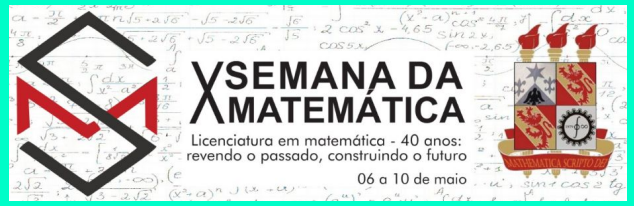
Hackeando Redes Neurais com Python

Diogo Melo



Sobre

Diogo Melo

Formação: Física - Computação

Interesses: Sistemas complexos/emergentes, NNs…

Profissional: Analista de dados @Intelivix

Sobre

Apresentação

Nível: Exposição ao tema, introdutório

Objetivo: O que foi/pode ser feito

Estilo: Exemplos - Link

Agenda

Introdução - Hackeando redes Neurais

Redes Neurais - Blocos de construção

Exemplos

Introdução

Redes Neurais?

Generalização para uma função: Domínio -> Contra Domínio

Ex.: Imagem -> Gato ou Cachorro

Texto -> Péssimo, ruim, … bom, ótimo

e-mail -> Spam ou não Spam

Dados de um Processo -> Probabilidade de perda

Hackear (raquear)?

“Explorar um sistema para usá-lo de uma forma não prevista”

“Adaptação grosseira e engenhosa”

Python?

Alto nível

Comunidade ativa (+github!!!)

Bibliotecas...

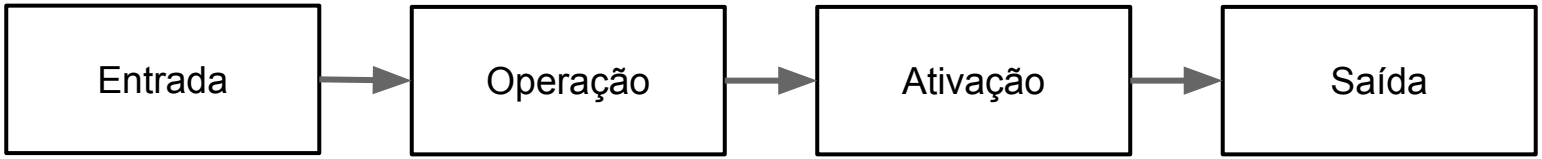
Várias outras….

Hackeando redes neurais com Python

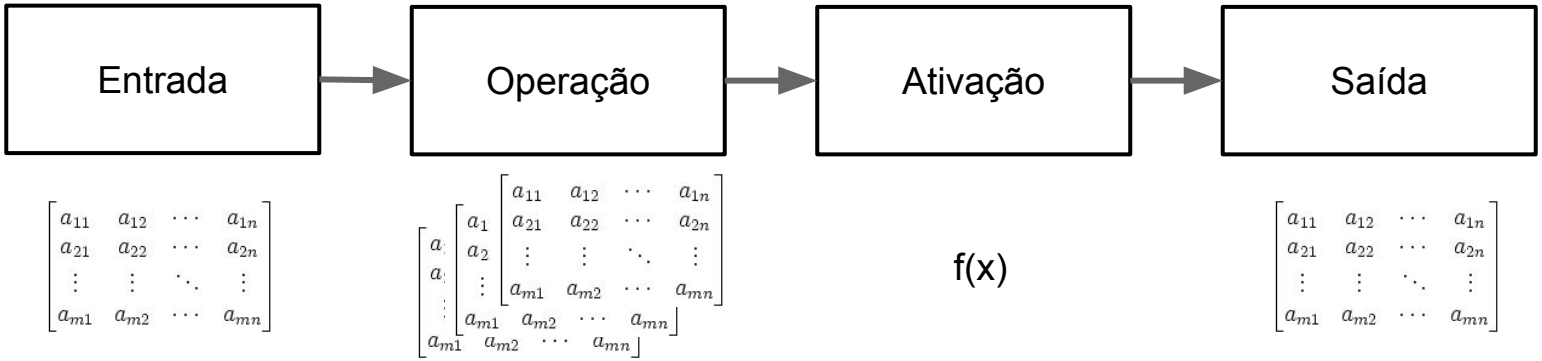
Usar generalizações de funções de formas não esperadas e engenhosas com abstrações de alto nível.

Redes Neurais

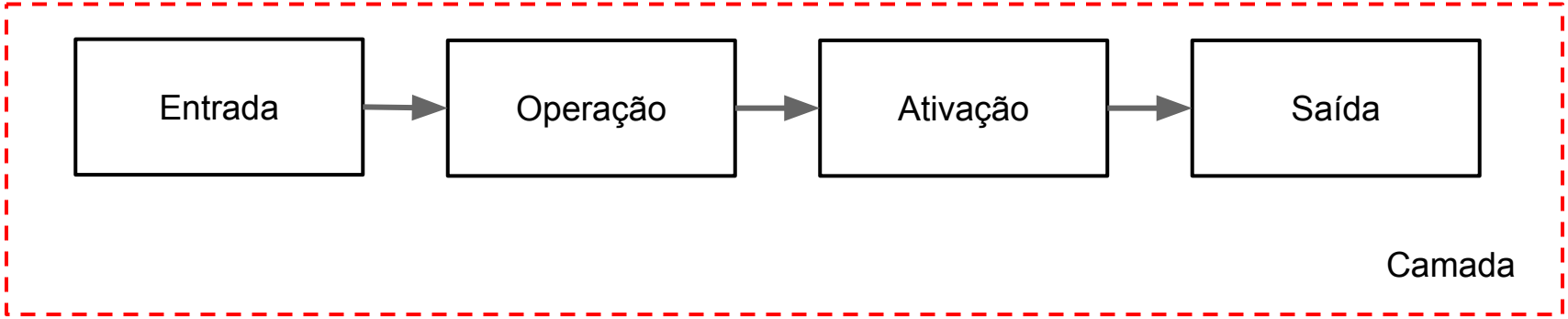
Redes Neurais - Blocos de Construção



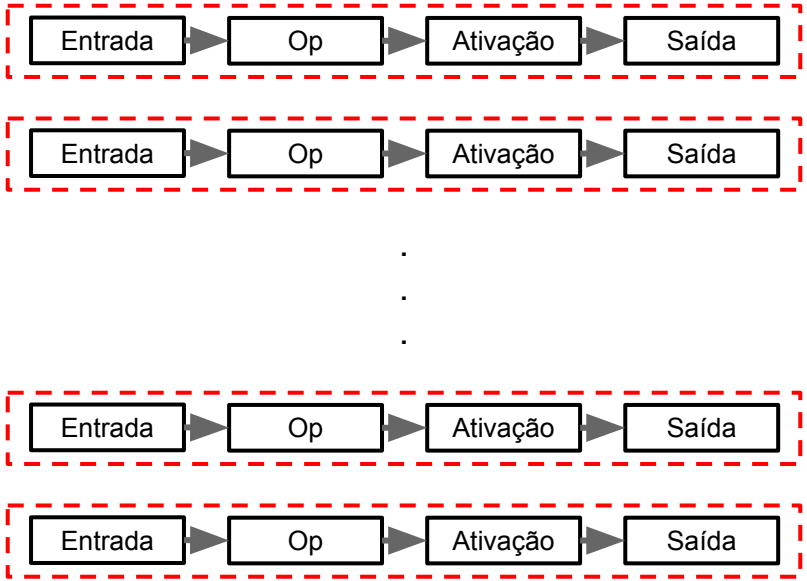
Redes Neurais - Blocos de Construção



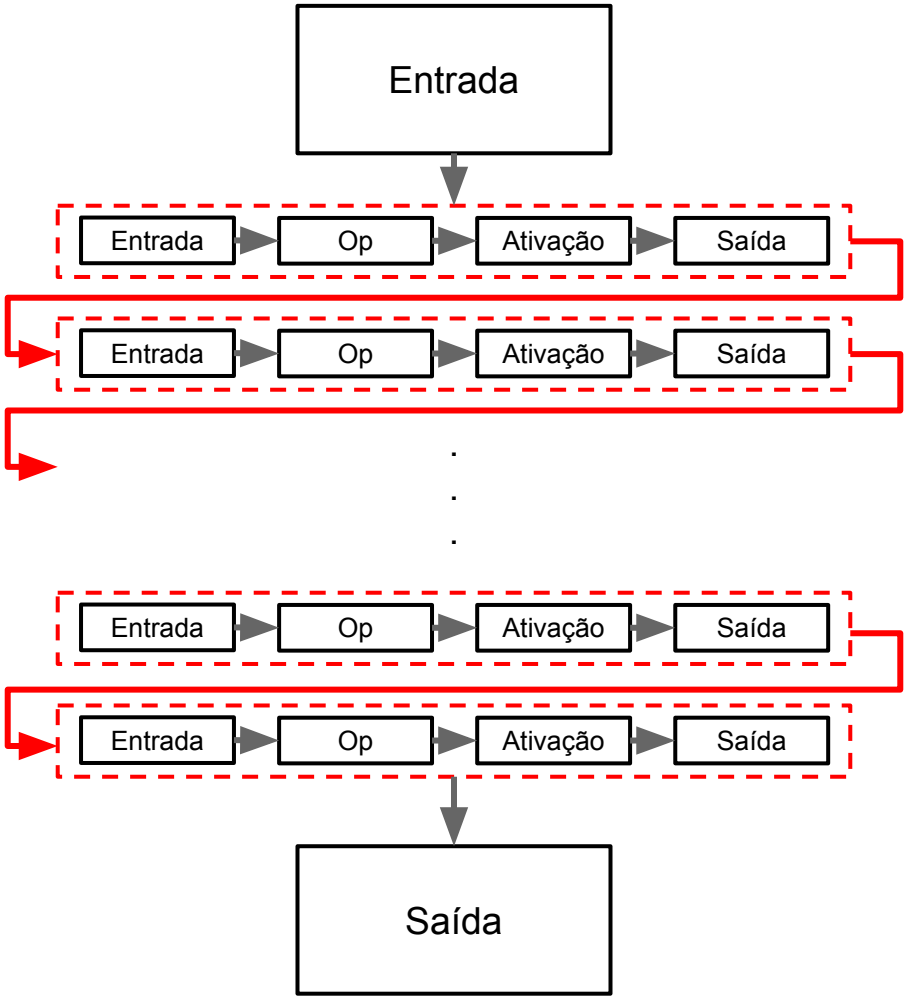
Redes Neurais - Blocos de Construção



Redes Neurais

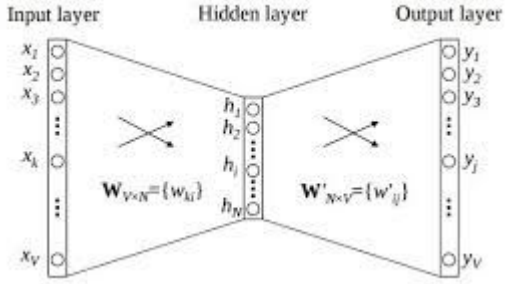


Redes Neurais

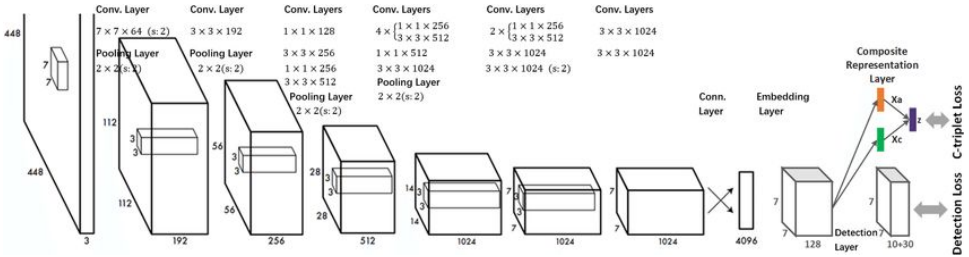


Redes Neurais

VGG16



word2vec



YOLO

Abordagens

Exemplos

Caixa Cinza

- Ajuste fino/Embeddings
- Abstrações

Caixa Preta

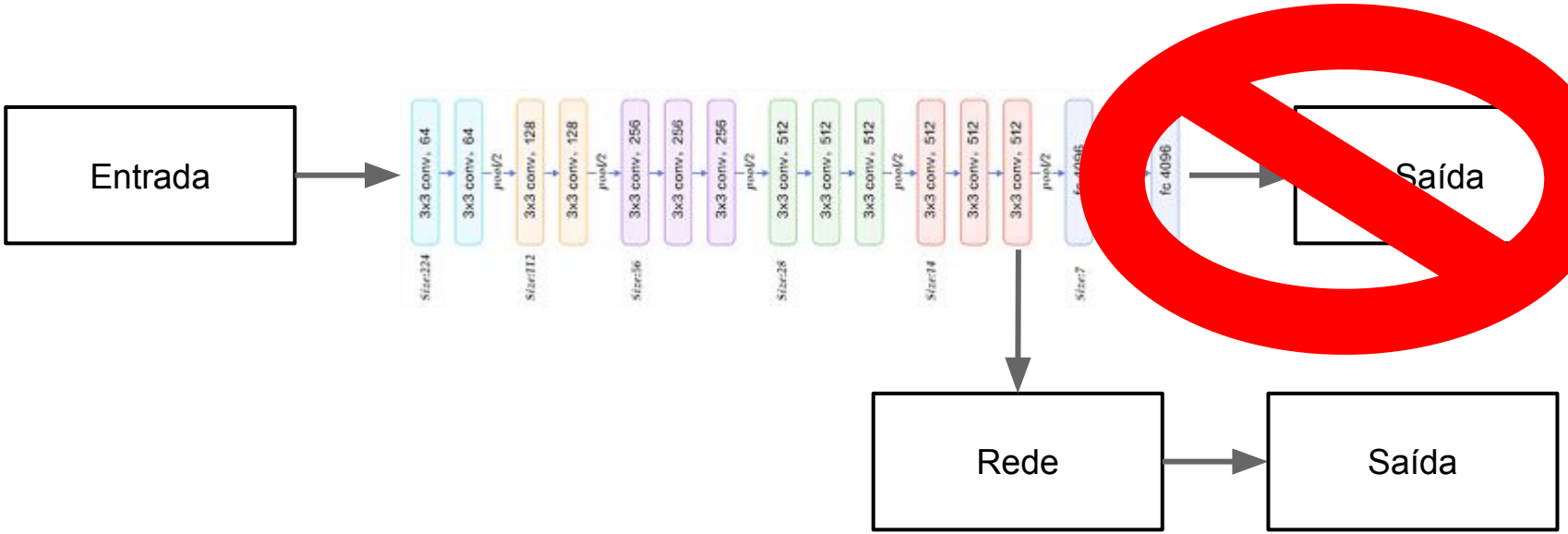
Caixa Cinza I - Ajuste fino / Embedding

Caixa Cinza I - Ajuste fino / Embedding

10 mi+ imagens!

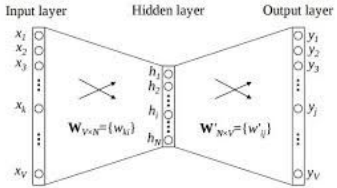
1000 categorias

Caixa Cinza I - Ajuste fino / Embedding



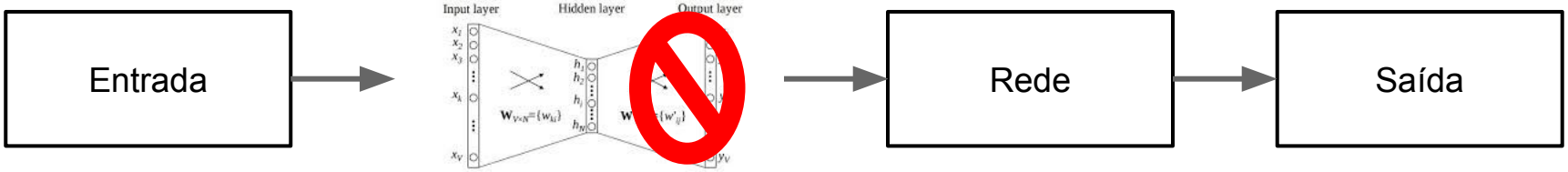
Caixa Cinza I - Ajuste fino / Embedding

Entrada



Saída

Caixa Cinza I - Ajuste fino / Embedding



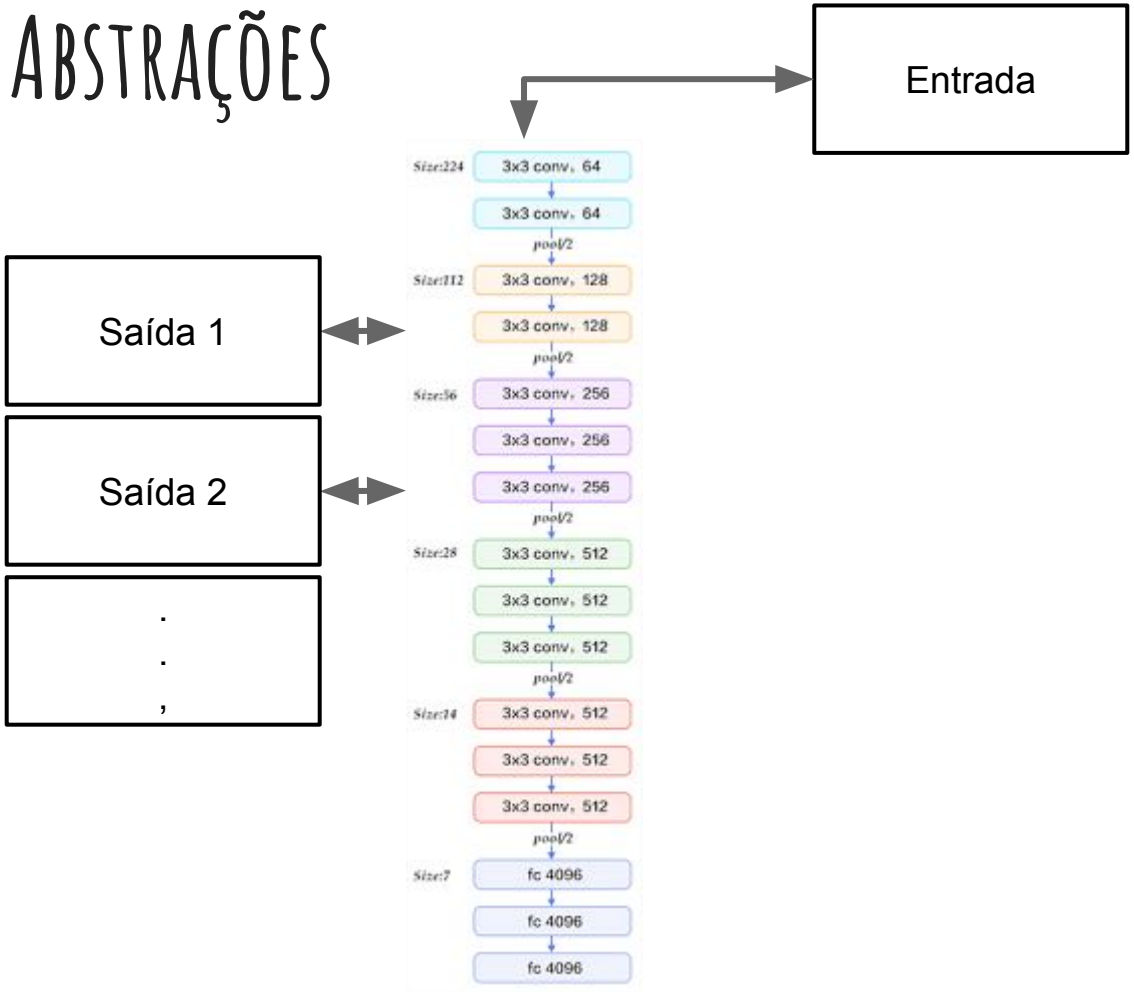
Caixa Cinza I - Ajuste fino / Embedding

Exemplo 1: Importando no Keras
https://github.com/keras-team/keras/blob/master/keras/applications/vgg16.py

Exemplo 2: Importando no Tensorflow
https://github.com/diogoffmelo/styletransfer/blob/master/src/vgg.py

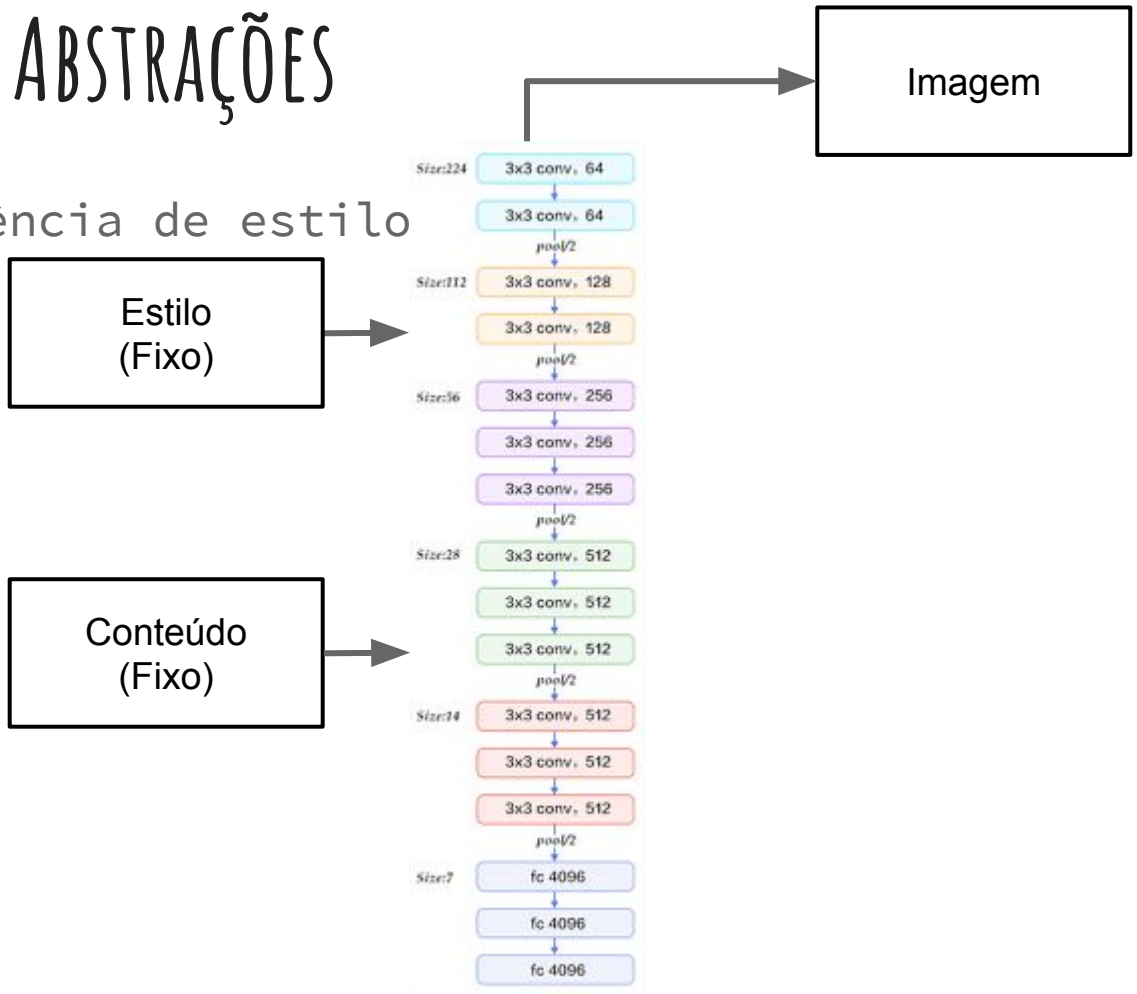
Exemplo 3: Felix yu
https://flyyufelix.github.io/2016/10/08/fine-tuning-in-keras-part2.html

Caixa Cinza II - Abstrações



Caixa Cinza II - Abstrações

Exemplo: Transferência de estilo



Caixa Cinza II - Abstrações

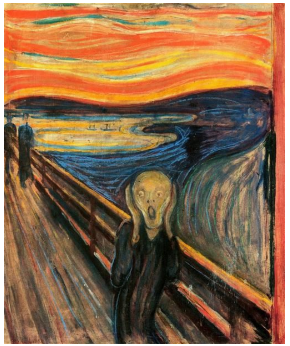
Exemplo: Transferência de estilo

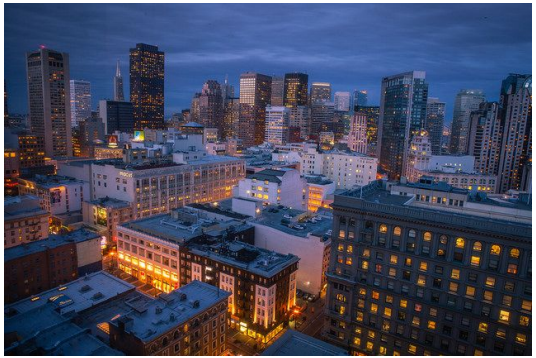
https://github.com/fzliu/style-transfer

"A Neural Algorithm of Artistic Style", L. Gatys, A. Ecker, and M. Bethge

Caixa Cinza II - Abstrações

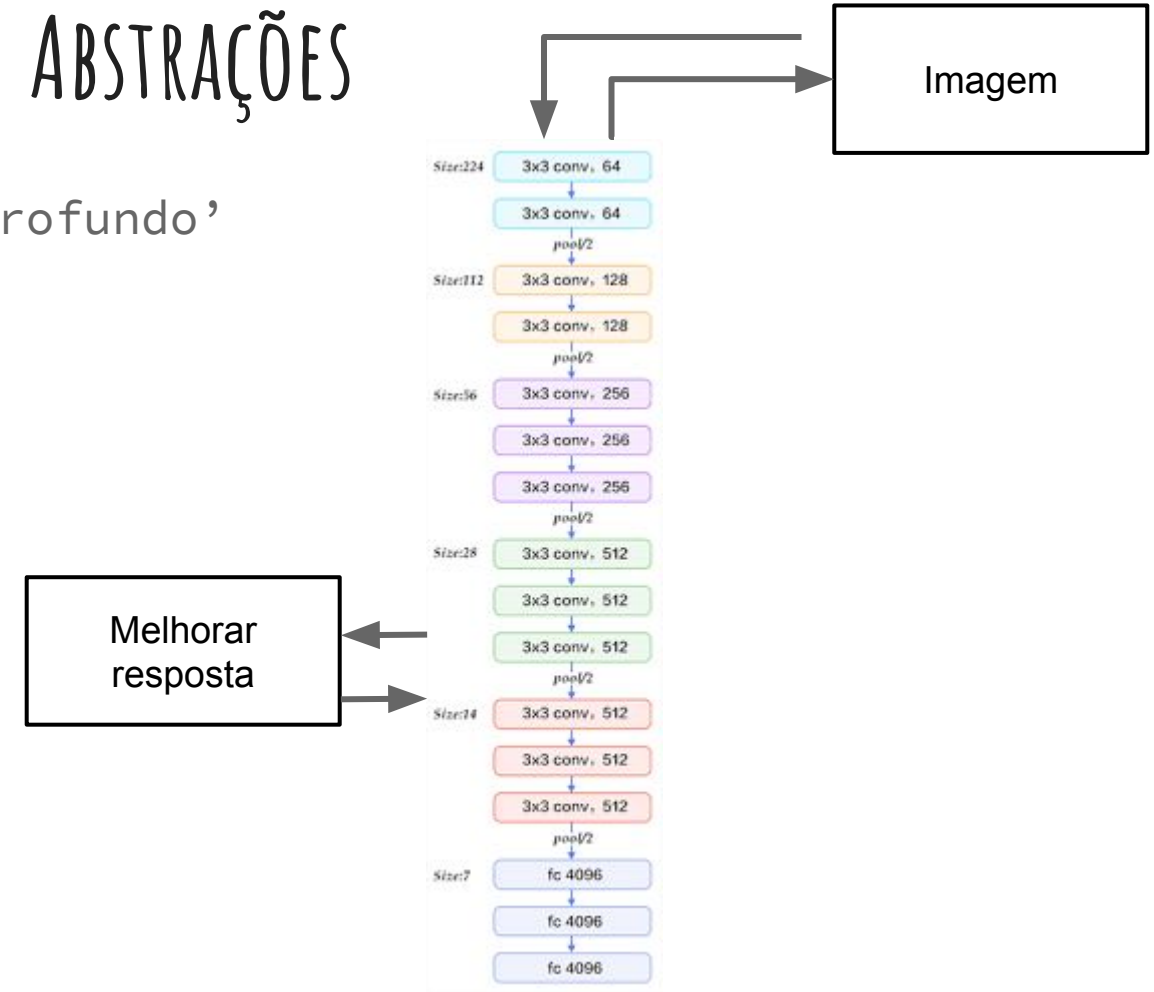
Exemplo: Transferência de estilo





Caixa Cinza II - Abstrações

Exemplo: ‘Sonho profundo’



Caixa Cinza II - Abstrações

Exemplo: ‘Sonho profundo’

https://github.com/google/deepdream/blob/master/dream.ipynb

https://github.com/kesara/deepdreamer

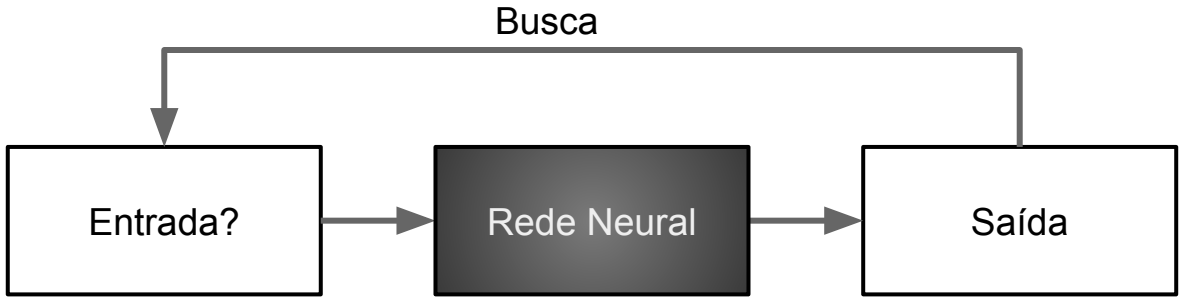
Caixa Cinza II - Abstrações

Exemplo: ‘Sonho profundo’

https://github.com/perellonieto/DeepTrip

https://users.ics.aalto.fi/perellm1/deep_dreams.shtml

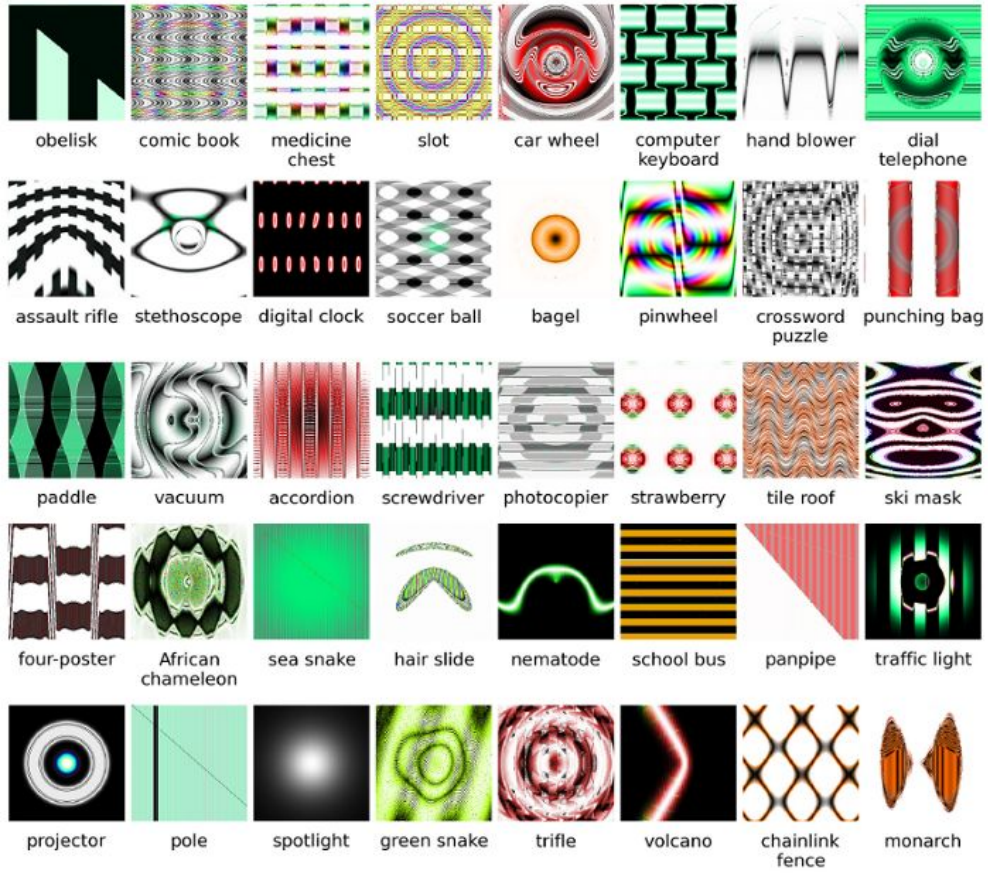
Caixa Preta



Caixa Preta

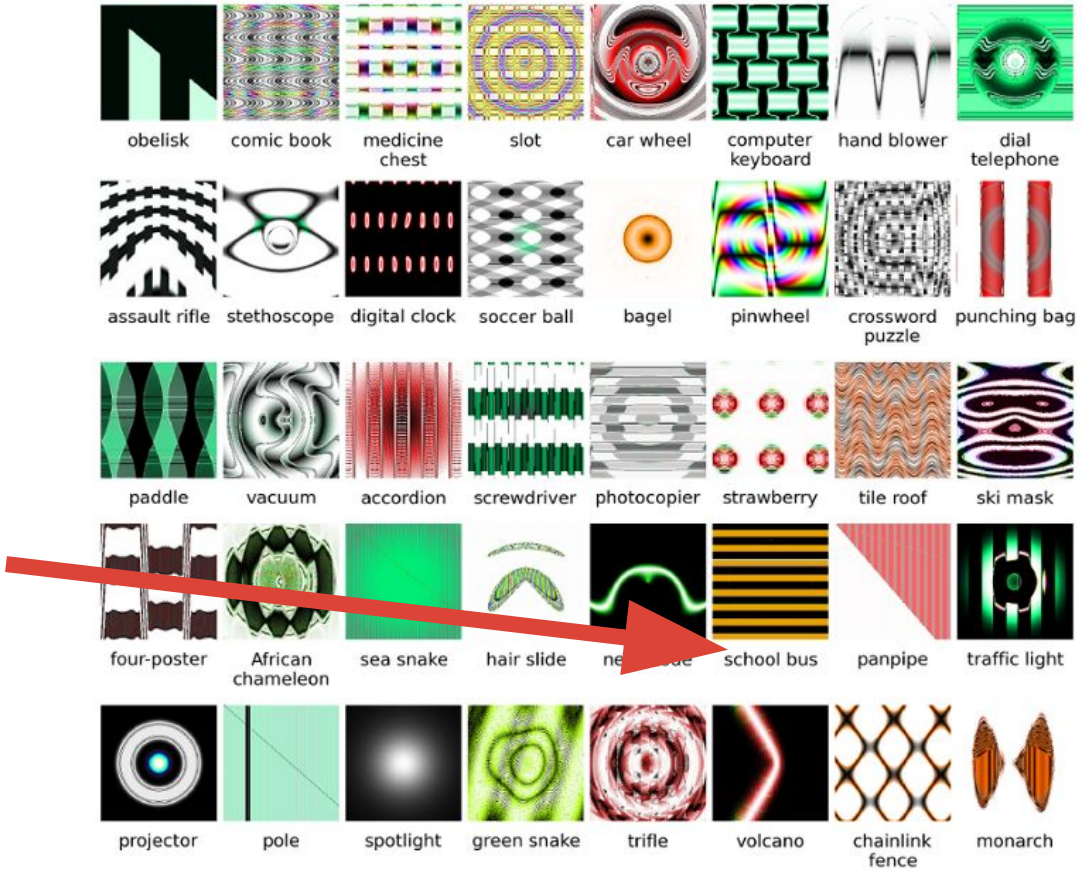
Busca por texturas

[Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images, A. Nguyen, J. Yosinski, J. Clune.]



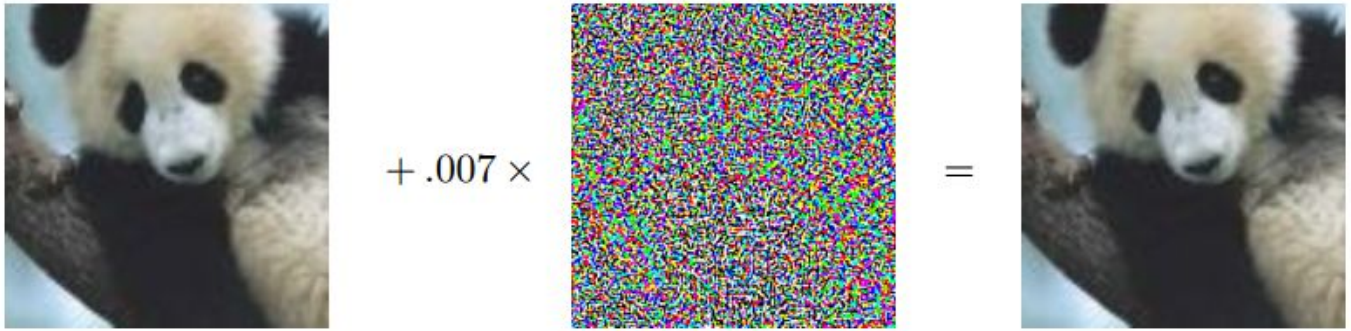
Caixa Preta

Busca por texturas:



Caixa Preta

Pequenas perturbações

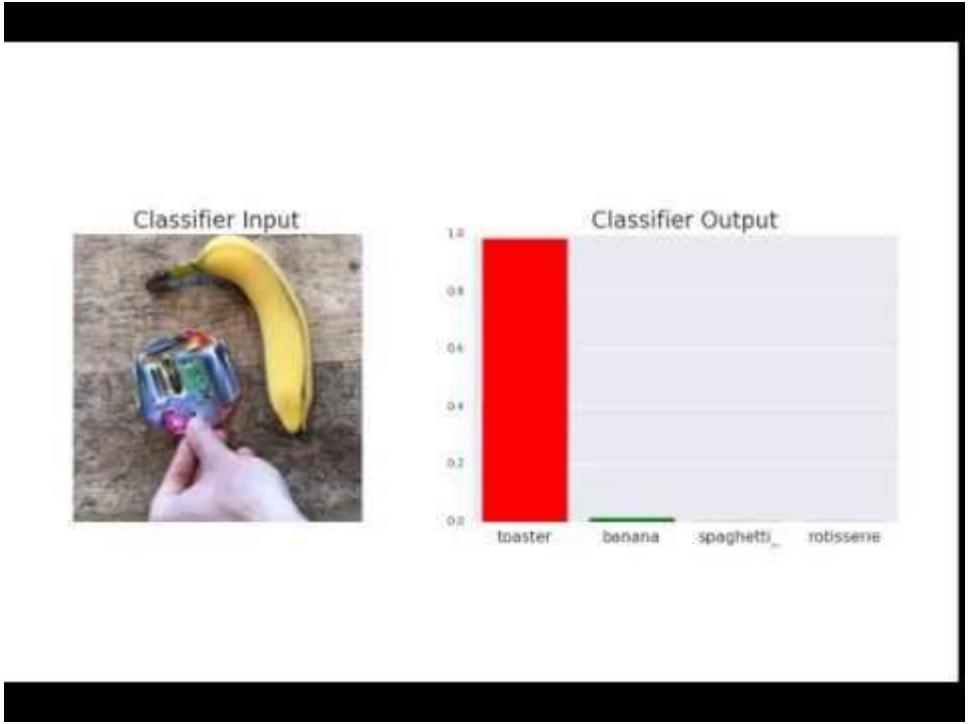


EXPLAINING AND HARNESSING ADVERSARIAL EXAMPLES, I. J. Goodfellow, J. Shlens, C. Szeged.

Caixa Preta

https://www.csail.mit.edu/news/fooling-neural-networks-w3d-printed-objects

Caixa Preta



https://www.youtube.com/watch?v=i1sp4X57TL4

Conclusões

Conclusões

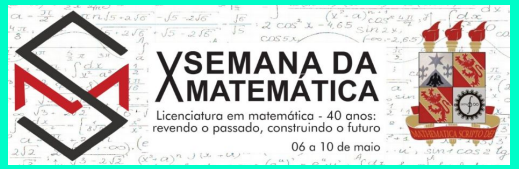
Python + NN + Hacking = <3

Recombinação, Reuso

Cuidado!

- Segurança?
- Confiabilidade?
- ALGORITHMIC JUSTICE LEAGUE

Obrigado!


SEMANA DA
MATEMÁTICA
Licenciatura em matemática - 40 anos:
revendo o passado, construindo o futuro
06 a 10 de maio