ESTEGANOGRAFIA

Jiyan Yari

Premissa:

Informação é poder ... !

Objetivo:

Esconder a informação de tal forma que somente o destinatário possa ter acesso ao seu conteúdo. Somente o remetente e o destinatário podem saber onde e como está escondida a informação.

Motivação:

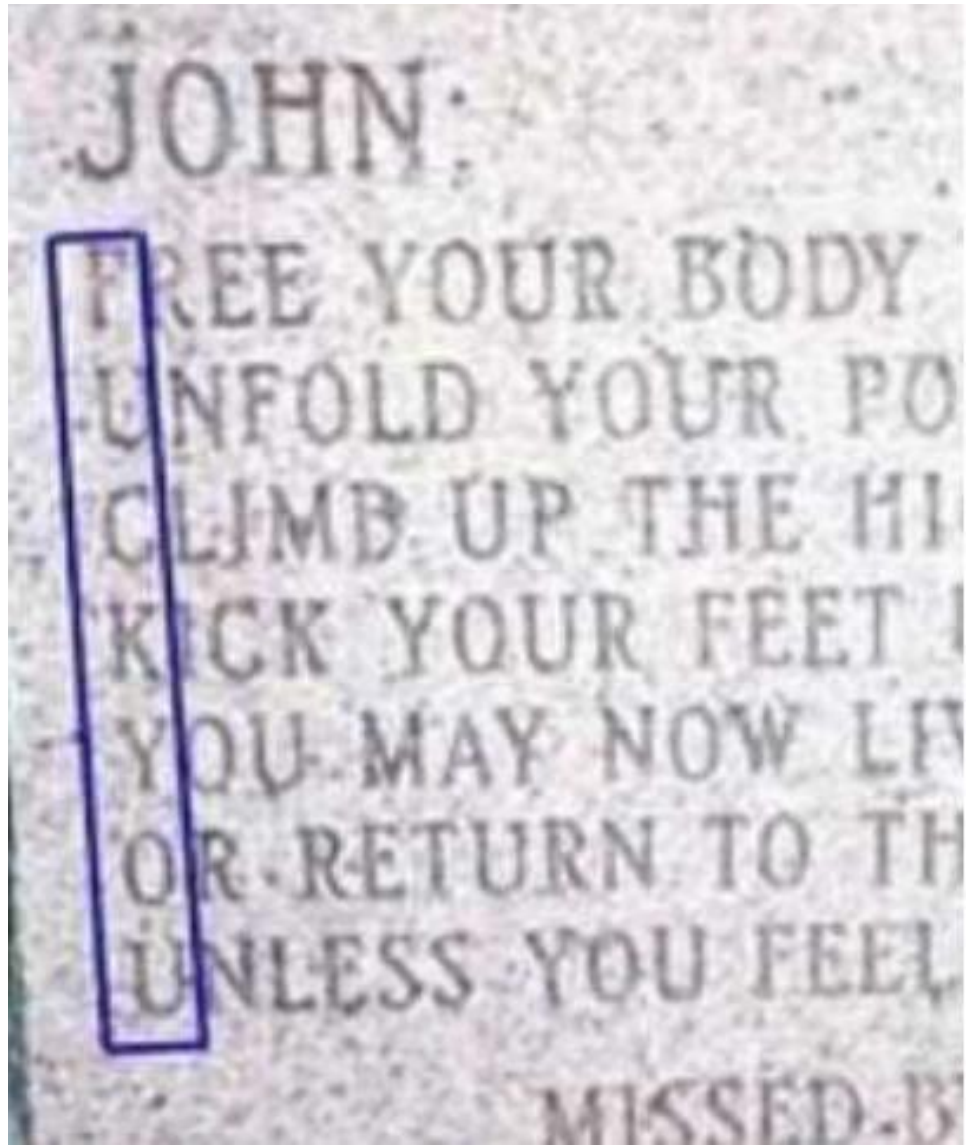
- segredos militares;
- políticos;
- religiosos;
- comércio (e-commerce);
- certificação digital;
- sentimentais/amorosos;
- etc.

SteganoGrafia

steganos = escondido, coberto grafia = escrita

- técnica primitiva e ancestral;
- processo que se caracteriza exclusivamente pelo ocultamento;
- consiste em ocultar a informação de tal forma que sua existência não seja percebida;
- nenhum tratamento é feito para transformar a mensagem;
- não existe segurança dos dados caso seja interceptada durante transmissão (pode ser detectada através de filtros de ruídos).


JOHN


JOHN:
FREE YOUR BODY
UNFOLD YOUR PO
CLIMB UP THE HI
KICK YOUR FEET
YOU MAY NOW LI
OR RETURN TO TH
UNLESS YOU FEEL
MISSED B

Ex:

- Heródoto (Grécia) -> mensagem na cabeça do mensageiro;
- escrita com tinta invisível (Persas) -> tinta feita a partir de algumas plantas ou de fluidos orgânicos (como a urina);
- Giovanni Porta (cientista Italiano) -> mensagem dentro de uma casca de ovo cozido (mistura de alúmen e vinagre);
- mapas de piratas;
- Grelha de Cardano (foi muito usado por Richelieu) e reutilizada novamente na 2ª Grande Guerra Mundial;
- microponto (2ª Grande Guerra Mundial);
- depois deste período ficou em desuso e esquecido, até que recentemente ressurgiu.

Grelha de Cardano

Desenvolvida por Girolamo Cardano, médico, filósofo e matemático.

Texto camuflado/escondido

G	M	P	A	L	O	E	M	T	N
P	N	I	S	D	L	A	G	U	R
E	M	J	S	R	L	E	T	A	C
I	D	R	U	V	N	O	R	A	N
H	O	Q	U	E	Z	A	P	T	A

Texto limpo/aberto

	M					E			N
			S			A	G		
E	M		S			E			C
		R							
				E				T	A

Caça-palavras

A	G	K	H	Y	T	F	G	N	J
U	T	P	R	F	E	D	W	Q	A
I	P	O	N	T	A	V	V	F	T
N	J	R	B	G	V	F	R	D	E
S	W	A	D	Y	R	K	I	U	H
N	Y	T	G	R	F	E	D	W	S
C	V	B	N	M	H	P	Ç	L	O
K	I	J	U	Y	H	T	G	R	F
E	D	W	S	Q	P	L	O	K	M
J	U	H	B	G	T	B	V	F	R

Cartas-lacunas

Linux tem se tornado nos últimos anos o melhor Sistema Operacional, tanto para usuários avançados, como para usuários leigos, e tem amadurecido com relação a suas ferramentas de trabalho, o qual verifica-se o uso nos computadores populares que são financiados pelas lojas de departamento e pelos bancos, possibilitando a maior inclusão digital da população brasileira. Todos os telecentros criados no país tem como ferramenta o sistema operacional Linux.
Constantemente diversas palestras acontecem sobre Linux em todo o mundo.
Trata-se de uma tecnologia de ponta.
Portanto é o Sistema Operacional de maior crescimento e difusão na atualidade, sendo a quinta maior economia em Software no planeta.

Cifradores Nulos

São mensagens nas quais certas letras devem ser usadas para formar a mensagem e todas as outras palavras ou letras são consideradas nulas.

Para o uso do cifrador nulo, ambos os lados da comunicação devem usar o mesmo protocolo de uso das letras que formam a mensagem.

Por exemplo, usar sempre a primeira letra de cada palavra para compor a mensagem.

Este método é difícil de implementar, pois a mensagem de cobertura deve ter algum sentido, do contrário um inimigo desconfiará e quebrará o código.

Cifradores Nulos

“News Eight Weather: tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The highways are knowingly slippery. Highway evacuation is suspected. Police report emergencies in downtown ending near Tuesday”.

Usando as primeiras letras de cada palavra o texto que aparece é:

Newt is upset because he thinks he is president

MicroPonto

A técnica de Micropontos é também uma outra forma de esteganografia usada atualmente.

Um micro-ponto é uma fotografia (microfilme) da mensagem secreta que deve ser entregue.

Com a tecnologia avançando rapidamente, é possível tirar uma foto de uma mensagem e reduzí-la a uma fotografia circular de 0,05 polegadas ou 0,125 cm de diâmetro.

Esta minúscula fotografia é então colada em um sinal de pontuação de uma frase ou no "pingo"de uma letra "i"de uma outra mensagem qualquer que será entregue.

Somente aqueles que sabem onde procurar o microponto poderão detectar sua presença.

Atualmentente está muito em alta

- esconder informações em arquivos de texto, imagem, vídeo e som (Codificação de Huffman);

- usada na autenticação de documentos, dinheiro (marca d’água, impressão digital de produtos e etc.).

Codificação de Huffman (Compressão de Huffman)

- uma imagem -> conjunto de pixels;

- a cor é formada por três canais (vermelho, verde e azul) de 8 bits cada um;

- alterar o bit menos significativo não ocorrem mudanças perceptíveis na imagem;

- o tamanho do texto a esconder tem um limite, que o da figura que irá transportá-lo (no caso).

Codificação de Huffman (Compressão de Huffman)

Forma de compressão de dados em que representa-se cada um dos caracteres de um texto com códigos binários de comprimento variável.

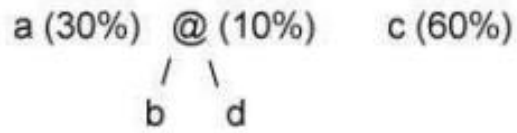
O tamanho do código varia conforme a frequência com que ocorre no texto.

Atribuindo-se códigos menores aos caracteres mais frequentes e maiores aos menos frequentes.

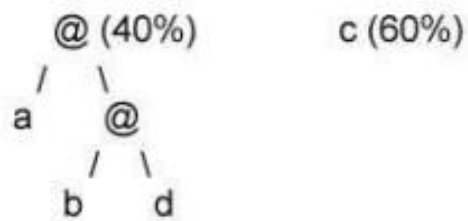
PRIMEIRA ETAPA

a (30%) b (4%) c (60%) d (6%)

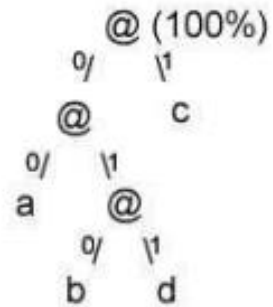
SEGUNDA ETAPA



TERCEIRA ETAPA



ÚLTIMA ETAPA



LSB Bit menos significativo (LSB – Least Significant Bit)

Baseadas na modificação dos bits menos significativos dos valores de pixel no domínio espacial.

Em uma implementação básica, estes pixels substituem o plano LSB inteiro com o stego-dados.

Com esquemas mais sofisticados em que locais de inclusão são adaptativamente selecionados, dependendo de características da visão humana, até uma pequena distorção é aceitavel.

Em geral, a inclusão de LSB simples é suscetível a processamento de imagem, especialmente a compressão sem perda.

LSB Técnicas baseadas em LSB podem ser aplicadas a cada pixel de uma imagem codificada em 32bits por pixel.

Estas imagens possuem seus pixels codificados em quatro bytes. Um para o canal alfa (alpha transparency), outro para o vermelho (red), outro para o verde (green) e outro para o azul (blue).

Seguramente, pode-se selecionar um bit (o menos signicativo) em cada byte do pixel para representar o bit a ser escondido sem causar alteracões perceptíveis na imagem.

Estas técnicas constituem a forma de masca-ramento em imagens mais difícil de ser detectada pois podem inserir dados em pixels não sequenciais, tornando complexa a detecção.

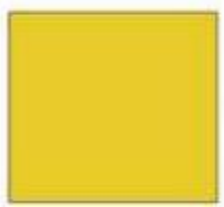
Bit menos significativo

1	0	0	1	0	1	0	1

Um pixel original

R = 233 = 11101001
G = 200 = 11001000
B = 37 = 00000101

Um pixel modificado



R = 232 = 11101000
G = 201 = 11001001
B = 36 = 00000100

Representação de Três Pixels de Uma Figura

01100100 10100011 10110111

10011011 01011100 01001000

11001110 11111001 11100011

Representação do Caracter "M" em ASCII

01001101

Pixels após a codificação da letra "M"

01100100 10100011 10110110

10011010 01011101 01001001

No caso de uma imagem com profundidade de cor de 24 bits, um bit de uma nova informação pode ser armazenado no bit menos significativo de cor dos pixels, ou seja, o bit menos significativo dos 24.

Considerando o valor dos caracteres em binário da palavra "linux" temos:

l : 0110 1100

i : 0110 1001

n : 0110 1110

u : 0111 0101

x : 0111 1000

Na forma acima a palavra "linux" é representada utilizando-se 40 bits (5 letras com 8 bits cada -> 5 x 8 = 40).

Sendo assim, precisa-se de uma imagem com quantos Pixels? 40 / 3 = **14**

Para armazenar a letra 'l', iremos utilizar o bit menos significativo de cor dos 8 primeiros pixels.

O primeiro bit do caracter 'l' é 0, se o bit menos significativo do primeiro pixel for 1, o valor é mantido, caso contrário é trocado para 1.

Caso o bit a ser armazenado tenha valor 0, por exemplo o quarto bit do caractere 'l', a mesma regra é usada, se o bit menos significativo do quarto pixel for 0, o valor é mantido, caso contrário é trocado.

Este procedimento deve ser repetido por todos os bits de cada caractere.

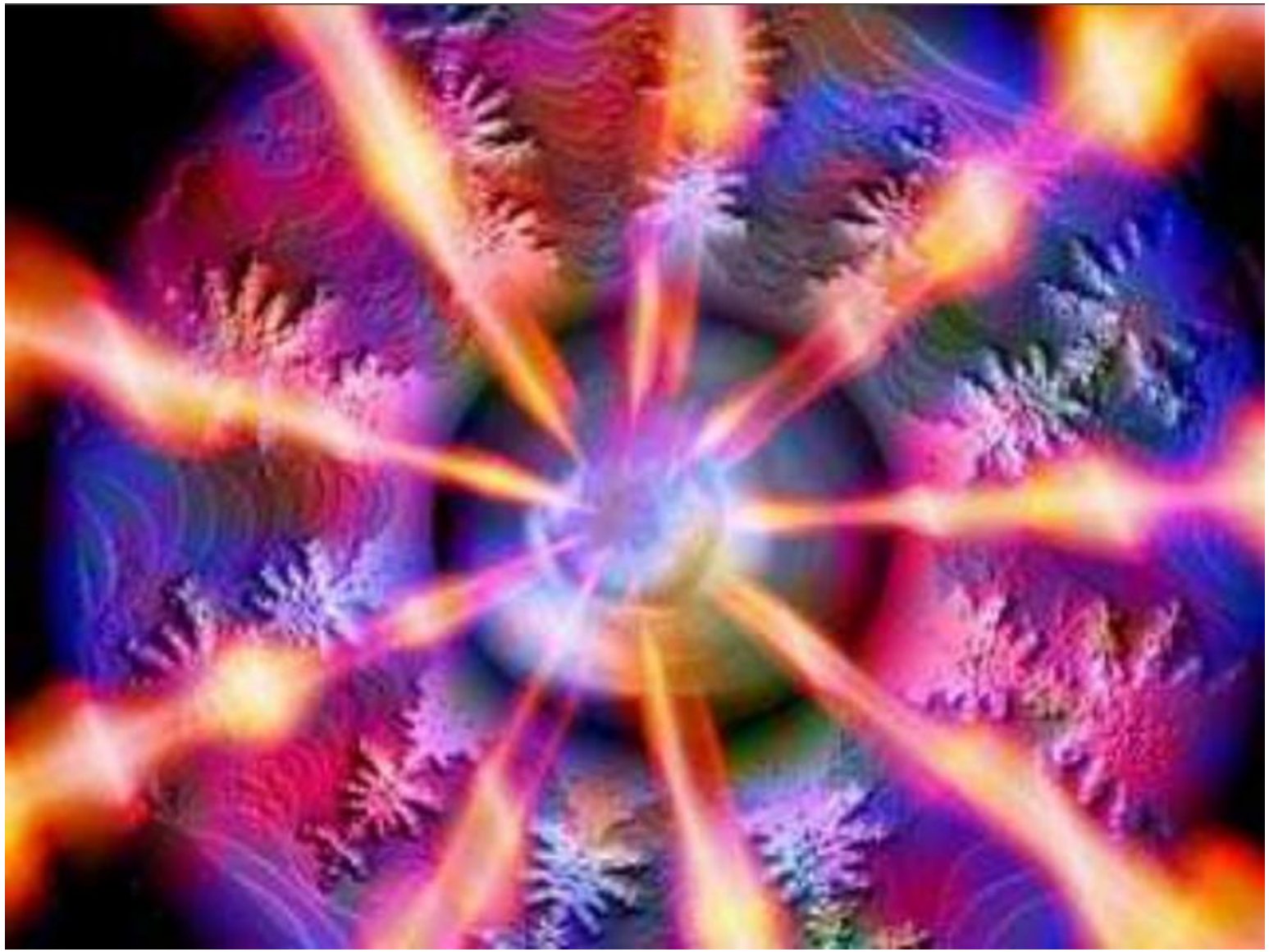
No fim teremos uma imagem armazenando a palavra "linux" com ruído de 1 bit por pixel.

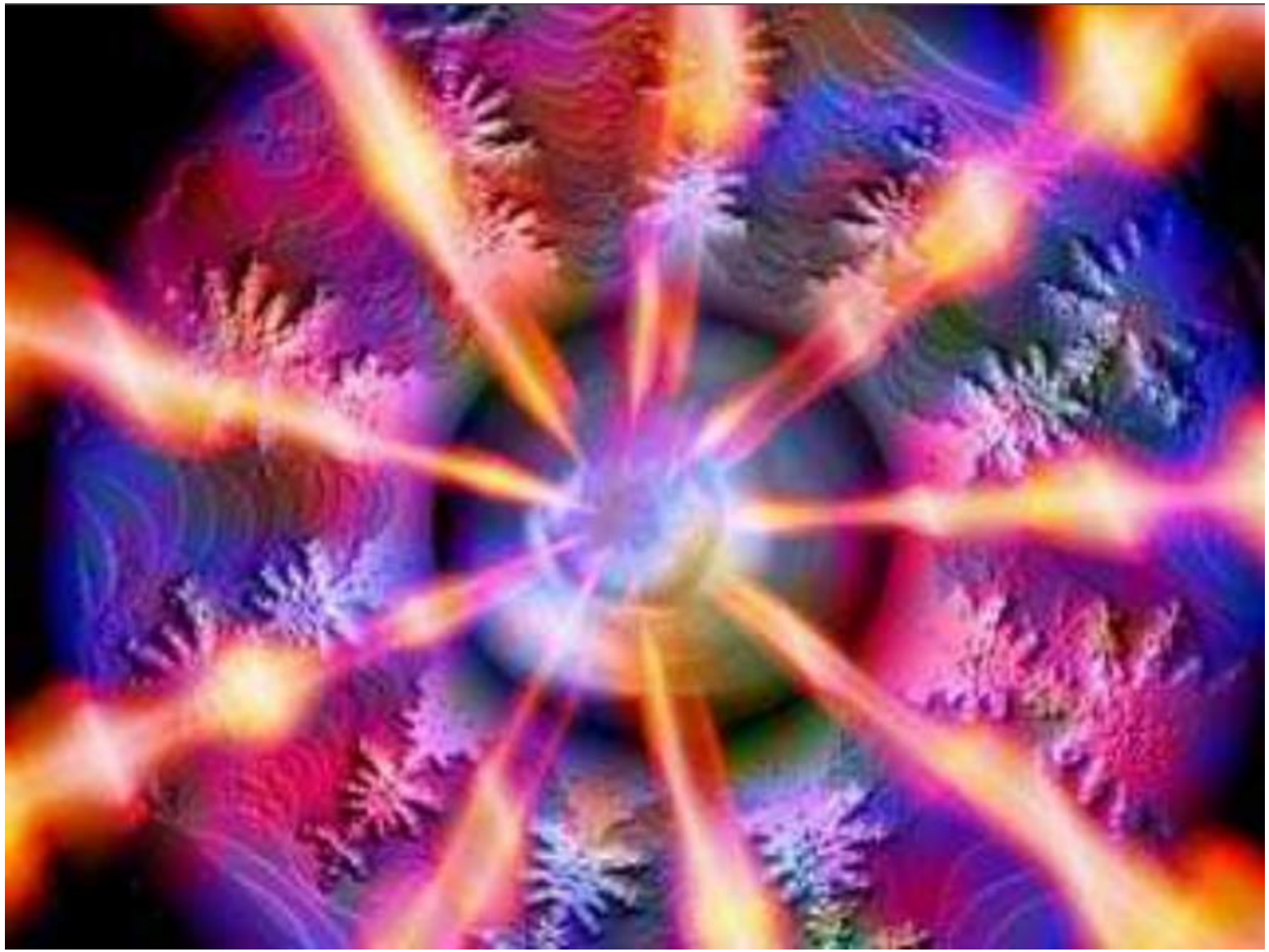
(a)

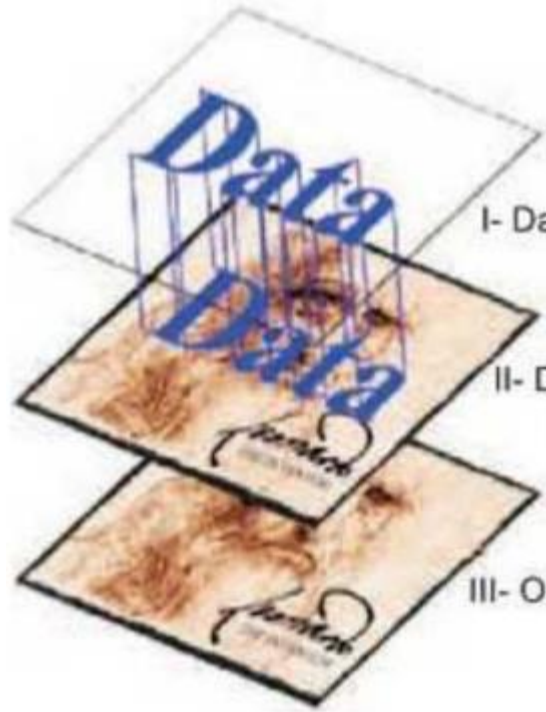
(b)

Troca de bit menos significativo em pixel de cor de imagem.

(a) 204aeb - 10000001001010111010 11
(b) 204aea – 10000001001010111010 10







I- Dado a ser escondido (dado embutido)

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

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

MARCA D’ÁGUA

O sistema de marcação tipo marca d’água se refere a métodos que escondem informações em objetos que são robustos e resistentes a modificações.

Neste sentido seria impossível remover uma marca d’água de um objeto sem alterar a qualidade visual do mesmo.

Uma diferença clara entre esteganografia e técnicas de marca d’água é que enquanto o dado embutido da esteganografia nunca deve ficar aprente, a marca d’água pode ou não aparecer no objeto marcado, dependendo da aplicação que se queira atender.

Algumas ferramentas de marca d’água:

WaterMark.ws (http://www.watermark.ws/)

TSR Watermark Image (http://www.watermark-image.com)

My Watermark (http://www.myportablesoftware.com/mywatermark.aspx)


Fibras Coloridas
Linhas Multidirecionais
Microimpressões
Marca D'Água
Registro Coincidente
REAIS
Marca Tátil
Imagem Latente
Fio de Segurança
Numeração

Site contendo listas de ferramentas de Steganografia:

http://www.jjtc.com/Security/stegtools.htm