

# IA para detecção de morphs faciais

Tasso Eliézer Daflon C. Canellas  
R. A.: 169247

# Introduzindo o problema

- Definição: Ataques que criam imagens híbridas combinando características de diferentes faces para enganar sistemas biométricos.
- Risco: Pode permitir que invasores se passem por outras pessoas e injetem morphs no banco de dados de referência.



# Introduzindo o problema

- Impacto: Problema crítico em segurança de fronteiras e controle de acesso. Por exemplo: Aeroportos
- Desafio: Falta de ferramentas abertas para detectar morphs eficazmente.
- Solução: Desenvolver modelos de classificação robustos, atualizados continuamente para enfrentar novas técnicas de morphing.



# Trabalhos anteriores

---

**“Are GAN-based Morphs  
Threatening Face Recognition?”**

Explora a ameaça que morphs representam para os sistemas biométricos

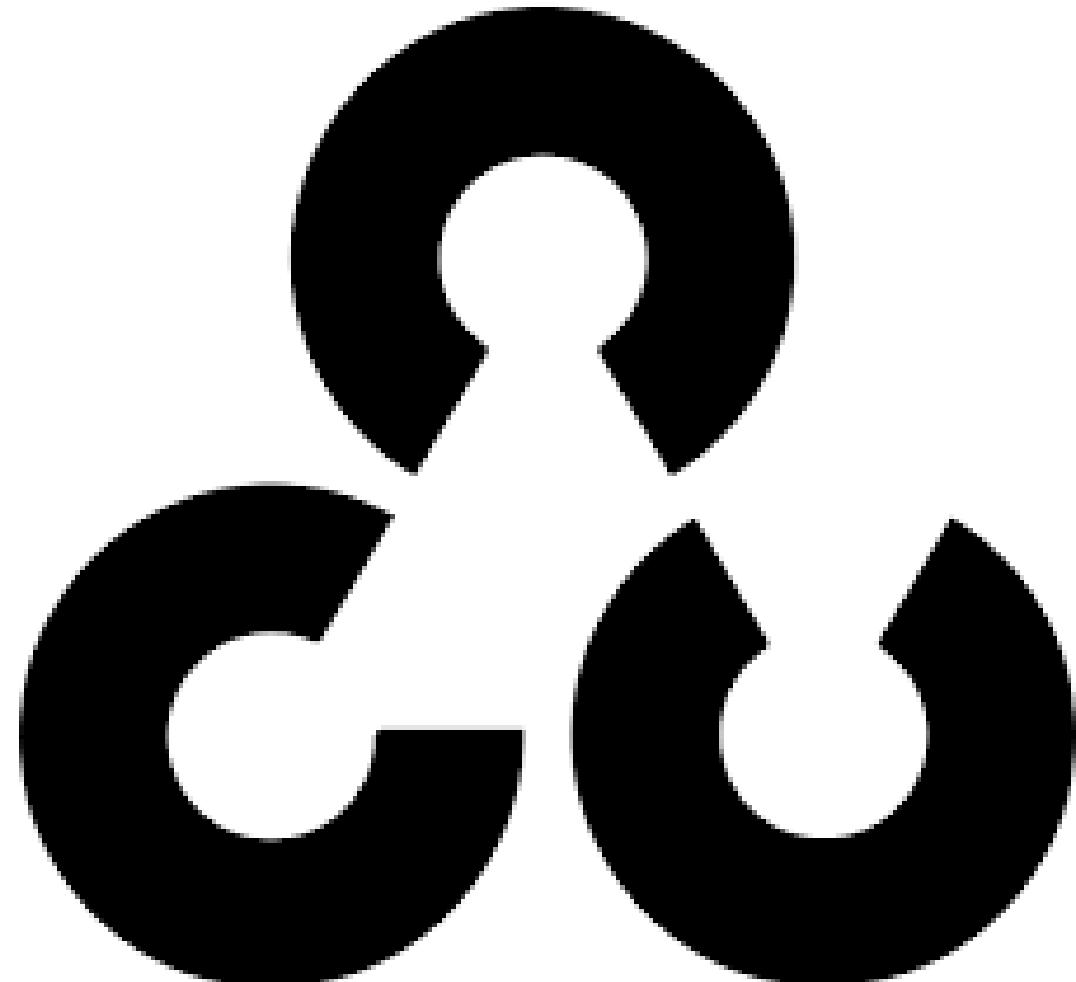
# Objetivos

Estudar, desenvolver e discutir, com base em trabalhos anteriores da literatura, a possibilidade de classificar morphing attacks utilizando os conhecimentos obtidos na disciplina de IA e nas pesquisas para o projeto.



# Bibliotecas

- OpenCV
- Bob
- Imutils
- PyTorch
- TensorFlow
- Matplotlib
- Conda



# Conceitos fundamentais

---

- **GANs**

Competição: Gerador  
x Discriminador

- **Espaço Latente**

Uma representação  
compacta e significativa de  
dados complexo.

- **Interpolação**

Geração de dados que  
ficam entre dois pontos  
no espaço latente.

$$z = (1-a) \cdot z_1 + a \cdot z_2$$



# Metodologia Experimental



# Base de Dados

Face Research Lab London Set



Chicago Face Database



- 102 Indivíduos de diferentes etnias
- Expressões neutras ou sorrindo
- 1350x1350

- 827 Indivíduos de diferentes etnias
- Expressões faciais variadas
- 2444x1718

# Pré-Processamento

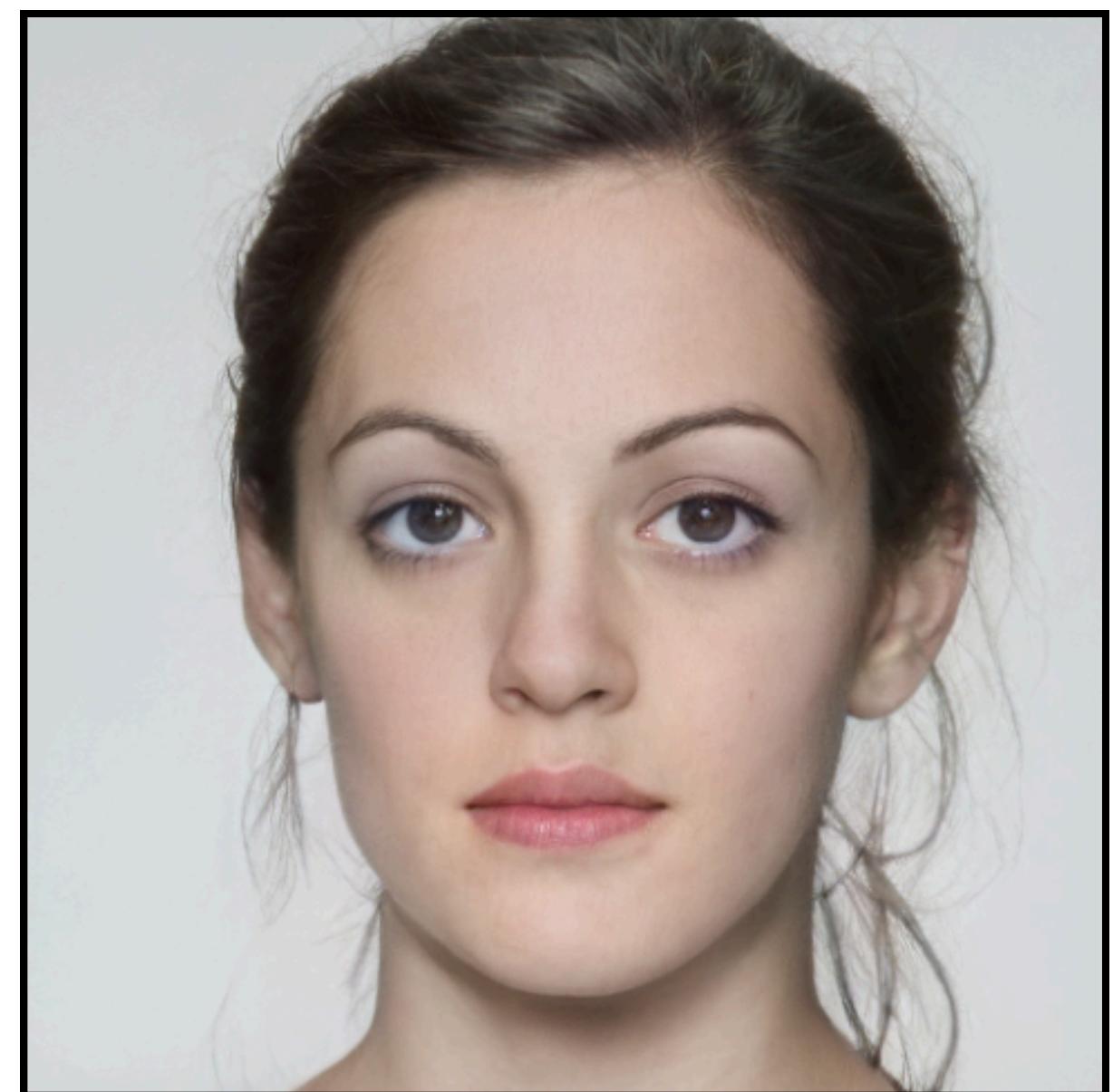
---

## 1. Morphing faces

Arquiteturas:

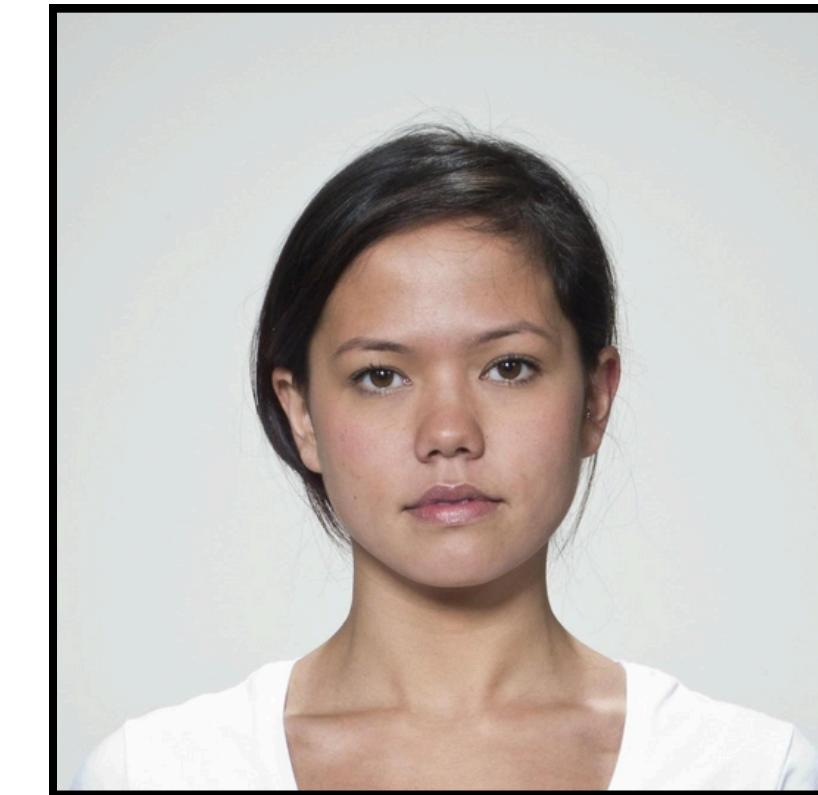
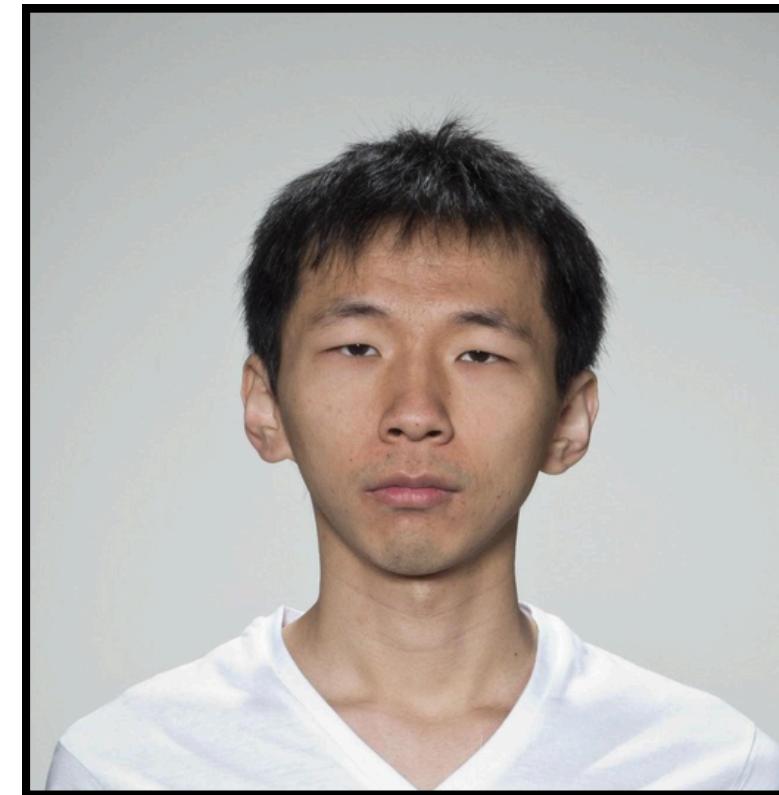
- Morph w/ OpenCV
- Facemorpher
- StyleGAN2
- MipGAN2

Alphas: 0.3, 0.5, 0.7



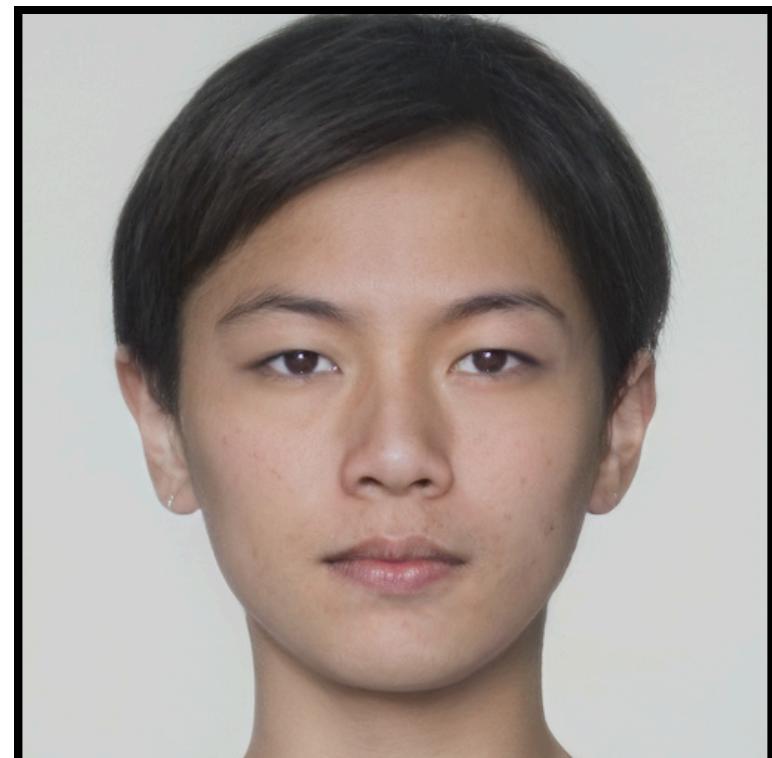


Indivíduo 5



Indivíduo 30

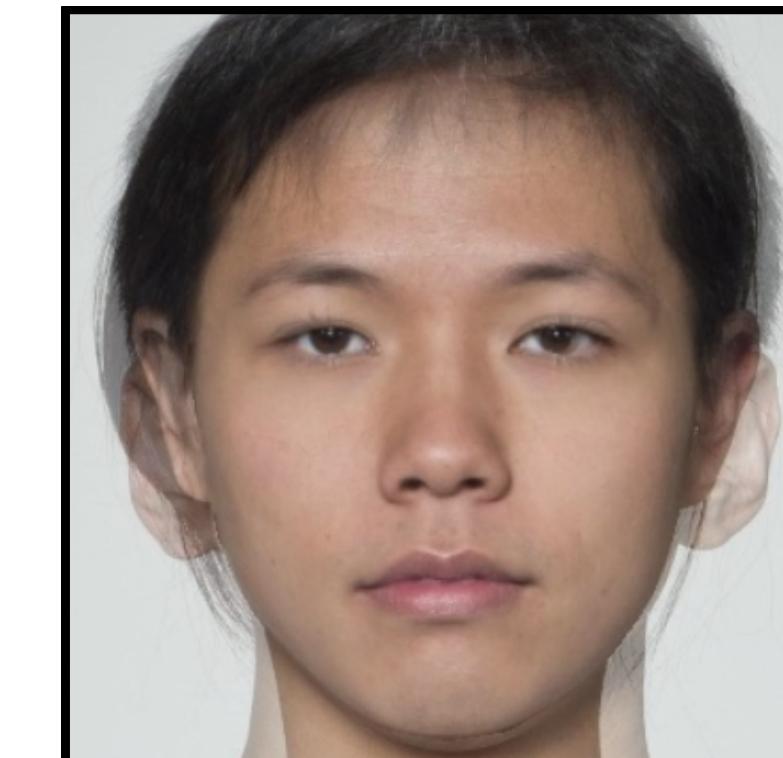
StyleGAN2



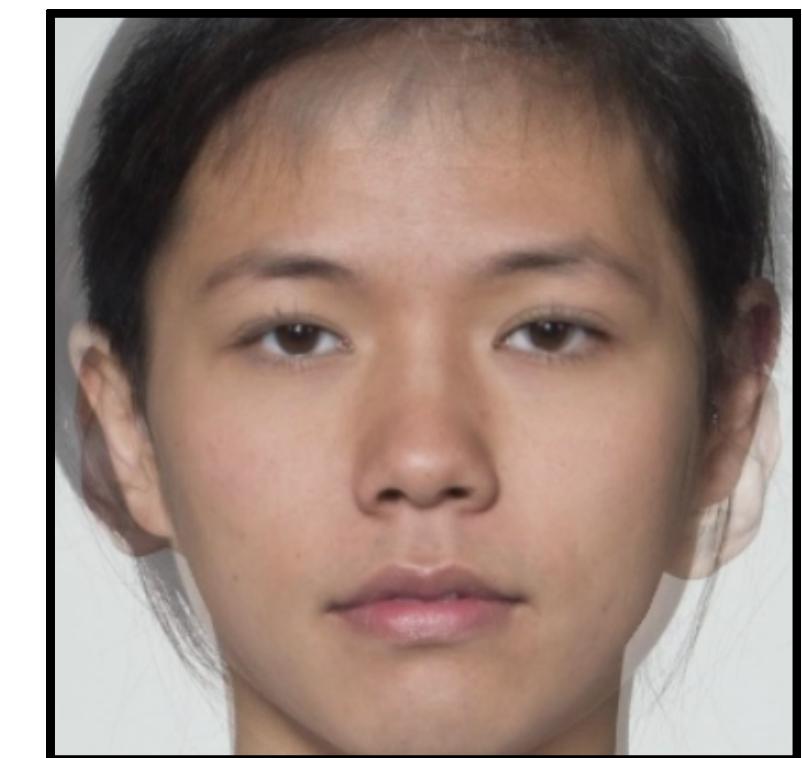
MipGAN2



OpenCV



Facemorpher



alpha = 0.5

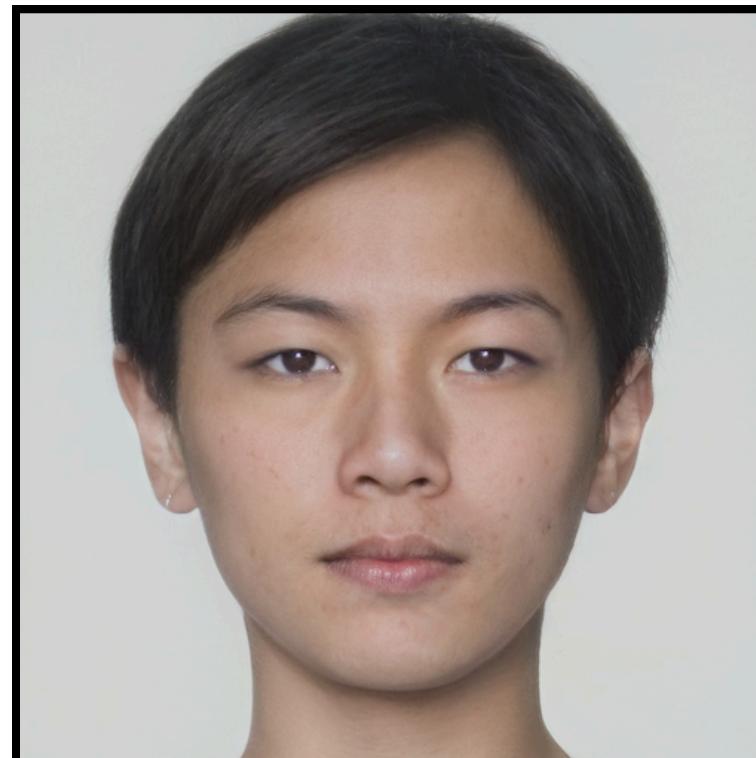
# Pré-Processamento

---

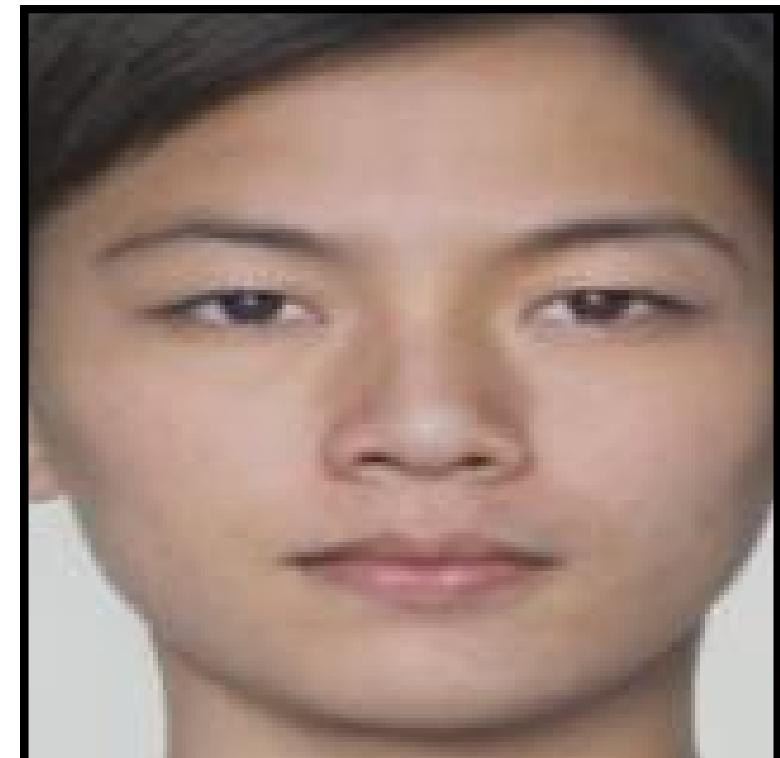
## 2. Redimensionamento e centralização no rosto

### Arquitetura

MTCNN: Multi-task Cascaded Convolutional Networks, é uma rede neural desenvolvida para a detecção de rostos em imagens.



Morph com StyleGAN2

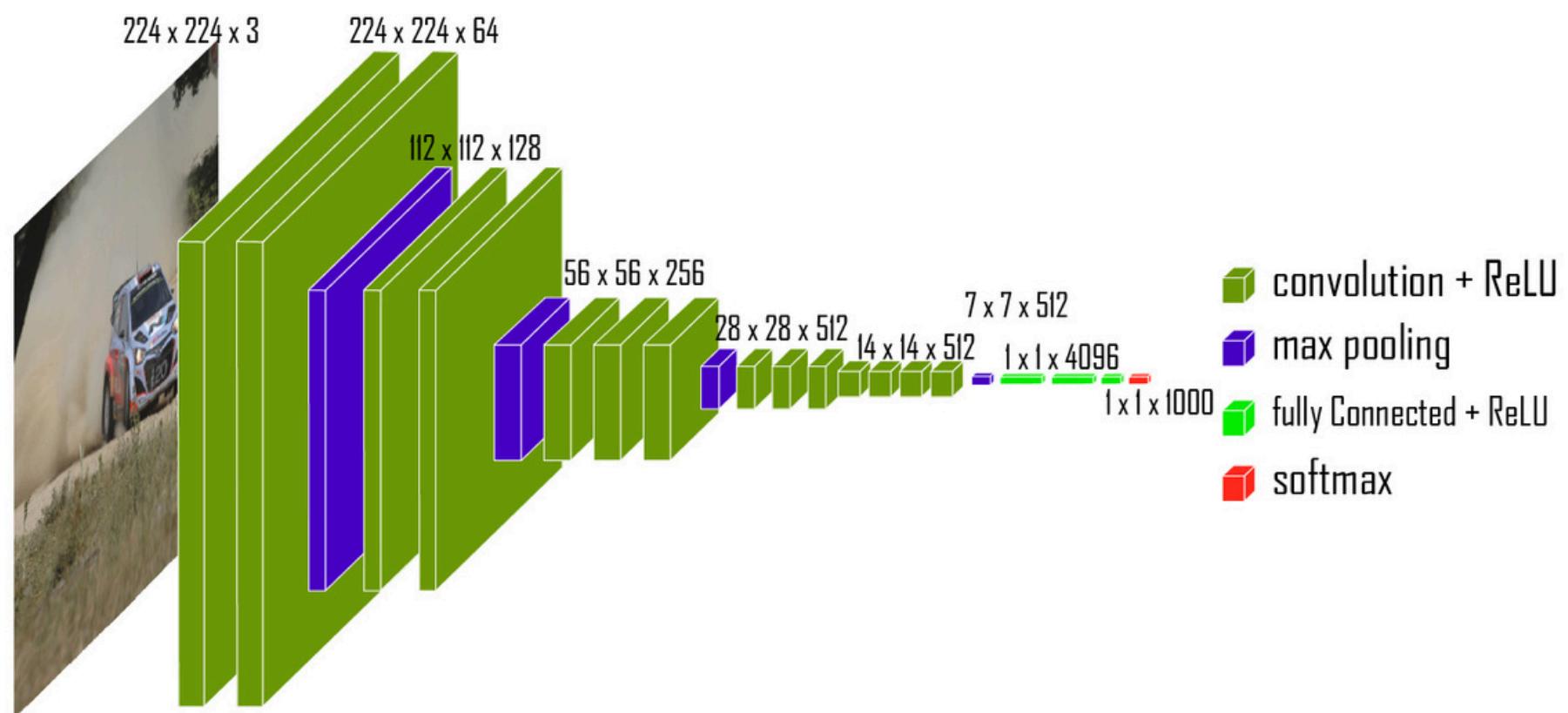


Centralizado na face e  
redimensionado

# Arquitetura

## VGG16

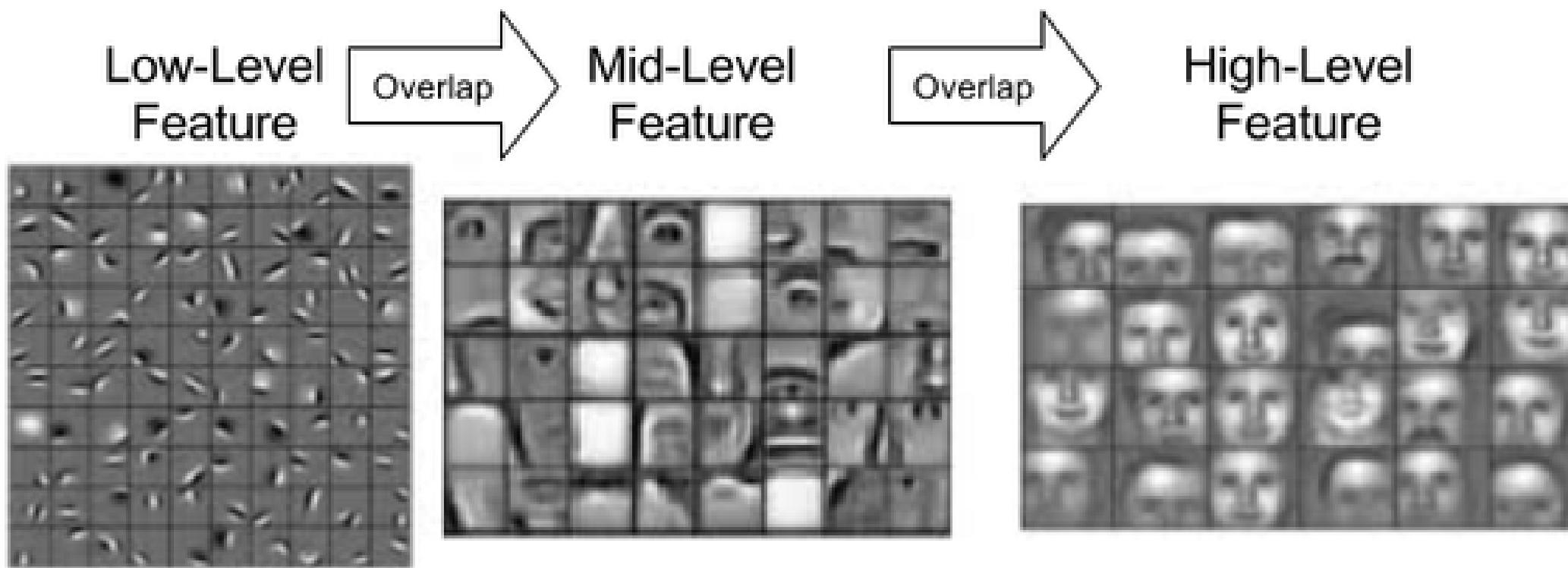
A arquitetura VGG16 é conhecida por sua simplicidade e eficácia em tarefas de reconhecimento de imagens, utilizando 16 camadas de convolução com filtros de 3x3 e camadas de pooling máximo de 2x2.



# Transfer Learning

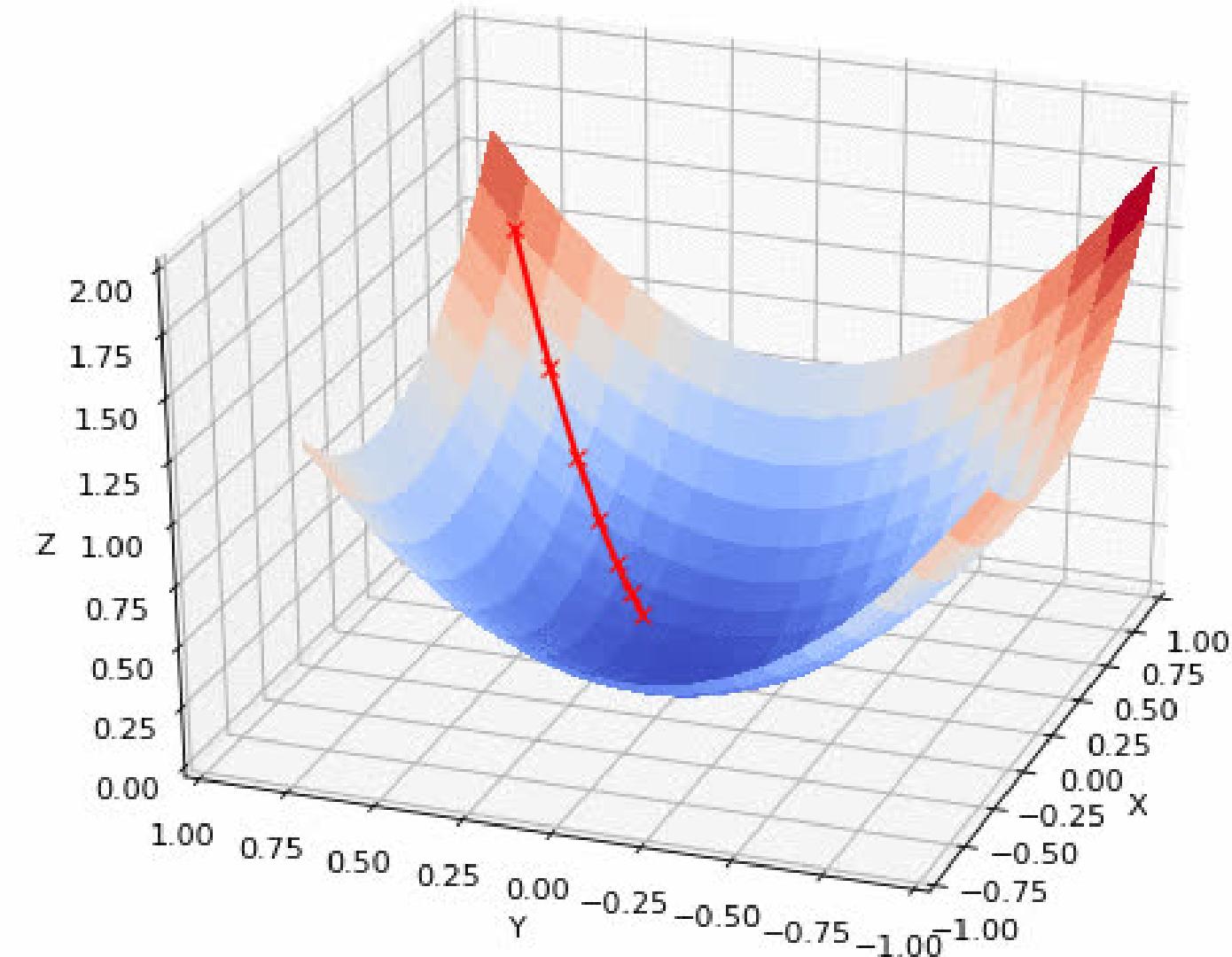
Fine Tuning para o treinamento da rede com os novos dados. A rede foi mantida congelada, com exceções das camadas Fully Connected e as últimas três camadas convolutivas

## Por que as últimas três?



# Validação

- SGD (Descida Estocástica pelo Gradiente): Learning rate =  $1e-4$
- Cross-Entropy
- 200 Épocas
- Checkpoint
- Acurácia, FNR, FPR
- Cross-Validation (5-Fold)



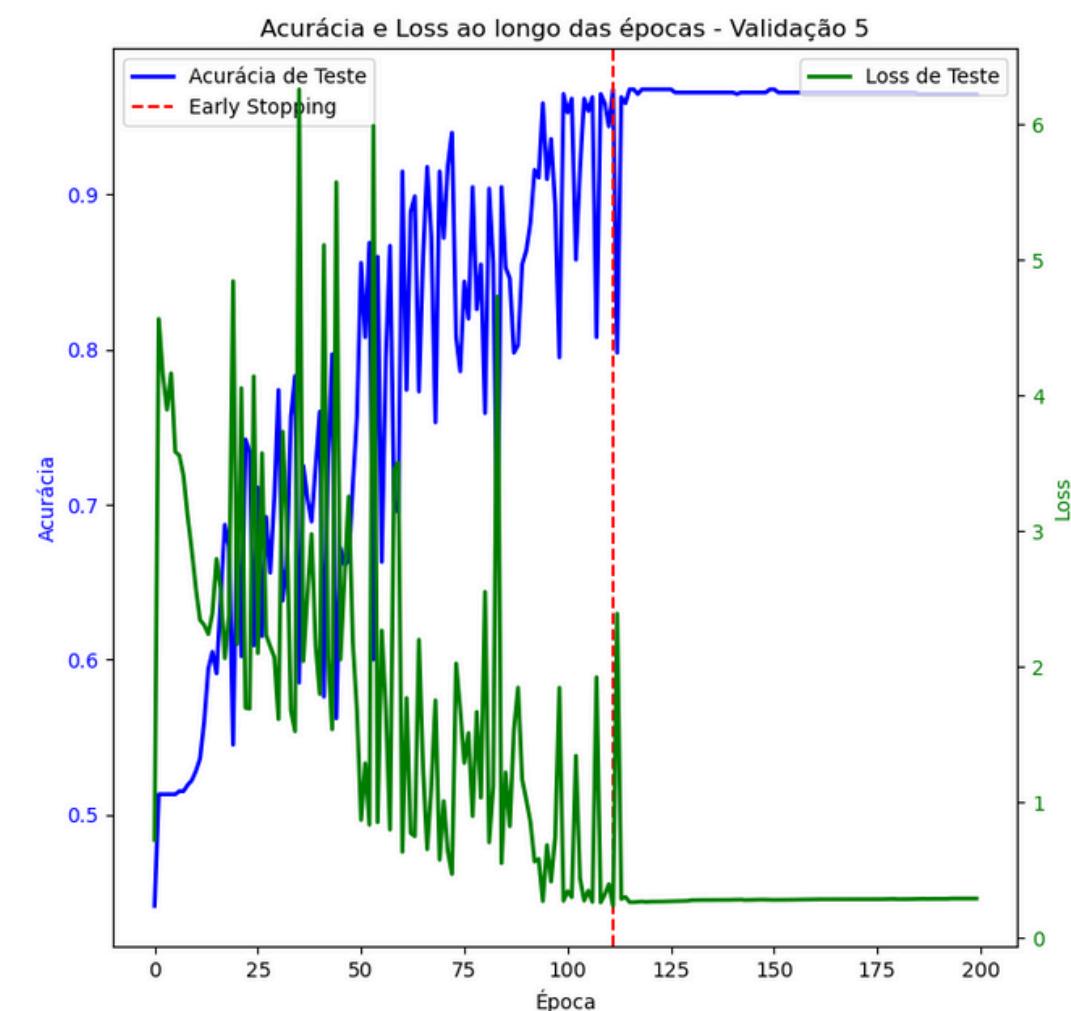
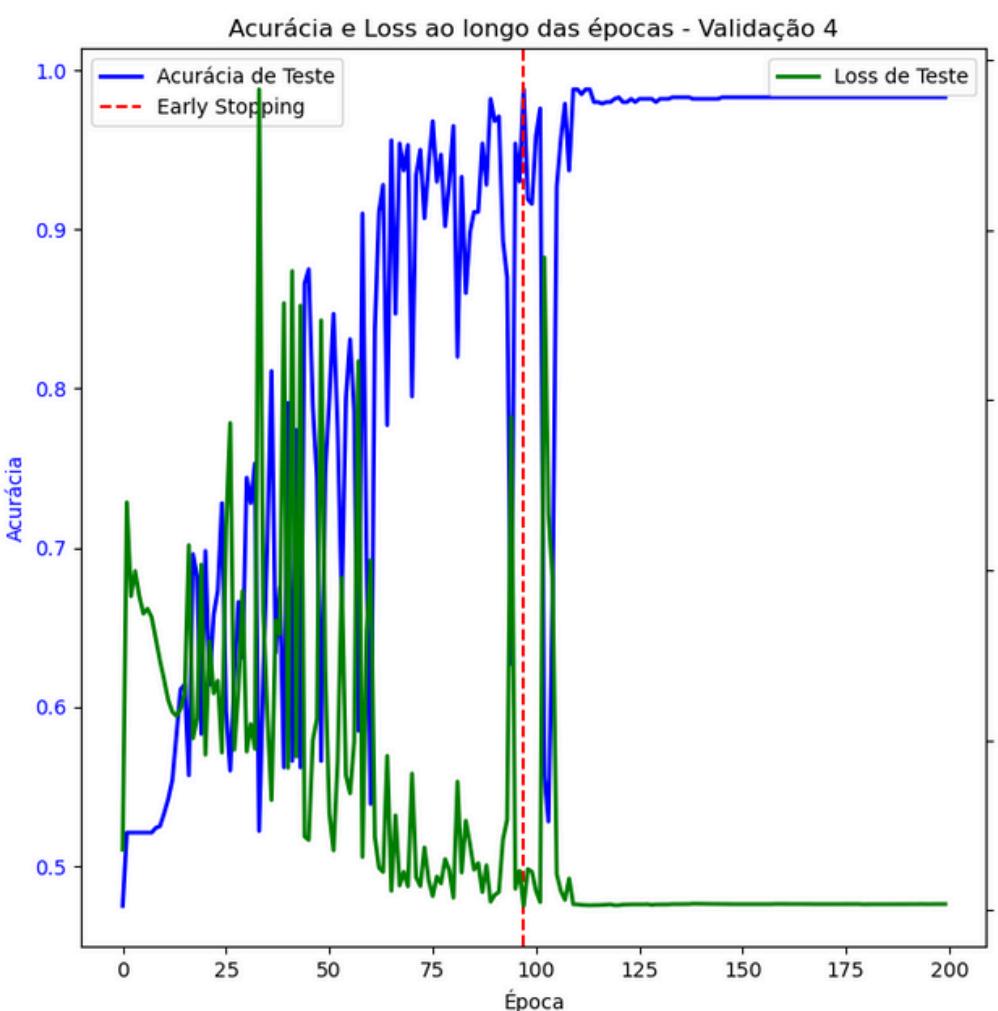
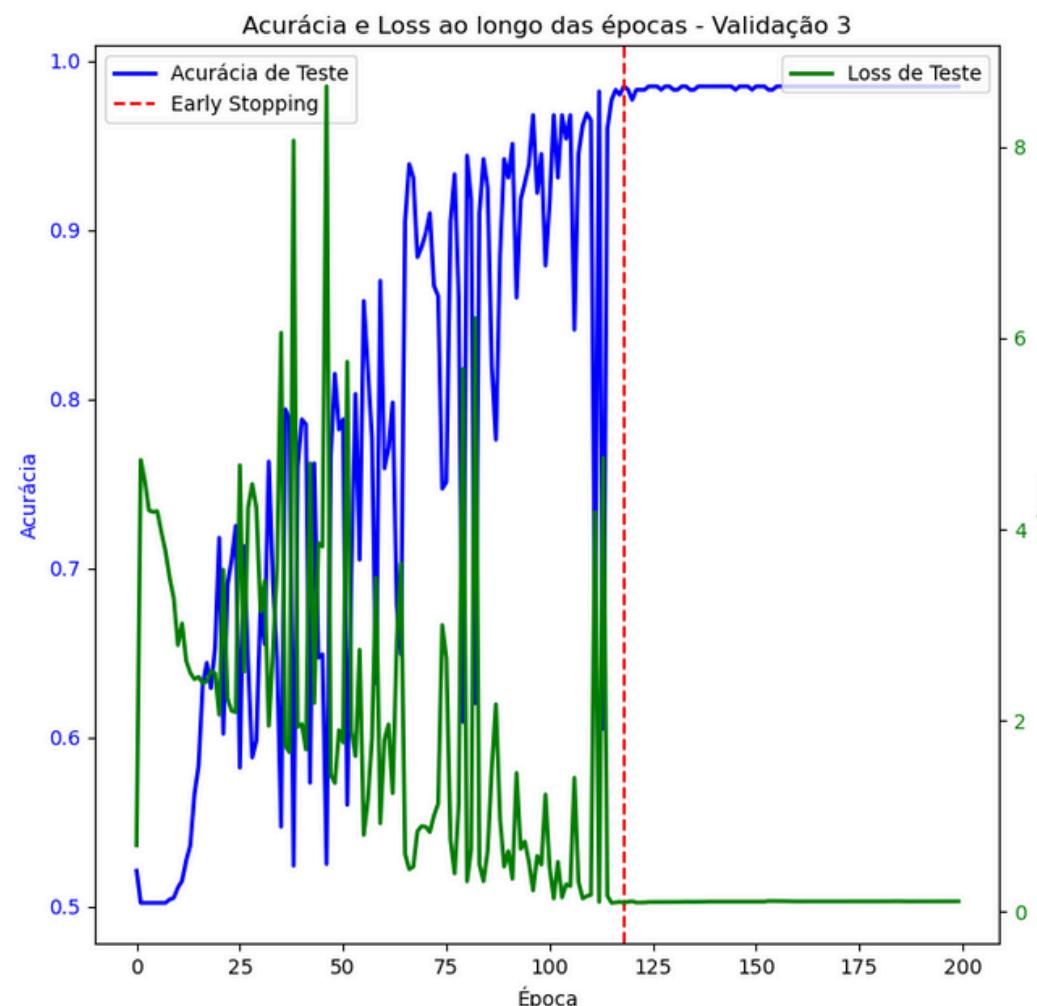
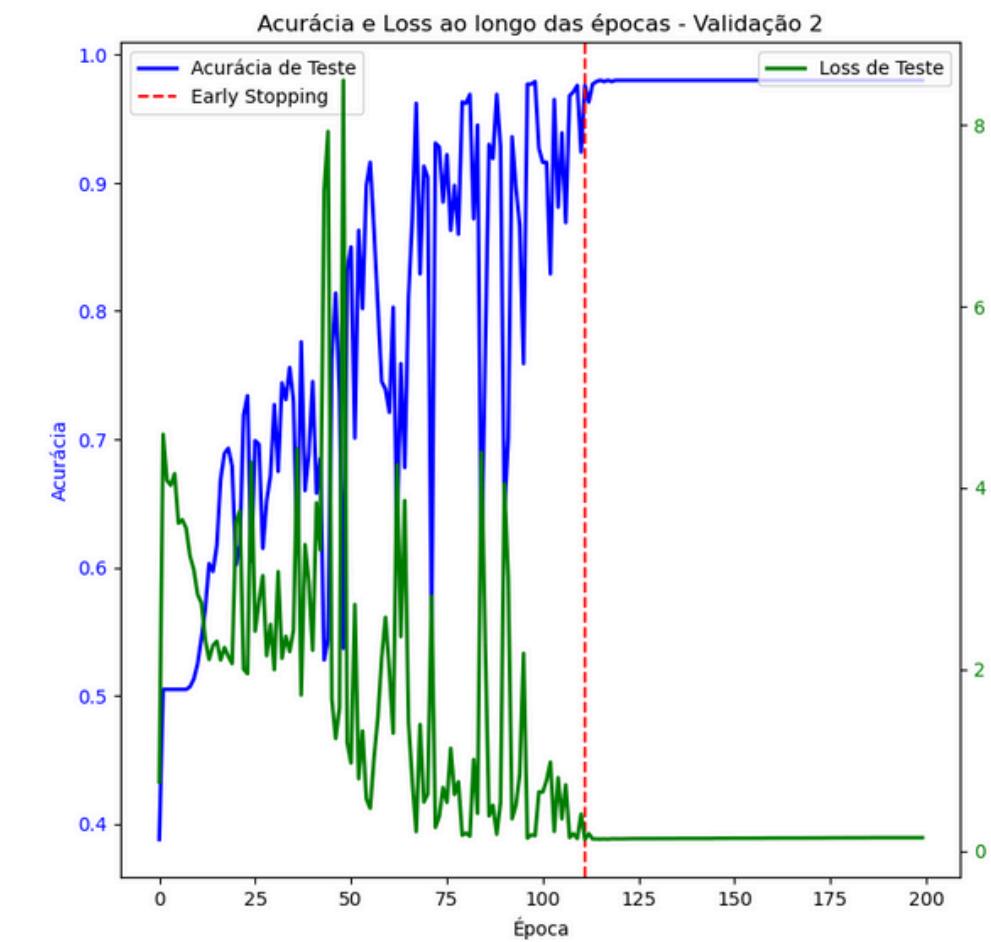
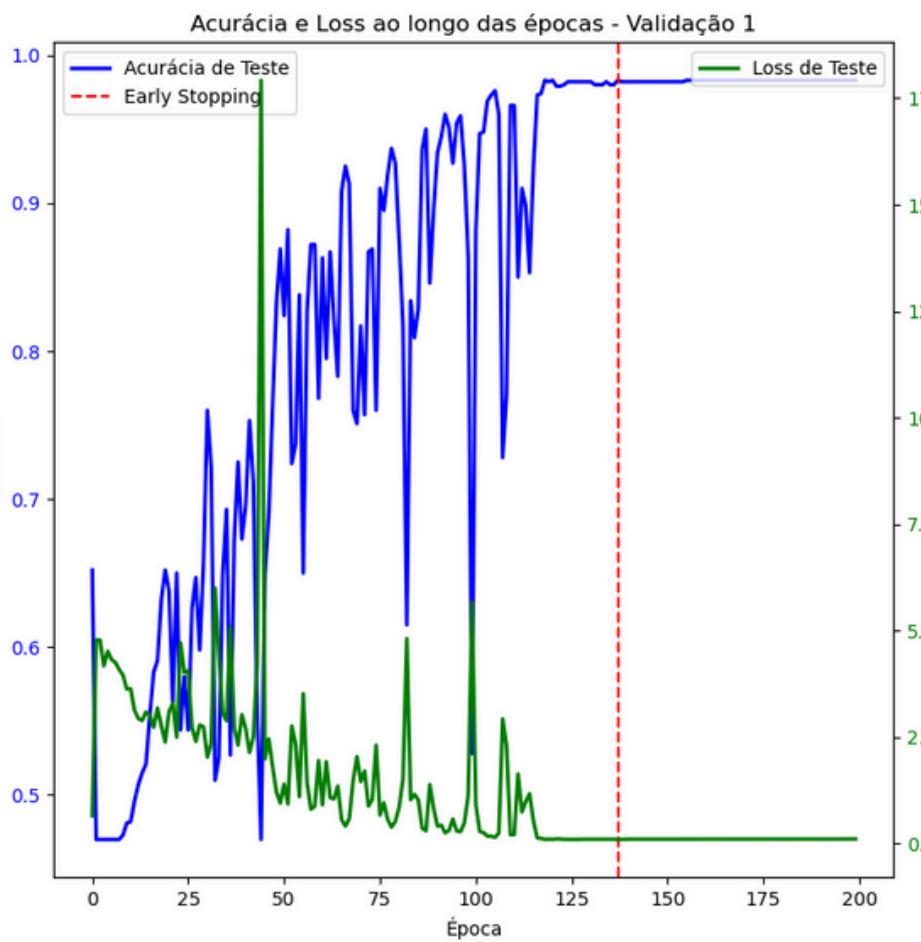
---

# **Resultados e discussões**



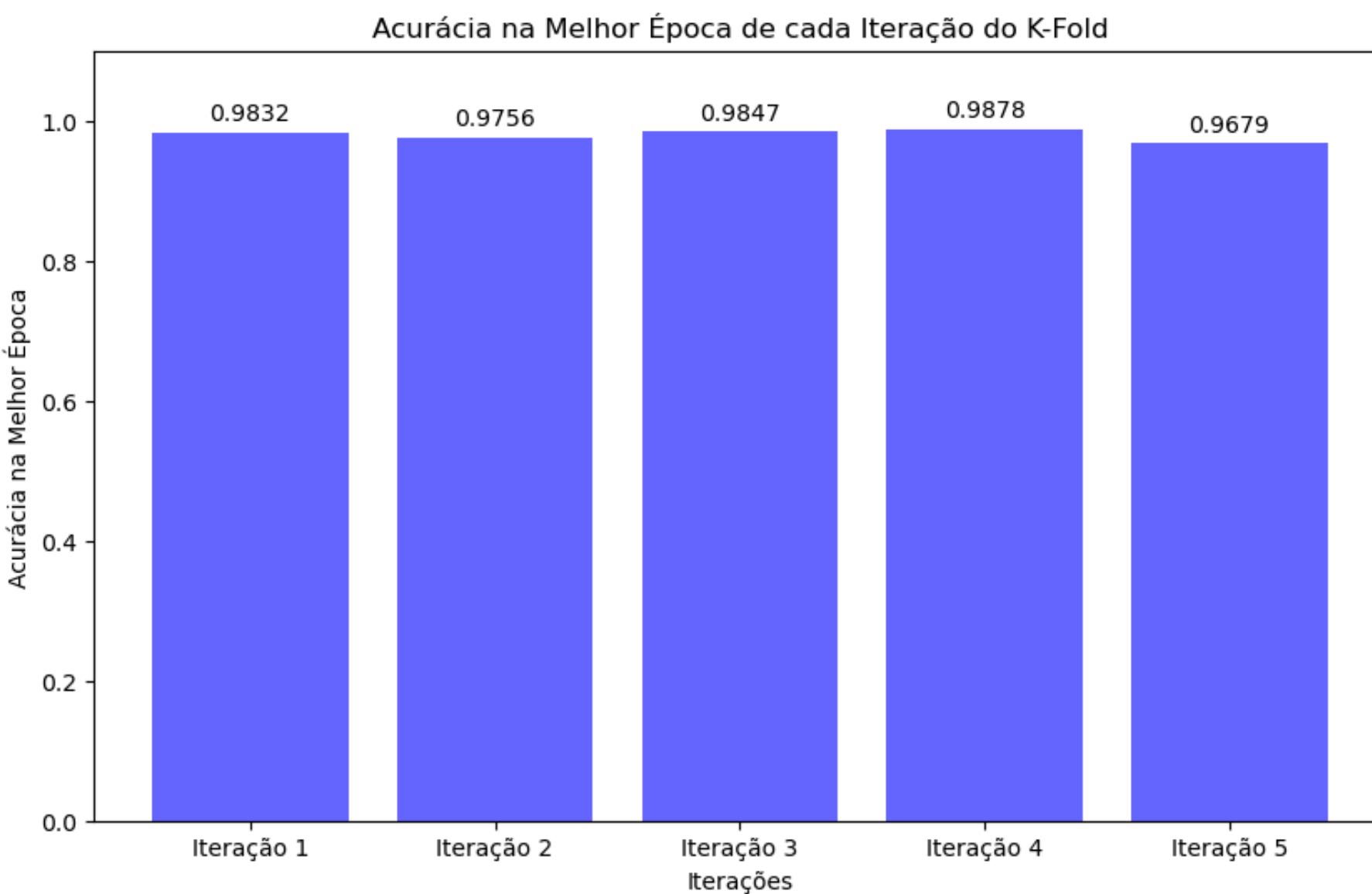
# Checkpoint

- Validação 1: Época 137
- Validação 2: Época 111
- Validação 3: Época 118
- Validação 4: Época 97
- Validação 5: Época 111



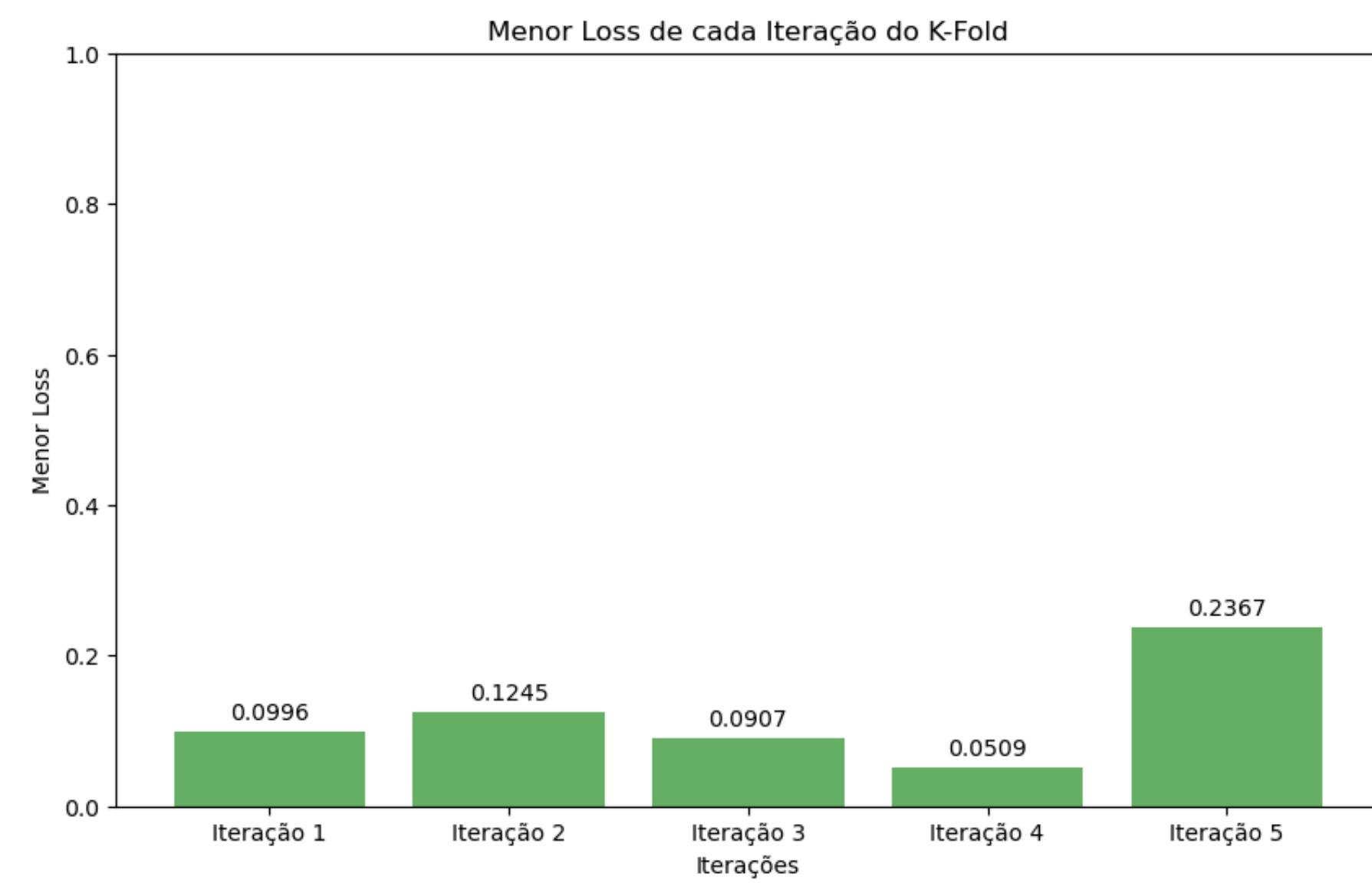
# Acurácia na melhor época

- Validação 1: 98,32%
- Validação 2: 97,56%
- Validação 3: 98,47%
- Validação 4: 98,78%
- Validação 5: 96,79%



# Melhor Loss

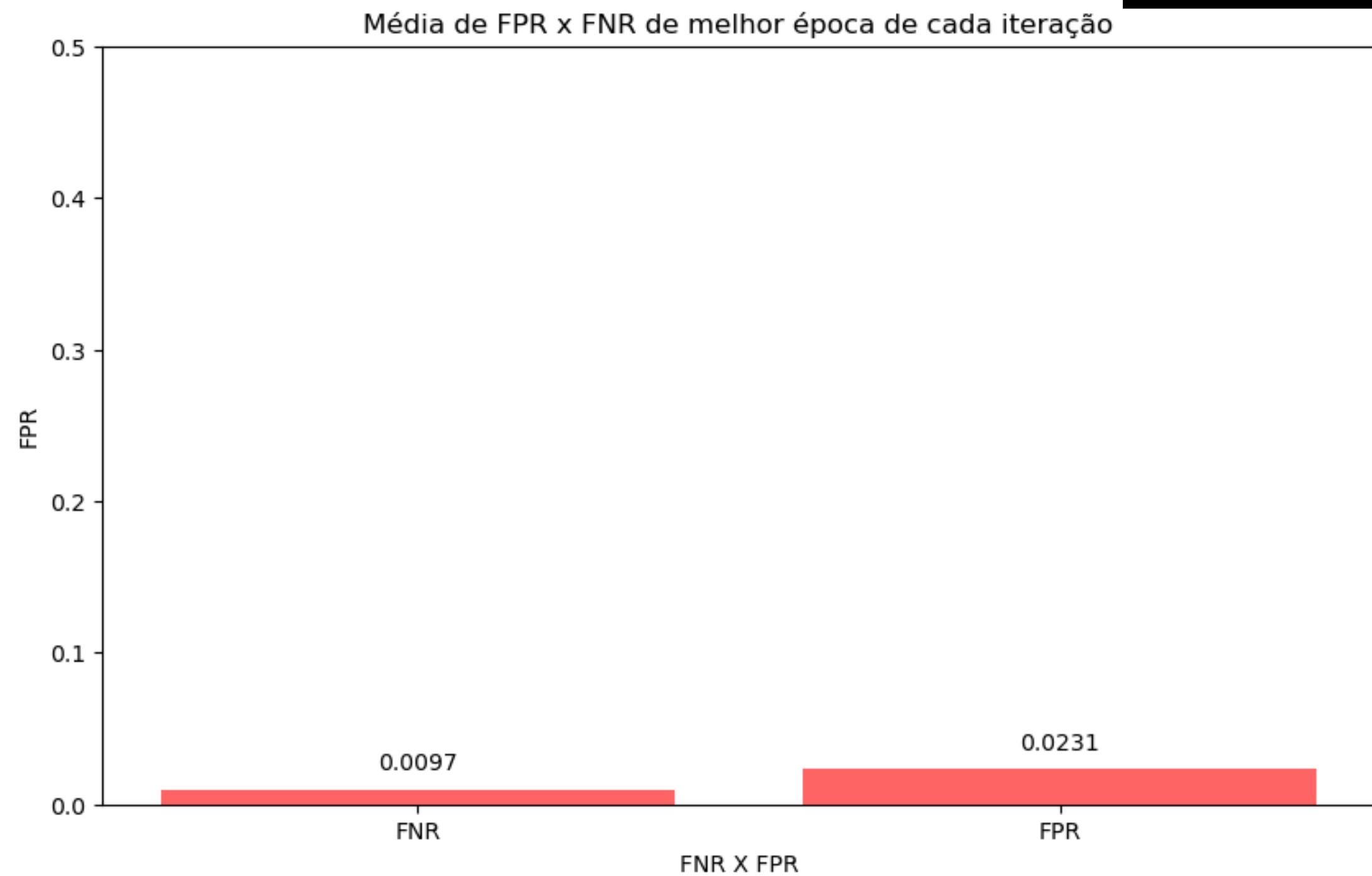
- Validação 1: 0.0996
- Validação 2: 0.12450
- Validação 3: 0.0907
- Validação 4: 0.0509
- Validação 5: 0.23670



# FPR x FNR

Média de melhores FPR:  
2,3%

Média de melhores FNR:  
0,97%



# Comparações

Table Resultados	Arquitetura		
	<i>ResNet 18</i>	<i>Inception V3</i>	<i>VGG16</i>
<i>Média das melhores acurárias</i>	61,8%	65,04%	97,98%
<i>Média das melhores Loss</i>	1,107	1,334	0,120
<i>Melhor FPR</i>	25,6%	6,68%	2,31%
<i>Melhor FNR</i>	16,5%	27,8%	0,97%

# Conclusões

Este estudo demonstrou que o modelo de rede neural foi altamente eficaz na classificação de morphs, alcançando alta precisão. Os resultados confirmam a viabilidade da abordagem e estabelecem uma base sólida para futuras pesquisas. Embora encorajadores, estes resultados representam um primeiro passo, com trabalhos futuros focados em aprimorar a complexidade dos morphs e refinar o modelo, visando enfrentar desafios mais complexos e explorar todo o seu potencial.

—  
Muito  
Obrigado!