Facial Recognition Model for Face Unlock

Author: Dallin Moore
Project: Project 2 - DATA 5610

Overview

I implemented a facial recognition system using a standard camera that distinguishes between "me" from "not_me" images. The model must generalize to unseen data, balancing security (low false positives) and usability (high true positives), despite an imbalanced dataset where "not_me" images vastly outnumber "me" images.

Approach

I built a binary classification model using TensorFlow and VGG16 (pretrained on ImageNet), with custom layers for my task. The pipeline included:

1. Data Preparation:

- **"me" Images**: 55 images of me, taken on my computer from different angles and with different lighting.
- **"not_me" Images**: 1,000 images from the LFW dataset.
- **Training/Validation**: Split 80% training (844) and 20% validation (211), shuffled and batched (32).
- **Test Set**: 22 new "me" images and 100 unseen LFW "not_me" images (total 122), ensuring no overlap with training/validation.
- **Augmentation**: Images resized to 250x250x3, normalized to [0, 1], labeled "me" (1) or "not_me" (0).

2. Model Architecture:

- Compiled with Adam optimizer, binary cross-entropy loss, and accuracy metric.

Layer (type)	Output Shape	Param #	Activation
input_layer_6 (InputLayer)	(None, 250, 250, 3)	0	
vgg16 (Functional)	(None, 7, 7, 512)	14,714,688	
flatten_4 (Flatten)	(None, 25088)	0	
dense_8 (Dense)	(None, 512)	12,845,568	ReLU
dropout_4 (Dropout)	(None, 512)	0	
dense_9 (Dense)	(None, 1)	513	Sigmoid

3. Training:

- 10 epochs with callbacks: EarlyStopping (patience=3), ReduceLROnPlateau (factor=0.5), and ModelCheckpoint (best `val_accuracy`).
- Validation accuracy hit 100% on epoch 1, prompting investigation (see Results).
- Model accuracy hit 100% for the third time on epoch 5 and the training stopped early.

4. Evaluation:

- Test set metrics computed using sklearn: precision, recall, F1-score, specificity, ROC-AUC, PR-AUC, and confusion matrix.
- Output misclassification images to diagnose errors.

5. Real-Time Testing:

- Webcam interface for live predictions, capturing and classifying images on-the-fly.

Results

- **Test Set Performance** (122 samples: 22 "me", 100 "not_me"):
  - **Precision**: 1.0000 (19/19 "me" predictions correct)
  - **Recall**: 0.8636 (19/22 "me" detected, 3 missed)
  - **F1-Score**: 0.9268 (balanced precision/recall)
  - **Specificity**: 1.0000
  - **ROC-AUC**: 1.0000
  - **PR-AUC**: 1.0000
  - **Confusion Matrix**: TN=100, FP=0, FN=3, TP=19
- **Validation Anomaly**: 100% accuracy on epoch 1 suggests potential overfitting or data leakage (e.g., overlap or trivial feature exploitation). Training accuracy improved gradually, but test results validate generalization.
- **Misclassifications**: 3 false negatives ("me" predicted as "not_me"), no false positives, shown via visualization of all test set errors.

Interpretation

- **Security**: Precision and specificity of 1.0 ensure no false positives, critical for face unlock—no unauthorized access.
- **Usability**: Recall of 0.8636 means 86.36% of "me" images are recognized, with 3 misses of the 22 in the test set (acceptable but improvable).
- **Overall**: F1-score of 0.9268 and perfect AUC scores indicate strong performance, beating the baseline of 0.833 (always guessing "not_me").
- **Validation Concern**: 100% epoch 1 accuracy likely due to imbalance (94.8% "not_me" in validation) or overfitting to a simple pattern (e.g., background). Test set results (97.5% accuracy) confirm robustness despite this.

Conclusion

The model achieves near-perfect security (no false positives) and strong usability (86% recall), suitable for face unlock with minor tweaks. The validation anomaly underscores the importance of robust data handling, but test set results confirm the pipeline's success for this assignment. Future iterations can enhance recall and scalability.

The misclassified images in the test set reveal that lighting and face angle have the most significant impact on performance. Future improvements could include gathering more training data in challenging conditions and implementing adaptive preprocessing to handle varying lighting conditions better. Adding in image augmentation that adjusts lighting may be beneficial.

This project demonstrates that effective facial verification is possible with relatively simple hardware, though deployment in security-critical applications would require additional measures to address potential vulnerabilities.