Grupo de Resposta a Incidentes de Segurança

Esteganografia

Luís Fernando Magalhães Novaes
luisfernando@gris.dcc.ufrj.br

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro

Esteganografia - Cronograma

1) Introdução
1.1) O que é?
1.2) Diferenças e semelhanças com criptografia

2) Técnicas
2.1) Técnicas Manuais e Históricas
.Cifra Nula
.Grelha
.Tinta Invisível

2.2) Técnicas Digitais
.Bit menos significativo
.Esteganografia BPCS

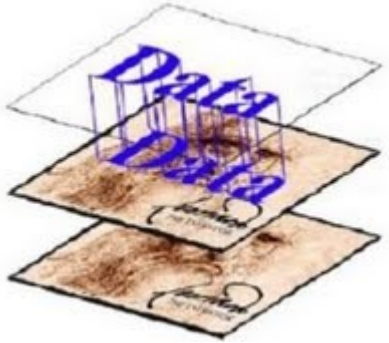
3) Esteganálise

4) Aplicativos

5) Notícias

Introdução

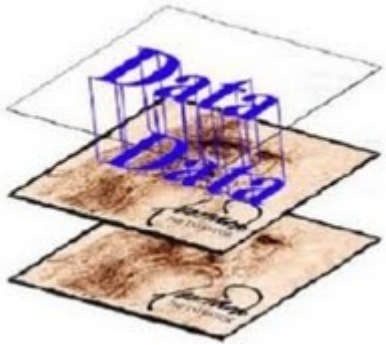
O que é Esteganografia?



Esteganografia, que vem do grego *steganós* que significa esconder/ocultar e *graphia* que significa escrita.

É o estudo e uso das técnicas para esconder a existência de uma mensagem dentro de outra.

Introdução

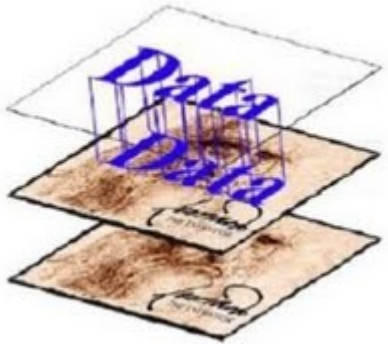


Semelhanças entre Esteganografia e Criptografia

. Tem mesma tradução (Escrita Escondida)

. São ramos particulares da Criptologia

Introdução



Diferenças entre Esteganografia e Criptografia

. Camuflagem

. Aplicação da técnica

. Legalidade

. Limite de tamanho p/ esconder a mensagem

Técnicas Manuais e Históricas

Cifra Nula

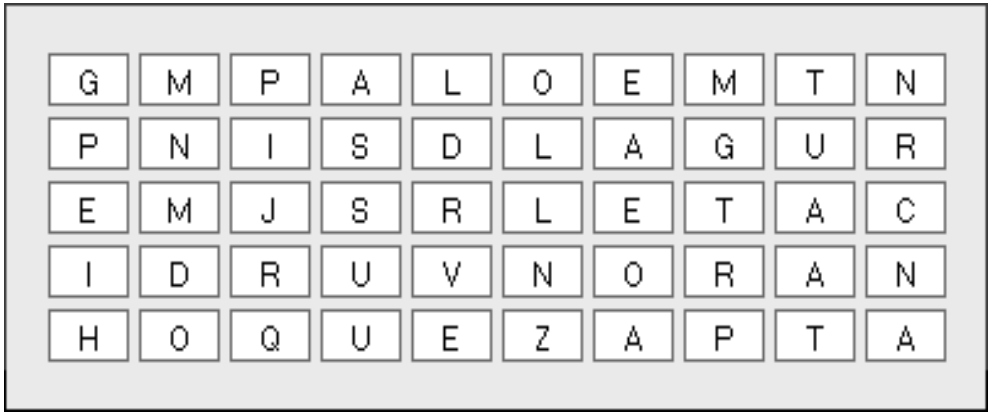
. Método trivial

. Esconde frase/palavra em outra

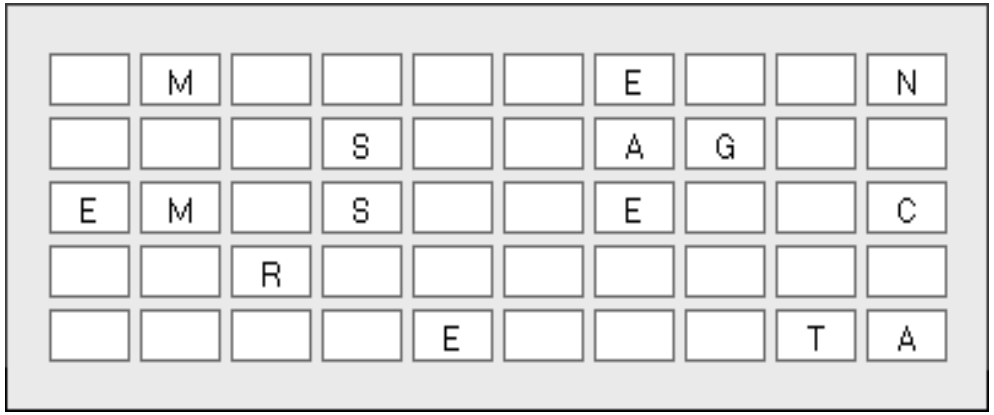
Fonte: http://carlosagreda.blogspot.com/2008/02/esteganografia-en-imagenes.html

Técnicas Manuais e Históricas

Grelha de Cardano



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

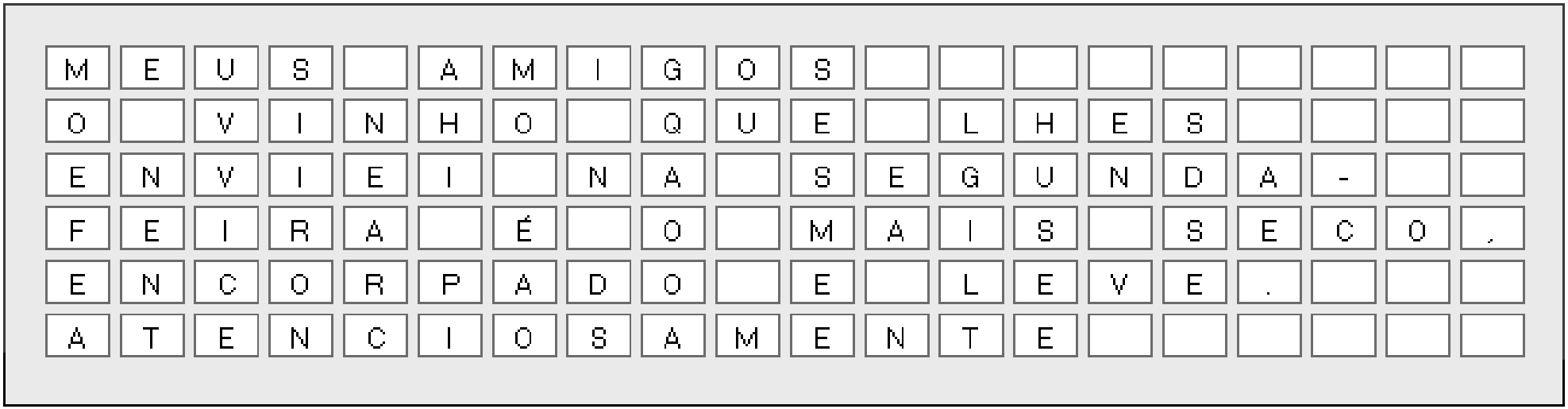


	M					E			N
			S			A	G		
E	M		S			E			C
		R							
				E				T	A

Fonte: http://www.numaboa.com/criptografia/esteganografia/163-grelha-de-cardano

Técnicas Manuais e Históricas

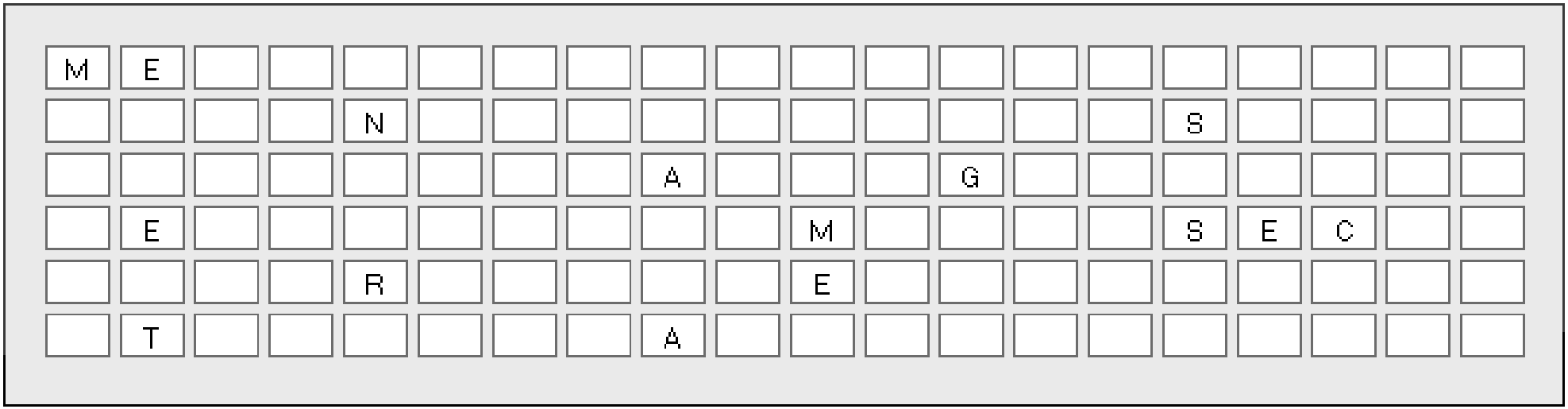
Grelha de Richelieu



Fonte: http://www.numaboa.com/criptografia/esteganografia/163-grelha-de-cardano

Técnicas Manuais e Históricas

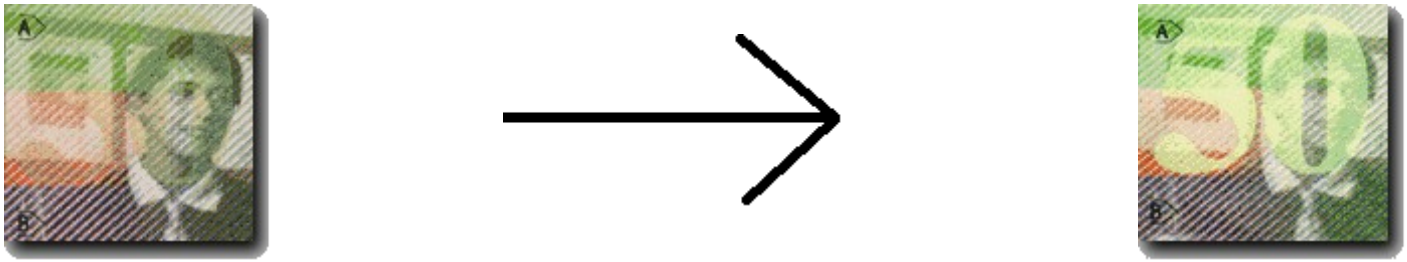
Grelha de Richelieu



Fonte: http://www.numaboa.com/criptografia/esteganografia/163-grelha-de-cardano

Técnicas Manuais e Históricas

Tinta “Invisível”



. Angulação da luz

. Reação química

. Temperatura

. Luz de frequência específica

Fonte: http://www.numaboa.com/criptografia/esteganografia/612-suica

Técnicas Manuais e Históricas

Outros métodos

. Mensagens escondidas em mesas cobertas de cera

. Tatuado no corpo de um mensageiro

. Astrogal

Outras finalidades

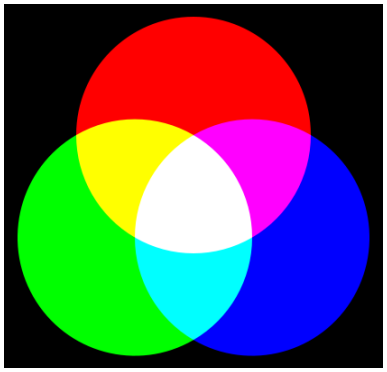
. Autenticidade da informação

. Confundir terceiros

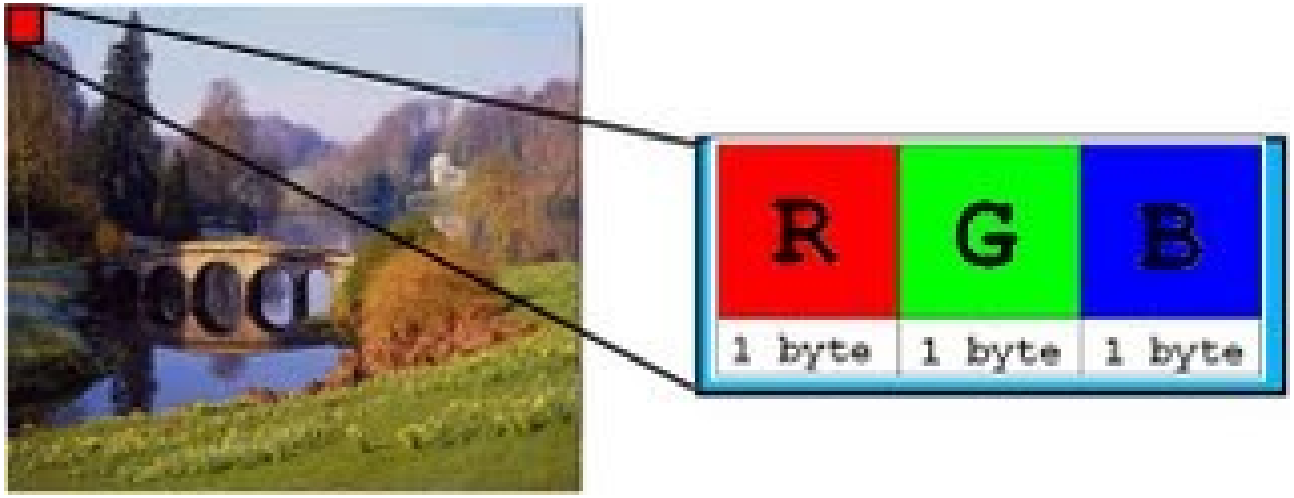
Técnicas Digitais

Bit menos significativo (LSB - Least Significant Bit)

RGB



Pixel



Fonte: http://carlosagreda.blogspot.com/2008/02/esteganografia-en-imagenes.html

Técnicas Digitais

Bit menos significativo

1	0	0	1	0	1	0	1

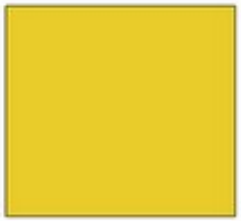
Um pixel original

R = 233 = 1110100**1**

G = 200 = 1100100**0**

B = 37 = 0000010**1**

Um pixel modificado



R = 232 = 1110100**0**

G = 201 = 1100100**1**

B = 36 = 0000010**0**

. Cada pixel = 3 bits de informação

. Cerca de 15% do tamanho da imagem original

Fonte: http://carlosagreda.blogspot.com/2008/02/esteganografia-en-imagenes.html

Técnicas Digitais

Representação de Três Pixels de Uma Figura

10100011 01100100 10110111

01011100 10011011 01001000

11111001 11001110 11100011

Representação do Caracter "M" em ASCII

01001101

Pixels após a codificação da letra "M"

10100010 01100101 10110110

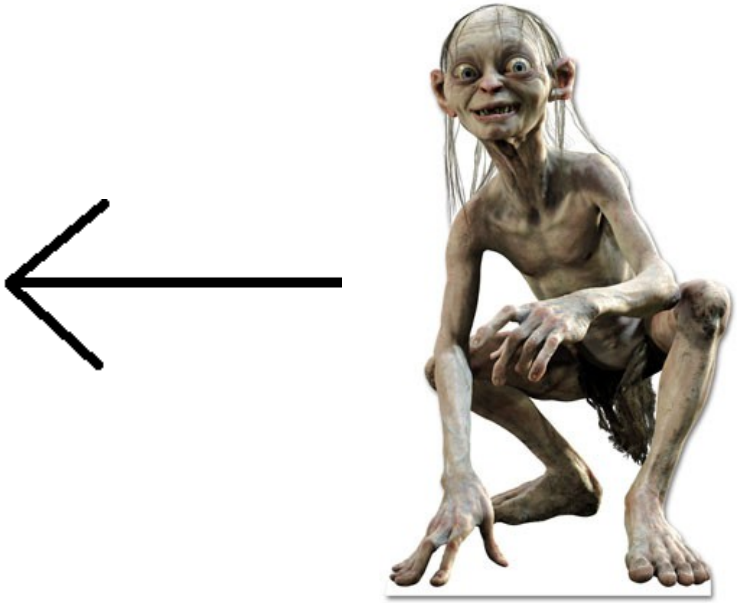
01011100 10011011 01001000

11111001 11001110 11100011

Técnicas Digitais

Bit menos significativo

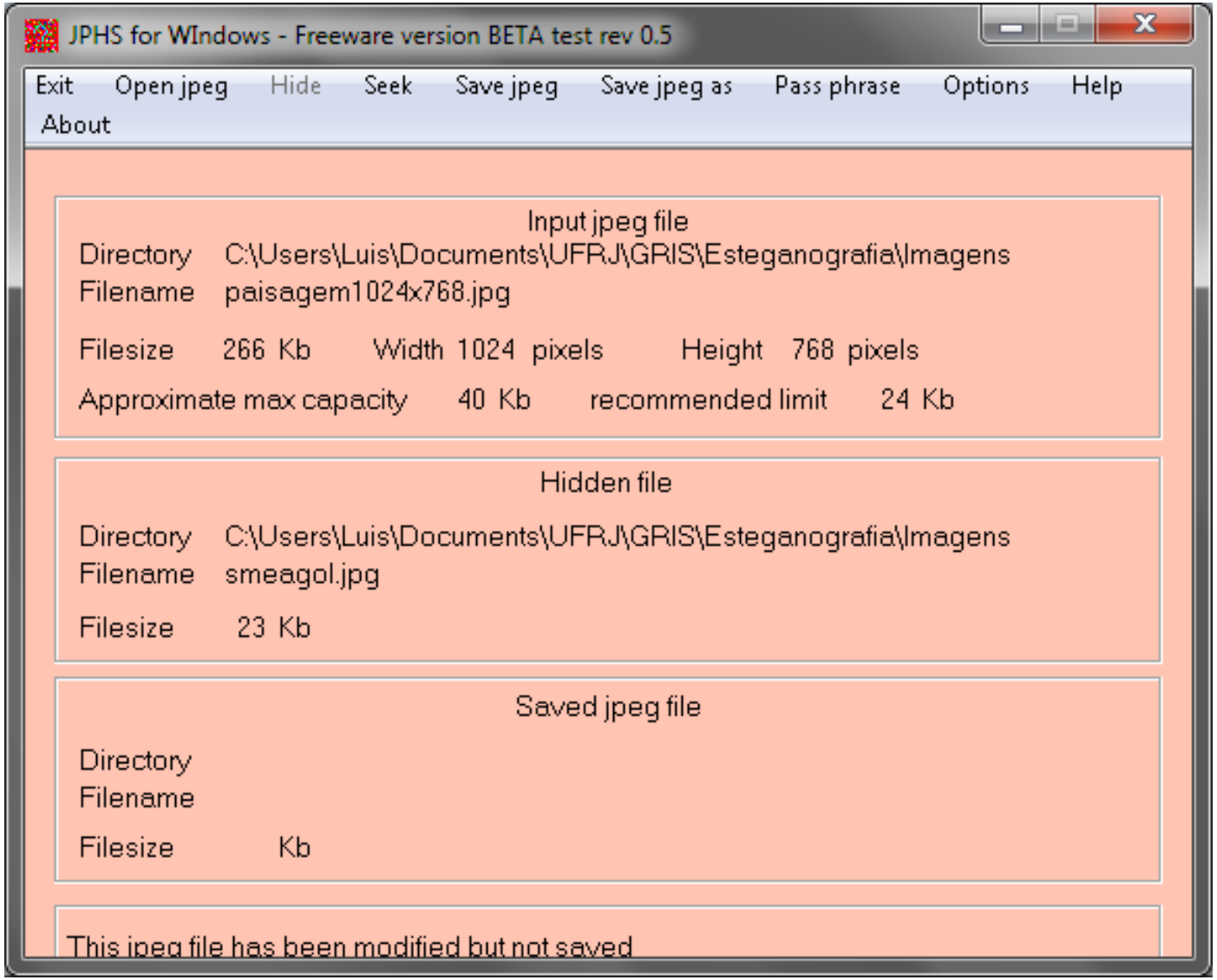
Paisagem 1024x768 - 266Kb



Smeagol - 23Kb

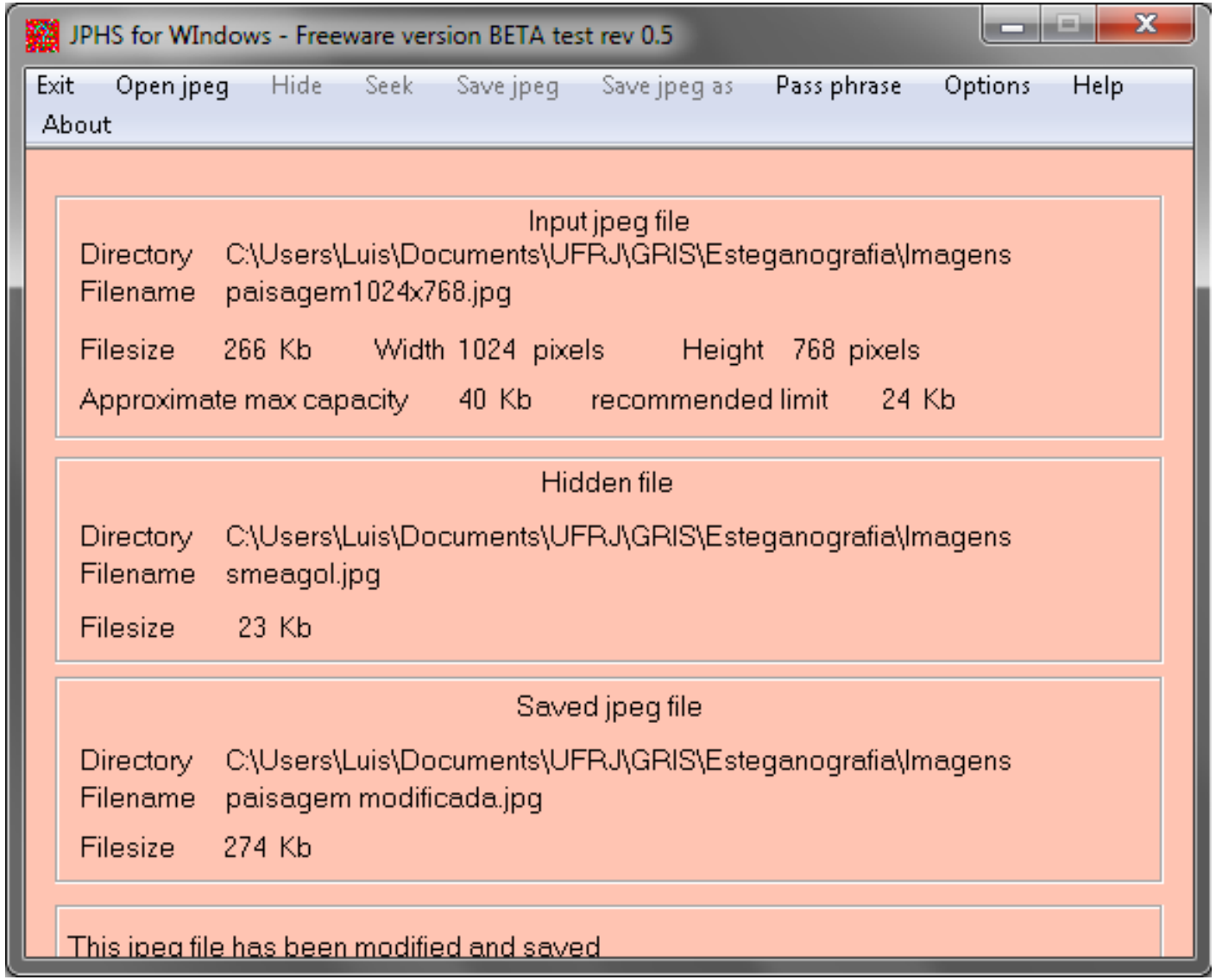
Técnicas Digitais

Bit menos significativo



Técnicas Digitais

Bit menos significativo



Técnicas Digitais

Bit menos significativo

(a)

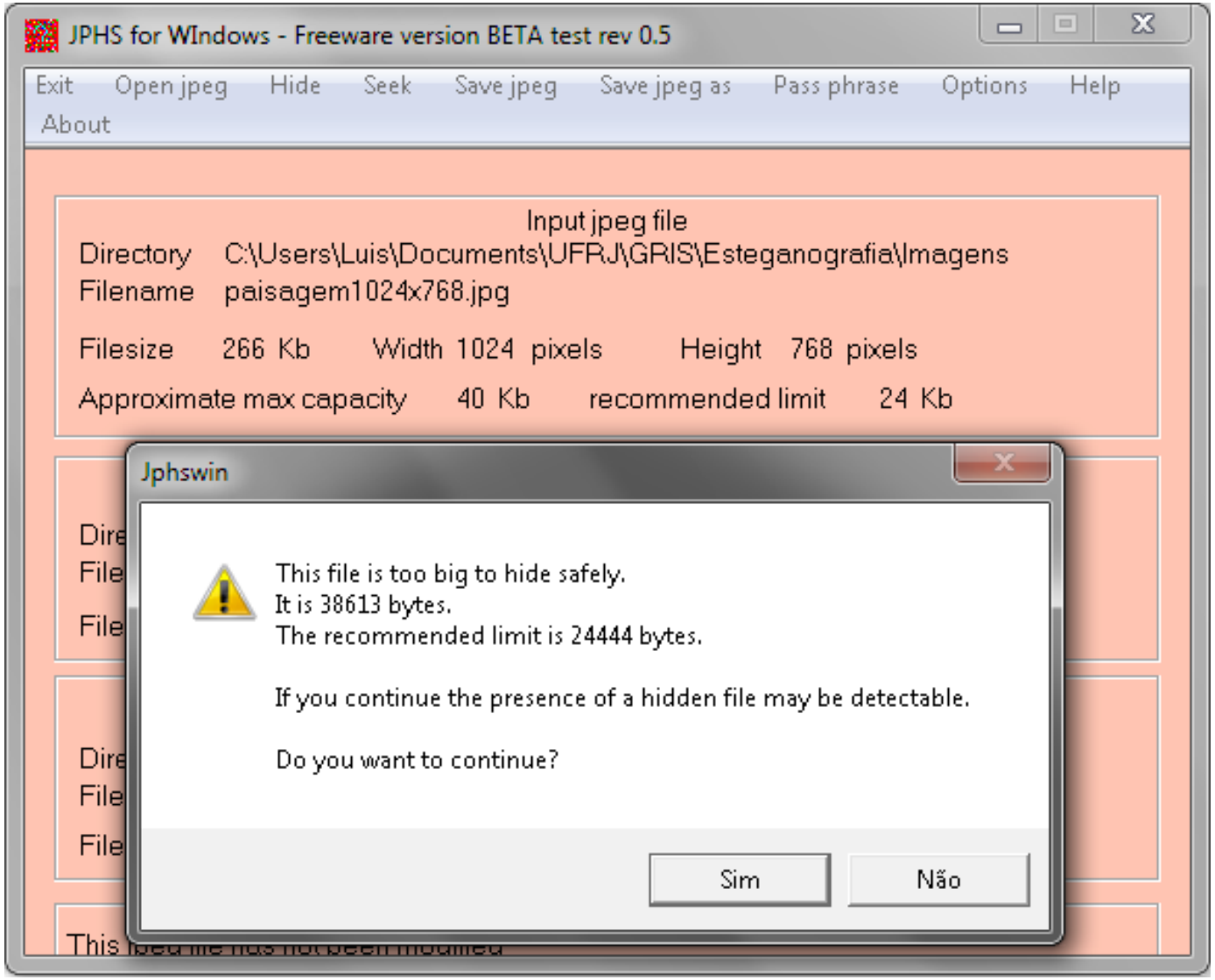
Técnicas Digitais

Bit menos significativo

Paisagem 2 290x290 - 38Kb

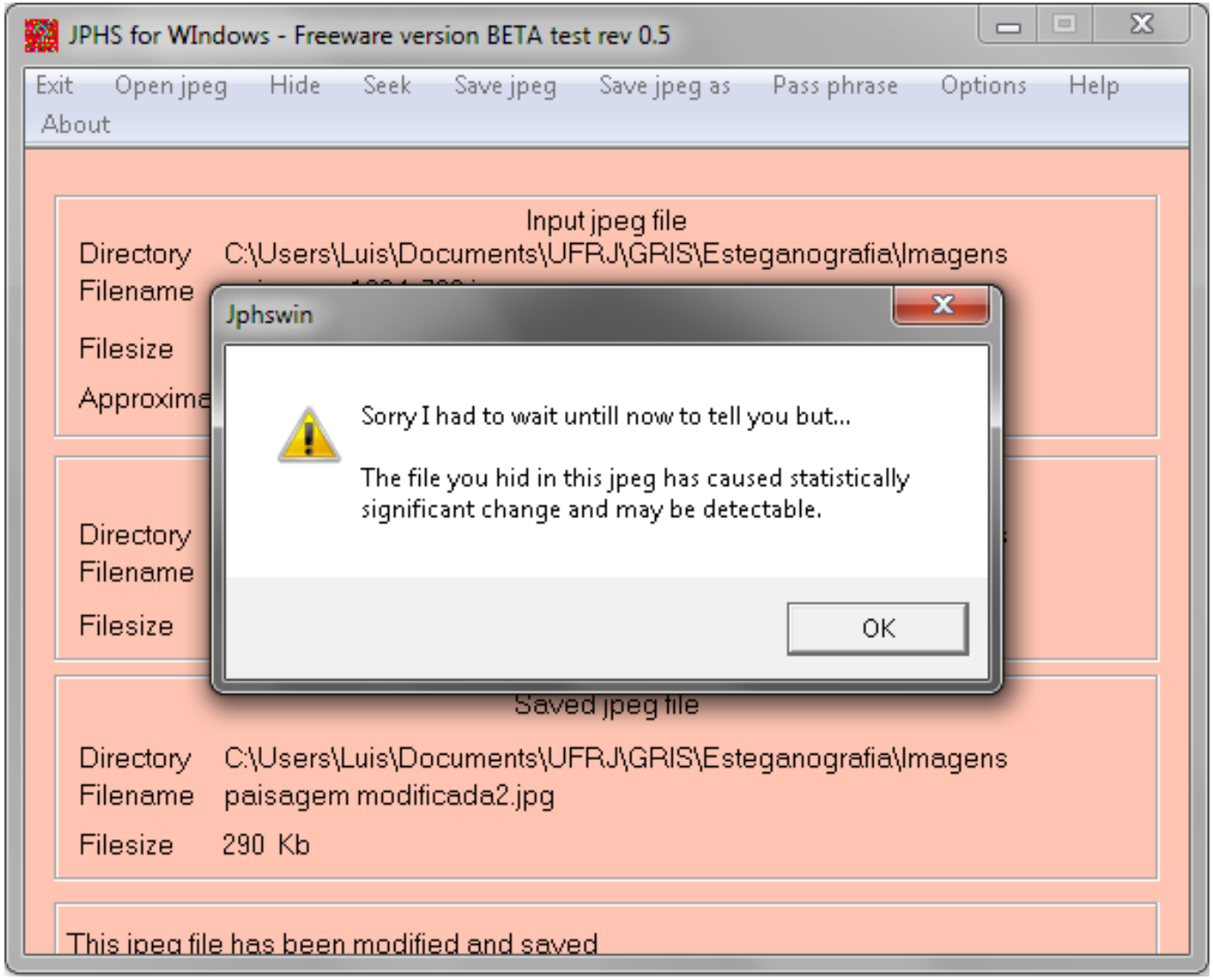
Técnicas Digitais

Bit menos significativo



Técnicas Digitais

Bit menos significativo



Técnicas Digitais

Bit menos significativo

(b)

Técnicas Digitais

Esteganografia BPCS (Bit-Plane Complexity Segmentation Steganography)

. Normalmente utilizada em arquivos BMP (True color – 24 bit)

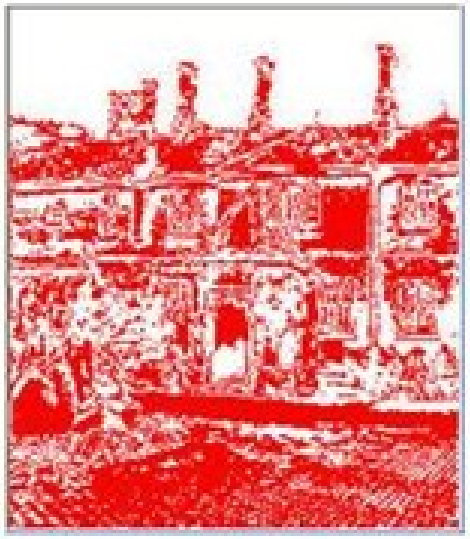
. Pode armazenar até um pouco mais do que 50% de informação, em relação ao tamanho da imagem original

. Utiliza-se de um padrão complexo para armazenar as informações entre os ruídos das imagens geradas pelo plano de bits da imagem

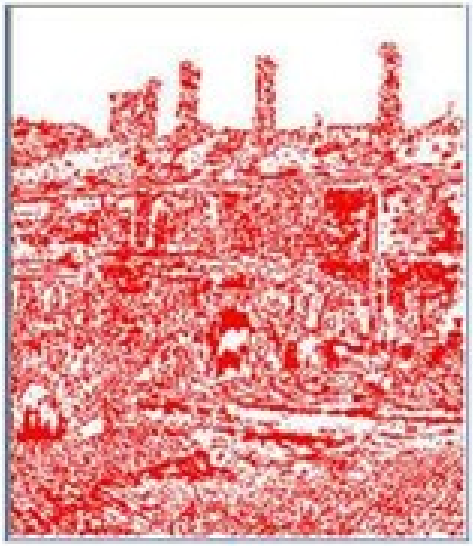
Técnicas Digitais

Esteganografia BPCS

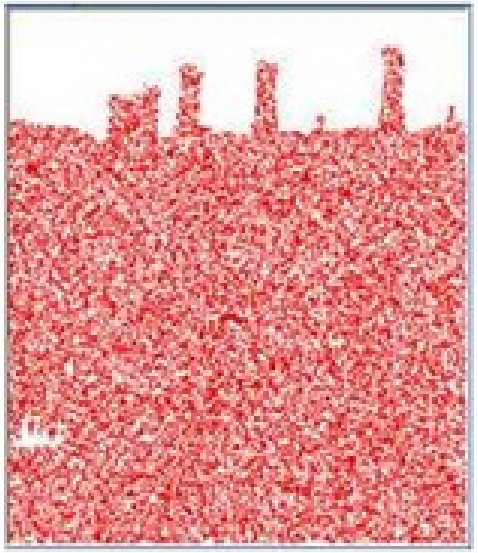
(a)



(b)



(c)



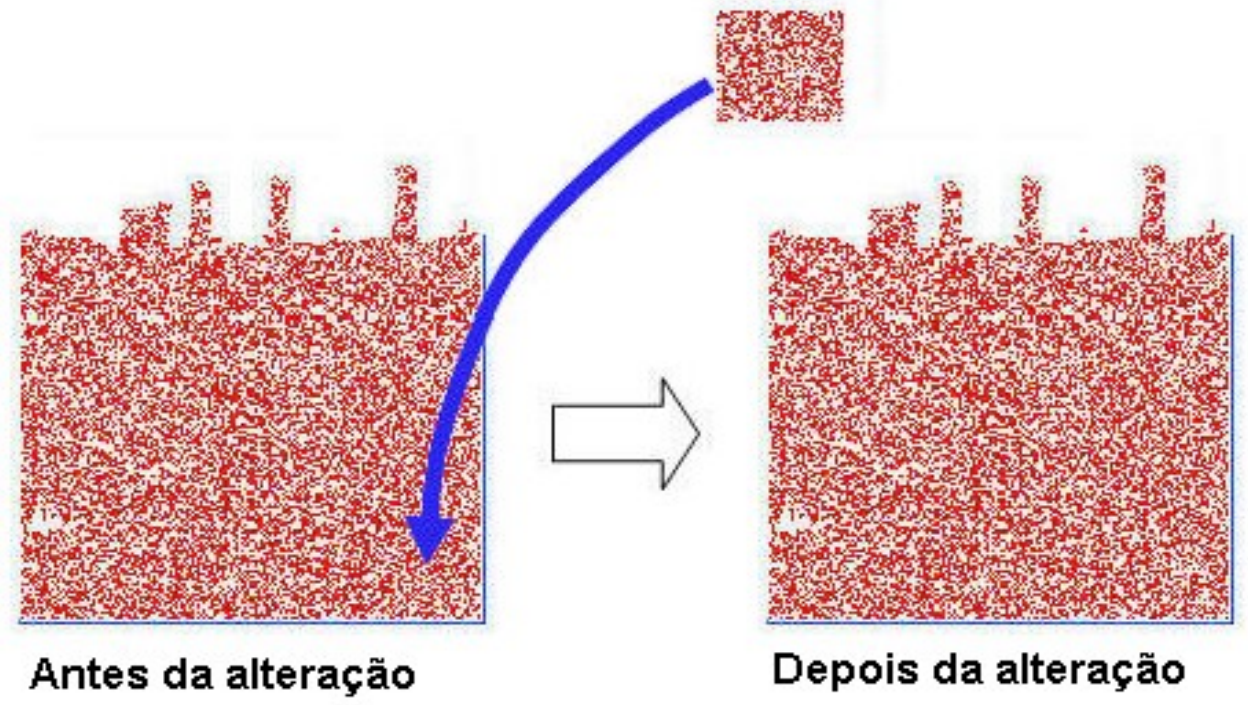
(d)

Imagem original, e sua cópia representado somente pelo bit mais significativo até o menos significativo

Fonte: http://www.datahide.com/BPCSe/principle-e.html

Técnicas Digitais

Esteganografia BPCS



Alterando um quadrado de “ruído” com a informação desejada
Imperceptível diferença ao olho humano

Fonte: http://www.datahide.com/BPCSe/principle-e.html

Técnicas Digitais

Esteganografia BPCS

(a)

(b)

(a) Imagem original de 834KB
(b) Nova imagem (ainda com 834KB) com um PDF de 361KB dentro da imagem

Fonte: http://www.datahide.com/BPCSe/principle-e.html

Técnicas Digitais

Outros métodos

. Marca d'água em arquivos (Autenticidade)

. Mensagens em arquivos de áudio

. Vídeos com frames esteganografados

. Imperceptíveis atrasos em pacotes de transmissão (rede ou dispositivo)

Esteganálise

O que é?

É o estudo de métodos que visam detectar a esteganografia

Alguns métodos:

. Comparação com o original
. Compressão de arquivos
. Randomização progressiva (checagem de ordem e localidade de uma possível mascaração)

O que dificulta a esteganálise:

. Uso de novos algoritmos de esteganografia
. Uso de criptografia na informação guardada

Notícias

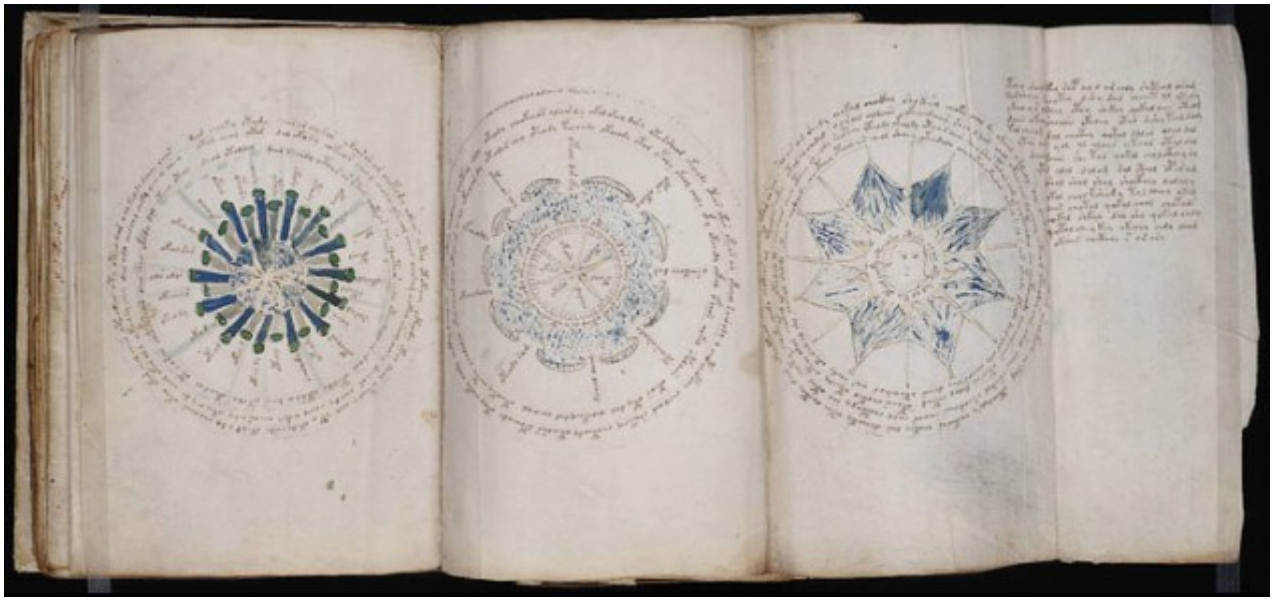
Juan Carlos Ramírez Abadía esconde mensagens de voz e de texto nas imagens da Hello Kitty
Folha de São Paulo - 10 de março de 2008

Steganography used by terrorists groups like Hamas, Hezbollah, al-Qaida and others
http://www.usatoday.com/tech/news/2001-02-05-binladen.htm

*In **October 2001**, the **New York Times** published an article claiming that **al-Qaeda** had used **steganographic** techniques to **encode messages into images**, and then transported these via e-mail and possibly via USENET to prepare and execute the **September 11, 2001 Terrorist Attack.***
http://www.experiencefestival.com/a/Steganography_-_Rumored_Usage_in_Terrorism/id/2097914

Notícias

"A self-described computer geek, Richard Rogers believes ***he has cracked*** *a code that has eluded scholars and researchers for* ***more than 500 years.*** *" (…)*
"Rogers has concluded that the manuscript is steganography, that is to say it has secret messages hidden within pictures."
http://www.havenews.com/articles/text-6327-code-rogers.html - 11/11/2009



Notícias

Steganography with TCP retransmissions
http://www.h-online.com/security/news/item/Steganography-with-TCP-retransmissions-741809.html - 29/05/2009

Real-time Steganography with RTP
"Real-time Transfer Protocol (RTP) is used almost ubiquitously by Voice over IP technologies to provide an audio channel for calls."
04/08/2007 - DEFCON 15
http://druid.caughq.org/presentations/

Aplicativos

JPHS for Windows – BETA test rev 0.5 (1999)
http://linux01.gwdg.de/~alatham/stego.html

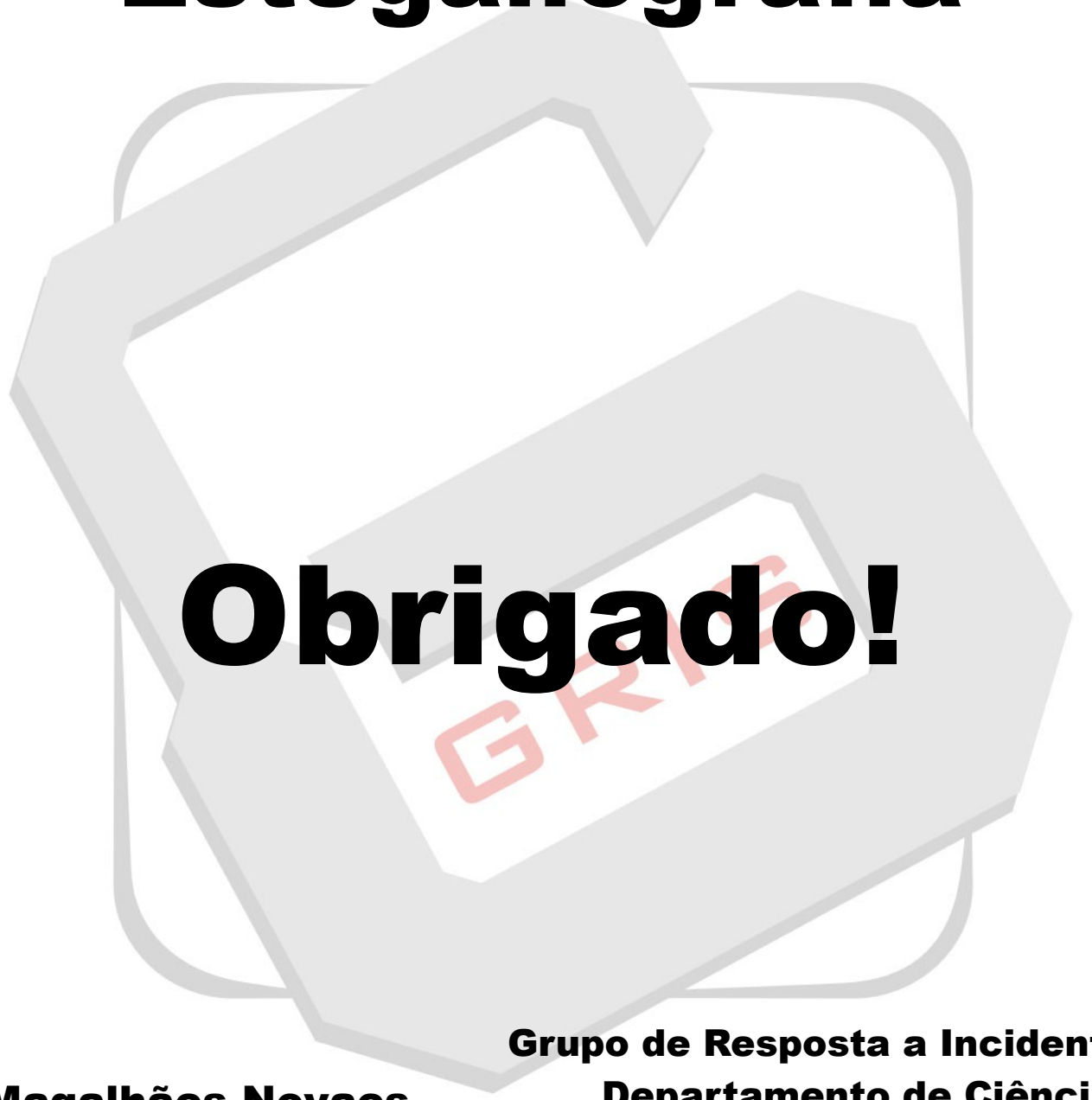
Lista de softwares para Esteganografia em diversos tipos de arquivos e SO's.
http://www.jjtc.com/Security/stegtools.htm

An automated tool to detect the presence and extraction of steganography
http://www.sarc-wv.com/stegalyzeras.aspx
http://www.sarc-wv.com/stegalyzerss.aspx

Esteganografia

Dúvidas?

Esteganografia



Obrigado!

Luís Fernando Magalhães Novaes
luisfernando@gris.dcc.ufrj.br

Grupo de Resposta a Incidentes de Segurança
Departamento de Ciência da Computação
Instituto de Matemática
Universidade Federal do Rio de Janeiro