

Esteganografia 2

Palestra 5 - 07/06

IMEsec 

Esteganografia

Do grego: Steganos (escondida) + Graphein (escrita)

Ocultar uma mensagem dentro de outra

!= Criptografia

Esconder que a mensagem existe em primeiro lugar





Dennis Farrell

@DennisFarrell



Imagine being held at gunpoint (bear with me) by a literate animal, and the only hope of rescue is (BEAR WITH ME) tweeting a coded message

4/26/17, 9:23 AM

6,226 RETWEETS **11.4K** LIKES

Esconder informação em imagens

Imagem original



Informação
confidencial

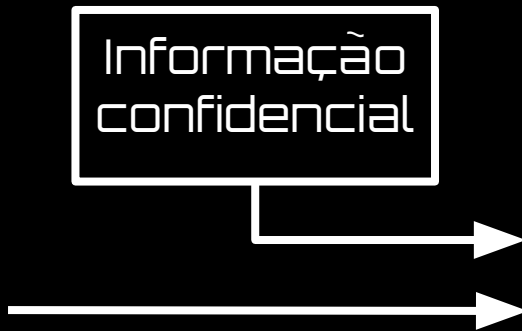


Imagem com a
informação oculta



Imagem original



Informação
confidencial



Imagem com a
informação oculta



LSB - Least Significant Bits

Método mais comum e popular nos dias de hoje

Esconder a informação nos bits menos significativos de uma
imagem

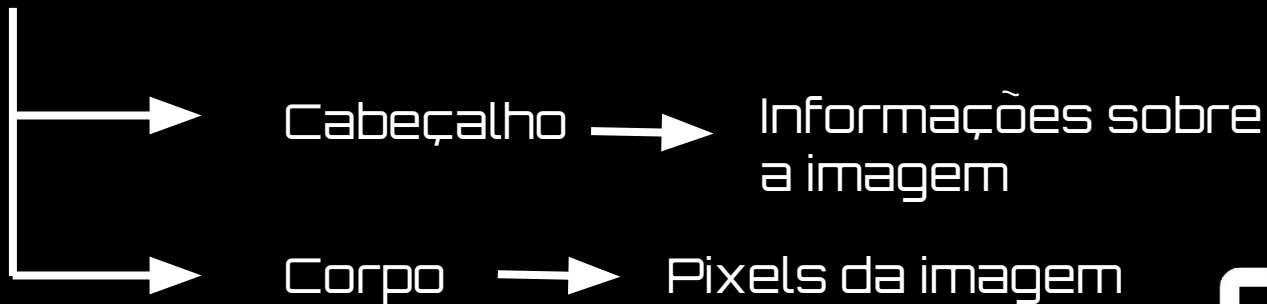


Representação da imagem



= 01010111010....

Imagens são apenas 0's e 1's



Representação da imagem (lossless)

Pixel de 24 bits



00101011

10001110

11001111



Escondendo na imagem por LSB

Imagem de 3 pixels

Mensagem: 01101101

Pixel 1: 10100101 11101100 11000100

Pixel 2: 11110011 11101100 11000010

Pixel 3: 00100010 00100010 11000000



Escondendo na imagem por LSB

Imagem de 3 pixels

Mensagem: 01101101

Pixel 1: 10100100 11101101 11000101

Pixel 2: 11110010 11101101 11000011

Pixel 3: 00100010 00100011 11000000



Escondendo na imagem por LSB

Imagem de 3 pixels

Mensagem: 01101101

Pixel 1: 10100100 11101101 11000101

Pixel 2: 11110010 11101101 11000011

Pixel 3: 00100010 00100011 11000000

→ Nova Imagem



Extraindo a mensagem por LSB

Imagem de 3 pixels

Pixel 1: 10100100 11101101 11000101

Pixel 2: 11110010 11101101 11000011

Pixel 3: 00100010 00100011 11000000



Extraindo a mensagem por LSB

Imagem de 3 pixels

Pixel 1: 10100100 11101101 11000101

Pixel 2: 11110010 11101101 11000011

Pixel 3: 00100010 00100011 11000000



mensagem

01101101



Problemas com LSB

- Mensagem não tão protegida -> pode ser criptografado
- Testes estatísticos revelam o uso de LSB



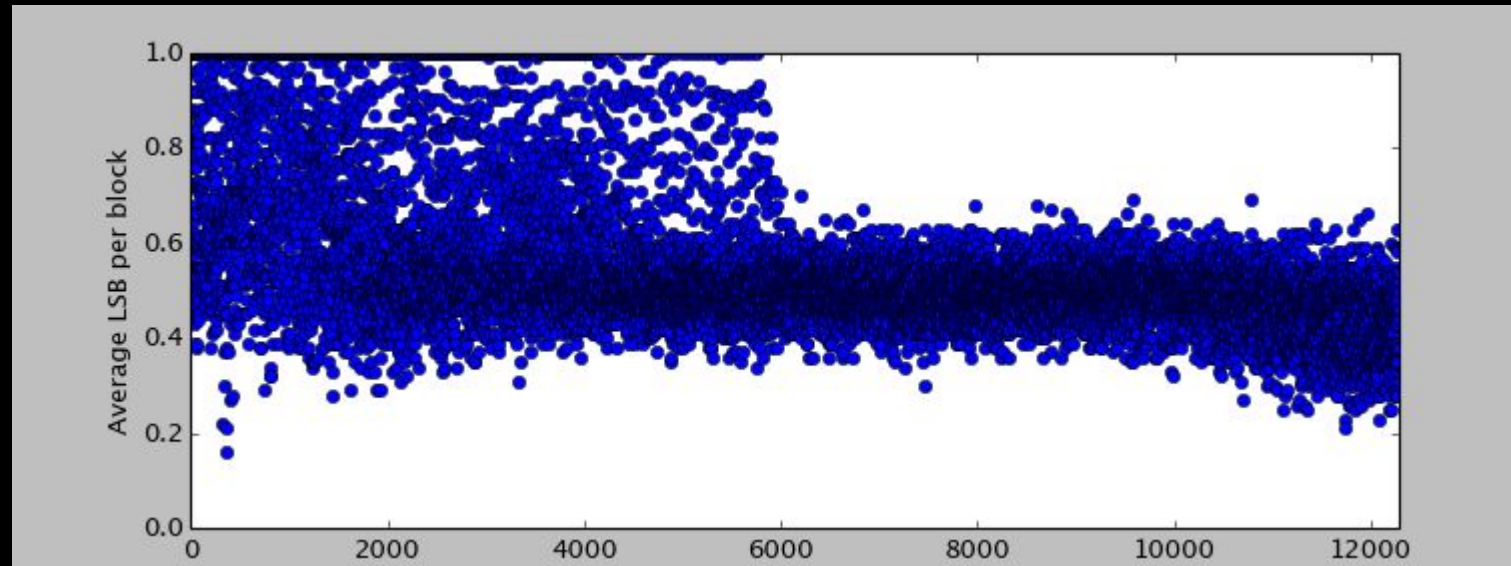


Imagem sem esteganografia



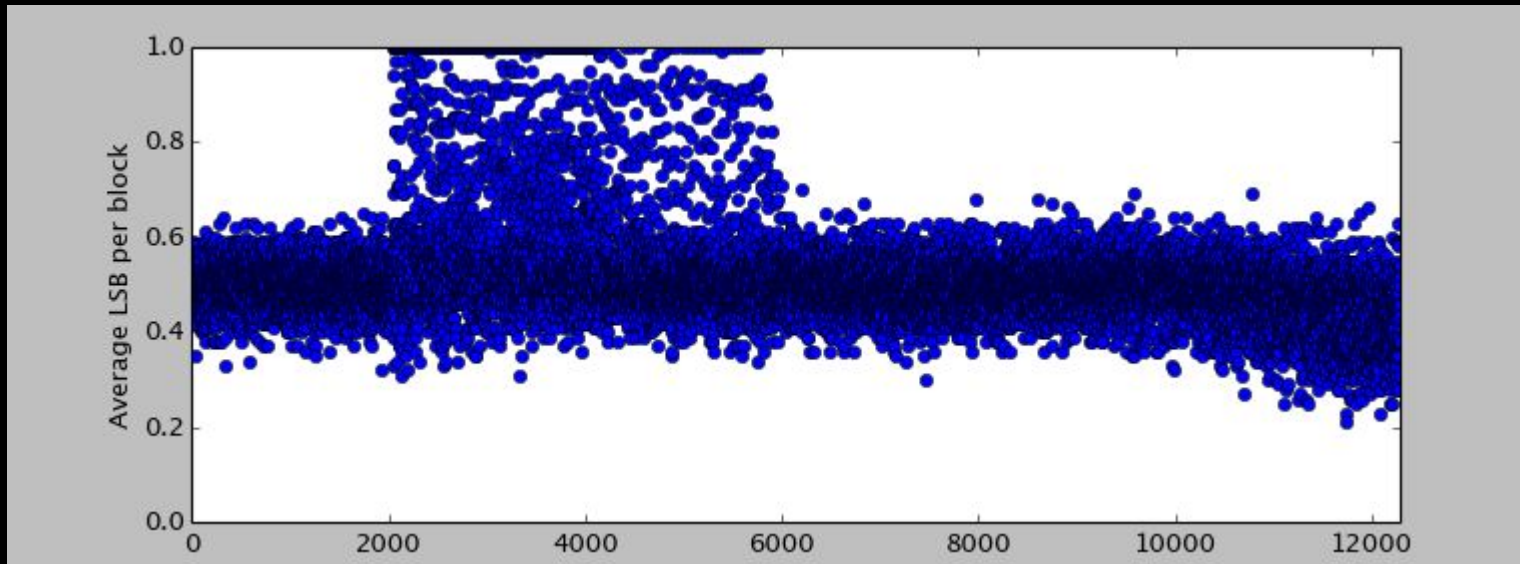
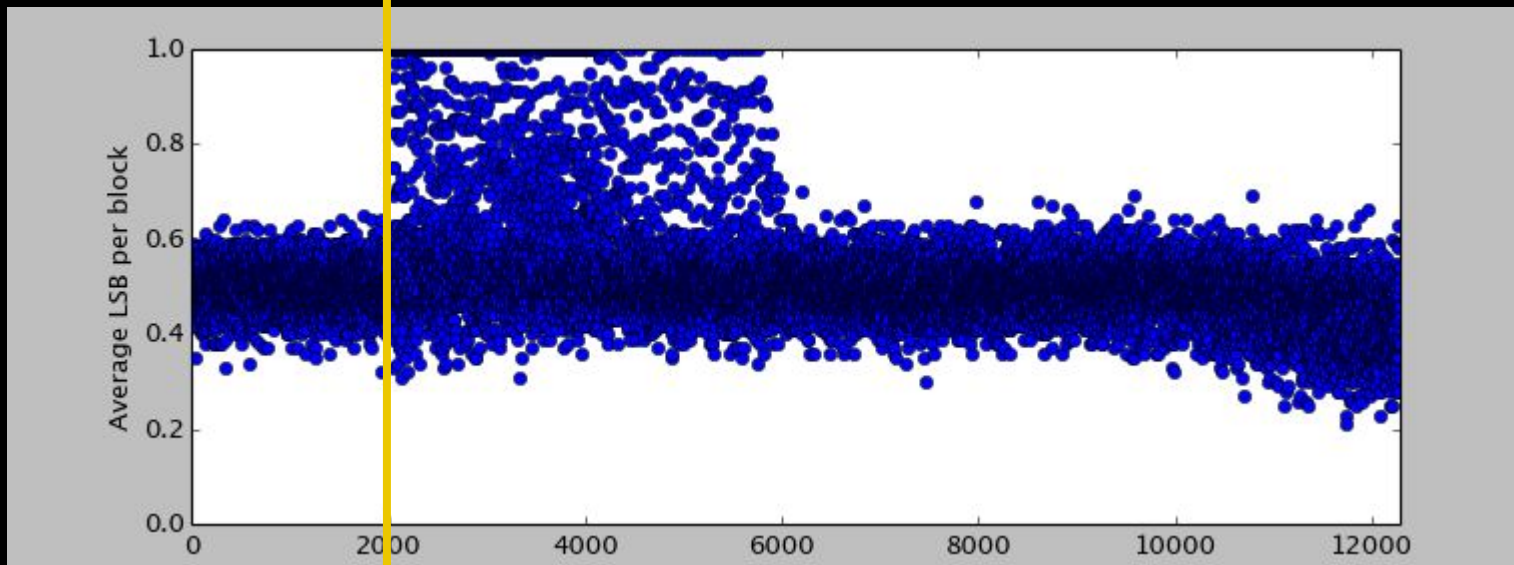


Imagem **com** esteganografia





Parte com esteganografia



Exemplo prático



Marca d'agua

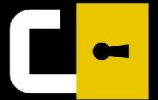


Copyright \$(BANCO_DE_IMAGENS_GENERICO)

Imagem baixada por:
Andrew Lopes em 2018-06-07:14:30



Marca d'agua escondida



Marca d'agua escondida

- Marca d'agua escondida → Usuário não sabe que ela está lá



Marca d'agua escondida

- Marca d'agua escondida → Usuário não sabe que ela está lá
- Informações sobre quem baixou a imagem (essa pessoa pode ser identificada se a imagem for vazada)

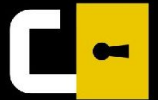


Marca d'agua escondida

- Marca d'agua escondida → Usuário não sabe que ela está lá
- Informações sobre quem baixou a imagem (essa pessoa pode ser identificada se a imagem for vazada)
- Não está nos metadados do arquivo e é resistente a compressão (difícil de remover)



Zip e PDF



5 This ZIP is also a PDF

by Julia Wolf

We the editors have lost touch with the author, who submitted the following napkin sketches in lieu of the traditional LaTeX or ASCII prose. Please note when forming your own submissions that we do not accept napkins, except when they are from Julia Wolf or from John McAfee.

<https://github.com/filcab/pocorgtfo/blob/gh-pages/pocorgtfo01.pdf>



```
$ cat foo.pdf bar.zip foo.pdf > baz.pdf  
$ zip -A baz.pdf
```



Foremost

Data Carver:

Procura em blocos de 512 bytes
por cabeçalhos de arquivos



COPYRIGHT

This program is a work of the US Government. In accordance with 17 USC 105, copyright protection is not available for any work of the US Government.



```
$ foremost baz.pdf
```



Esconder em áudio

Exemplo:

-> Imagem bmp

-> Spectrology

-> Transforma a imagem em música

-> Junta as duas músicas usando Audacity



Obrigado!

DISCLAIMER: Conteúdo apenas para fins educacionais

