Estudo Comparativo Entre Arquiteturas de Deep Learning Para Detecção de Falsificações em Imagens.

•••

Por Thales A. Paletti Pomari
Orientado por Prof. Dr. Tiago Carvalho

Sumário

Introdução

- Volume de imagens circulando;
- Softwares de edição;
- *Splicing*.

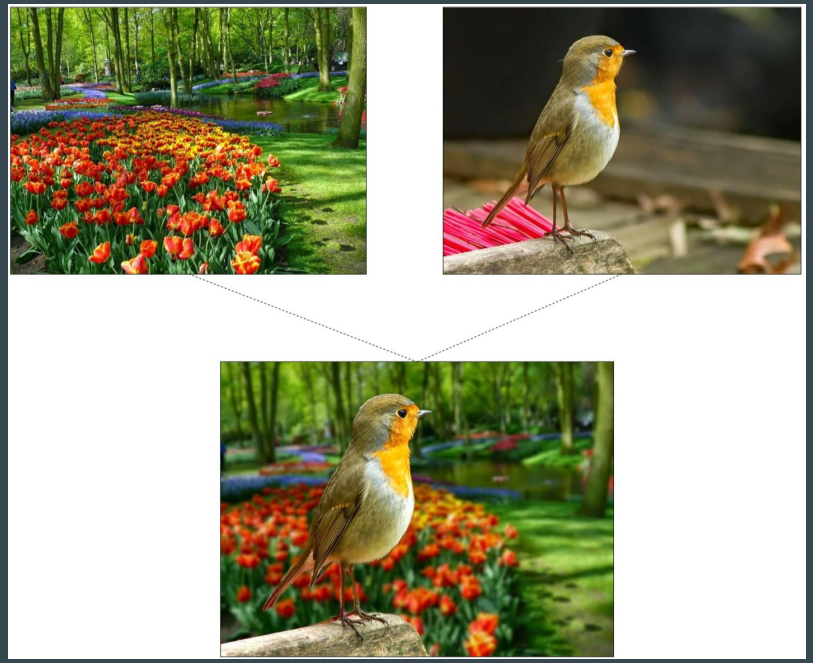

Imagem 1: Exemplo de falsificação do tipo *splicing*.

Introdução

- Perigo de *Fake News*;
- Técnicas de reconhecimento de padrões;

Imagem 2: Exemplo de Fake News utilizando imagens.

Justificativa

Avaliar o desempenho de diferentes arquiteturas de CNN desenvolvidas para o contexto de reconhecimento de objetos, porém aplicadas ao problema de detecção de falsificações de imagens compostas.

Objetivo Geral

- Realizar um estudo comparativo entre as arquiteturas tradicionais de reconhecimento de padrões para o problema de classificação de imagens falsas.

Objetivos Específicos

- Analisar o desempenho do uso de propriedades de iluminação das imagens;
- Estudar e comparar as arquiteturas estado da arte;

Fundamentação Teórica

Propriedades de Iluminação

- Mapa de Iluminância;
  - grau de incidência da onda;
- Baseados em física e estatística;
- Característica de difícil replicação.

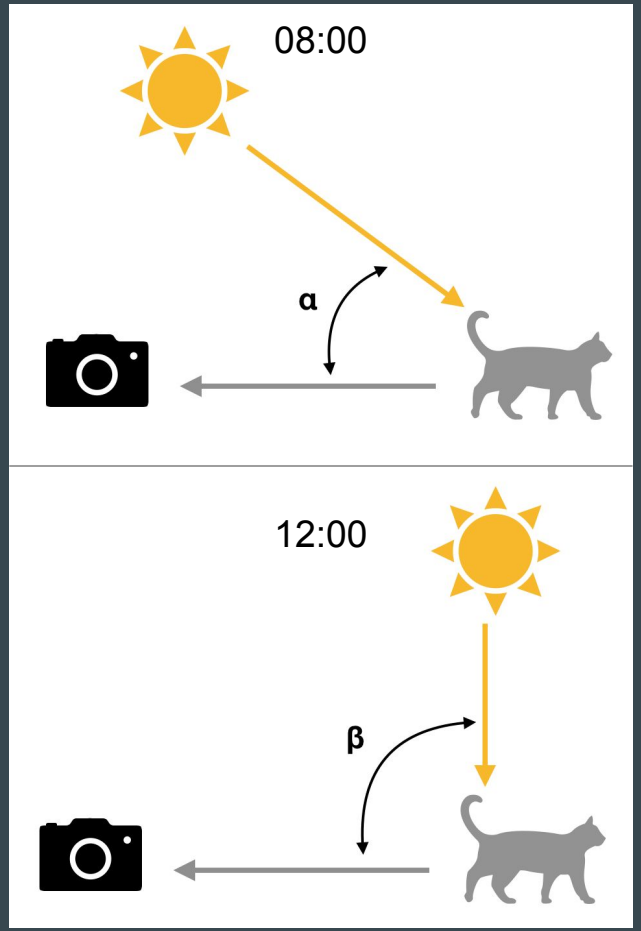

Imagem 3: Exemplo do grau de Incidência.

Exemplo dos Mapas de Iluminância

Imagem 4: Splicing RGB.

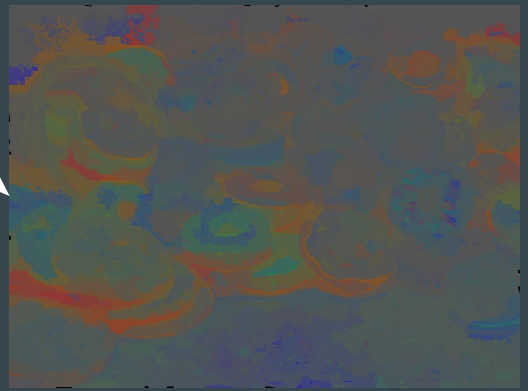

Imagem 5: Splicing GGE.

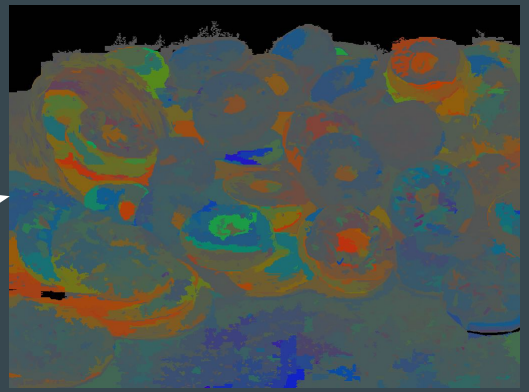

Imagem 6: Splicing IIC.

Redes Neurais

- Conceito de 1940;
- Baseia-se nas sinapses;
- Composta por neurônios e camadas.

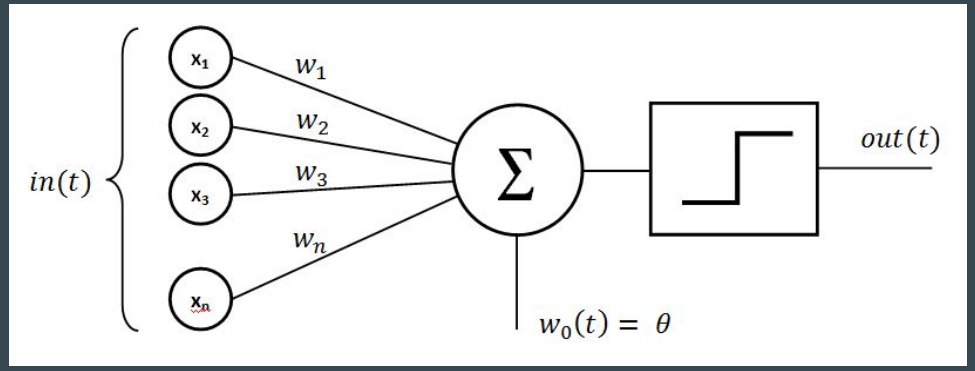

Imagem 7: Modelo de um neurônio..

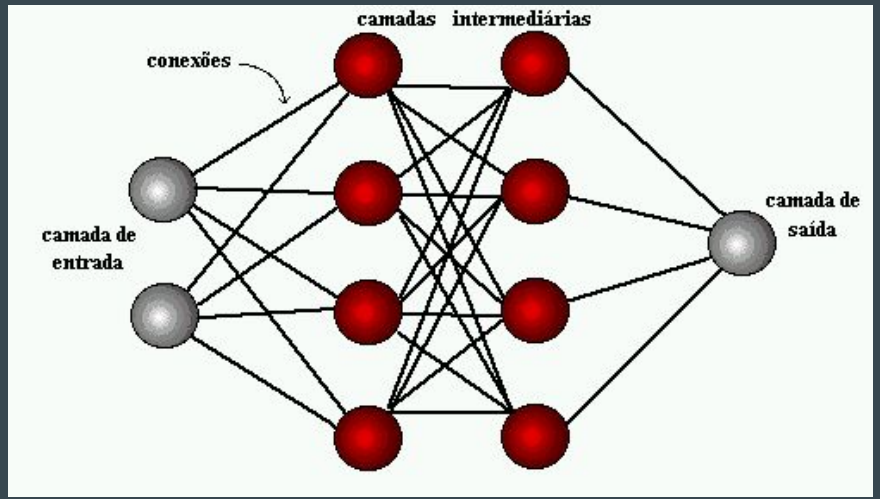

Imagem 8: Exemplo de uma rede.

Redes Neurais Profundas

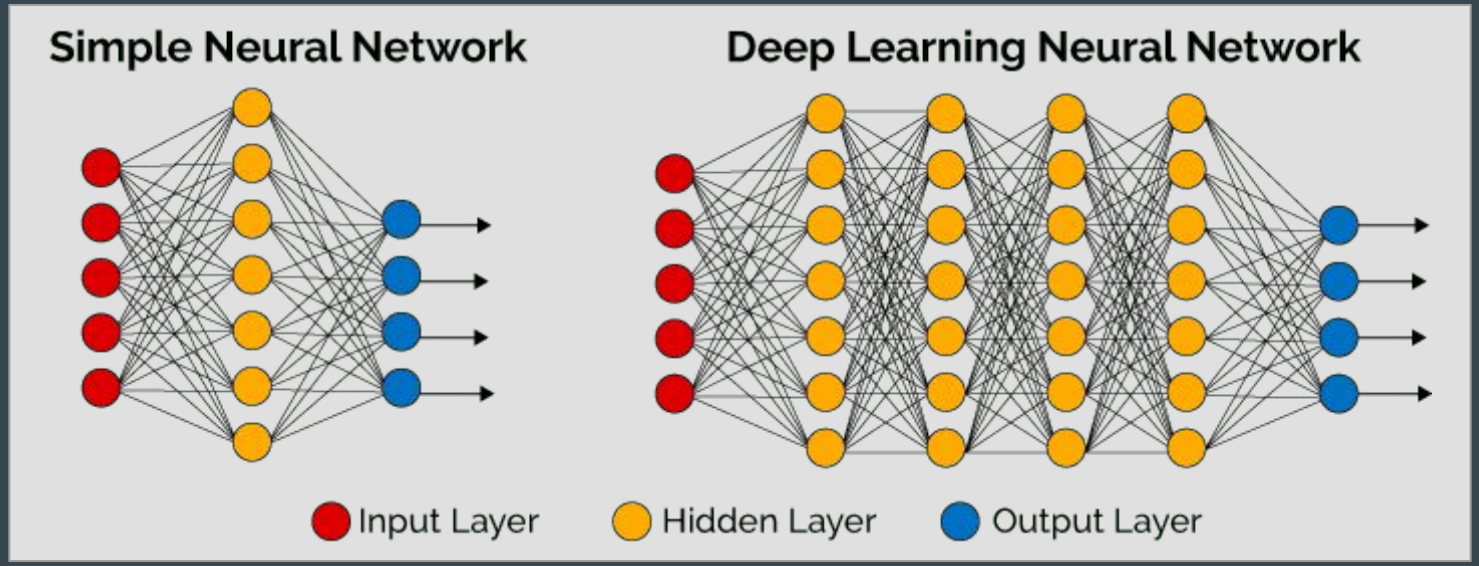

Imagem 9: Diferença entre redes simples e profundas.

Redes Neurais Convolucionais

- Propostas para imagens;
- Adição da camada de convolução:
  - aplicação de filtros;
- Alto poder de reconhecimentos de padrões.

Imagem 10: Exemplo de convolução.[13]

Redes Neurais Convolucionais Profundas

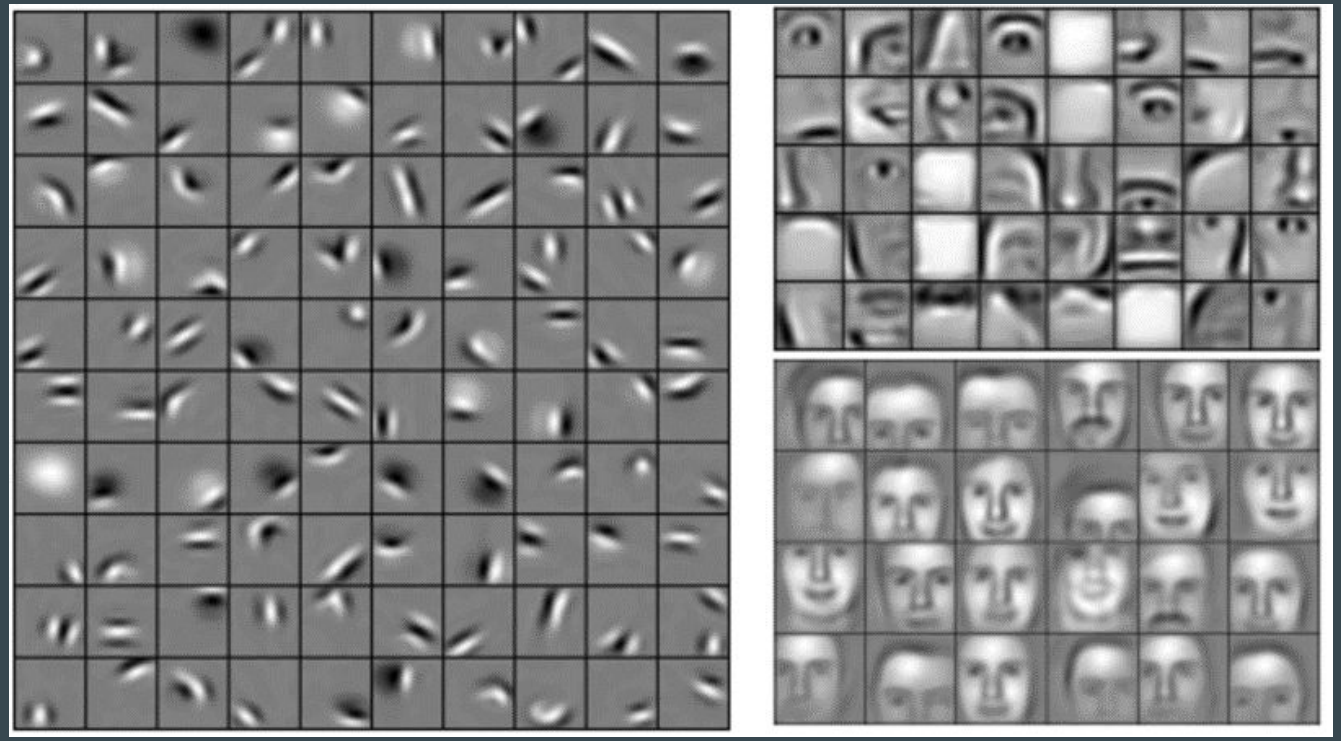

Imagem 11: Exemplos de filtros de características.

Arquiteturas Utilizadas

VGG

- Visual Geometry Group;
- Conceito clássico.

ResNet

- Microsoft Research;
- Conceito de bloco residual.

Inception

- Google;
- Conceito do módulo Inception.

Classificador

- Sem o topo padrão;
- Treinamento supervisionado;
- Máquina de Vetores de Suporte (SVM).

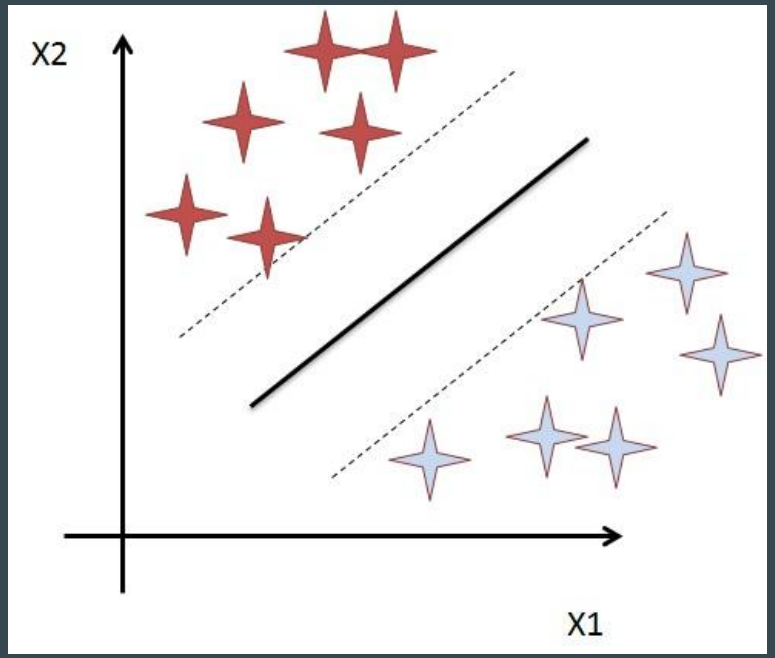

Imagem 12: Exemplo gráfico do SVM.

Análise de Resultado

- **Matriz de confusão;**
- **Confiabilidade da rede;**
- **Acurácia.**

	Splicing	Verdadeira
Splicing	Classificação Correta	Classificação Incorreta
Verdadeira	Classificação Incorreta	Classificação Correta

Imagem 13: Matriz de confusão.

Metodologia

Metodologia

- Dividida em 4 Etapas:
  1. Extração dos Mapas;
  2. Pré-processamento das imagens;
  3. Extração das Características;
  4. Treinamento e Validação do Classificador.

1 - Extração dos Mapas

- Utiliza imagens em seu tamanho original;

2 - Pré-Processamento das Imagens

- Separação de canais RGB;
- Redimensionamento;
- Normalização do valor de cada pixel.

3 - Extração das Características

- Alimentação da rede;
- Aplicação do transfer learning;
- Vetor de características;

4 - Treinamento e Validação do Classificador

- Separação das Amostras em 5 partes;
- Realização do treino e teste;
- Geração dos gráficos de avaliação.

Experimentos e Resultados

Ambiente de Desenvolvimento e Ferramentas

- Ambiente de testes:
  - Intel(R) Xeon(R) E5-2620;
  - 100 GB RAM;
  - 1 GPU Titan X;
  - Python 3.5.
- Principais bibliotecas:
  - Keras 2.0.3;
  - Tensorflow 1.0.1;
  - ScikitLearn 0.19.1;
  - MatPlotLib 3.0.3.

Bases de Dados

- DSO - 200 imagens;
- Columbia - 363 imagens;
- DSI - 50 imagens.

Imagem 14: DSO.

Imagem 15: Columbia.

Imagem 16: DSI.

Quantidade de Testes Realizados

Redes Neurais

1. ResNet50
2. VGG16
3. VGG19
4. InceptionV3
5. InceptionResNetV2

Variações por Base

DSO	Columbia	DSO
A. IIC	A. IIC	A. IIC
B. GGE	B. GGE	B. GGE
C. RGB	C. RGB	C. RGB

Resultados

- DSO:
  - VGG19 = 94%;
- DSI:
  - ResNet50 = 90%;
- Columbia:
  - ResNet50 = 82,3%.

IIC			
Rede	**DSO**	**DSI**	**Columbia**
ResNet50	91%	**90%**	**82,3%**
VGG16	91,5%	86%	77,9%
VGG19	**94%**	84%	78,5%
InceptionV3	87%	84%	63,1%
InceptionResNetV2	93%	86%	51,8%

Imagem 17: Tabela de resultados IIC.

Resultados

- DSO:
  - ResNet50 = 60,5%;
- DSI:
  - ResNet50 = 68%;
- Columbia:
  - ResNet50 = 81,5%.

GGE			
Rede	**DSO**	**DSI**	**Columbia**
ResNet50	**60,5%**	**68%**	**81,5%**
VGG16	59,5%	60%	77,7%
VGG19	59%	62%	81%
InceptionV3	53,5%	60%	73%
InceptionResNetV2	45,5%	44%	60%

Imagem 18: Tabela de resultados GGE.

Resultados

- DSO:
  - InceptionV3 = 63%;
- DSI:
  - VGG19 = 74%;
- Columbia:
  - ResNet50 = 84,6%.

RGB			
Rede	**DSO**	**DSI**	**Columbia**
ResNet50	58,5%	72%	**84,6%**
VGG16	58,5%	72%	82%
VGG19	53,5%	**74%**	82%
InceptionV3	**63%**	42%	63%
InceptionResNetV2	56%	56%	70%

Imagem 19: Tabela de resultados RGB.

Conclusões

CONCLUSÕES

- Relação entre acurácia e quantidade de amostras;
- Eficácia dos mapas de iluminância;
- Acurácia não é o único parâmetro de decisão;
- Desempenho da ResNet.

BIBLIOGRAFIA

1. Por ano, 125 bilhões de imagens são compartilhadas na rede. - https://oglobo.globo.com/economia/por-ano-125-bilhoes-de-imagens-sao-compartilhadas-na-rede-8301345
2. É #FAKE imagem em que Manuela D'Ávila aparece com camiseta 'Jesus é travesti' - https://extra.globo.com/fato-ou-fake/e-fake-imagem-em-que-manuela-davila-aparece-com-camiseta-jesus-travesti-23119933.html
3. Luminância vs. Iluminância - http://sensing.konicaminolta.com.br/2015/09/luminancia-vs-iluminancia/
4. Redes Neurais - HAYKIN, Simon. Redes neurais: princípios e prática . [S.l.]: Bookman Editora, 2007. 61 p.
5. O Que São Redes Neurais Artificiais Profundas ou Deep Learning? - http://deeplearningbook.com.br/o-que-sao-redes-neurais-artificiais-profundas/
6. Máquina de Vetores de Suporte- JAKKULA, Vikramaditya. Tutorial on support vector machine (svm). School of EECS, Washington State University, v. 37, 2006.

Obrigado a todos.

VGG

- Visual Geometry Group;
- Conceito padrão;

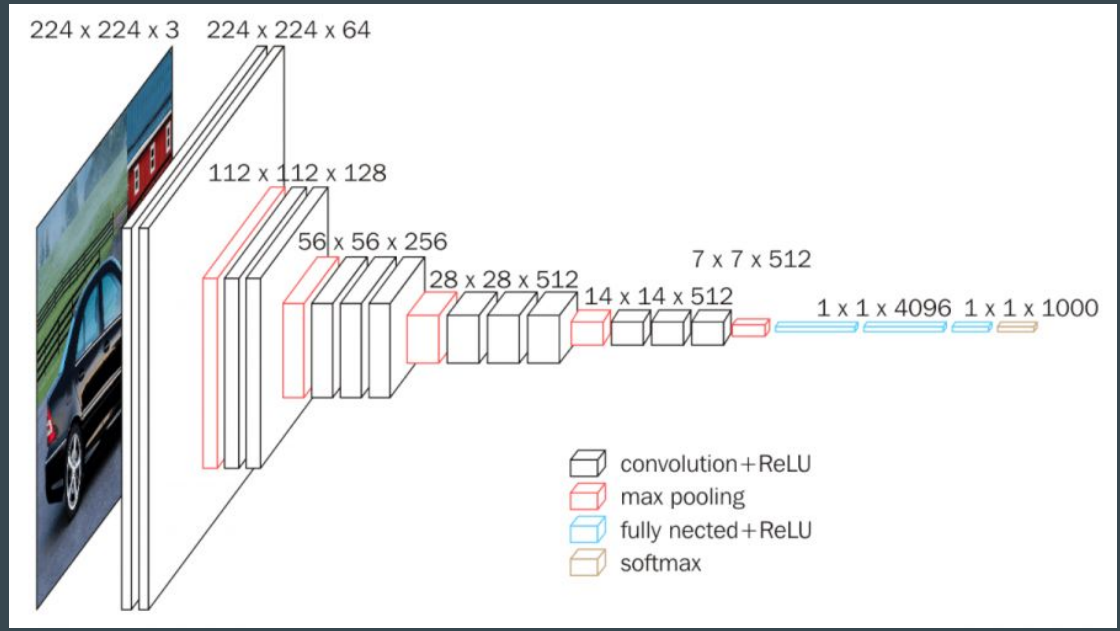

Imagem 10: Diagrama da VGG16.

ResNet

- Microsoft Research;
- Introdução do conceito residual;

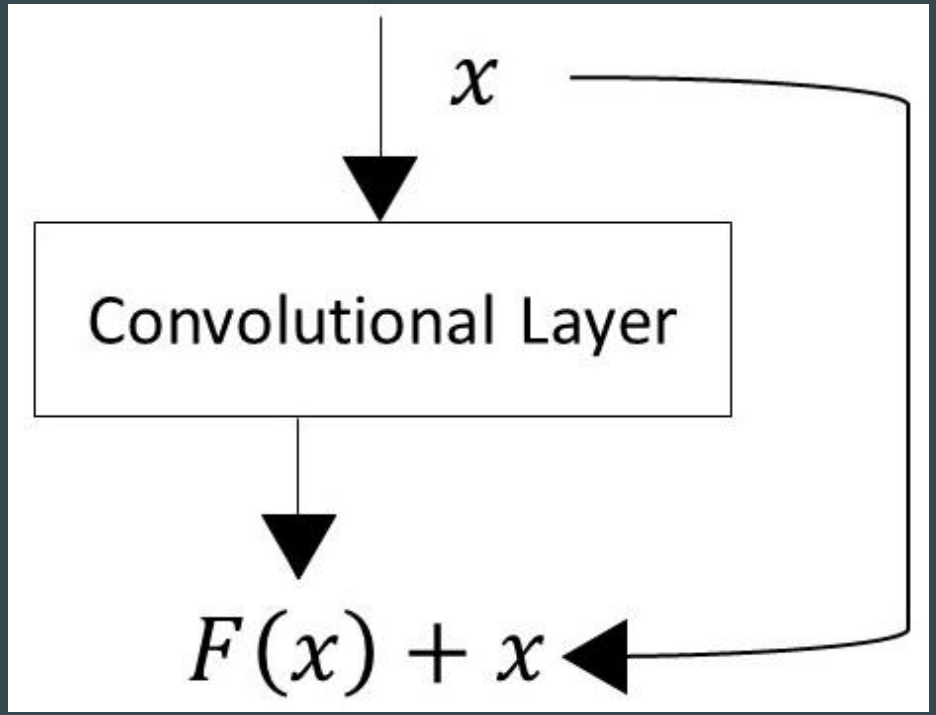

Imagem 11: Bloco de convolução.

Inception

- Google;
- Módulo Inception;

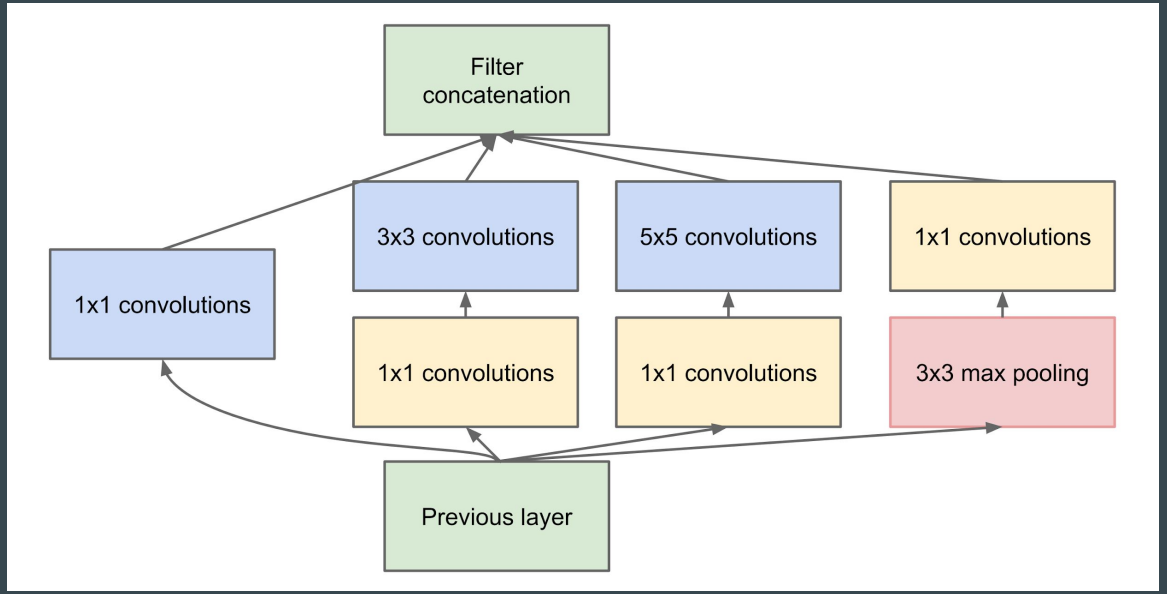

Imagem 12: Módulo Inception.