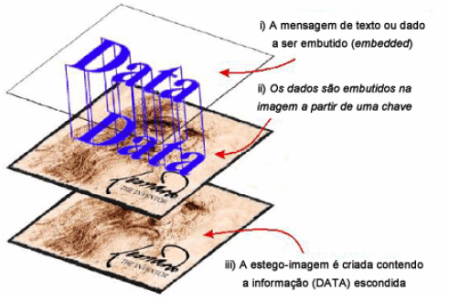
Técnicas de Esteganografia

- 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



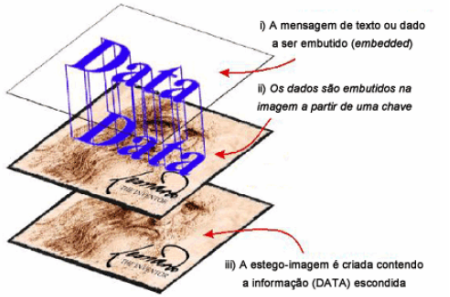
Técnicas de Esteganografia

- **Para prover maior robustez em inserções LSB**
  - Trabalhar com *streamgenerators* capazes de escolher várias posições diferentes e aleatórias na imagem de cobertura
  - Utilizar chaves esteganográficas seguindo o estilo da criptografia de chave pública



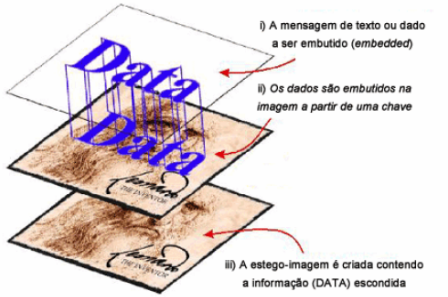
Técnicas de Esteganografia

- **Técnicas de filtragem e mascaramento**
  - São restritas às imagens em tons de cinza (*grayscale*)
  - Escondem a informação através da criação de uma imagem semelhante às marcações de *copyright* em papel
    - Isto acontece porque as técnicas de *watermarking* garantem que, mesmo se a imagem for modificada por métodos de compressão, a marcação não será removida



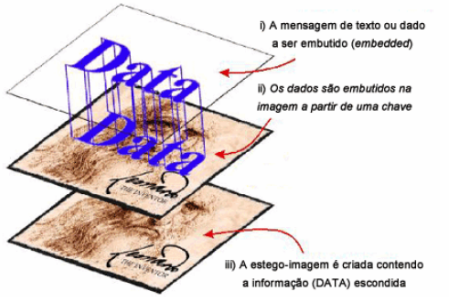
Técnicas de Esteganografia

- São técnicas mais robustas que a inserção LSB no sentido de gerarem estego-imagens imunes a técnicas de compressão e recorte
- Trabalham com modificações nos bits **mais** significativos das imagens
- As imagens de cobertura devem ser em tons de cinza porque estas técnicas não são eficientes em imagens coloridas
  - Modificações em bits mais significativos de imagens em cores geram alta quantidade de “ruído” tornando as informações detectáveis



Técnicas de Esteganografia

- **Algoritmos e transformações**
  - Manipulações LSB são rápidas e relativamente fáceis de serem implementadas
    - Produzem estego-imagens que podem ser facilmente destruídas através do manuseio da imagem com recorte e/ou compressão
  - Por outro lado, a compressão de imagens é uma das formas mais eficientes de armazenar imagens de alta qualidade
    - Algoritmos de transformação geralmente trabalham com brilho, saturação e compressão das imagens
  - Técnicas como a transformada discreta de cosseno, transformada discreta de Fourier e transformada Z
    - Usam como aliado o principal inimigo da inserção LSB: a compressão
    - Configuram-se como as mais sofisticadas técnicas de mascaramento de informações em imagens conhecidas



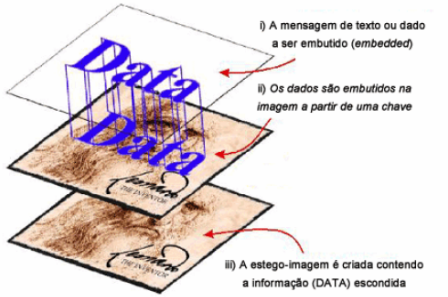
Técnicas de Esteganografia

- **Transformada Discreta de Cosseno (DCT)**
  - Baseada em cossenos, muito utilizada em processamento digital de imagens e compressão de dados. O valor da função da DCT de um vetor *p* de *pixels* de comprimento *n* é:

$$G_f = \frac{1}{2} C_f \sum_{t=0}^{n-1} p_t \cos\left(\frac{(2t+1)f\pi}{2n}\right),$$

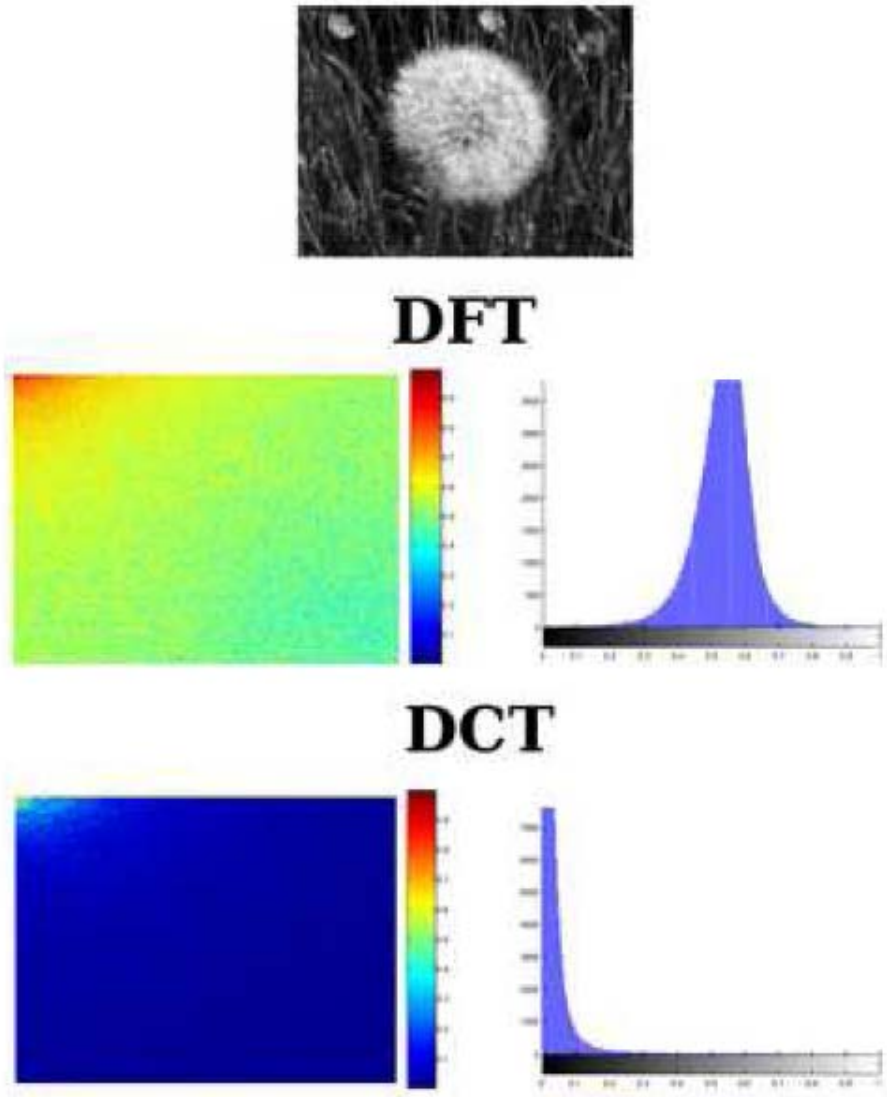
$$onde:\ C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f = 0 \\ 1 & f > 0 \end{cases} \text{para } f = 0, 1, \ldots, n-1.$$

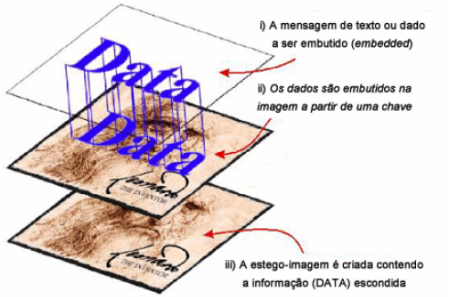
  - Muito utilizada na compressão de dados pois transfere a maior parte da informação contida para os primeiros elementos do vetor
    - otimizando o armazenamento (para compressão sem perdas)
    - facilitando a quantização dos valores (para compressão com perdas)



Técnicas de Esteganografia

- **Comparação entre DFT e DCT**

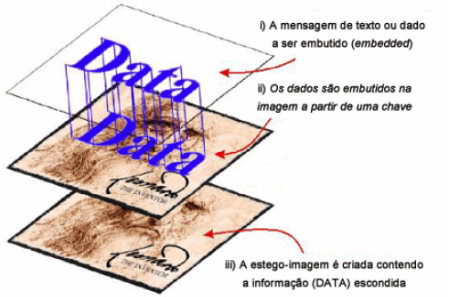




Técnicas de Esteganografia

- A recuperação dos dados transformados pode ser feita com a operação inversa, chamada de IDCT (*Inverse Discrete Cosine Transform*), que é dada pela fórmula:

$$p_t = \frac{1}{2} \sum_{j=0}^{n-1} C_f G_j \cos\left(\frac{(2t+1)j\pi}{2n}\right), \text{para } t = 0, 1, \ldots, n-1$$

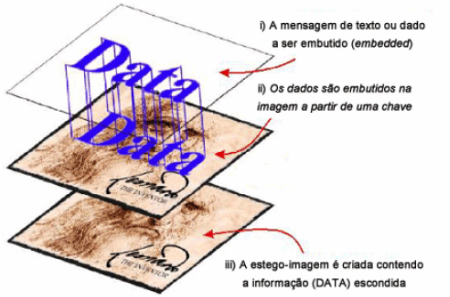


Técnicas de Esteganografia

- Em compressão de imagens e vídeos a maioria dos padrões usa a transformada discreta de cosseno do vetor p com n = 8 (JPEG e MPEG)
  - Os pixels de uma imagem tem correlação com seus vizinhos nas duas dimensões da imagem, e não apenas em uma, a DCT para ser usada na compressão de imagens também deve ser uma transformada bidimensional
  - A fórmula para uma matriz (ou seja uma imagem) **p** de tamanho **n**x**n** é:

$$G_{ij} = \frac{1}{\sqrt{2n}} C_i C_j \sum_{x=0}^{n-1} \sum y = 0^{n-1} p_{xy} \cos\left(\frac{(2y+1)j\pi}{2n}\right) \cos\left(\frac{(2x+1)i\pi}{2n}\right), \text{para } 0 \le i, j \le n-1$$

$$onde\, C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f = 0 \\ 1, & f > 0 \end{cases}$$

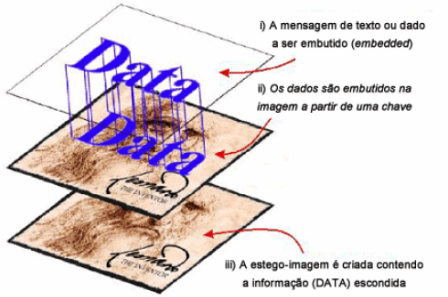


Técnicas de Esteganografia

- Essa transformada pode ser considerada como uma rotação (ou duas rotações consecutivas, uma em cada dimensão). A recuperação dos dados transformados pode ser feita usando a transformação inversa, conhecida como IDCT bidimensional:

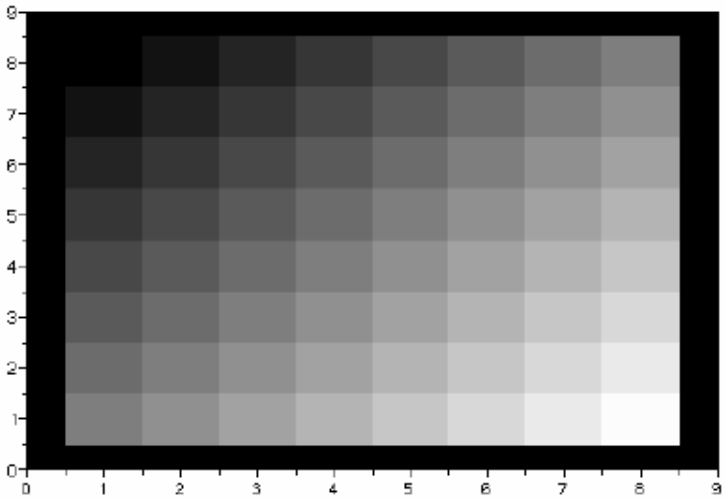
$$p_{xy} = \frac{1}{4} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \cos\left(\frac{(2x+1)i\pi}{2n}\right) \cos\left(\frac{(2y+1)j\pi}{2n}\right)$$

- Analogamente à transformada unidimensional, a transformada bidimensional resulta em uma matriz onde os coeficientes mais significativos se acumulam no canto superior esquerdo (início da matriz)

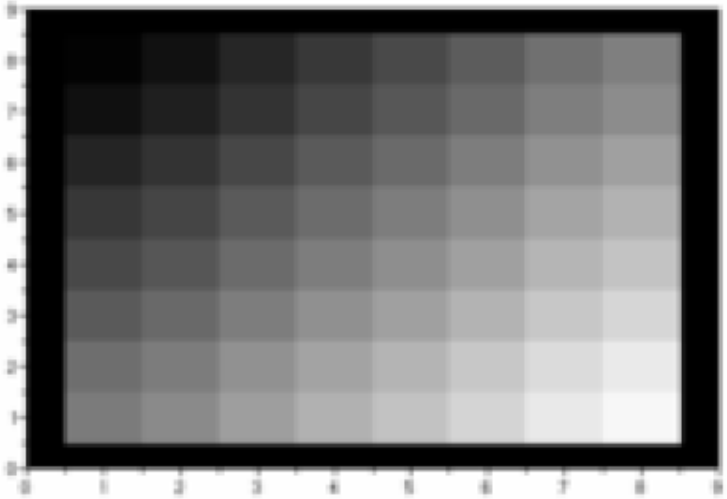


Técnicas de Esteganografia

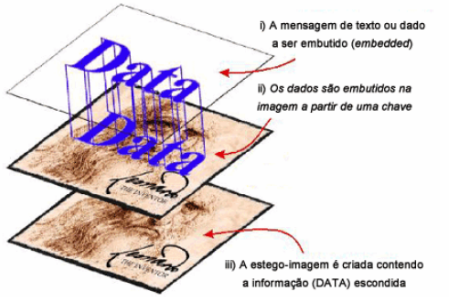
- **Exemplos**



(a) Degradê cinza sem passar por DCT



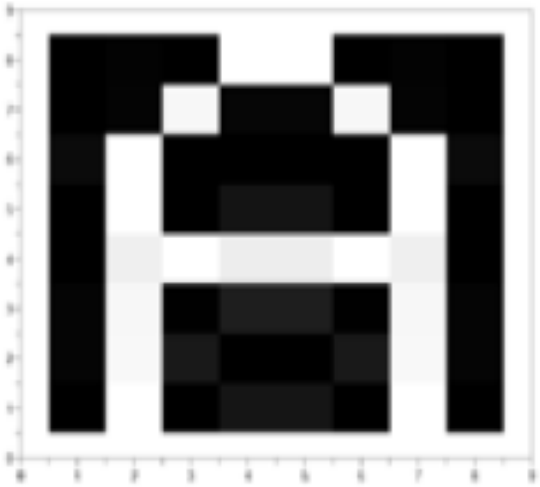
(b) Degradê cinza após DCT



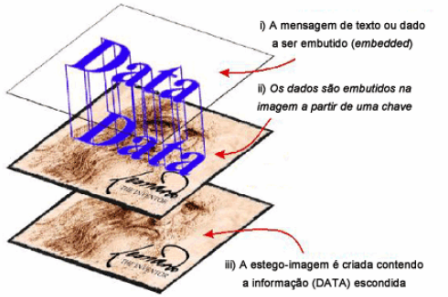
Técnicas de Esteganografia

- **Exemplos**

(c) Letra com fundo preto sem passar por DCT

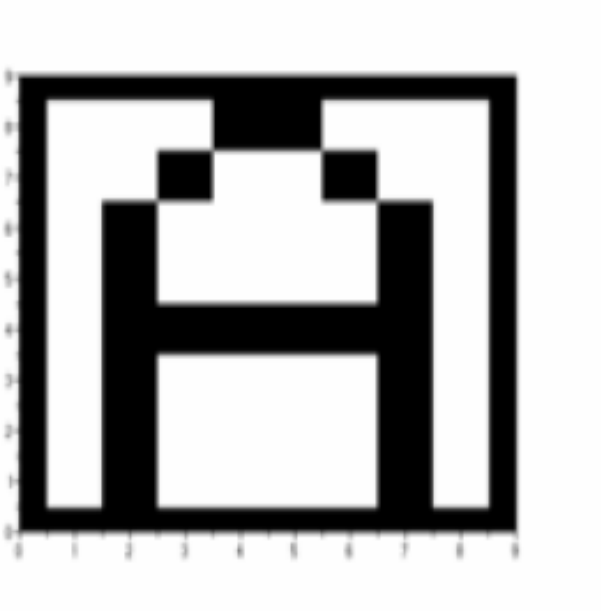


(d) Letra com fundo preto após passar por DCT

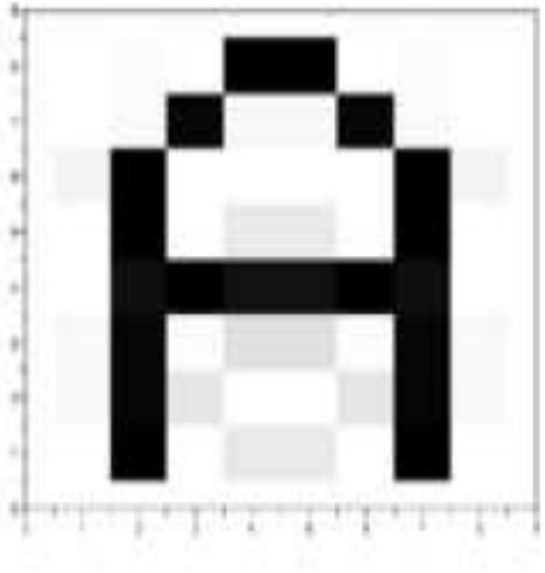


Técnicas de Esteganografia

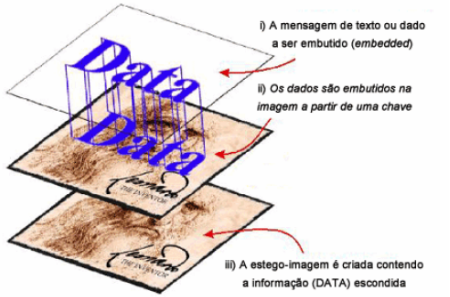
- **Exemplos**



(e) Letra com fundo branco sem passar por DCT



(f) Letra com fundo branco após passar por DCT



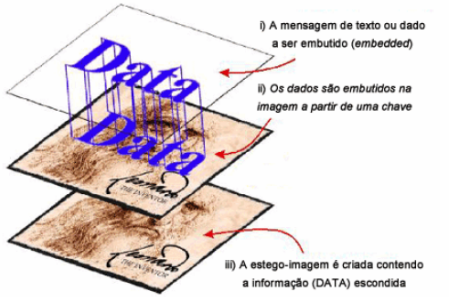
Técnicas de Esteganografia

- O padrão MPEG usa para a compressão de áudio uma variante da DCT conhecida como MDCT (*Modified Discrete Cosine Transform*). Esta transformada é bastante parecida com a transformada de cosseno unidimensional e sua fórmula é:

$$S_i = \sum_{k=0}^{n-1} x_k \cos\left(\frac{\pi}{2n}\left[2k+1+\frac{n}{2}\right](2i+1)\right), i = 0, 1, .., \frac{n}{2}-1$$

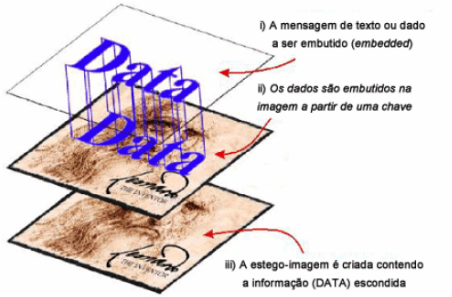
- E sua inversa, conhecida como IMDCT é dada por:

$$x_k = \sum_{i=0}^{n/2-1} S_i \cos\left(\frac{\pi}{2n}\left[2k+1+\frac{n}{2}\right](2i+1)\right), k = 0, 1, .., n-1$$



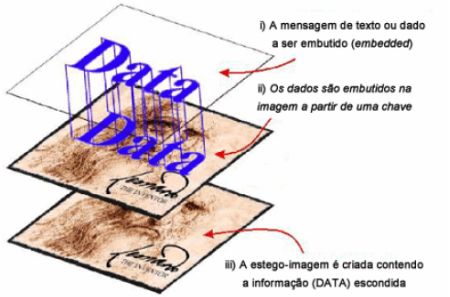
Técnicas de Esteganografia

- **Técnicas de Espalhamento de Espectro**
  - Nesta técnica, os dados escondidos são espalhados ao longo da imagem de cobertura
  - Uma stego-chave é usada para selecionar randomicamente os canais de freqüência
  - Utilizada em *frameworks* de comunicação, onde os dados parecem um ruído na transmissão dos dados



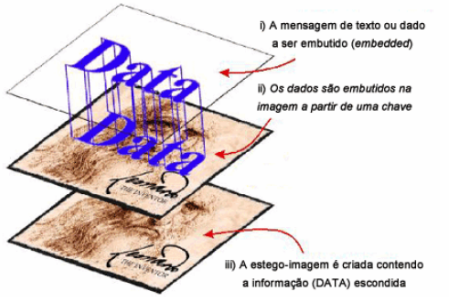
Técnicas de Esteganografia

- **Técnicas de Esteganografia em Vídeo**
  - Quando informações são escondidas dentro de um vídeo, normalmente é usado o método da DCT
    - É 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



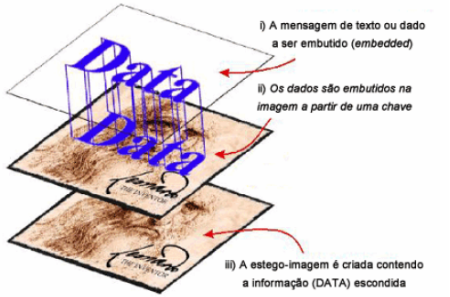
Técnicas de Esteganografia

- **Técnicas de Esteganografia em Áudio**
  - Desafio, pois o sistema auditivo humano (SAH) pode trabalhar em uma faixa muito grande de freqüências
    - O SAH pode captar até um bilhão de potências diferentes de sinais (altura) e até mil freqüências de sinais distintas
    - A sensitividade a ruído também é muito apurada. Uma perturbação em um arquivo de som pode ser detectada tão baixa quanto uma em 10 mihões de partes ou 80 dB em um ambiente comum
    - Apesar de ser tão poderoso para captar sinais e freqüências, o SAH não consegue fazer diferenciação de tudo que recebe
      - sons mais altos tendem a mascarar sons mais baixos



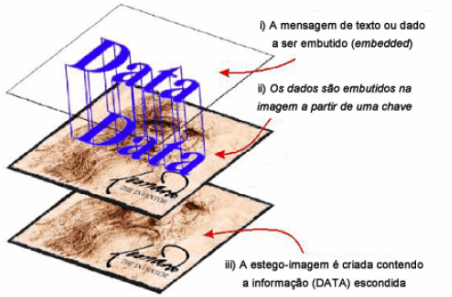
Técnicas de Esteganografia

- **Técnicas de Esteganografia em Áudio**
  - Há pelo menos dois aspectos que devem ser considerados: a representação digital do sinal que será usado e o caminho de transmissão do sinal
    - Quanto à representação digital, existem dois parâmetros críticos: método de quantização da amostra e taxa de amostragem temporal
      - Um dos formatos mais populares para representar amostras de áudio digital com alta qualidade é uma quantização linear de 16 bits chamada *Windows Audio-Visual* (WAV) e *Audio Interchange File Format* (AIFF)
      - Um outro formato popular para áudio de menor qualidade é a escala logarítmica de 8 bits μ−law. Estes métodos de quantização introduzem uma distorção no sinal que é mais evidente no caso da quantização de 8 bits μ−law



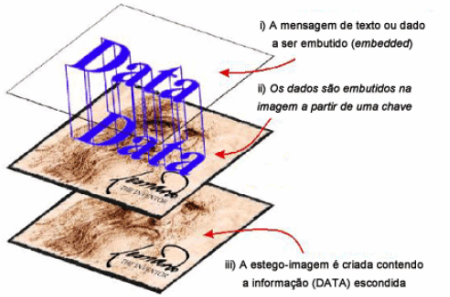
Técnicas de Esteganografia

- **Técnicas de Esteganografia em Áudio**
  - Taxas de amostragem típicas para áudio incluem 8kHz, 9,6 kHz, 10 kHz, 12 kHz, 16 kHz, 22,05 kHz e 44,1 kHz
    - Impactam na esteganografia à medida que impõem uma barreira para a porção usável do espectro de freqüências
    - Não é possível, por exemplo, introduzir modificações que têm componentes de freqüência acima de 4 kHz se o sinal foi amostrado a uma freqüência de 8 kHz
  - A última representação a ser considerada é a que produz perdas através do uso de algoritmos de compressão, tal como o MPEG-AUDIO
    - Estas representações modificam drastricamente o sinal, preservando somente as caracterísiticas que o ouvido humano pode perceber trabalhando com um modelo psico-acústico
    - Isso quer dizer que o som resultante será similar ao original, mesmo que o sinal resultante seja totalmente diferente



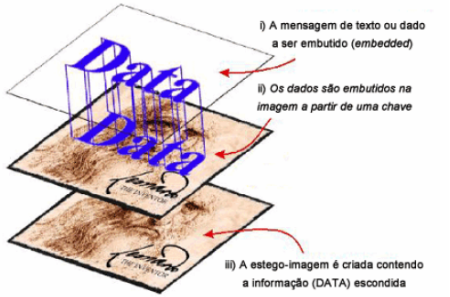
Técnicas de Esteganografia

- **Técnicas de Esteganografia em Áudio**
  - Existem muitos meios de transmissão pelos quais um sinal pode passar no caminho do codificador até o decodificador
    - A primeira classe de meios de transmissão que pode ser considerada é um ambiente digital fim a fim
      - O arquivo de som é copiado de uma máquina para outra e não é modificado. Como resultado, a amostra é exatamente a mesma, tanto no codificador quanto no decodificador
      - É a classe que menos impõe barreiras aos métodos esteganográficos
    - A próxima classe de meios de transmissão é quando um sinal é re-amostrado para uma taxa de amostragem maior ou menor que a original, mas permanece digital
      - Esta transformação preserva a magnitude absoluta e a fase da maioria dos sinais, mas muda as características temporais do mesmo



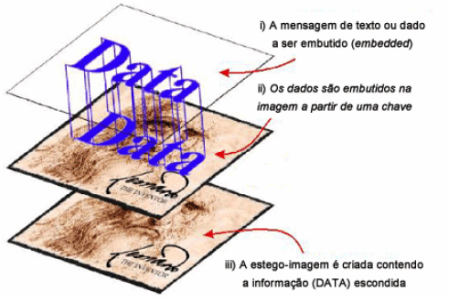
Técnicas de Esteganografia

- **Técnicas de Esteganografia em Áudio**
  - A terceira classe é a que apresenta um sinal que é "tocado" dentro de um dispositivo analógico, transmitido em uma linha analógica razoavelmente sem ruídos e depois re-amostrado (digital-analógico-digital)
    - Não são preservados a magnitude do sinal, a quantização inicial e a taxa de amostragem
    - Somente a fase do sinal é preservada
  - O último caso é quando um sinal é transmitido pelo ar ("tocado") e depois sofre nova amostragem com um microfone
    - O sinal estará possivelmente sujeito a modificações não lineares, resultando em mudanças de fase, amplitude, ecos e mudança de componentes
- **A representação do sinal e o caminho de transmissão devem ser considerados na escolha de um método de esteganografia**
  - A taxa de dados é muito dependente da taxa de amostragem e do tipo de som que está sendo codificado. Um valor típico de taxa é 16 bps, mas este valor pode variar de 2 bps a 128 bps



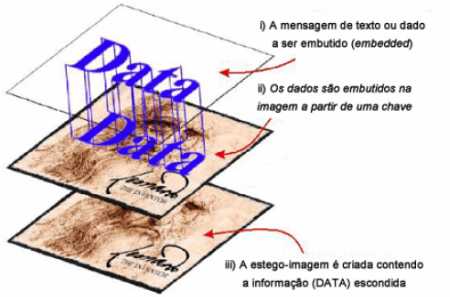
Técnicas de Esteganografia

- **Codificação *Low-bit***
  - Maneira mais simples de embutir dados dentro de outra estrutura
  - Através da substituição LSB de cada amostra por um codificador binário, é possível codificar uma grande quantidade de dados em um áudio
  - De maneira ideal, a capacidade do canal deve ser de pelo menos 1kb por segundo (kbps) por 1kHz,
    - Em um canal sem ruído, a taxa de transmissão será de 8kbps em uma amostra de 8kHz e 44kbps em uma amostra de 44kHz
    - Como conseqüência desta grande capacidade, ruídos audíveis são sempre introduzidos
    - O impacto destes ruídos diferem de acordo com o conteúdo do sinal
      - Em um stream de áudio de uma partida de futebol, o barulho da torcida ao fundo mascarará o ruído introduzido pela técnica de codificação low-bit
      - Em um stream de música clássica, o ruído seria audível



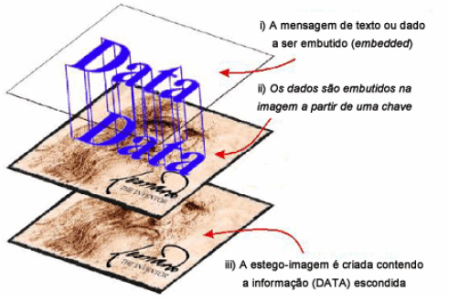
Técnicas de Esteganografia

- Codificação *Low-bit*
  - A maior desvantagem deste método é a sua baixa imunidade a manipulação
    - A informação codificada pode ser destruída pelo ruído do canal, na re-amostragem, entre outros
      - A menos que esta informação tenha sido codificada utilizando técnicas de redundância
  - Para serem robustas, estas técnicas reduzem a taxa de transmissão de dados normalmente pela metade
    - Na prática, este método deve ser utilizado somente em ambientes de transmissão digitais (digital-digital)



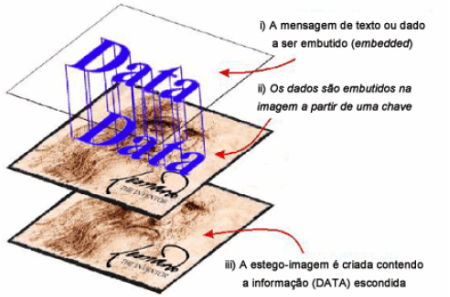
Técnicas de Esteganografia

- **Codificação em Fase**
  - Trabalha substituindo a fase de um segmento inicial de áudio por uma fase de referência que representa os dados a serem escondidos
  - É um dos mais efetivos métodos de codificação em termos de sinal percebido quando comparado com a percepção do ruído
    - Quando a relação de fase entre cada componente de freqüência é mudada muito drasticamente, uma dispersão de fase será notada
    - Entretanto se as modificações das fases forem pequenas, uma codificação inaudível é obtida
  - A codificação em fase trabalha com o fato de que os componentes de fase de um som não são tão perceptíveis pelo ouvido humano quanto é o ruído



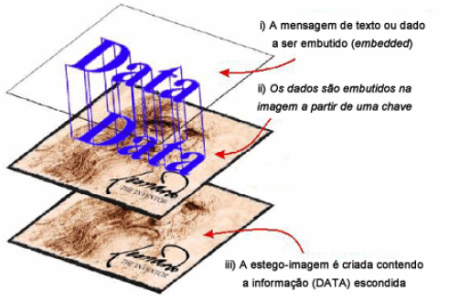
Técnicas de Esteganografia

- ***Spread Spectrum***
  - No contexto de esteganografia em áudio, o *spread spectrum* (SS) tenta espalhar informações secretas sobre o espectro de freqüências de áudio tanto quanto possível
  - A codificação usando SS é análoga à LSB que randomicamente espalha os bits da mensagem sobre todo o arquivo de som
    - Entretanto, diferentemente da codificação LSB, o SS espalha a mensagem secreta sobre o espectro de freqüências do arquivo de som utilizando um código que é independente do sinal
    - Assim, o sinal resultante ocupa uma banda superior à utilizada para a transmissão do sinal original



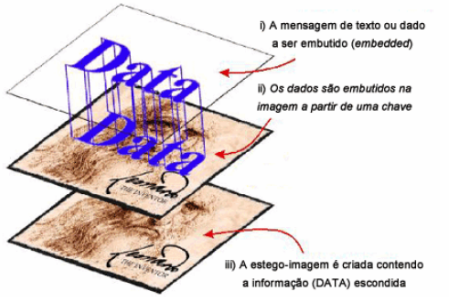
Técnicas de Esteganografia

- **Spread Spectrum**
  - Duas versões de SS podem ser utilizadas na esteganografia: *Direct-Sequence Spread Spectrum* (DSSS) e *Frequency Hopping Spread Spectrum* (FHSS)
    - No DSSS, a mensagem secreta é espalhada utilizando uma chave chamada *chip rate* e depois modulada com um sinal pseudo-randômico. Então a mensagem modulada é misturada com o sinal de cobertura
    - No FHSS, o espectro de freqüência do arquivo de áudio é alterado de tal forma que a mensagem seja codificada segundo um padrão de saltos entre as freqüências do espectro
  - O método utilizando SS tem bom potencial e é melhor em algumas circunstâncias que o LSB e a técnica de codificação em fase, pois oferece taxa de transmissão moderada enquanto mantém alto nível de robustez contra técnicas de remoção
    - Entretanto, o método SS tem a desvantagem de introduzir ruído no som de cobertura, assim como a abordagem LSB



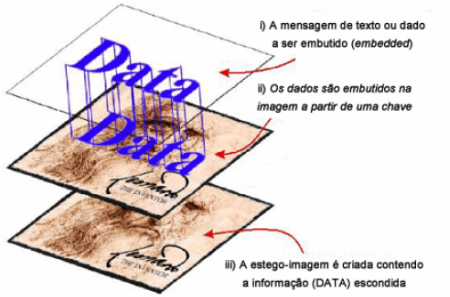
Técnicas de Esteganografia

- **Escondendo Informações com Eco**
  - Nas técnicas de esteganografia utilizando eco, a informação é escondida em um arquivo de som através da introdução de um eco
    - Assim como o método de SS, também apresenta a vantagem de permitir uma maior taxa de transmissão e robustez superior quando comparado com outros métodos indutores de ruído
  - Para esconder os dados de maneira eficaz, variam-se três parâmetros do sinal de eco: amplitude, taxa de deterioração e variação do sinal original (*offset*)
    - Os três parâmetros são configurados abaixo dos limites que o ouvido humano pode perceber facilmente
      - O *offset* é utilizado para representar a mensagem binária codificada. O codificador utiliza dois valores de tempo de atraso: um para representar o bit 1 (*offset*) e outro para representar o bit 0 (*offset* mais *delta*)



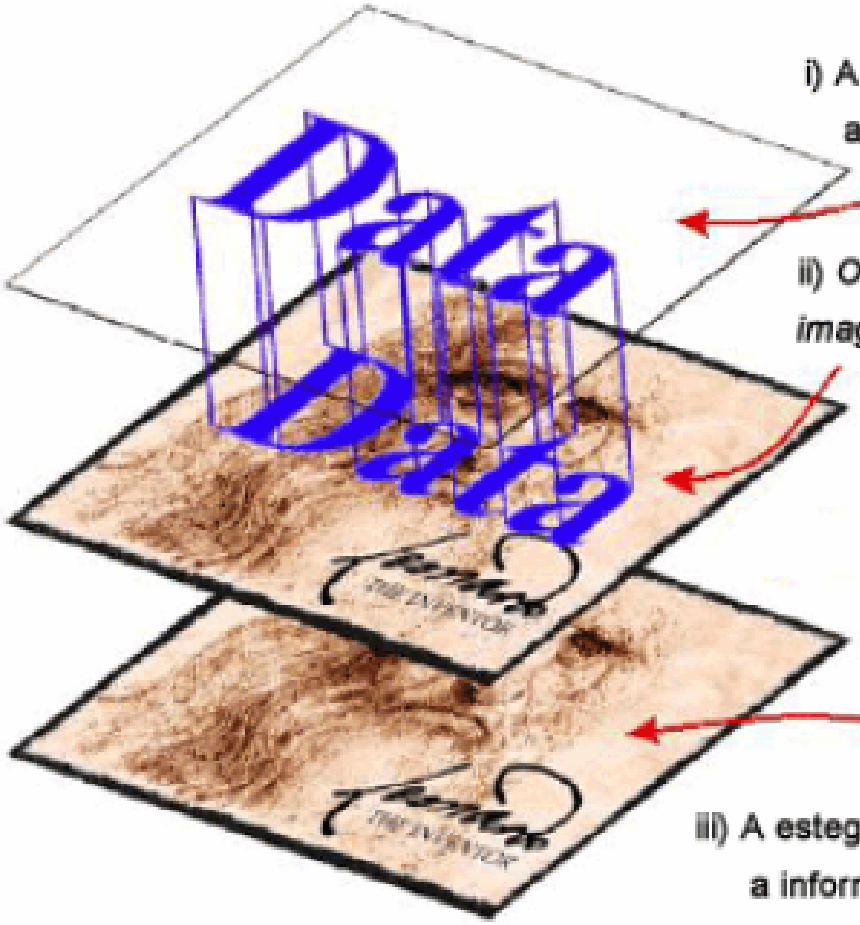
Técnicas de Esteganografia

- **Escondendo Informações com Eco**
  - Se um eco do sinal original for produzido, somente um bit de informação será codificado
    - Por isso, o sinal original é quebrado em blocos antes do processo de codificação começar. Uma vez que o processo de codificação é completado, os blocos são concatenados novamente
    - A cada bloco é assinalado o valor “1” ou “0” baseado na mensagem que será transmitida
  - Ao utilizar esta implementação de esteganografia em eco, o processo pode resultar em um sinal que possui uma mistura de ecos, acarretando no aumento do risco de detecção

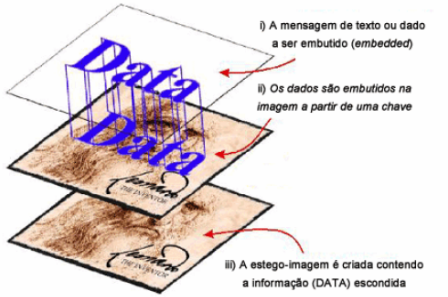


Técnicas de Esteganografia

- **Escondendo Informações com Eco**
  - Para extrair a mensagem secreta do stego-sinal, o receptor deve quebrar o sinal na mesma seqüência do bloco usada durante o processo de codificação
    - A função de autocorrelação do sinal (uma transformada de *Fourier* no espectro de freqüência do sinal) pode ser usada para decodificar a mensagem, pois revela um ponto em cada *offset* do tempo do eco, permitindo que a mensagem seja reconstruída
  - Através da utilização dos métodos descritos é possível codificar e decodificar informações na forma de bits dentro de um fluxo de áudio com alterações mínimas do som original em uma taxa aproximada de 16 bps
    - Estas alterações mínimas são as que, na média, o ouvido humano não pode diferenciar entre o sinal original e o sinal alterado

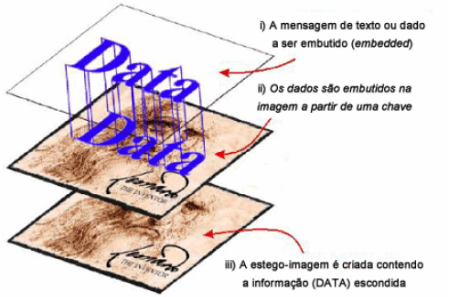


Técnicas de Esteganálise



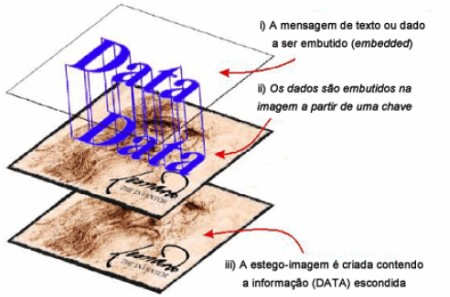
Técnicas de esteganálise

- Grande parte das técnicas de esteganografia possuem falhas e/ou inserem artefatos (padrões) detectáveis nos objetos de cobertura
- Algumas vezes, basta um agressor (alguém interessado em descobrir indevidamente a mensagem) fazer um exame mais detalhado destes artefatos para descobrir que há mensagens escondidas
- Outras vezes, o processo de mascaramento de informações foi robusto e as tentativas de recuperar ilicitamente as mensagens podem ser bastante difíceis
- Ao campo das pesquisas relacionado às tentativas de descobrir mensagens secretas dá-se o nome de **esteganálise**, uma alusão à criptoanálise, o campo de pesquisas relacionado à quebra de códigos



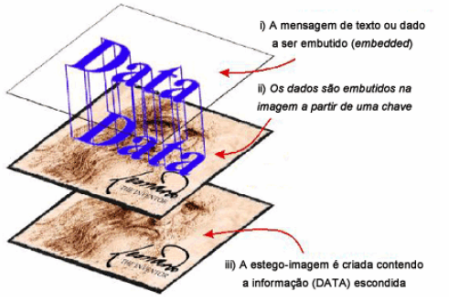
Técnicas de esteganálise

- **Atualmente, as pesquisas em esteganálise estão mais concentradas em simplesmente identificar a presença de mensagens escondidas ao invés de extraí-las**
  - Recuperar os dados escondidos, no momento, está além da capacidade da maioria dos testes porque muitos algoritmos de mascaramento utilizam geradores aleatórios criptográficos muito seguros para misturar a informação no processo de mascaramento
  - Na maioria das vezes, os bits são espalhados pelo objeto de cobertura
- **Os melhores algoritmos de esteganálise não são capazes de dizer onde está a informação, mas, provavelmente, podem dizer que os dados estão presentes**



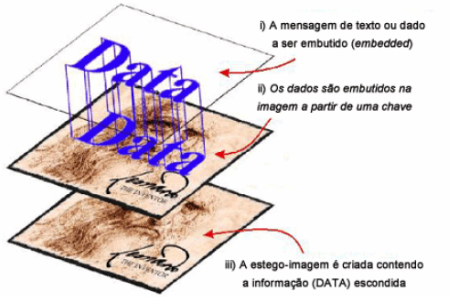
Técnicas de esteganálise

- **A identificação da existência de uma mensagem escondida é suficiente para um agressor**
  - As mensagens são, muitas vezes, frágeis e um agressor pode, sem muita dificuldade, destruir a mensagem mesmo sem tê-la recuperado
  - Algumas vezes, os dados podem ser destruídos simplesmente destruindo o objeto de cobertura
  - Ou, basta aplicar um gerador de números aleatórios nos bits menos significativos destruindo qualquer mensagem (informação) ali presente



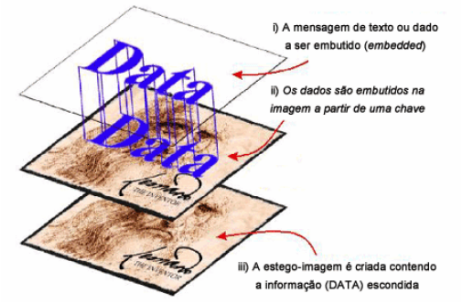
Técnicas de esteganálise

- Todos os ataques dependem da identificação de algumas características de um objeto de cobertura (como imagens, vídeos, sons) que foram alteradas pelo processo de mascaramento
- Não há qualquer garantia de que um algoritmo *esteganográfico* possa resistir à *esteganálise*



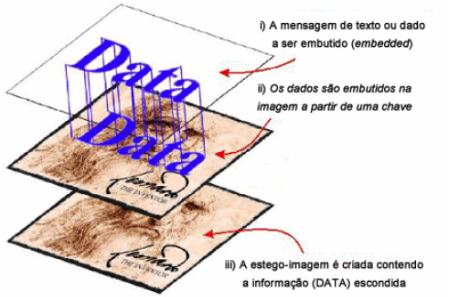
Técnicas de esteganálise

- **Tipos de Ataques**
  - Ataques aurais
    - Alguns ataques retiram 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 signifitivos da imagem
    - Ruído completamente randômico freqüentemente revela a existência de uma mensagem escondida, uma vez que as imperfeições de câmeras, scanners e outros meios digitalizadores sempre deixam marcas de grande estrutura nos bits menos significativos
    - Além disso, o cérebro humano é capaz de descobrir as mais sutis diferenças. Esta é a razão pela qual muitas marcações de áudio (*audio watermarking*) de grandes gravadoras são frustradas graças aos ouvidos de músicos bem-treinados



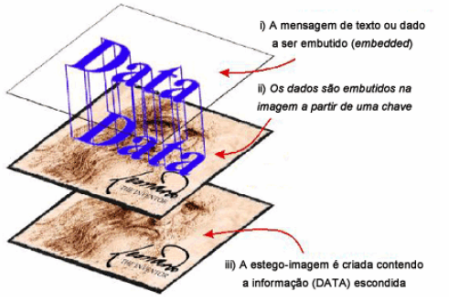
Técnicas de esteganálise

Ataques aurais



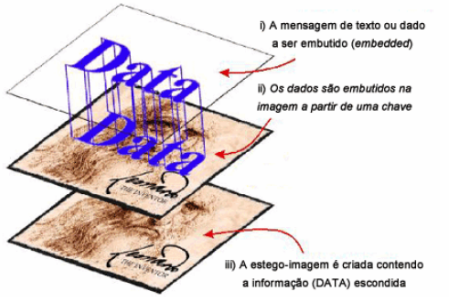
Técnicas de esteganálise

- **Ataques Estruturais**
  - O formato do arquivo de dados freqüentemente muda assim que outra mensagem é inserida. Nesses casos, um sistema capaz de analisar padrões estruturais seria capaz de descobrir a mensagem escondida
    - Por exemplo, ao esconder mensagens em imagens indexadas (baseadas em paletas de cores), pode ser necessário usar versões diferentes de paletas
      - muda as características estruturais da imagem de cobertura, logo as chances de detecção de uma mensagem escondida aumentam



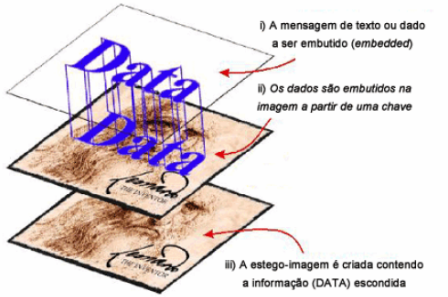
Técnicas de esteganálise

- **Ataques estatísticos**
  - Os padrões dos pixels e seus bits menos significativos freqüentemente revelam a existência de uma mensagem secreta nos perfis estatísticos
  - Os novos dados não têm os mesmos perfis esperados
  - Muitos dos estudos de matemática estatística objetivam classificar se um dado fenômeno ocorre ao acaso
    - Estas técnicas estatísticas também podem ser usadas para determinar se uma dada imagem e/ou som têm alguma mensagem escondida
    - Isto é possível porque, na maioria das vezes, os dados escondidos são mais aleatórios que os dados que foram substituídos no processo de mascaramento
      - Alguns testes conhecidos são X2 (*Chi Squared Test*), e o *RS-Steganalysis*



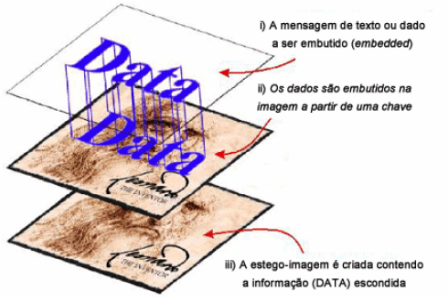
Principais Técnicas (ataques estatísticos)

- **X^2 (*Chi-Square Test*)**
  - O teste *Chi-quadrado* permite verificar a semelhança entre categorias discretas e mutuamente exclusivas (por exemplo, diferenças de comportamento entre homens e mulheres). Cada indivíduo ou item deve pertencer a uma e somente uma categoria
  - As seguintes suposições precisam ser satisfeitas:
    a) Os dois grupos são independentes
    b) Os itens de cada grupo são selecionados aleatoriamente
    c) As observações devem ser freqüências ou contagens
    d) Cada observação pertence a uma e somente uma categoria
    e) A amostra deve ser relativamente grande (pelo menos 5 observações em cada célula e no caso de poucos grupos (2 x 2) pelo menos 10)



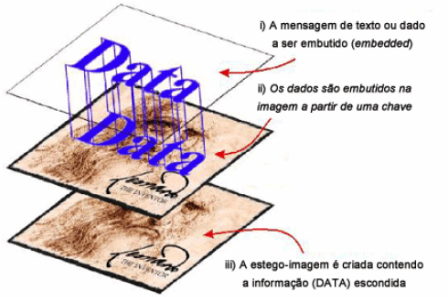
Principais Técnicas (ataques estatísticos)

- **X^2 (*Chi-Square Test*)**
  - A hipótese H0 é que não existe diferença entre as freqüências (contagens) dos grupos
  - A hipótese alternativa é que existe diferença
  - Para se testar as hipóteses é preciso testar se existe diferença significativa entre as freqüências observadas e as esperadas em cada extrato



Principais Técnicas (ataques estatísticos)

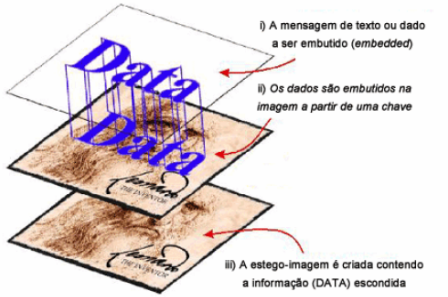
- **X^2 (*Chi-Square Test*)**
  - Exemplo: Deseja-se saber se existe diferença na percepção de homens e mulheres em relação a uma afirmativa feita
    - As categorias são homens e mulheres e número total de mulheres é diferente do número total de homens
    - Cada item pertence a uma e somente uma destas categorias
    - Da mesma maneira, cada indivíduo poderá responder somente de uma forma
    - O resultado deve ser comparado com o que seria obtido se não houvesse diferença entre os grupos
    - Para ilustrar, supõe-se 99 homens e 99 mulheres na amostra. Neste caso, se os grupos se comportassem da mesma forma e respondessem igualmente para cada situação o resultado seria 33 pessoas em cada célula



Principais Técnicas (ataques estatísticos)

- Em geral os grupos não são igualmente distribuídos
- O valor esperado de cada célula é uma proporção do valor total

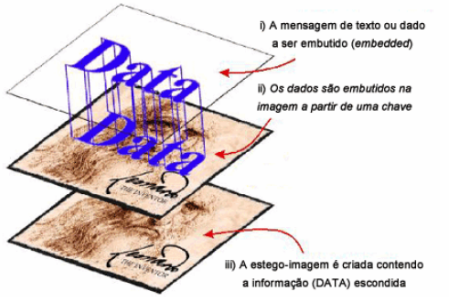
	Homens	Mulheres	Total
Concorda	58	35	93
Neutro	11	25	36
Não concorda	10	23	33
Total	79	83	162



Principais Técnicas (ataques estatísticos)

- Os valores esperados para cada célula são obtidos multiplicando o percentual da coluna pelo total da linha, isto é, total da linha x (total coluna/total)
  - Por exemplo: 45,35 = 93 x 79/162
- O valor de chi-quadrado para cada célula é a diferença ao quadrado entre o valor esperado e o valor medido dividido pelo valor esperado, conforme fórmula a seguir

$$\chi^2 = \frac{(ValorEsperado - ValorMedido)^2}{ValorEsperado}$$

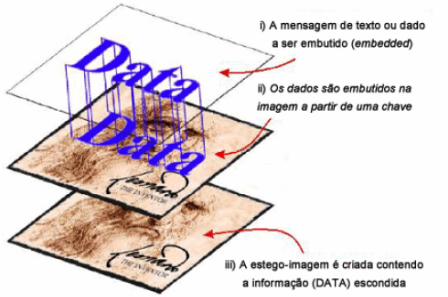


Principais Técnicas (ataques estatísticos)

- O *chi* total é a soma dos valores de cada célula. O valor de X^2 calculado deve ser comparado com o valor de *chi* tabelado. Quanto maior o valor de *chi* calculado, maior a diferença. Para obter o valor de *chi* tabelado (tabela de distribuição X^2) deve-se escolher o valor do nível de significância (alfa) adequado para a situação

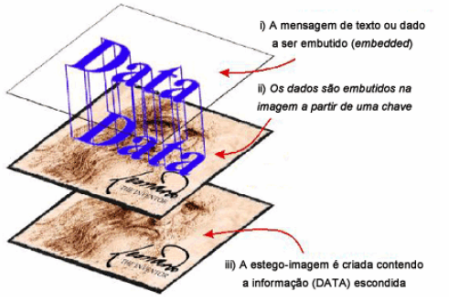
Cálculo do X^2

Esperado				
		Homens	Mulheres	Total
	Concorda	45,35185	47,64815	93
	Neutro	17,55556	18,44444	36
	Não concorda	16,09259	16,90741	33
	Total	79	83	162
Chi				
		3,527434	3,357437	
		2,447961	2,329987	
		2,306632	2,195469	
Chi Tabelado =	2			



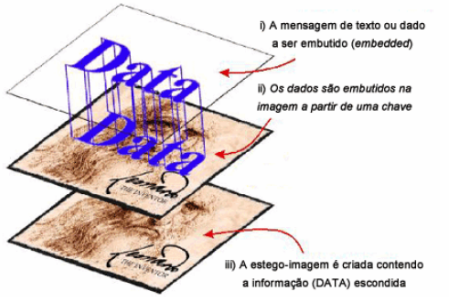
Principais Técnicas (ataques estatísticos)

- Em esteganografia, as funções de cobertura de alguns softwares, por exemplo o Ezstego reescrevem os bits menos significativos dos bytes sorteados para tal fim guardando seus índices. Isso gera valores modificados de bytes que só diferem, quando diferem, no último bit
- Este par de valores (iniciais e transformados) será chamado de PoVs (*Pair of Values*). Se os bits usados para escrever no bit menos significativo são igualmente distribuídos, a freqüência dos valores de cada PoV se torna igual. A idéia dos ataques estatísticos é comparar uma distribuição de freqüência teórica esperada em um histograma com algumas distribuições observadas em possíveis imagens que podem ter sido modificadas. A distribuição de freqüência teórica é obtida com o chi tabelado usando o nível de significância adequado (alfa)



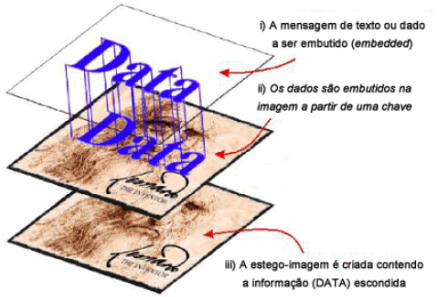
Principais Técnicas (ataques estatísticos)

- Um ponto crítico é como obter a distribuição de freqüência teórica
- Esta freqüência não deve ser derivada da amostra que está sendo analisada pois a amostra pode ter sido modificada por esteganografia
- O problema é que na maioria dos casos não se tem a amostra original para comparar
- Na amostra original, a freqüência teórica esperada é a média aritmética das duas freqüências de um PoV
  - Isso porque a função mascaramento do método esteganográfico sobrescreve os bits menos significativos e isso não muda a soma destas duas freqüências (freqüência de um PoV). A contagem dos valores de freqüência pares é transferida para o valor ímpar correspondente de freqüência em cada PoV e vice-versa. Este fato permite obter a distribuição de freqüência esperada da amostra analisada, não necessitando da original para o teste



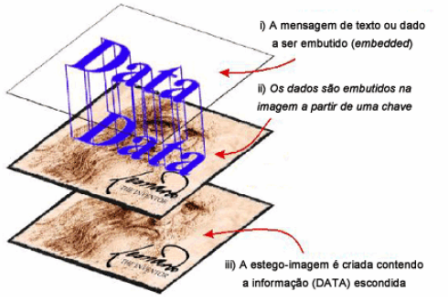
Principais Técnicas (ataques estatísticos)

- Análise RS
  - Consiste na análise das inter-relações entre os planos de cores presente nas imagens analisadas. A classificação é feita pontualmente, sem utilização de treinamento e é dependente do contexto da imagem analisada
  - Este é um dos métodos de detecção mais robustos disponíveis. Para análise podem ser utilizadas imagens coloridas ou em tons de cinza
  - Não existe distinção na profundidade de cores na imagem analisada, isto pode ser válido tanto para imagens de 8 bpp (*bits por pixel*) quanto para imagens de 32 bpp



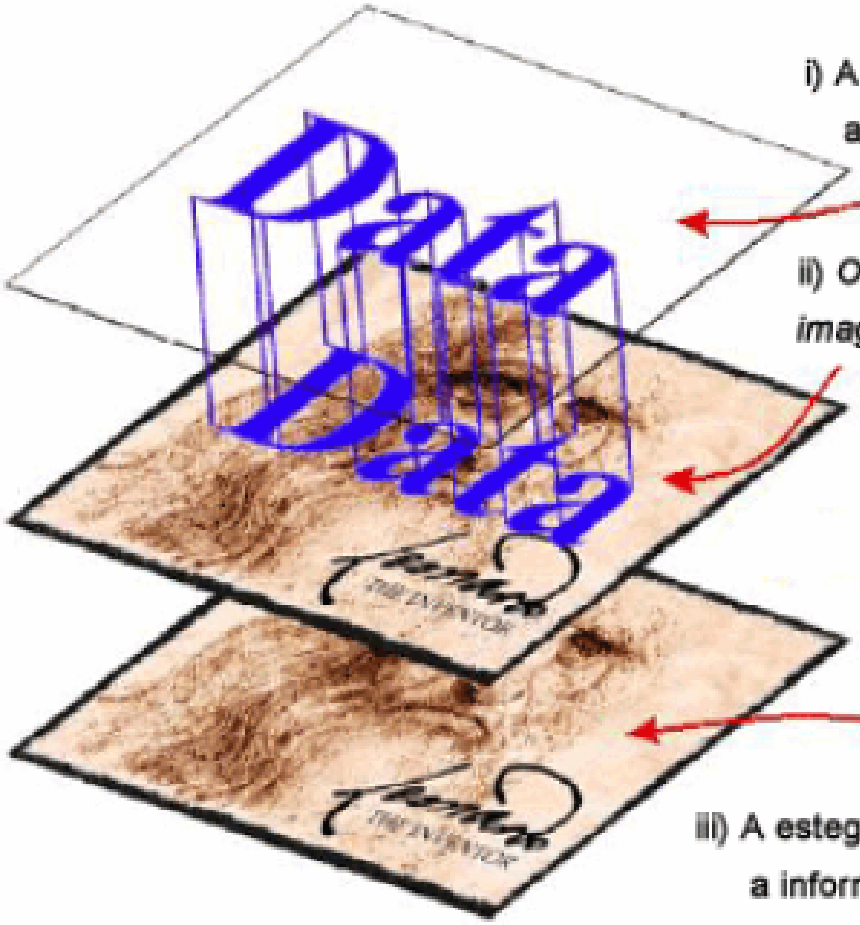
Principais Técnicas (ataques estatísticos)

- **Métricas de qualidade de imagens (*Image Quality Metrics*)**
  - São utilizadas, de forma geral, na avaliação de codificação de artefatos, predição de desempenho de algoritmos de visão computacional, perda de qualidade devido a inadequabilidade de algum sensor, entre outras aplicações
  - Nesta abordagem, essas mesmas métricas são utilizadas para construir um discriminador de imagens de cobertura (sem conteúdo escondido) de estego-imagens (com conteúdo escondido) através da utilização de regressão multi-variada. A classificação é feita por um discriminante linear após um certo treinamento (estabilização dos coeficientes da regressão multi-variada)

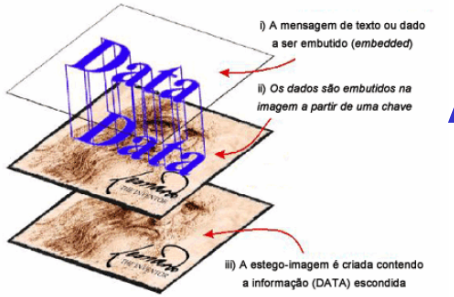


Principais Técnicas (ataques estatísticos)

- **Métricas de tons contínuos e análise de pares de amostragem (*Continuous Tone Metrics and Sample Pair Analysis*)**
  - Consiste em analisar as relações de identidade estatística existentes sobre alguns conjuntos de pixels considerados
  - As identidades observadas são muito sensíveis ao mascaramento LSB e as mudanças nestas identidades podem indicar a presença de conteúdo escondido

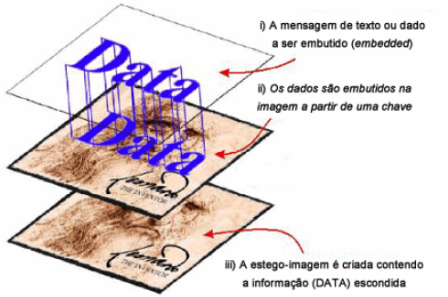

i) A mensagem de texto ou dado
a ser embutido (*embedded*)
ii) *Os dados são embutidos na*
imagem a partir de uma chave
iii) A estego-imagem é criada contendo
a informação (DATA) escondida

Aplicações



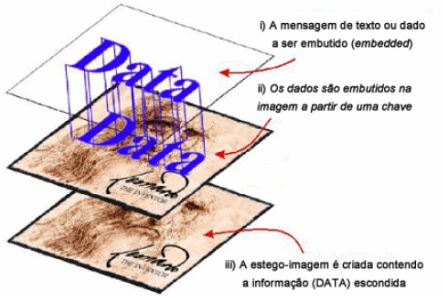
Aplicações Militares

- Em atividades militares, a descoberta de comunicações secretas pode levar a um ataque imediato do inimigo
- Mesmo com a criptografia, a simples detecção do sinal é fatal pois descobre-se não somente a existência de inimigos como também a sua posição
- Unindo o conceito de ocultamento de informação com técnicas como modulação em espalhamento de espectro torna-se mais difícil de os sinais serem detectados ou embaralhados pelo inimigo



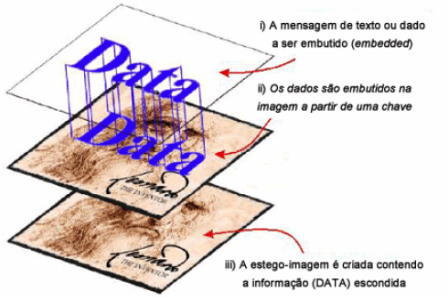
Aplicações Militares

- Várias técnicas relacionadas a ocultamento de informação levam em consideração sistemas com níveis de segurança
- Em redes de computadores militares existem vários níveis de segurança. Um vírus ou um programa malicioso se propaga dentro do sistema passando de níveis de segurança inferiores para os superiores
- Uma vez que alcança seu objetivo, tenta passar informações sigilosas para setores de nível de segurança menores
- Para isso, ele se utiliza de técnicas de ocultamento para esconder informações confidenciais em arquivos comuns de maneira que o sistema lhe permita ultrapassar níveis de segurança diferentes



Aplicações
Escondendo o remetente

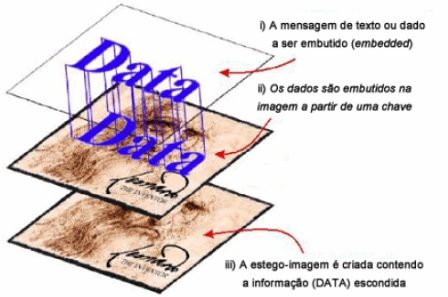
- Existem situações onde se deseja enviar uma mensagem sem que seja possível descobrir quem a enviou
- Geralmente, esse tipo de situação é mais uma característica de atividades ilegais onde os criminosos envolvidos não desejam ser descobertos se sua mensagem for rastreada
- Entretanto, essa situação também tem aplicações em atividades legais onde se deseja que a privacidade do remetente seja mantida
  - ➢ Exemplo
    - registros médicos ou votações online



Aplicações
Ética

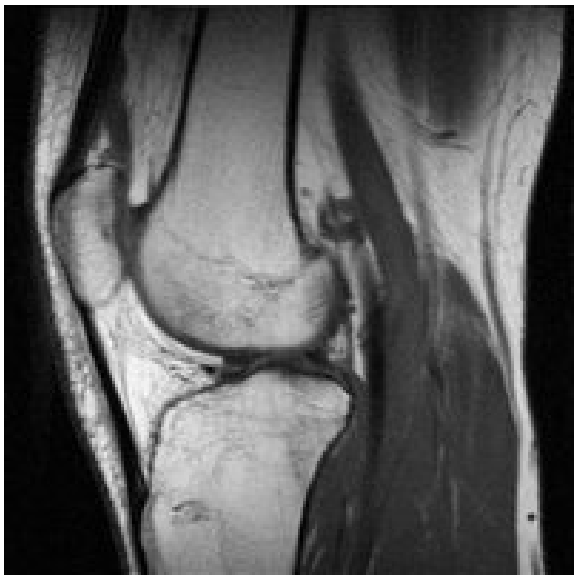
- Um tema importante a ser considerado pelo criador das técnicas de ocultamento de informação é a ética
- Algumas pessoas podem encontrar meios de se aproveitar das vantagens dessa 'comunicação invisível e não rastreável' para executar ações ilícitas como difamações, chantagens ou seqüestros
- É um dever dos desenvolvedores de sistemas de ocultamento de informação prestar atenção aos abusos que podem ocorrer

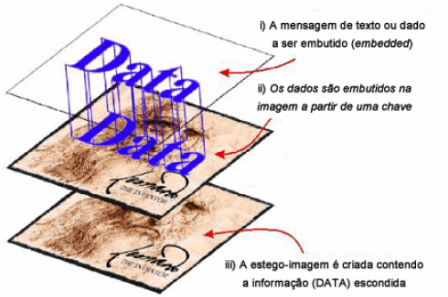
SERÁ ??



Aplicações DICOM

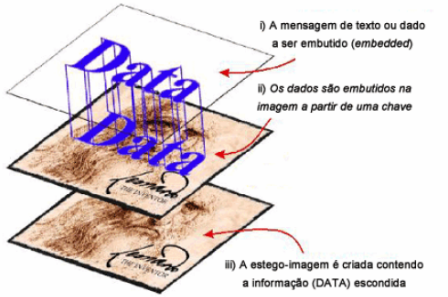
- Existem também grandes aplicações na área da indústria médica no que diz respeito a imagens médicas
- Normalmente, é usada uma forma de comunicação padrão chamada DICOM (*digital imaging and communications in medicine*) que separa a imagem das informações relativas ao paciente e ao exame como o nome, data e o médico





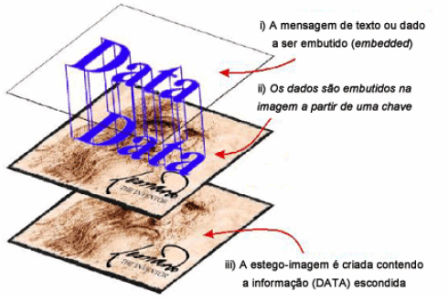
Aplicações DICOM

- **Em alguns casos, a ligação entre os dados e a imagem é perdida**
  - Se as informações fossem ocultadas dentro da própria imagem, não haveria risco de a imagem se separar dos dados
  - Estudos recentes na área de compressão de imagens médicas revelam que tais procedimentos não são impeditivos



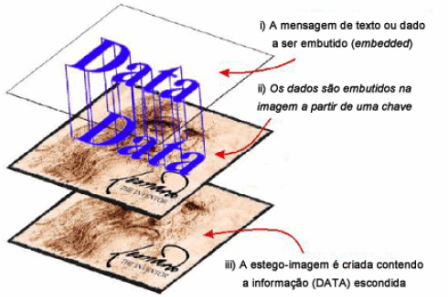
Aplicações Copyright

- Em alguns casos, se deseja monitorar um dado arquivo com direitos autorais que está sendo distribuído na Internet, por exemplo
- Utiliza-se um programa robô que procura em *sites* a divulgação desses arquivos
- O programa baixa os arquivos, tenta retirar qualquer informação que possa estar escondida e compara com a informação do arquivo original
- Caso as informações sejam compatíveis, sabe-se que o arquivo está sendo distribuído de maneira ilegal



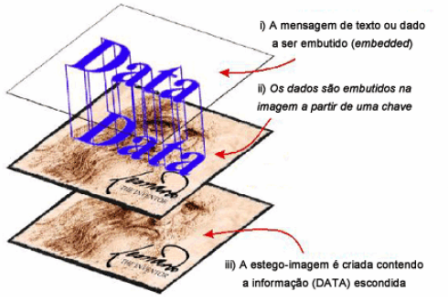
Aplicações
Economia de banda

- Pode-se também inserir pedaços de informações dentro dos dados que estão sendo transmitidos para que o público que a receba possa usar
- Como exemplo, pode-se ter informações de um dado produto anunciado por uma rádio onde o cliente, com um simples apertar de botão, pode descobrir o preço, local de venda mais próximo ou fabricante
- Essas informações são enviadas sem a necessidade de se usar outra banda para transmissão pois ela é inserida no próprio sinal de rádio sem prejudicar a qualidade do mesmo



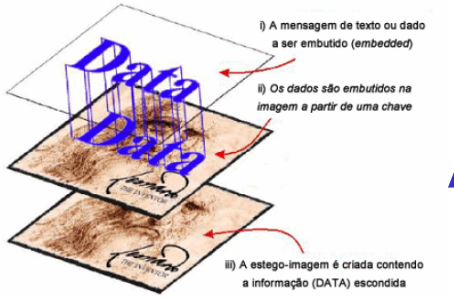
Aplicações Música

- Outra aplicação seria inserir uma forma de indexação de músicas a serem armazenadas no banco de dados de uma estação de rádio para que elas sejam acessadas de maneira mais fácil
- Pode-se inserir também dados da transmissão como país de origem, autor e produtora



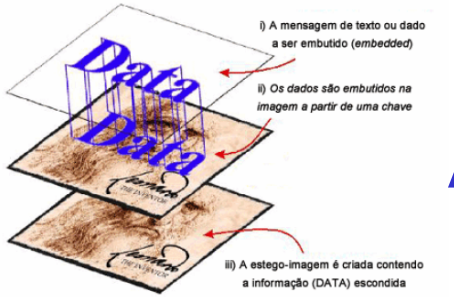
Aplicações

- Atualmente a esteganografia tem sido também explorada em ramos de sistemas de detecção de intrusão e em sistemas de arquivos
- Outras aplicações de esteganografia incluem as técnicas de autenticação, criptografia e rastreamento de documentos, que por serem utilizadas normalmente em conjunto com a técnica de marca d'água



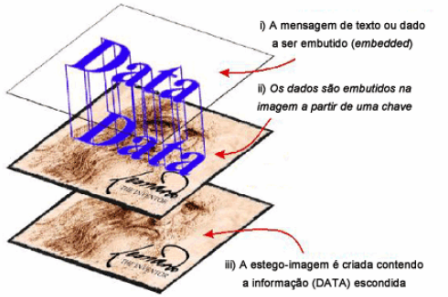
Aplicações

- Marcas D'Água
  - O grande crescimento dos sistemas de multimídia interligados pela rede de computadores nos últimos anos apresenta um enorme desafio nos aspectos tais como propriedade, integridade e autenticação dos dados digitais (áudio, vídeo e imagens estáticas). Para enfrentar tal desafio, o conceito de marca d'água digital foi definido
  - Uma marca d'água é um sinal portador de informação, visualmente imperceptível, embutido em uma imagem digital
  - A imagem que contém uma marca é dita imagem marcada ou hospedeira



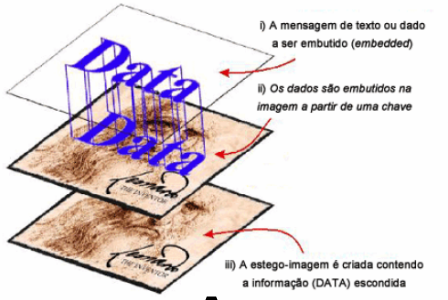
Aplicações

- Marcas D'Água
  - Apesar de muitas técnicas de marca d'água poderem ser aplicadas diretamente para diferentes tipos de dados digitais, as mídias mais utilizadas são as imagens estáticas
  - Existe uma certa confusão entre as marcas d'água imperceptíveis e as visíveis utilizadas em cédulas de dinheiro, por exemplo
  - As visíveis são usadas em imagens
    - Aparecem sobrepostas sem prejudicar muito a percepção da mesma
    - São usadas geralmente para que se possa expor imagens em locais públicos como páginas na Internet sem o risco de alguém copiá-la
    - É possível também inserir digitalmente marcas visíveis em vídeo e até audíveis em música



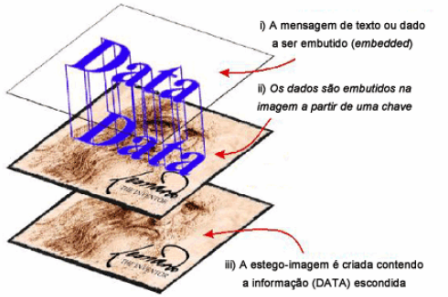
Aplicações
Marcas - Tipos

- Marcas Robustas e Frágeis
  - As marcas d'água digitais são classificadas, de acordo com a dificuldade em removê-las
  - Robustas, frágeis e semifrágeis
  - Esta classificação também normalmente determina a finalidade para a qual a marca será utilizada



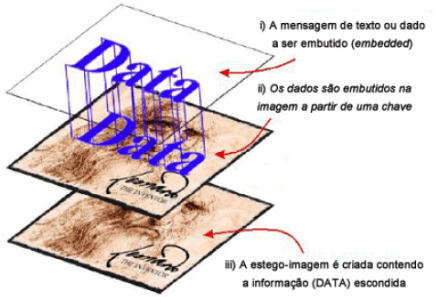
Aplicações
Marcas Robustas

- **As marcas robustas são projetadas para resistirem a maioria dos procedimentos de manipulação de imagens**
- **A informação embutida em uma imagem através de uma marca robusta poderia ser extraída mesmo que a imagem hospedeira sofresse rotação, mudançade escala, mudança de brilho/contraste, compactação com perdas com diferentes níveis de compressão, corte das bordas (*cropping*), etc.**
  - Uma boa marca d'água robusta deveria ser impossível de ser removida, a não ser que a qualidade da imagem resultante deteriore a ponto de destruir o seu conteúdo visual
  - Correlação entre uma imagem marcada e a marca robusta nela inserida deveria permanecer detectável mesmo após um processamento digital
  - Por esse motivo, as marcas d'água robustas são normalmente utilizadas para a verificação da propriedade (*copyright*) das imagens



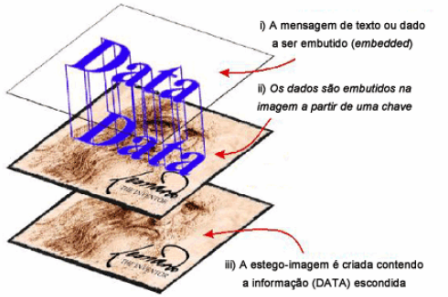
Aplicações
Marcas Frágeis

- **As marcas frágeis são facilmente removíveis e corrompidas por qualquer processamento na imagem**
  - Este tipo de marca d'água é útil para checar a integridade e a autenticidade da imagem, pois possibilita detectar alterações na imagem
  - Em outras palavras, uma marca d'água frágil fornece uma garantia de que a imagem marcada não seja despercebidamente editada ou adulterada
  - As marcas frágeis de autenticação detectam qualquer alteração na imagem. Às vezes, esta propriedade é indesejável



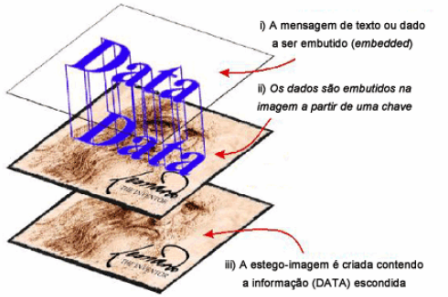
Aplicações Semifrágeis

- **Assim, foram criadas as marcas d'água semifrágeis**
- **Uma marca semifrágil também serve para autenticar imagens**
  - Procuram distinguir as alterações que modificam uma imagem substancialmente daquelas que não modificam o conteúdo visual da imagem
  - Uma marca semifrágil normalmente extrai algumas características da imagem que permanecem invariantes através das operações permitidas e as insere de volta na imagem de forma que a alteração de uma dessas características possa ser detectada



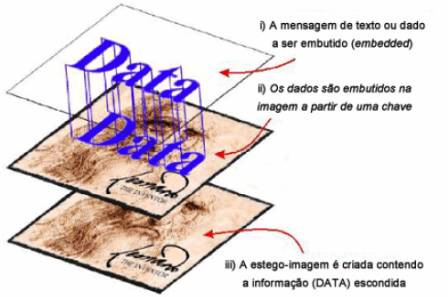
Aplicações
Marcas de Autenticação

- Tipos de Marcas de Autenticação
  - Pode-se subdividir as marcas de autenticação (tanto frágeis como semifrágeis) em três subcategorias:
    - Sem chave, com chave secreta (cifra simétrica) e com chave pública/privada (cifra assimétrica)
  - Sem chave
    - Útil para detectar as alterações não intencionais na imagem tais como um erro de transmissão ou de armazenamento
    - Funciona como uma espécie de *checksum*
    - Se o algoritmo de autenticação sem chave estiver disponível publicamente, qualquer pessoa pode inserir este tipo de marca em qualquer imagem e qualquer pessoa pode verificar se uma imagem contém uma marca válida



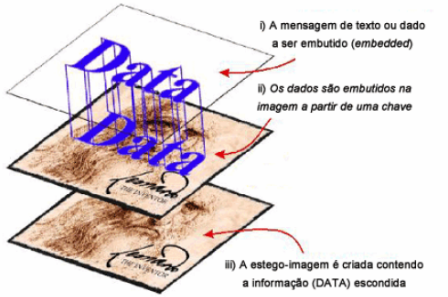
Aplicações
Marcas de Autenticação

- **Com chave secreta (cifra simétrica)**
  - Usada para detectar uma alteração que pode ser inclusive intencional ou maliciosa
  - Similar aos códigos de autenticação de mensagem, sendo que a única diferença é que o código de autenticação é inserido na imagem ao invés de ser armazenado separadamente
  - Os algoritmos para inserção e detecção deste tipo de marca podem ser disponibilizados publicamente, e uma chave secreta é usada em ambas as fases



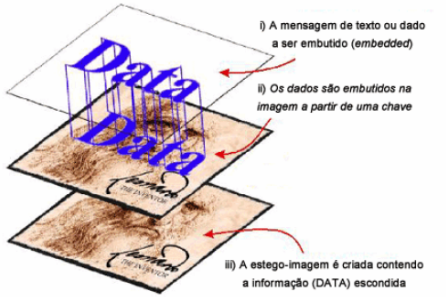
Aplicações
Marcas de Autenticação

- **Com chave pública (cifra assimétrica)**
- **Utilizam a criptografia de chave pública para inserir uma assinatura digital na imagem**
- **Usando uma cifra de chave pública, a autenticidade de uma imagem pode ser julgada sem a necessidade de se tornar pública qualquer informação privada**



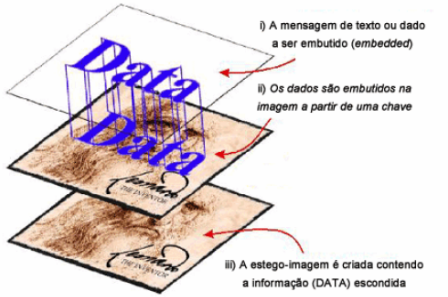
Aplicações
Marcas de Autenticação

- Em Imagens de Tonalidade Contínua e Imagens Binárias
  - Existe uma forma natural de embutir as marcas de autenticação em imagens de tonalidade contínua (*contone*) não compactadas
  - Inserir os dados nos bits menos significativos (LSBs)
  - Alterar os LSBs afeta muito pouco a qualidade da imagem, ao mesmo tempo em que se conhece exatamente os bits que serão afetados pela inserção da marca



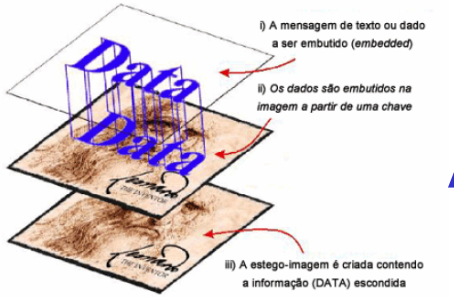
Aplicações
Marcas de Autenticação

- Não ocorre o mesmo com as imagens binárias
- Cada *pixel* consiste de um único bit, de forma que não existe LSB
- Isto traz dificuldades especiais para projetar marcas de autenticação para este tipo de imagem



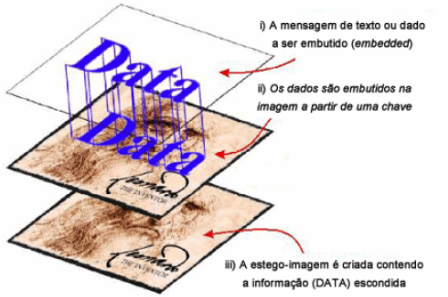
Aplicações
Marcas de Autenticação

- Entre os três tipos de marca de autenticação, a de chave pública é a que oferece mais recursos
- Alguns possíveis usos de uma marca de autenticação de chave pública:
  - câmera digital segura
  - autenticação de imagens distribuídas pela rede
  - fax confiável



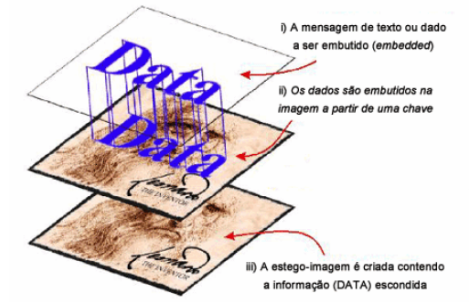
Aplicações

- Câmera digital segura
  - A câmera digital produz dois arquivos de saída para cada imagem capturada:
    - A própria imagem digital capturada
    - A segunda é uma assinatura digital produzida aplicando a chave privada da câmera
    - O usuário deve tomar cuidado para guardar os dois arquivos, para que se possa autenticar a imagem mais tarde
  - A integridade e a autenticidade da imagem podem ser verificadas usando um programa para decodificar a assinatura digital, que pode ser distribuído livremente aos usuários
  - O programa de verificação recebe como entrada a imagem digital, a assinatura digital e a chave pública da câmera
  - Calcula a função *hash* da imagem digital, decriptografa a assinatura digital e verifica se as duas impressões digitais obtidas são iguais



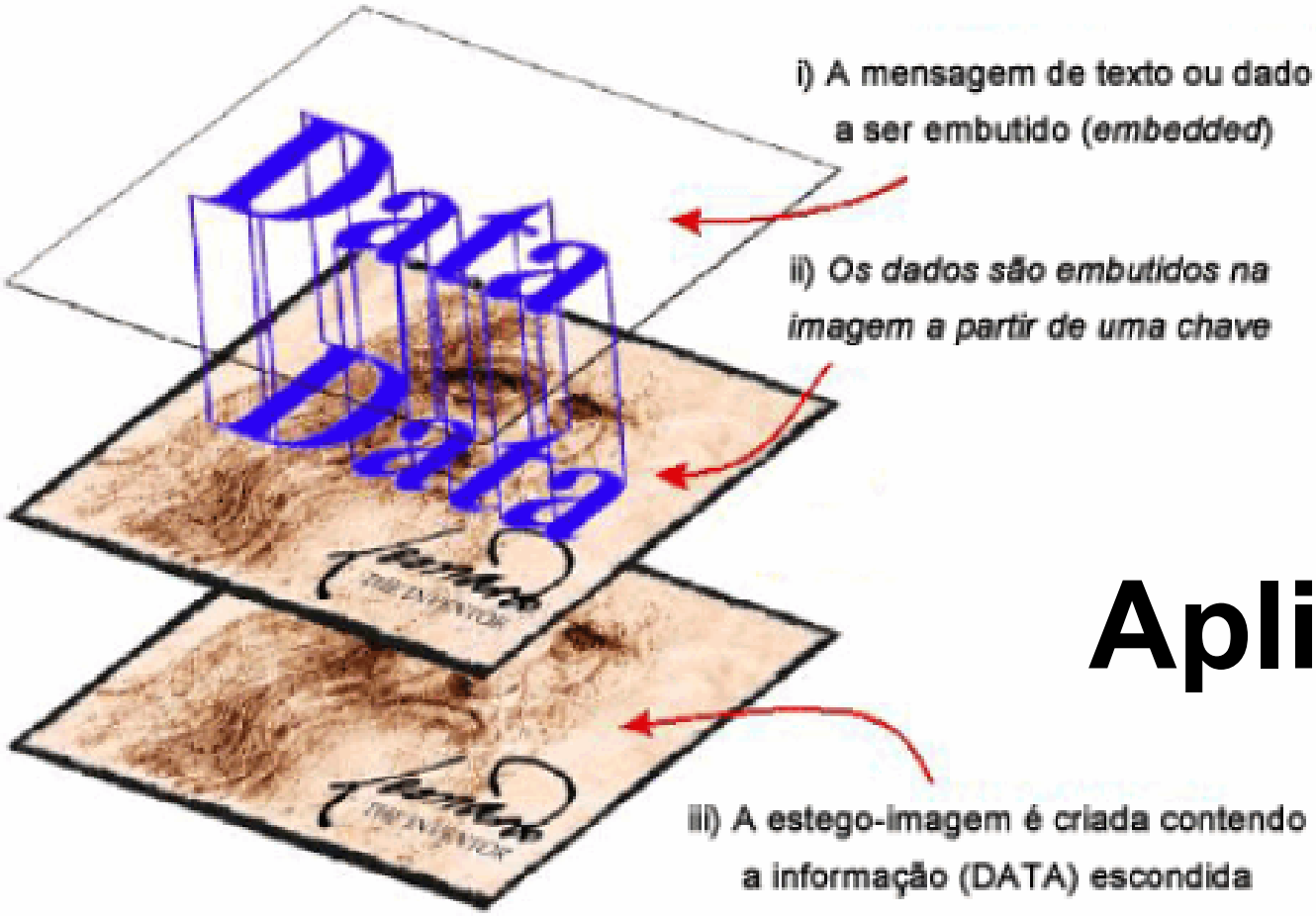
Aplicações

- Autenticação de imagens distribuídas pela rede
  - Uma agência de notícias necessita distribuir pela Internet uma fotografia jornalística, com alguma prova de autenticidade de que a foto foi distribuída pela agência e que ninguém introduziu alterações maliciosas na foto
  - A agência pode inserir uma marca d'água de autenticação na imagem e distribui a foto marcada;

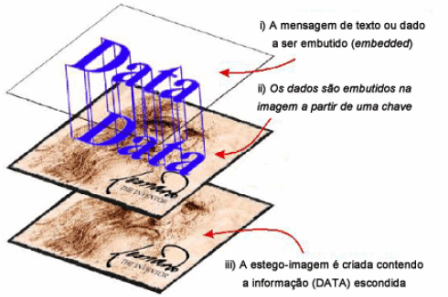


Aplicações

- Fax confiável
  - Uma “máquina de FAX confiável” poderia conter internamente uma chave privada e inserir uma marca d’água em todos os documentos transmitidos
  - O receptor de FAX, usando a chave pública da máquina transmissora, poderia verificar que o documento foi originado de uma máquina específica de FAX e que o documento não foi manipulado

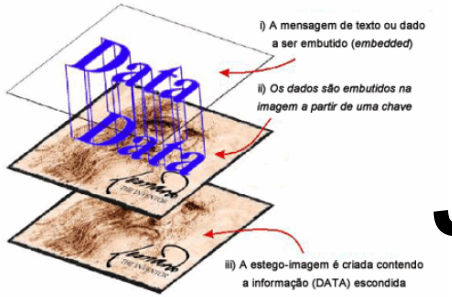


Aplicativos



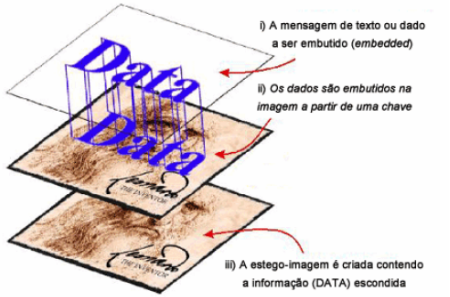
Marca d'Água Signit da AlpVision

- Proteger o direito de copyright das imagens
- Esconde um ID Number nas imagens
- Recupera o ID Number das imagens
- É preciso registrar-se no site da AlpiVision para ter o direito de testar
- Disponível em http://www.alpivison.com
- Outros softwares: http://home.earthlink.net/~emilbrandt/stego/watermrk.html



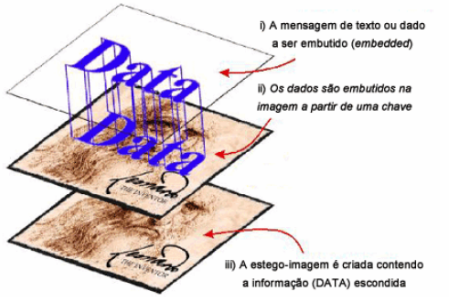
Esteganografia
JPHIDE and Seek for Windows

- Interface Windows para dois programas:
  - JPHIDE: Esconder dados em imagens
  - JPSEEK: Recuperar os dados que foram escondidos
- Usa técnica LSB
- Mais efetivo com imagens em escala de cinza
- Usa um gerador pseudo-randômico de números para espalhar os dados pelos pixels
- Nem todos pixels contém dados
- Utiliza IDEA para cifrar os dados com a chave fornecida pelo usuário



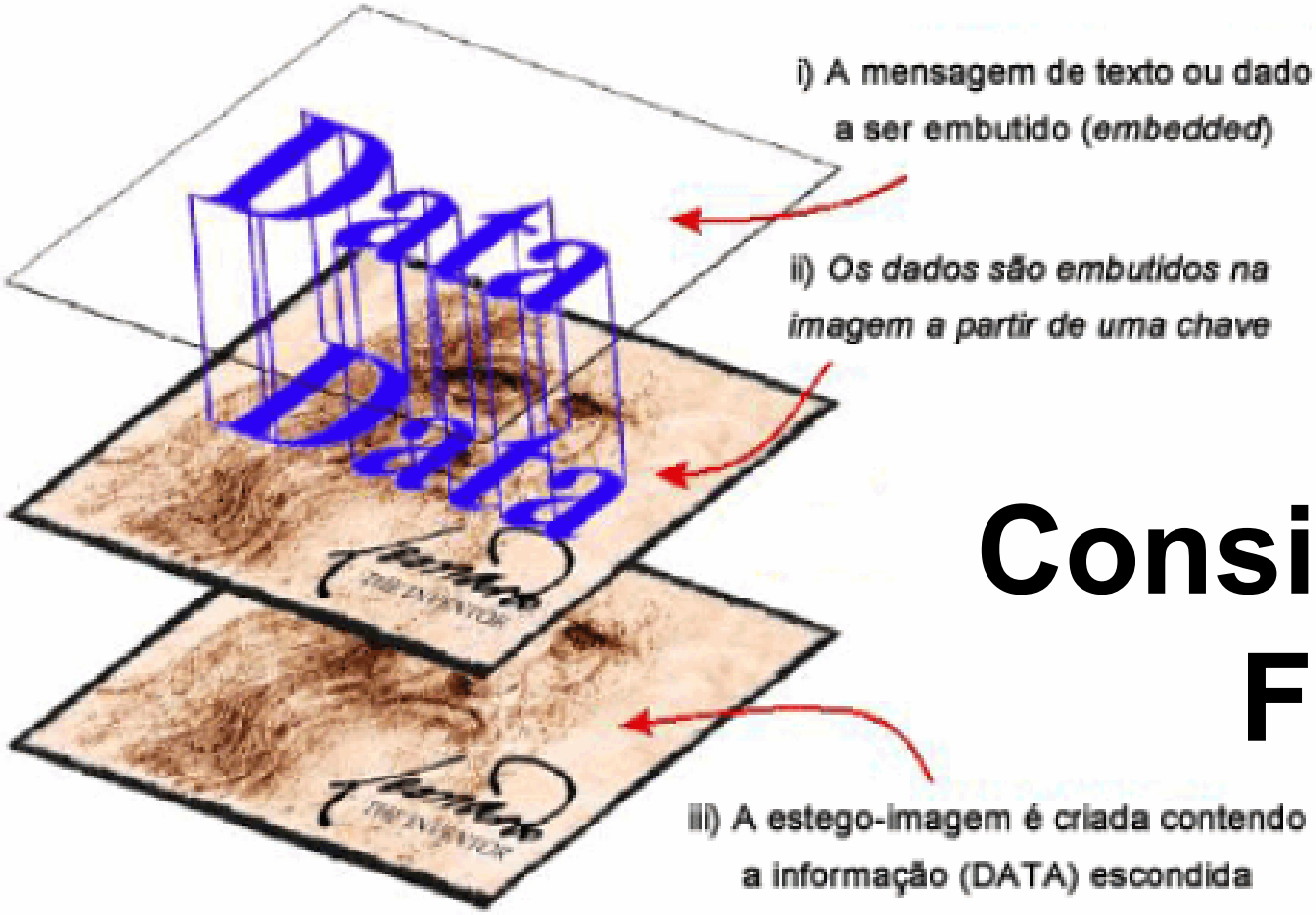
Outros Aplicativos de Esteganografia

- Ezstego
- Stego Online
- Revelation
- Outgess
- Jsteg
- Sites para consulta:
  - http://www.jijtc.com/security/stegtools.htm
  - http://www.petitcolas.net/fabien/steganography/

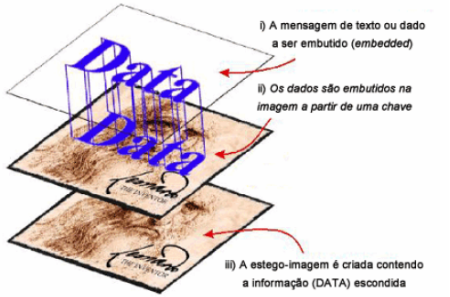


Esteganálise

- **Stego Spy**
  - Procura por assinaturas nos arquivos para informar se o arquivo possui dados escondidos
  - Não recupera os dados
  - Identifica Hiderman, JPHide and Seek, Masker, JPegX e Invisible Secrets
  - Disponível em http://www.spyhunter.com
- **StegDetect**
  - Também busca assinaturas em arquivos JPEG. Na última versão dispõe de análise LDA para detectar qualquer estego-sistema
  - StegBreak – Utilitário de força bruta para tentar quebrar a chave do arquivo JPEG e decifrá-lo
  - Detecta Jsteg, JP Hide and Seek
  - Disponível em http://www.outguess.org/detection.php

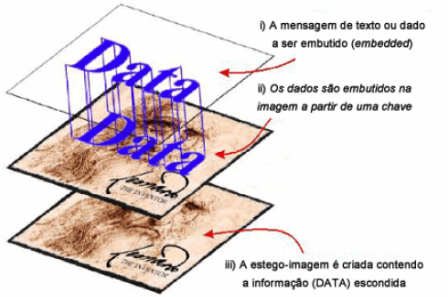


Considerações Finais



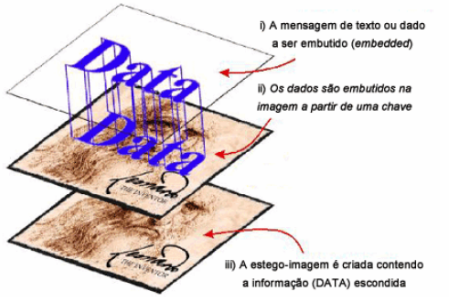
Considerações Finais

- Esteganografia vs. Marca d'água
  - Técnicas para ocultar uma comunicação dentro de uma informação disfarce
  - Esteganografia:
    - comunicação ponto-a-ponto
    - não é robusto (robustez limitada)



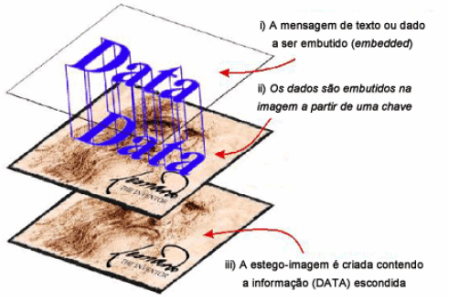
Considerações Finais

- Esteganografia vs. Marca d'água
  - Marcas d'água
    - Foco na robustez
    - Não existe comunicação ponto-a-ponto
    - Imagem pode circular por quaisquer canais típicos da aplicação
    - Proteger contra cópias sem autorização
    - Deve ser possível decodificar a marca mesmo em imagens alteradas
    - Provaria de autoria
    - Detecção não é tão importante, apesar de que, se o observador não perceber a marca, ele talvez nem tente removê-la



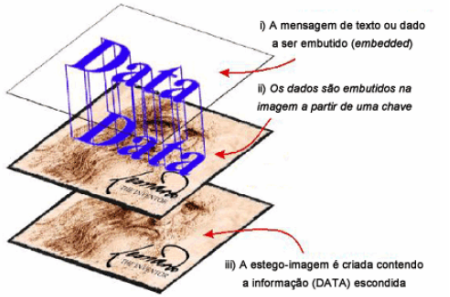
Considerações Finais

- Marcar uma imagem para verificar se ela sofrerá alterações
  - Caso a imagem seja modificada de alguma forma, a marca será destruída, mostrando que o ato realmente aconteceu
  - A robustez ou a ausência dela define a aplicação da marca utilizada
    - As marcas d'água robustas devem resistir a ataques e alterações na imagem
    - As marcas frágeis devem ser destruídas caso a imagem sofra alterações



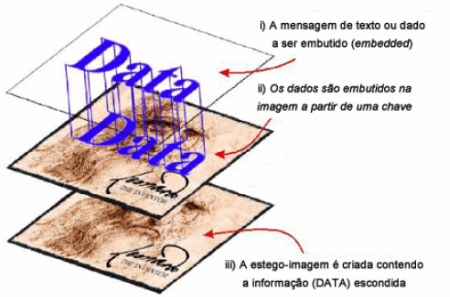
Considerações Finais

- Técnicas esteganográficas
  - Uso legal
    - Proteção de direitos e propriedade intelecutais, principalmente quando se considera as novas formas de comercialização utilizando mídia digital
    - Neste sentido as técnicas de marca dágua parecem ser um campo profícuo de pesquisa e aplicações no futuro



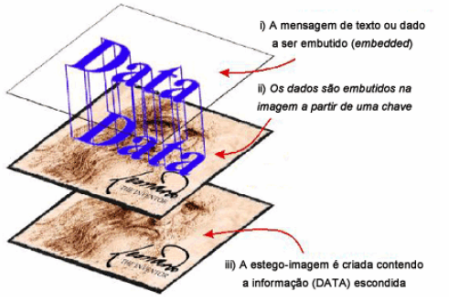
Considerações Finais

- Uso ilegal
  - Usar esteganografia para transitar mensagens ou até pequenas imagens de pornografia ou pedofilia é possível e provável
  - comunicações criminosas
  - fraudes
  - hacking
  - pagamentos eletrônicos
  - pornografia e pedofilia
  - ofensas a propriedade intelectual
  - propagação de vírus e cavalos de tróia



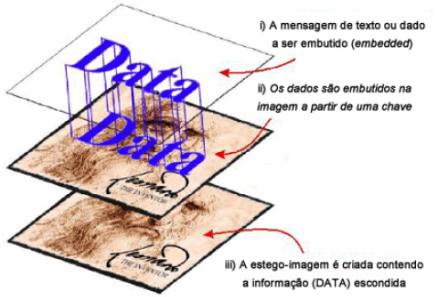
Considerações Finais

- Outras áreas de interesse
  - Uma área com uso potencial em várias aplicações é o desenvolvimento de protocolos que usam esteganografia
  - As técnicas e ferramentas esteganográficas podem ser utilizadas em conjunto com outras aplicações para automaticamente extrair informações escondidas sem a intervenção do usuário



Conclusão

- Evolução da esteganografia ao longo da história
- Suas aplicações modernas com a chamada esteganografia digital
- Técnicas de mascaramento e, em especial, mascaramento em imagens
- A esteganografia
  - Fornece meios eficientes e eficazes na busca por proteção digital
- Associação de criptografia e esteganografia



Esteganografia e suas Aplicações

Perguntas?

Eduardo Julio, Wagner Brazil, Célio Albuquerque

{ejulio, wbrazil, celio}@ic.uff.br

Instituto de Computação

Universidade Federal Fluminense