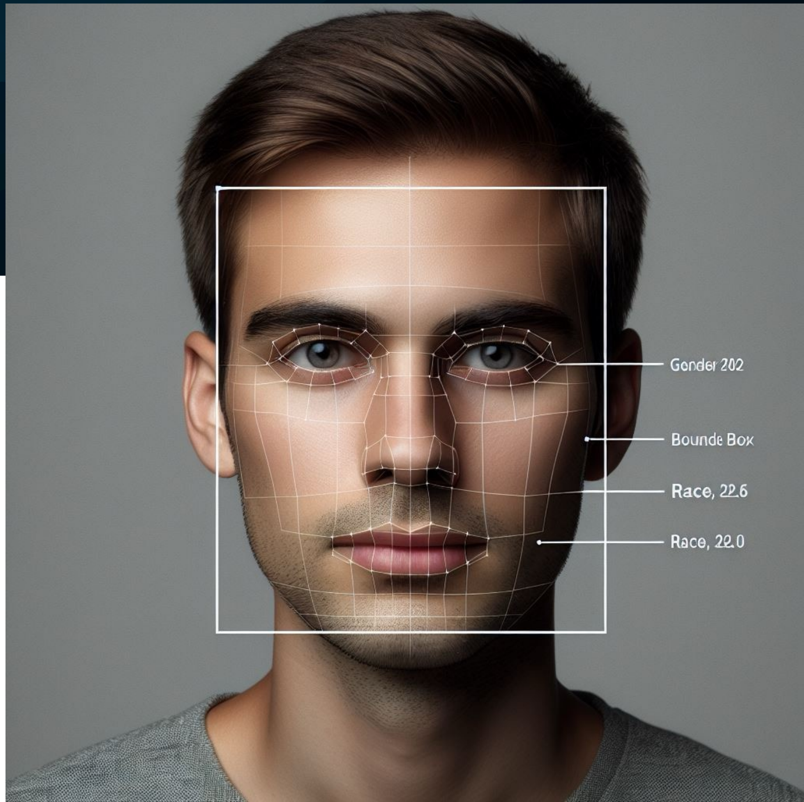
Enhanced ATM Security: Facial Analysis for Profile Monitoring and Alerting



Prepared by Pius Yee (DSI-SG-42)

Introduction

- Automated Teller Machines (ATMs) have become an essential part of our daily lives
- However, the physical cards and PINs exposes them to theft, such as ATM skimming
- ATM skimming is a type of payment card fraud.
    - It’s a way of stealing PINs and other information off credit cards and debit cards by rigging machines with hidden recording devices.

Become a Member | Apply for a Loan

Northwest
COMMUNITY CREDIT UNION
A division of TwinStar Credit Union®

EN ESPAÑOL | LOCATIONS & ATMS | LEARN ▾ | ABO

How to Spot an ATM Skimmer

Skimming device cases are becoming more frequent in the United States.

Northwest Community Credit Union has invested in technology to monitor our ATMs for potential placement of skimming devices. However, in order to make sure your card is safe while using an ATM terminal we've put together this guide to help you identify and avoid ATM skimmers.

Here's an example of what false PIN pad looks like:

Card slot

False PIN pad

Source: https://www.nwcu.com/learn/how-spot-atm-skimmer

3 NEWS | NEWS | WEATHER | FEATURES | TRAFFIC | GAME CENTER | WATCH

Skimming Scam Alert: Las Vegas thieves nab half a million in April alone

by Denise Rosch | Sat, April 27th 2024 at 4:28 PM
Updated Sat, April 27th 2024 at 6:14 PM

thumb_65634.png

Raising cases of ATM skimming even in year 2024!

Source: https://news3lv.com/news/local/skimming-scam-alert-las-vegas-thieves-nab-half-a-million-in-april-alone

Persona

- Sarah relies on ATMs for quick cash access but expects a secure and efficient experience.
- With the rise of ATM skimming scams, she worries that using an ATM might expose her card details or PIN.
- She feels particularly unsafe when using ATMs in isolated locations, where the risk of skimming might be higher.

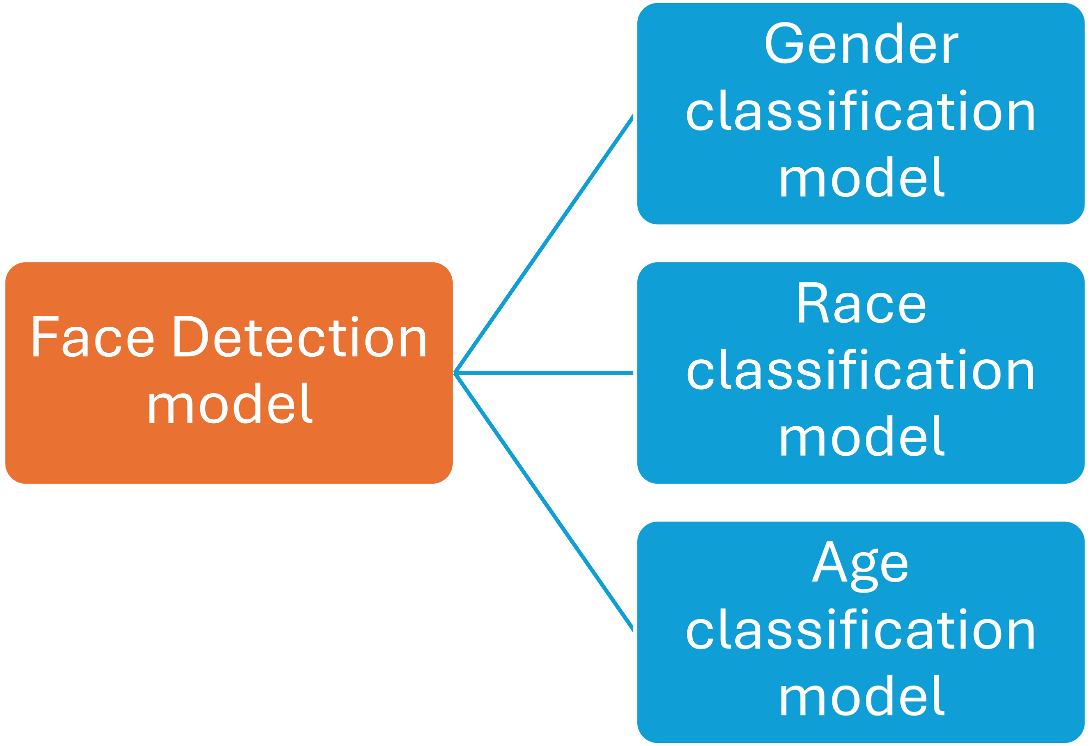
Problem Statement

- Existing security measures might not be sufficient to identify and prevent fraudulent withdrawal. Therefore, we need a system that leverages existing ATM infrastructure to introduce an additional layer of security.
- **How can we utilize profiling using computer vision to provide additional security for bank customers?**

How does it work?

1. Analyze video footage captured by ATM cameras
2. Detect the age, gender, and race of the ATM user
3. Compare with the cardholder’s profile
4. Identify discrepancies that might be suspicious
5. Trigger real-time alerts to the cardholder or bank

Machine learning models



Data collection and pre-processing

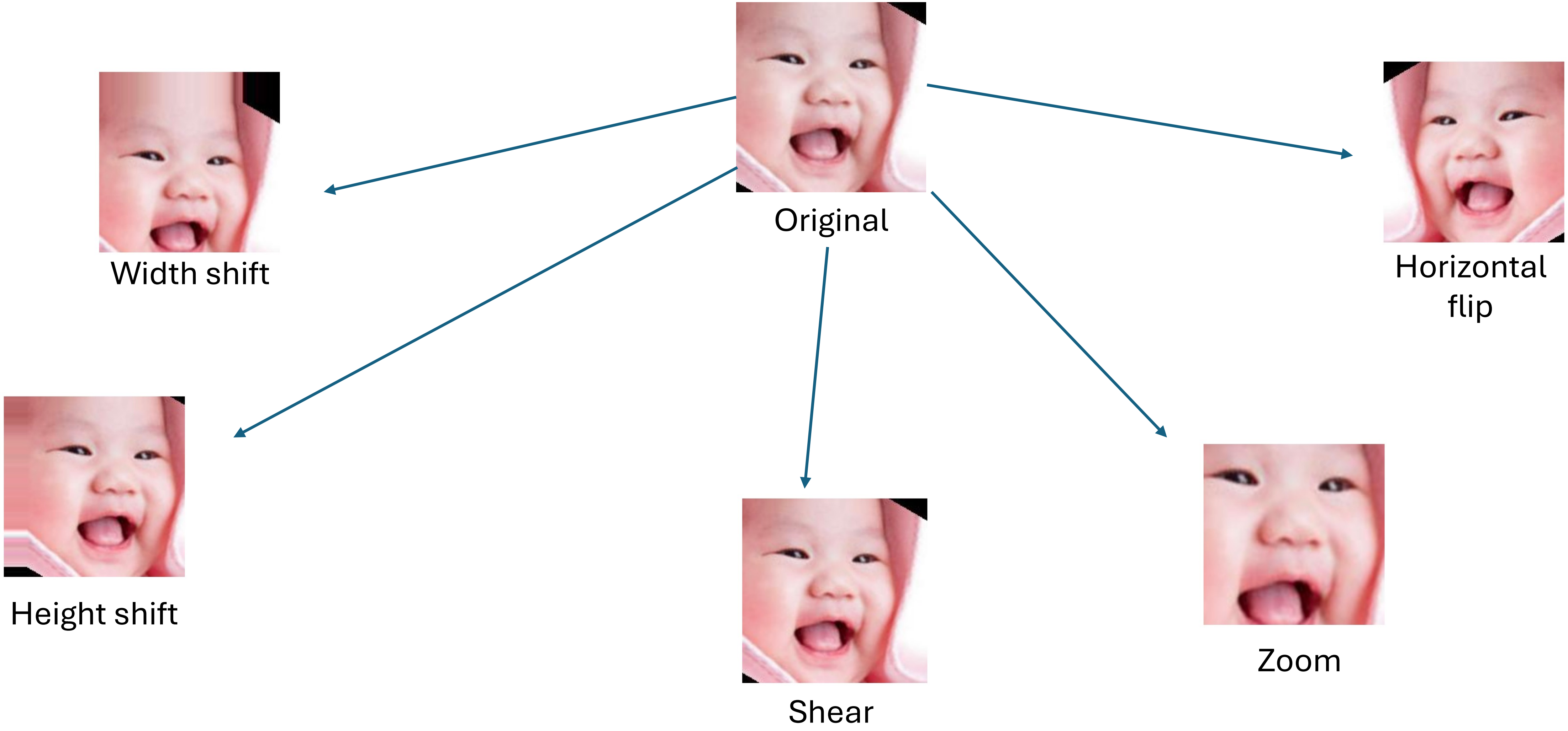
Dataset used

- UTKFace
  - ➢ The raw data utilized for this project is the UTKFace dataset.
  - ➢ It is a large-scale face dataset encompassing a wide age range, from 0 to 116 years old.
  - ➢ The dataset comprises over 23,000 face images annotated with
    - **Gender**
    - **Race**
    - **Age**

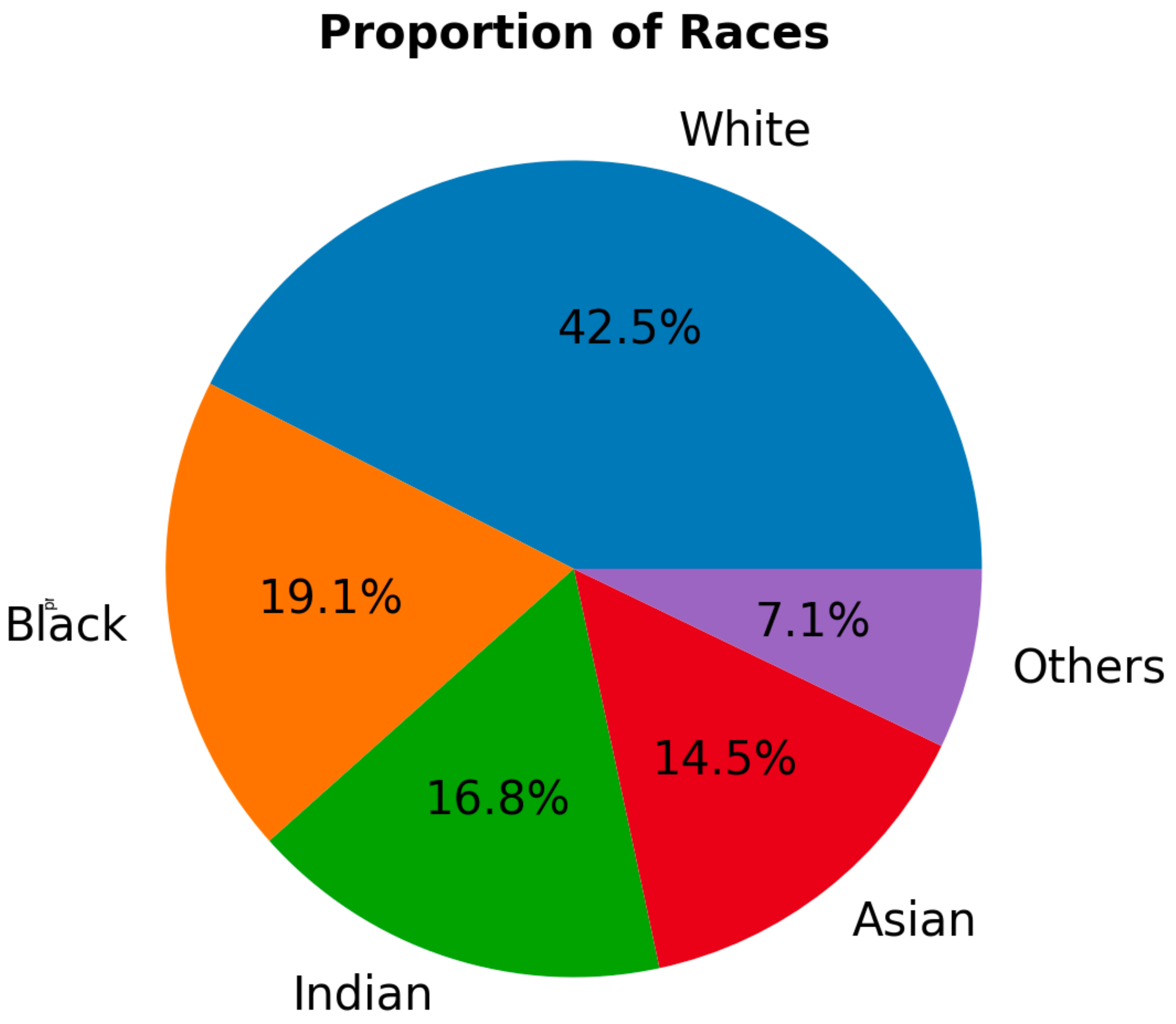
Augmentation on training datasets

Augmentation types	Value	Description
Width shift	20%	Randomly shifts the image horizontally along the width by up to 20% of the total width, enhancing model robustness to object position variations.
Height shift	20%	Randomly shifts the image vertically along the height by up to 20% of the total height, similar to the width shift but in the vertical direction.
Shear	20%	Applies a shear transformation, slanting the image along one axis, helping simulate perspective changes.
Zoom	20%	Randomly zooms the image in or out by up to 20%, making the model more resilient to changes in the object's apparent size.
Horizontal flip	NA	Randomly flips the image horizontally (like looking in a mirror), helping prevent the model from developing biases based on left/right orientation.

Augmentation on training datasets



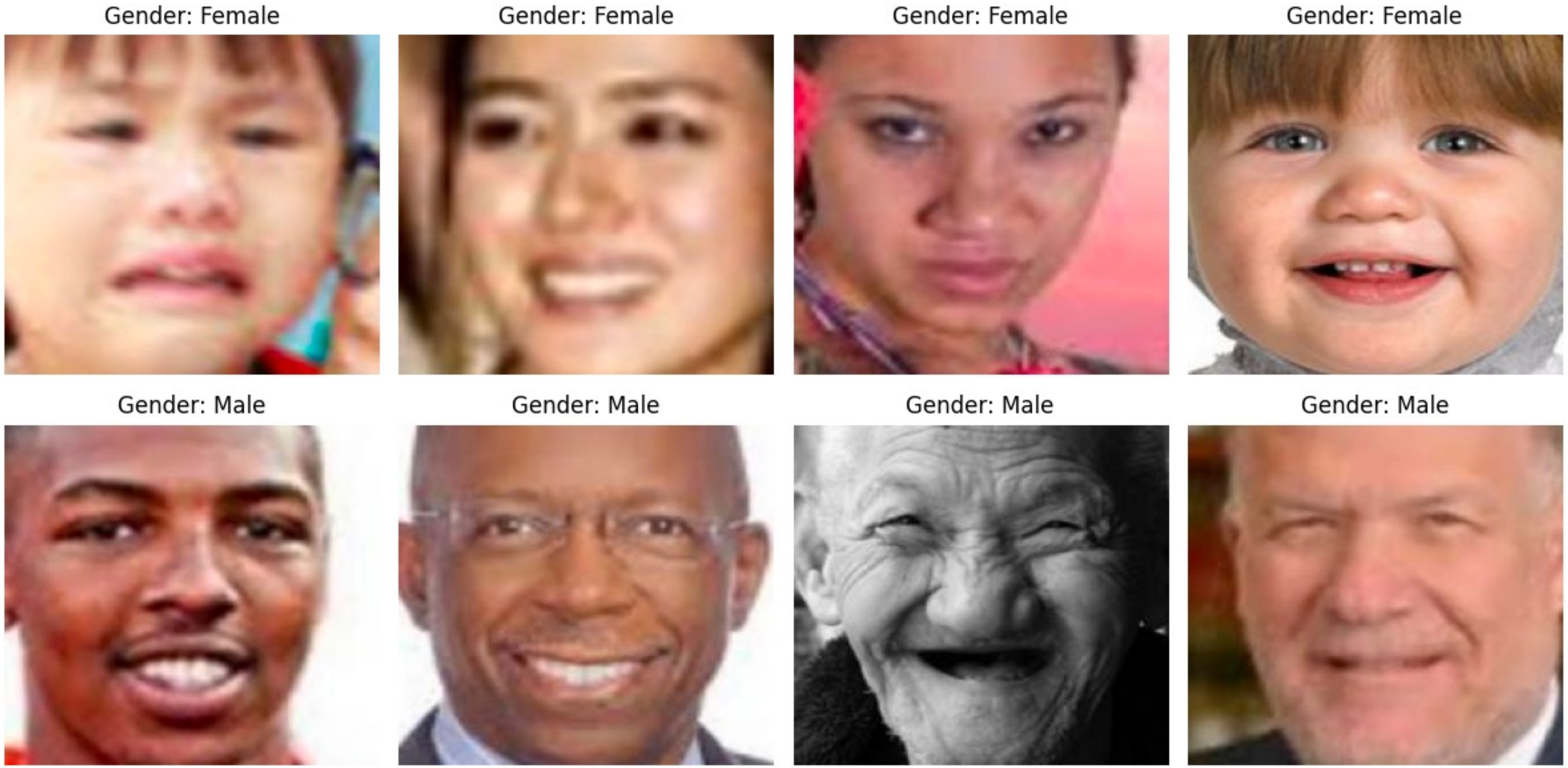
Gender proportion in the dataset



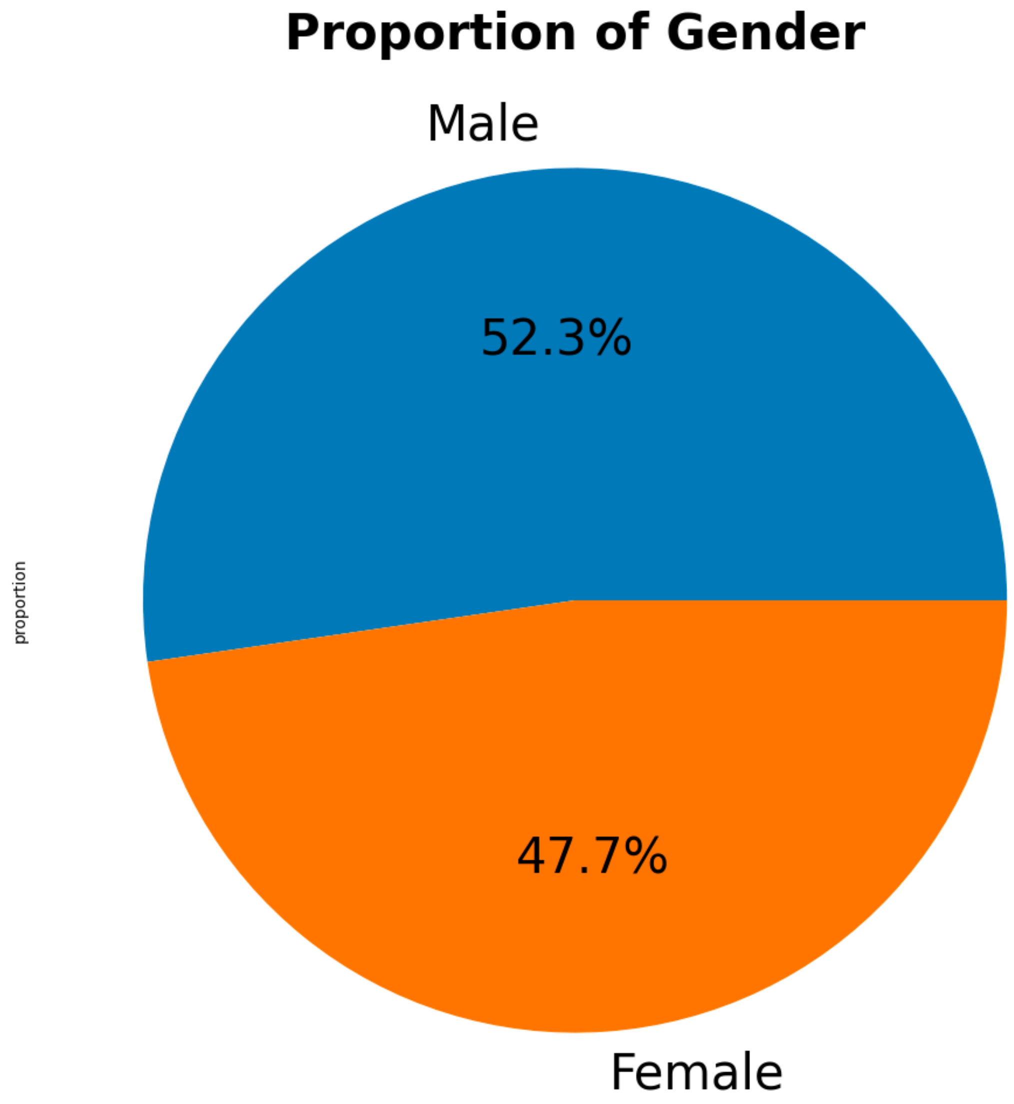
- The proportion of Male and female is balanced

Gender

- Some examples of Male and Female datasets:



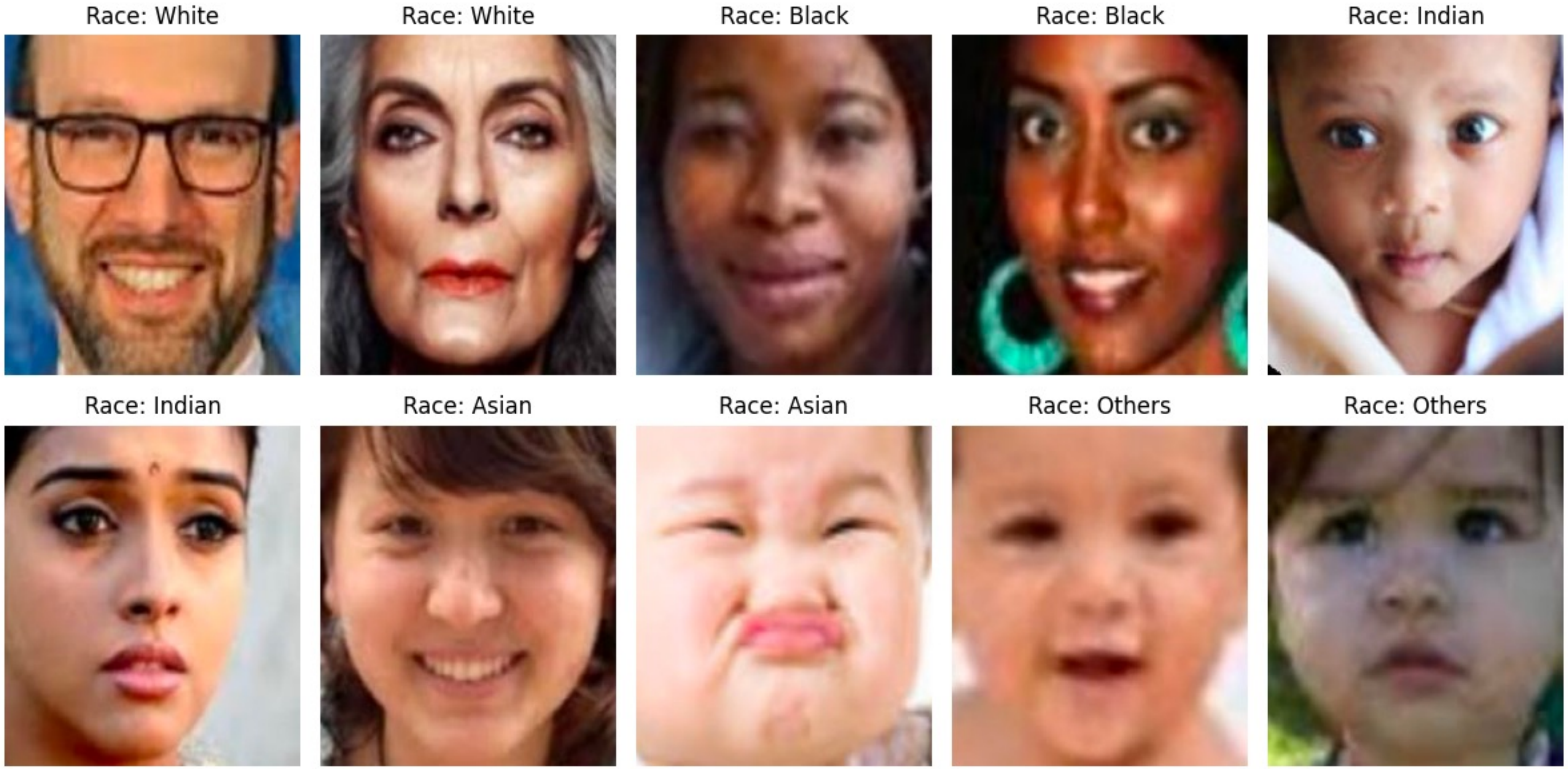
Race proportion in the dataset



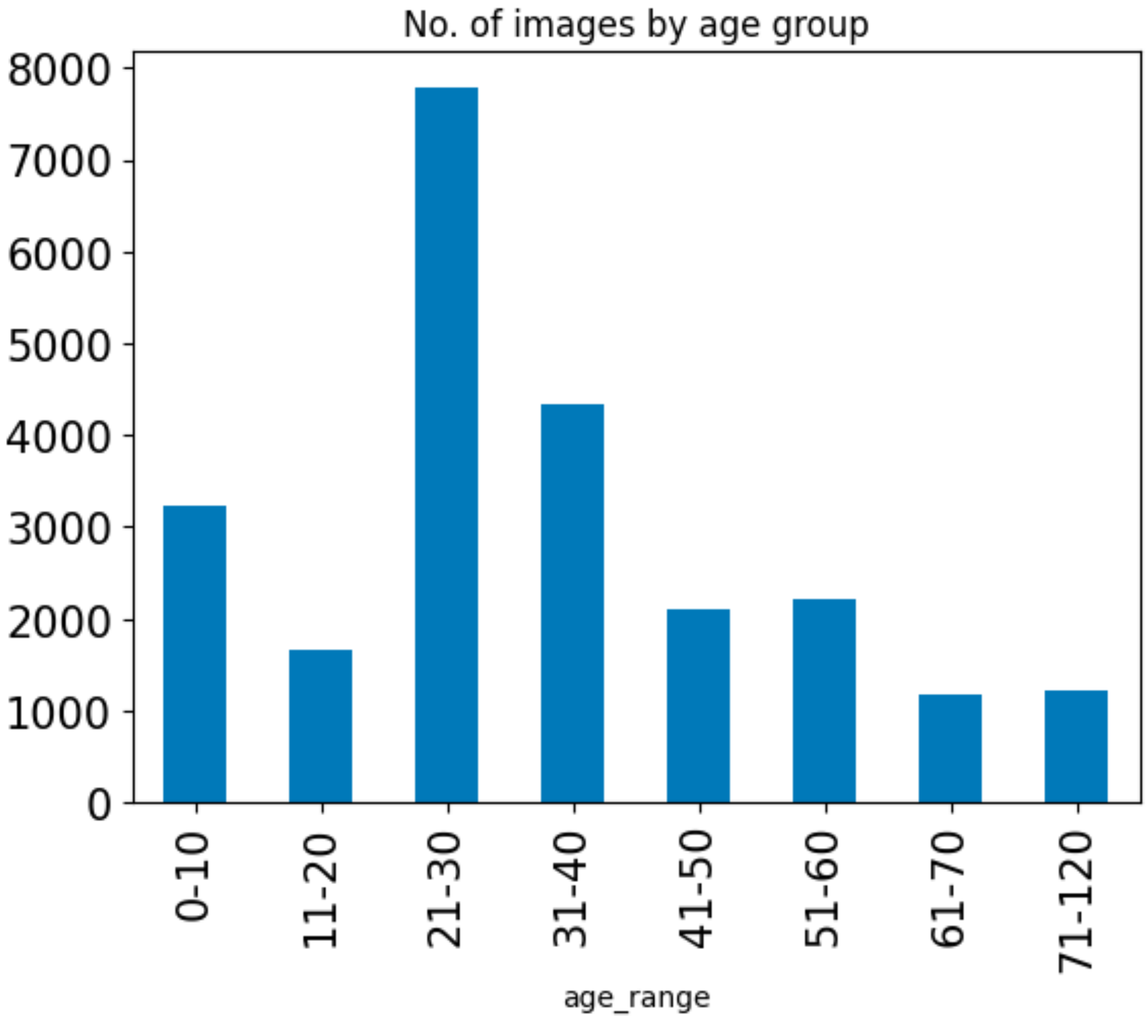
- White has the highest proportion in the dataset, followed by Black, Indian, Asian and Others.

Race

- Some examples of racial datasets:



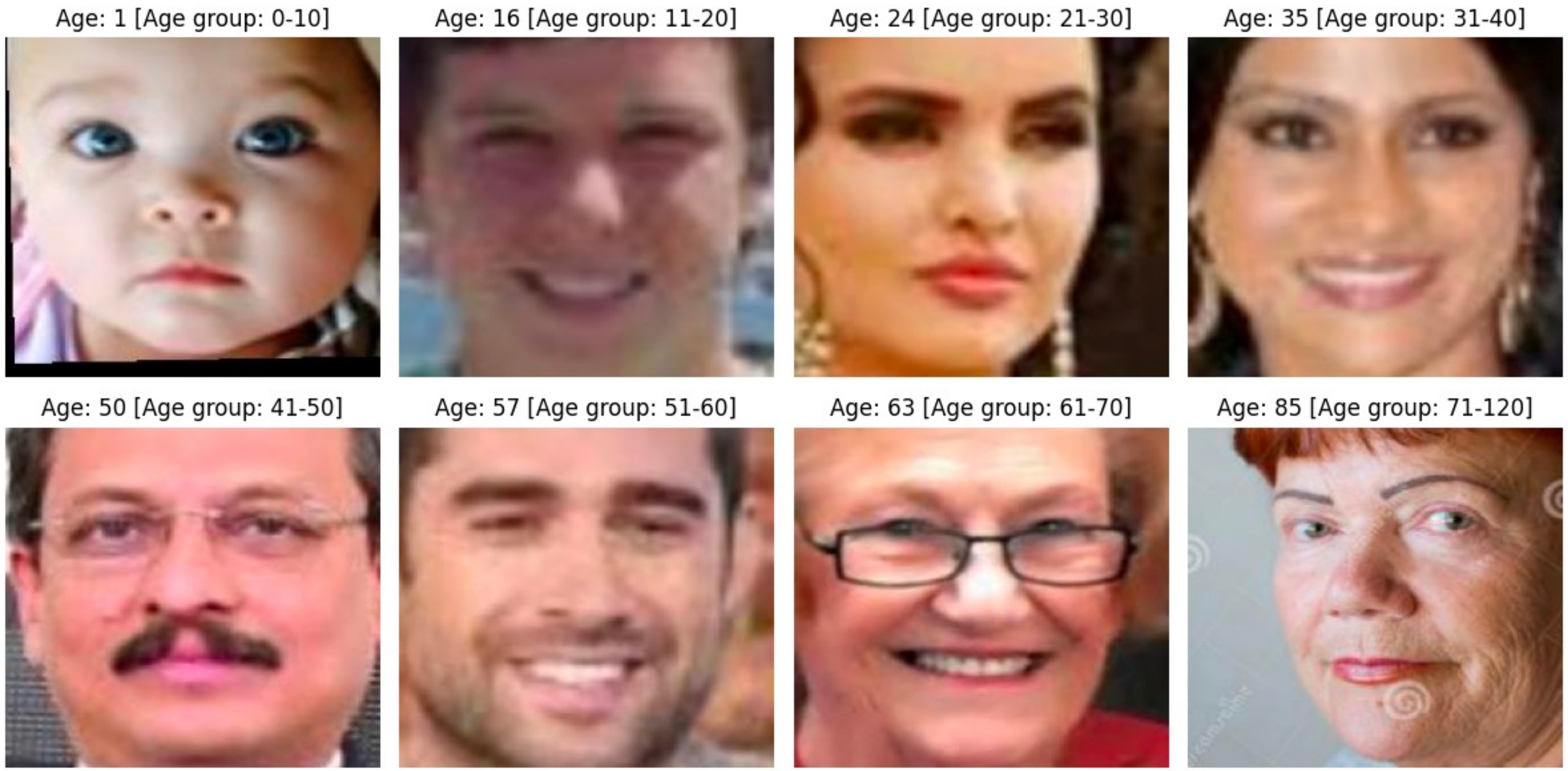
Age proportion in the dataset



- Age group ‘21-30’ has the highest proportion

Age

- Some examples of age datasets:



Modelling

CNN (Convolutional Neural Networks)

- Neural networks are like our brains, learning to find patterns in data.
- CNNs are special neural networks that excel at analyzing images. Think of them as image detectives with special magnifying glasses that look for shapes, colors, and patterns.

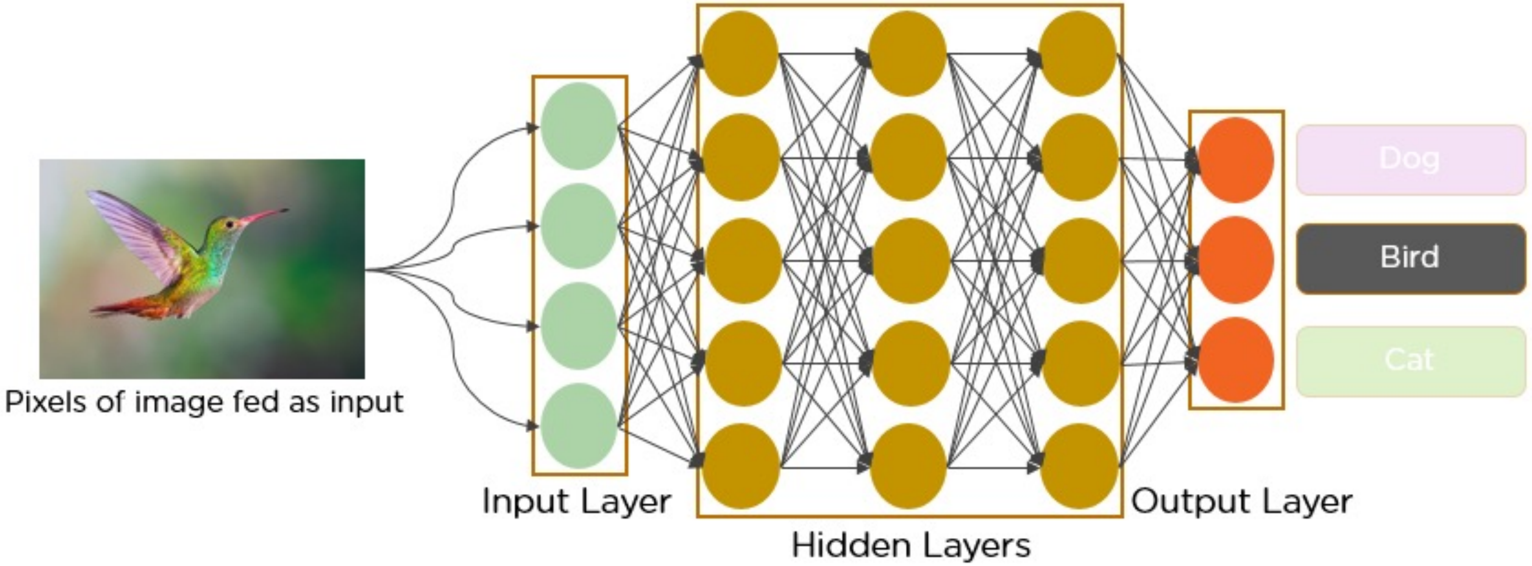


Image from: https://www.analyticsvidhya.com/blog/2021/05/convolutional-neural-networks-cnn/

Transfer learning of pre-trained model

- Transfer learning leverages a pre-trained model, using its learned features (weights) as a starting point, and fine-tuning it for the specific task with less data.

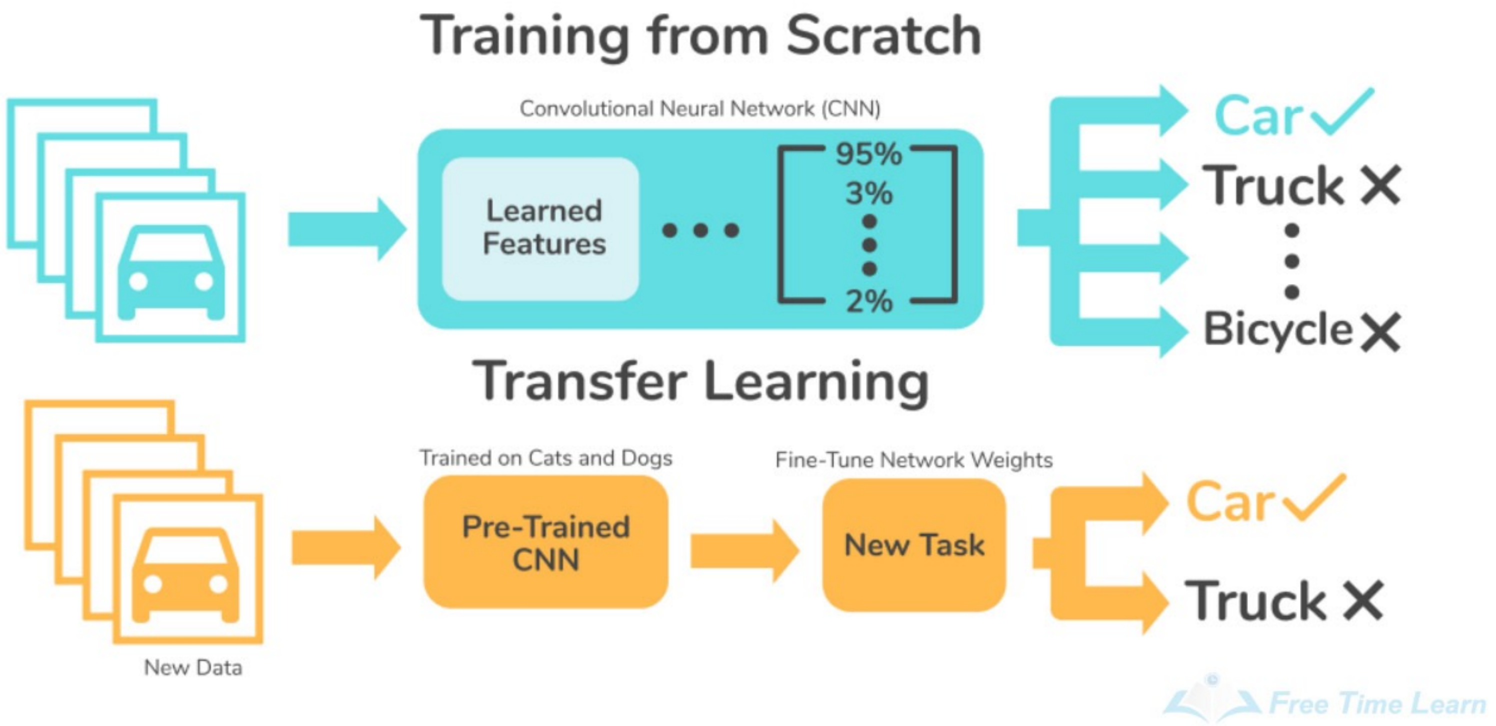
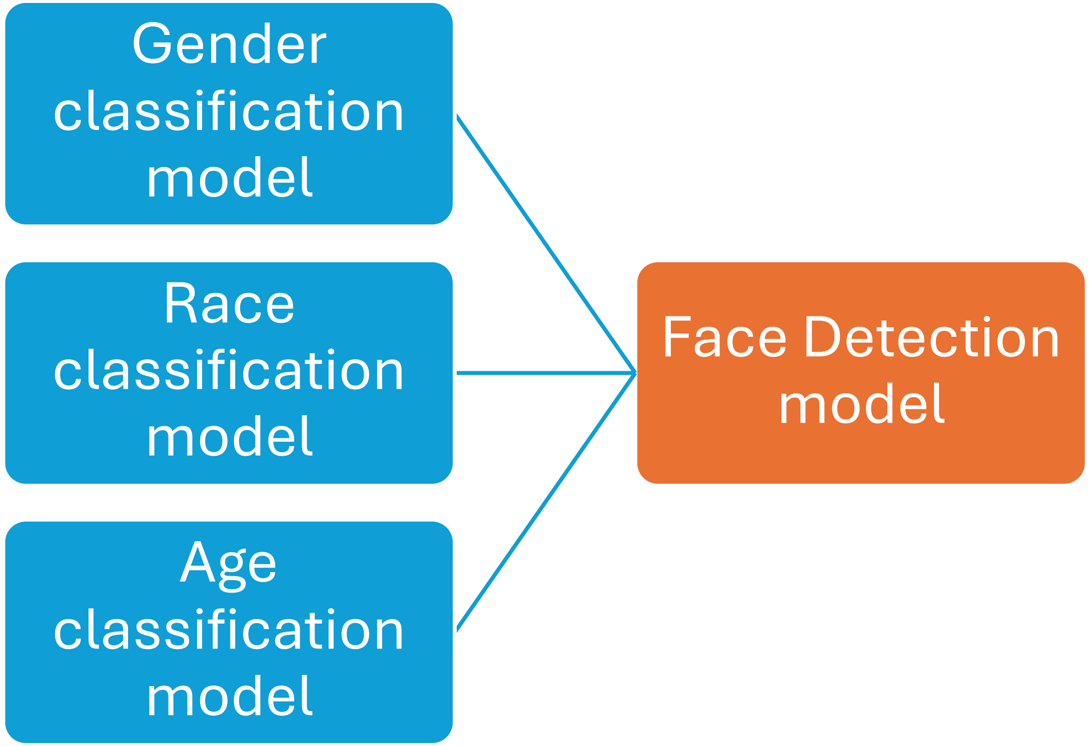
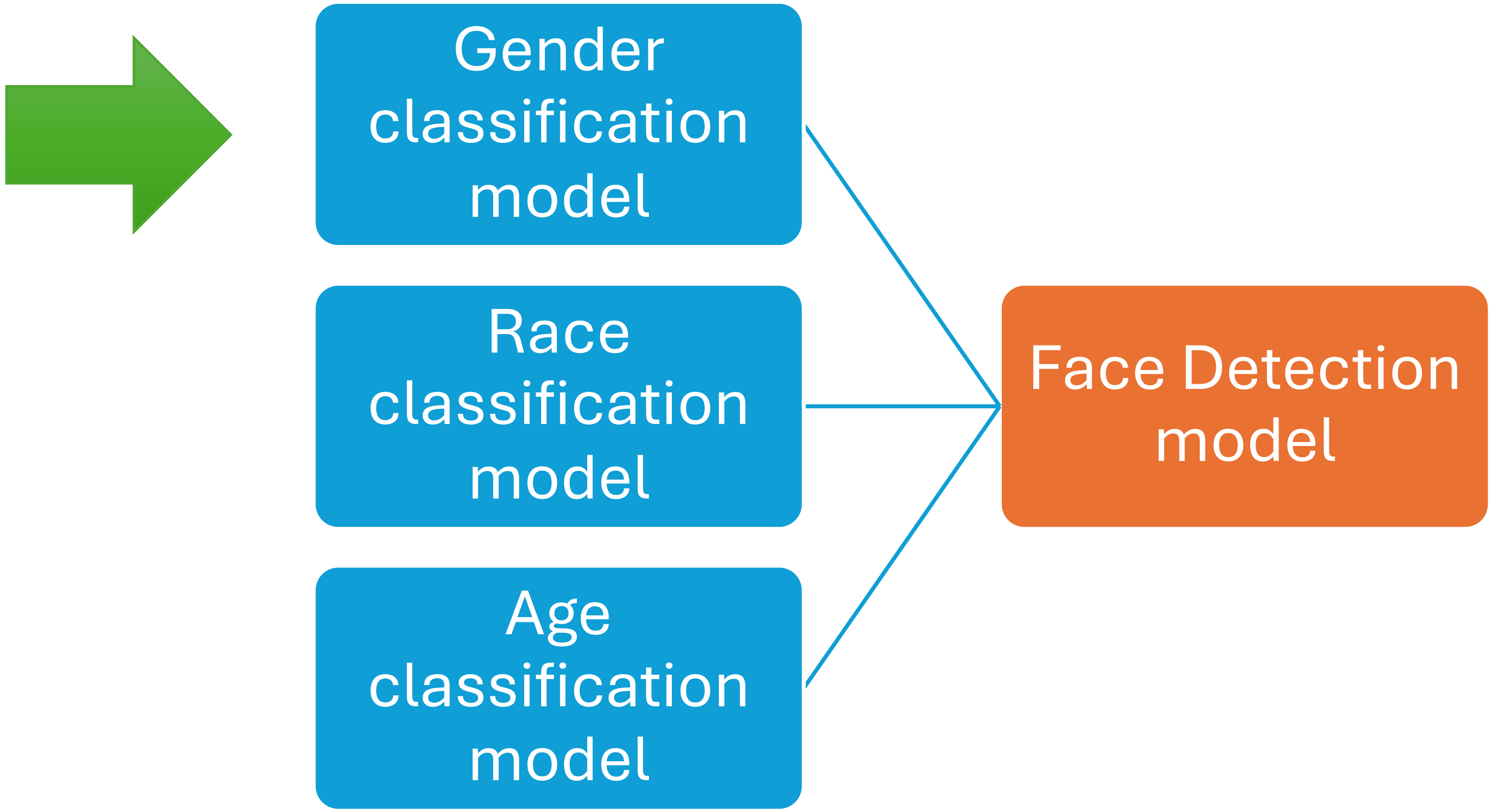


Image from: https://skyengine.ai/se/skyengine-blog/128-what-is-transfer-learning

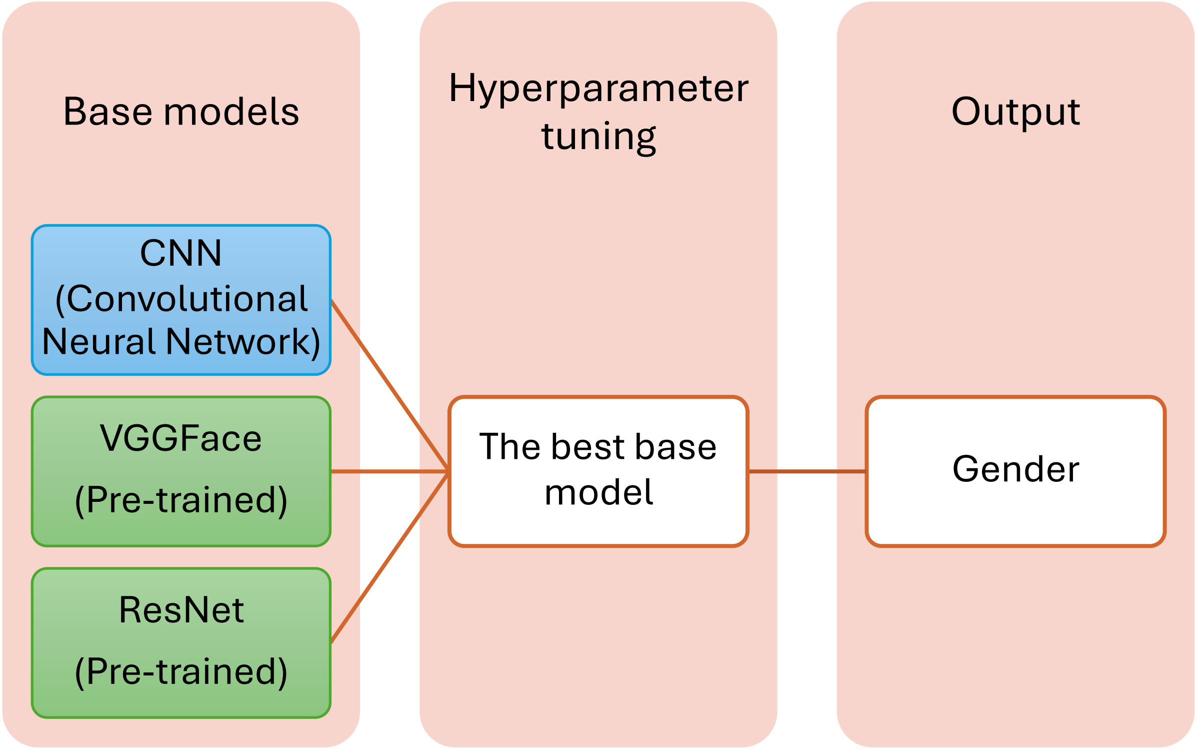
Machine learning models



Machine learning models



Modelling process



Base models

Base models

- CNN (Convolutional Neural Network)
- VGGFace (Pre-trained)
- ResNet (Pre-trained)

Gender | Race | Age

Model	Train Accuracy	Test Accuracy
CNN	0.7356	0.7687
VGGFace	0.9132	0.9264
ResNet 50	0.5233	0.5294

Base models

Base models

- CNN (Convolutional Neural Network)
- VGGFace (Pre-trained)
- ResNet (Pre-trained)

Gender | Race | Age

Model	Train Accuracy	Test Accuracy
CNN	0.7356	0.7687
VGGFace	0.9132	0.9264
ResNet 50	0.5233	0.5294

VGGFace is the best!

Base models

Base models

CNN (Convolutional Neural Network)

VGGFace (Pre-trained)

ResNet (Pre-trained)

Gender | **Race** | Age

Model	Train Accuracy	Test Accuracy
CNN	0.3141	0.2262
VGGFace	0.7993	0.8043
ResNet 50	0.3211	0.2895

Base models

Base models

CNN (Convolutional Neural Network)

VGGFace (Pre-trained)

ResNet (Pre-trained)

Gender | **Race** | Age

Model	**Train Accuracy**	**Test Accuracy**
CNN	0.3141	0.2262
VGGFace	0.7993	0.8043
ResNet 50	0.3211	0.2895

VGGFace is the best!

Base models

Base models

- CNN (Convolutional Neural Network)
- VGGFace (Pre-trained)
- ResNet (Pre-trained)

Gender | Race | **Age**

Model	Train Accuracy	Test Accuracy
CNN	0.2793	0.3070
VGGFace	0.5883	0.6096
ResNet 50	0.2476	0.3322

Base models

Base models

CNN (Convolutional Neural Network)

VGGFace (Pre-trained)

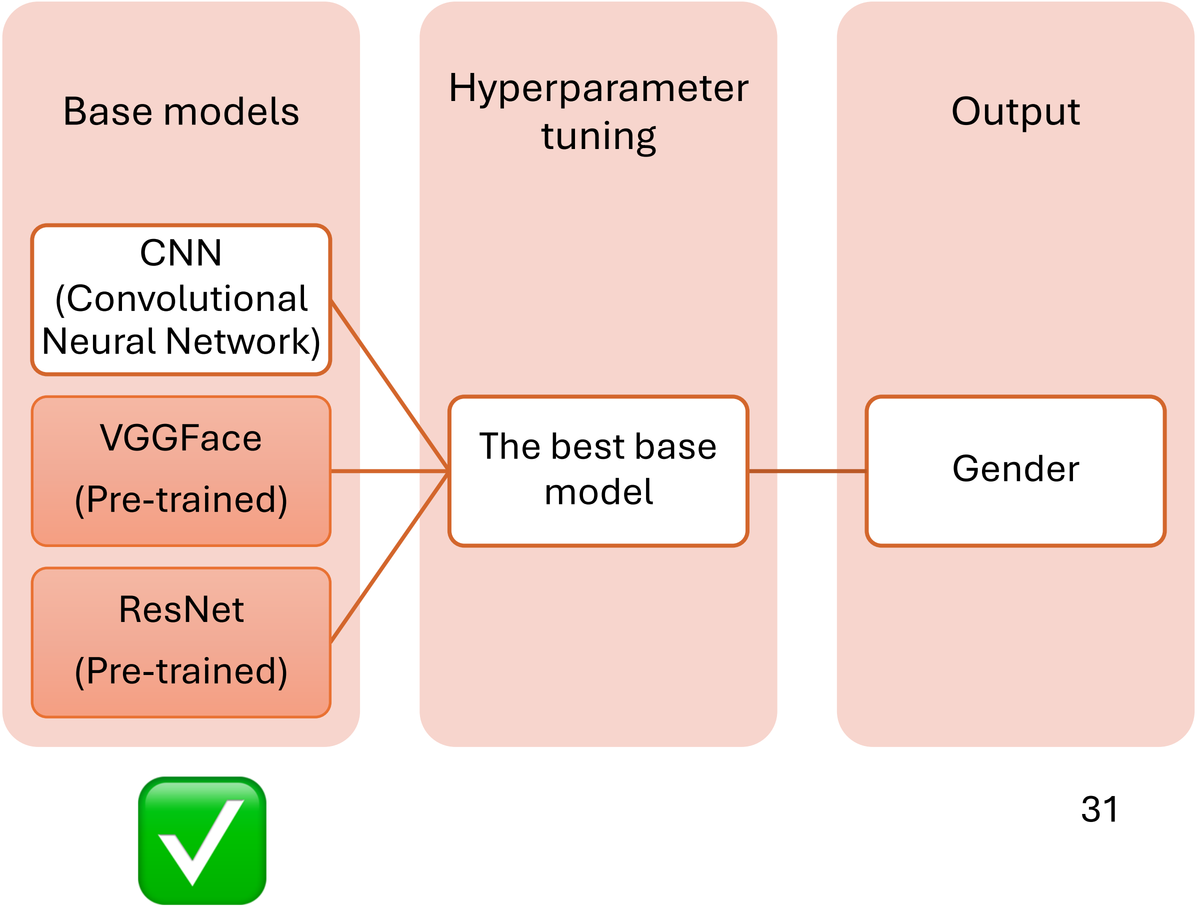
ResNet (Pre-trained)

Gender | Race | **Age**

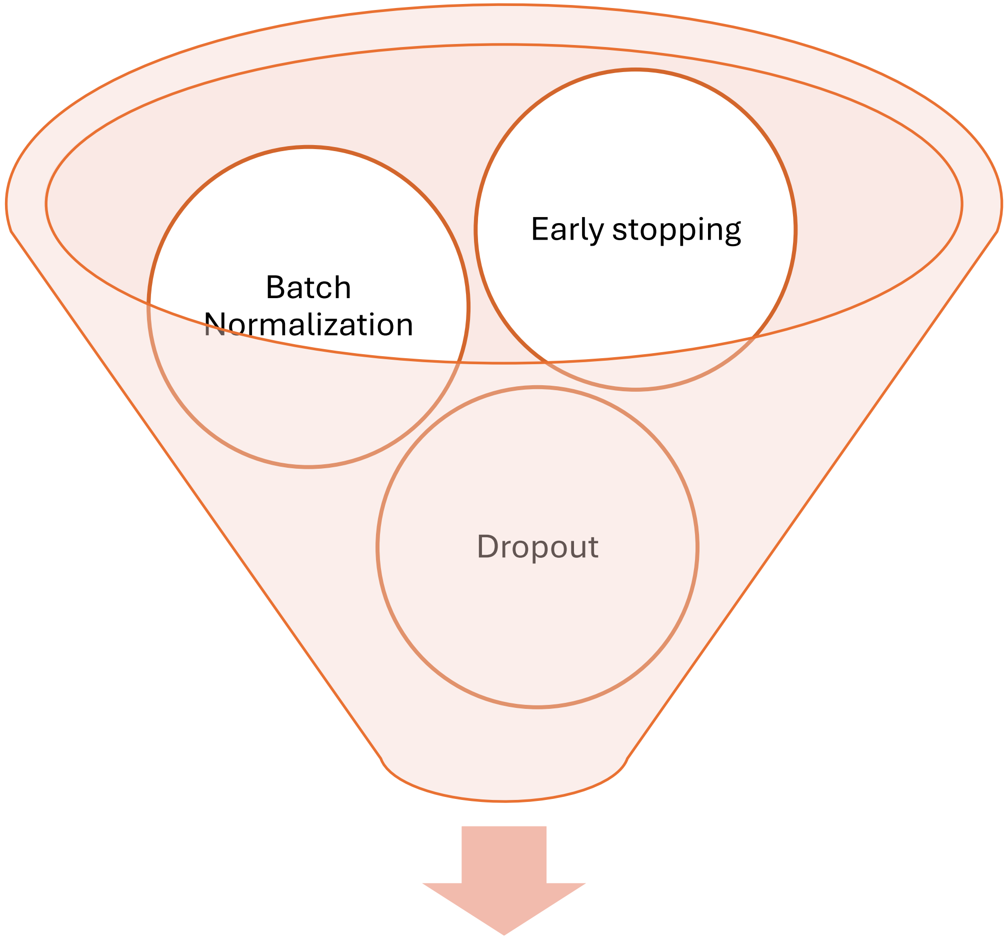
Model	Train Accuracy	Test Accuracy
CNN	0.2793	0.3070
VGGFace	0.5883	0.6096
ResNet 50	0.2476	0.3322

VGGFace is the best!

Modelling process



Fine Tuning – VGGFace



Model after fine-tuning

Hyperparameter tuning

Hyperparameter tuning

VGGFace

Gender

Race

Age

Model	Train Accuracy	Test Accuracy
CNN	0.7356	0.7687
VGGFace	0.9132	0.9264
ResNet 50	0.5233	0.5294
VGGFace (tuned)	0.9110	0.9321

Hyperparameter tuning

Hyperparameter tuning

VGGFace

Gender | Race | Age

Model	Train Accuracy	Test Accuracy
CNN	0.7356	0.7687
VGGFace	0.9132	0.9264
ResNet 50	0.5233	0.5294
VGGFace (tuned)	0.9110	0.9321

Hyperparameter tuning

Hyperparameter tuning

VGGFace

Gender | **Race** | Age

Model	Train Accuracy	Test Accuracy
CNN	0.3141	0.2262
VGGFace	0.7993	0.8043
ResNet 50	0.3211	0.2895
VGGFace (tuned)	0.8124	0.8379

Hyperparameter tuning

Hyperparameter tuning

VGGFace

Gender | Race | Age

Model	Train Accuracy	Test Accuracy
CNN	0.3141	0.2262
VGGFace	0.7993	0.8043
ResNet 50	0.3211	0.2895
VGGFace (tuned)	0.8124	0.8379

Hyperparameter tuning

Hyperparameter tuning

VGGFace

Gender | Race | **Age**

Model	**Train Accuracy**	**Test Accuracy**
CNN	0.2793	0.3070
VGGFace	0.5883	0.6096
ResNet 50	0.2476	0.3322
VGGFace (tuned)	0.6128	0.6312

Hyperparameter tuning

Hyperparameter tuning

VGGFace

Gender | Race | **Age**

Model	Train Accuracy	Test Accuracy
CNN	0.2793	0.3070
VGGFace	0.5883	$\boxed{0.6096}$
ResNet 50	0.2476	0.3322
VGGFace (tuned)	0.6128	$\boxed{0.6312}$ ↑

Other metrics – VGGFace (fine-tuned)

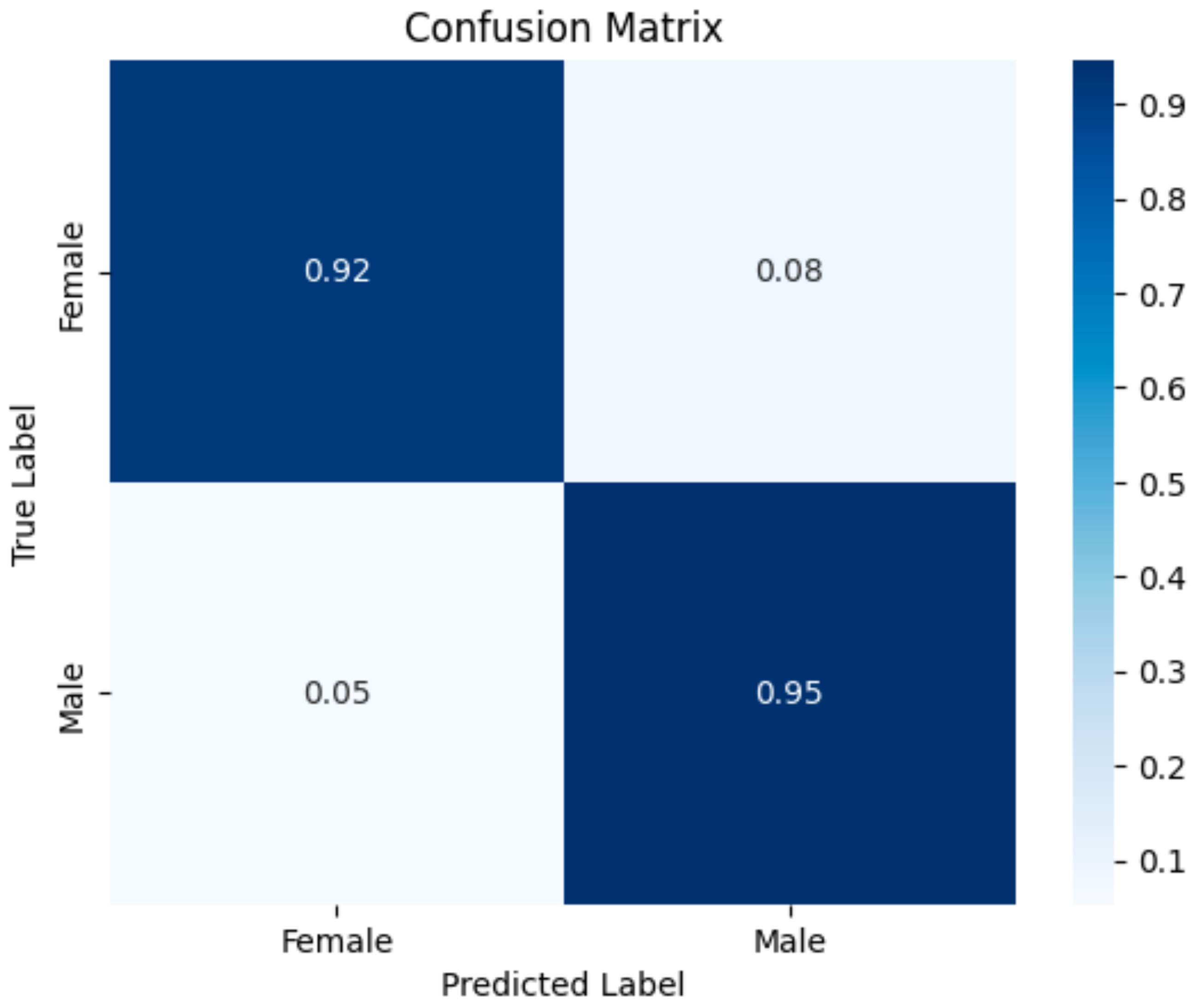
	Gender	Race	Age
Accuracy	0.93	0.84	0.63
Precision	0.93	0.83	0.63
Recall	0.93	0.84	0.63
F1 Score	0.93	0.84	0.62

Confusion Matrix

Gender

Race

Age

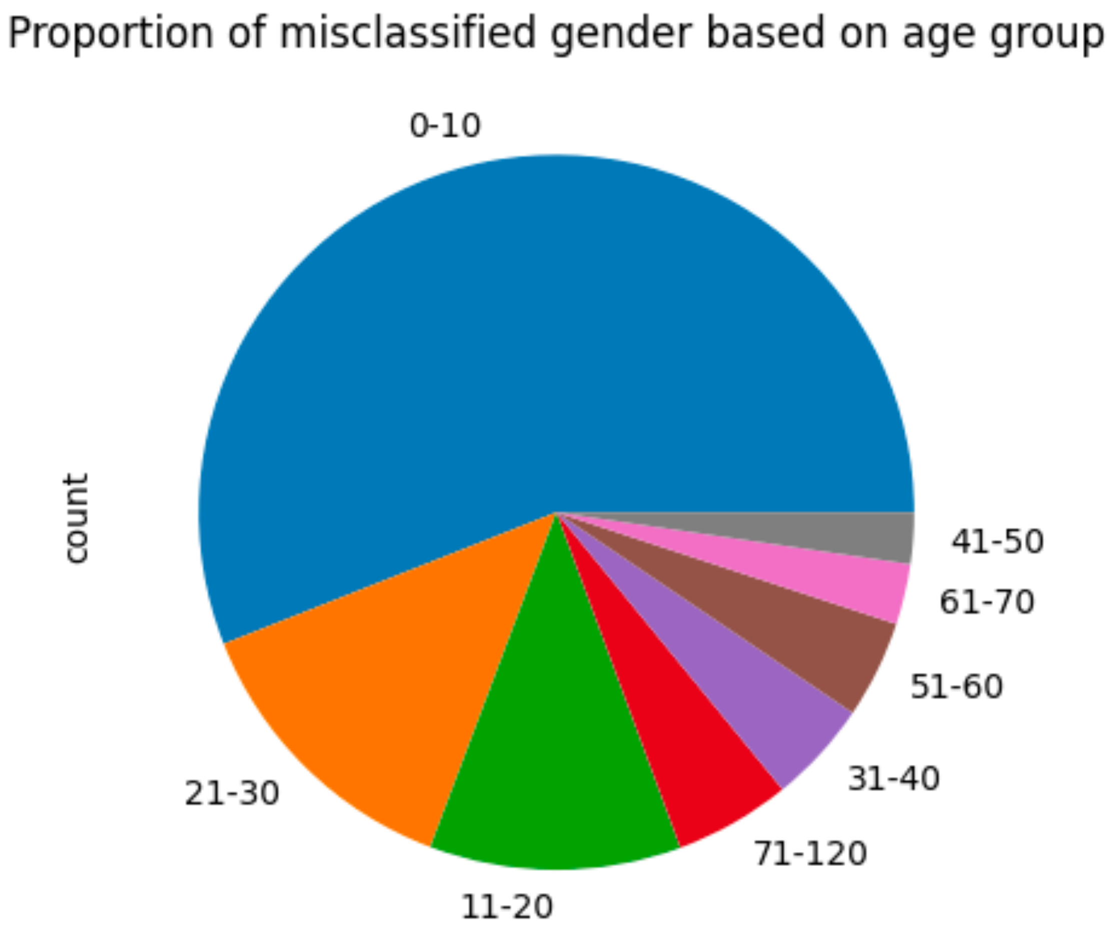


*% over total True Label

Samples of True Prediction

Samples of False Prediction

Proportion of misclassified gender based on age group

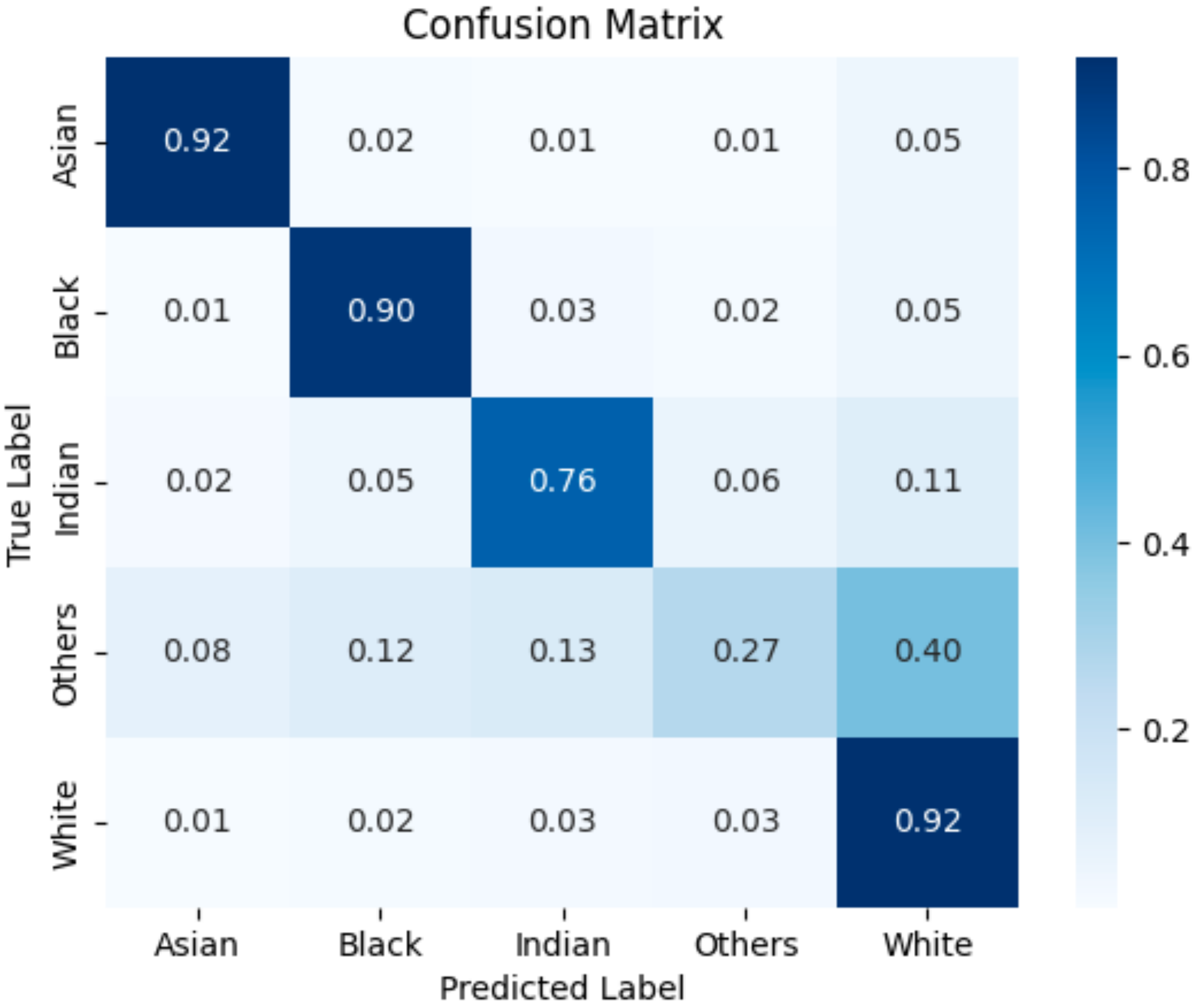


Confusion Matrix

Gender

Race

Age



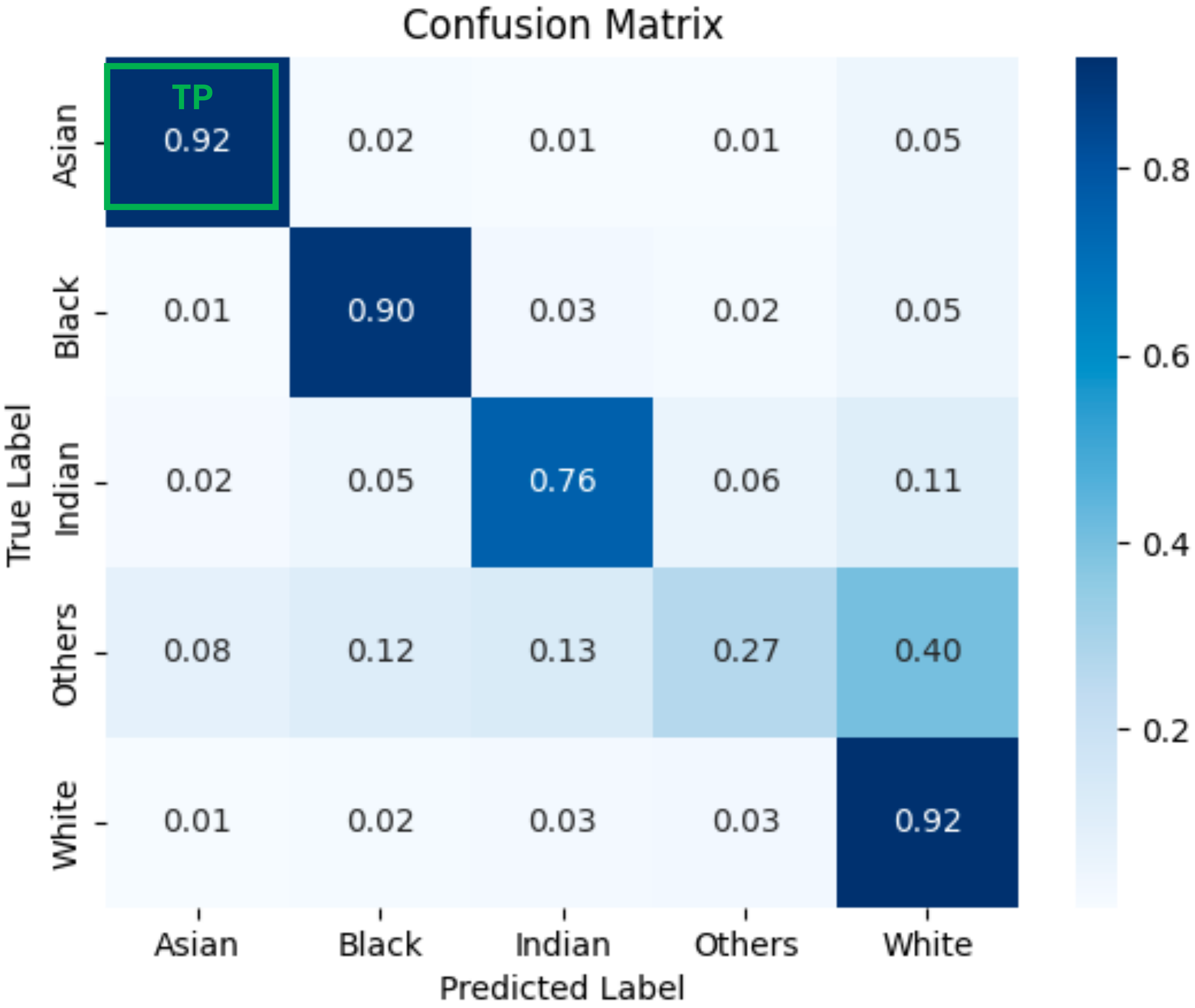
*% over total True Label

Confusion Matrix

Gender

Race

Age



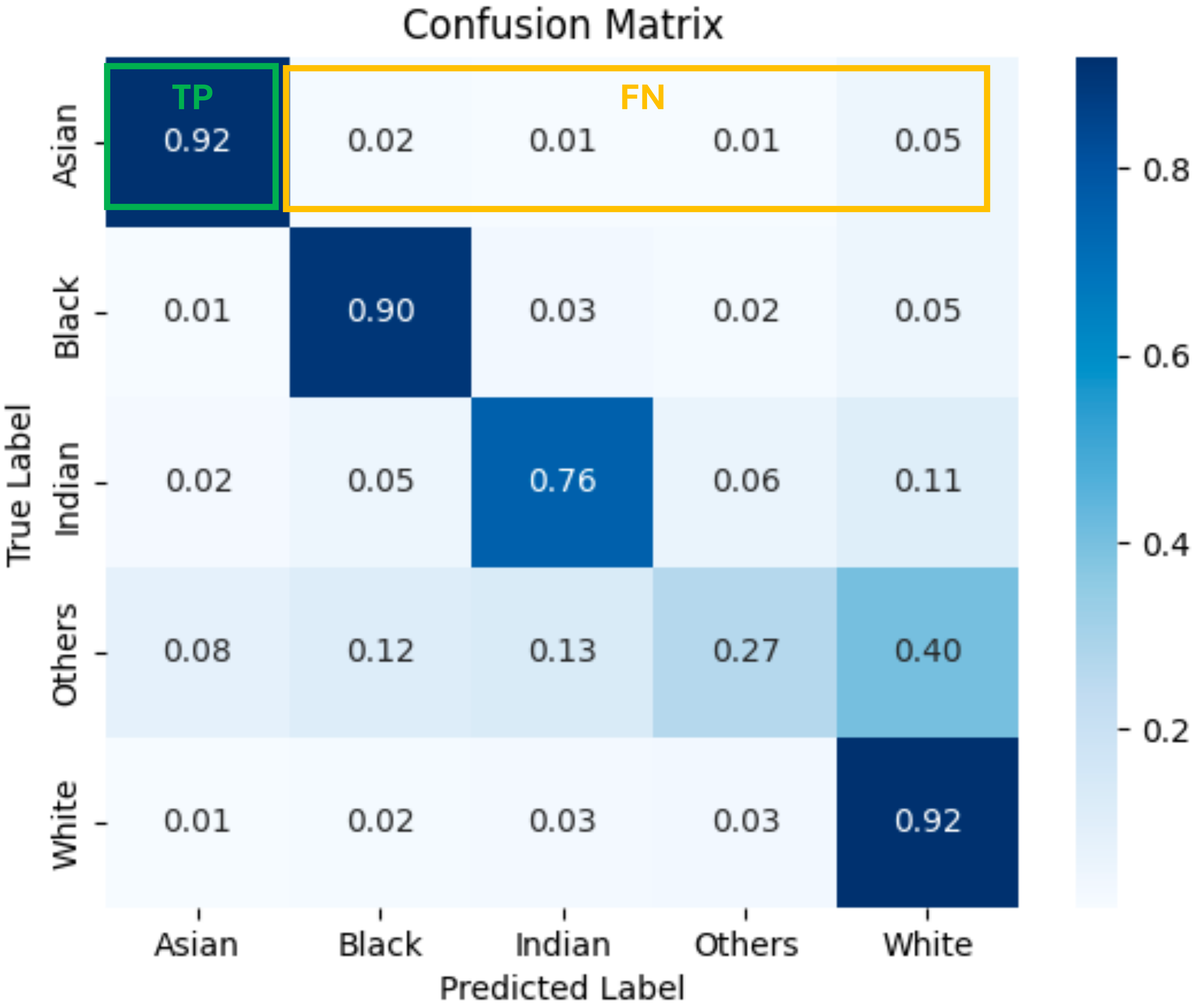
*% over total True Label

Confusion Matrix

Gender

Race

Age



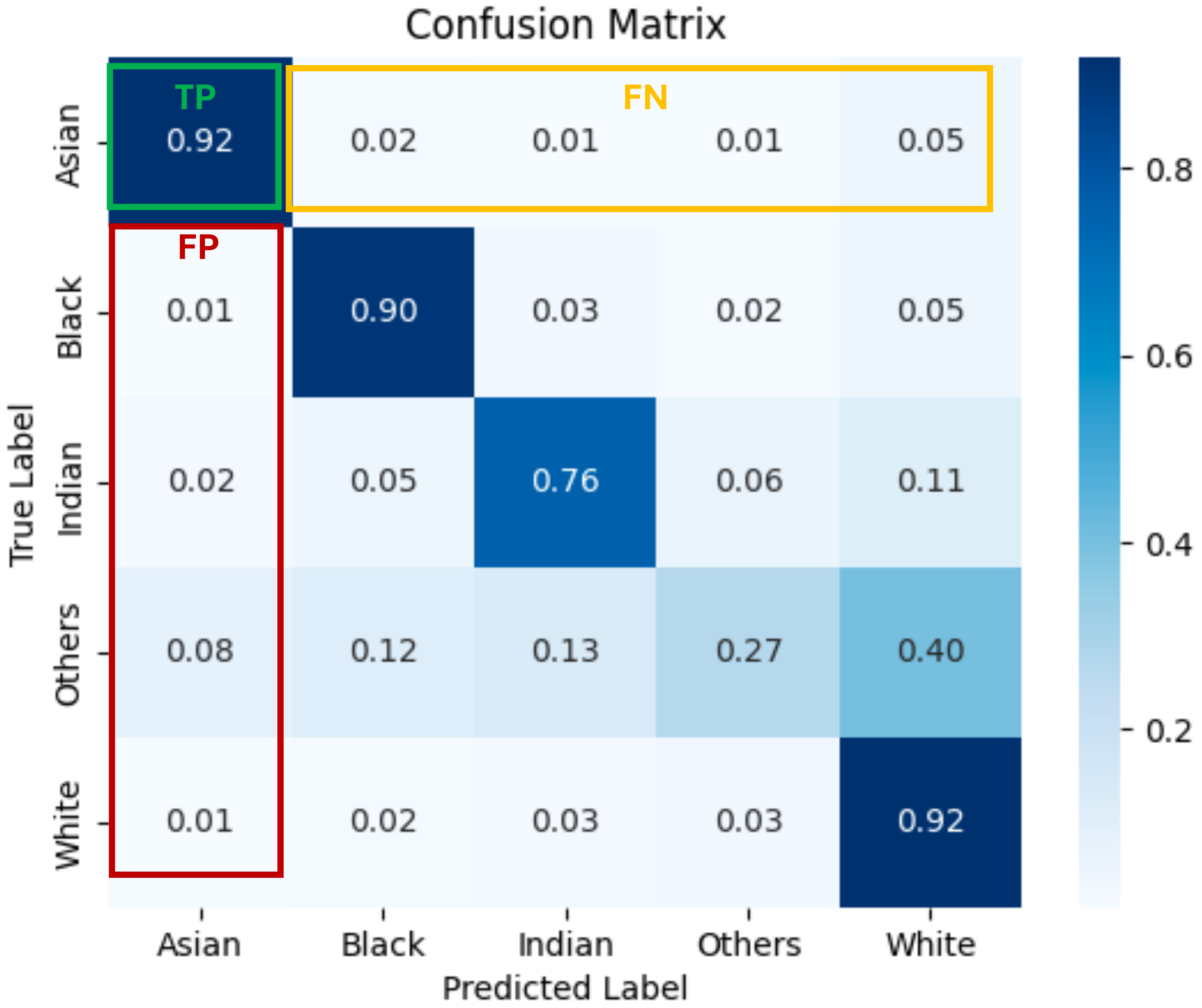
*% over total True Label

Confusion Matrix

Gender

Race

Age



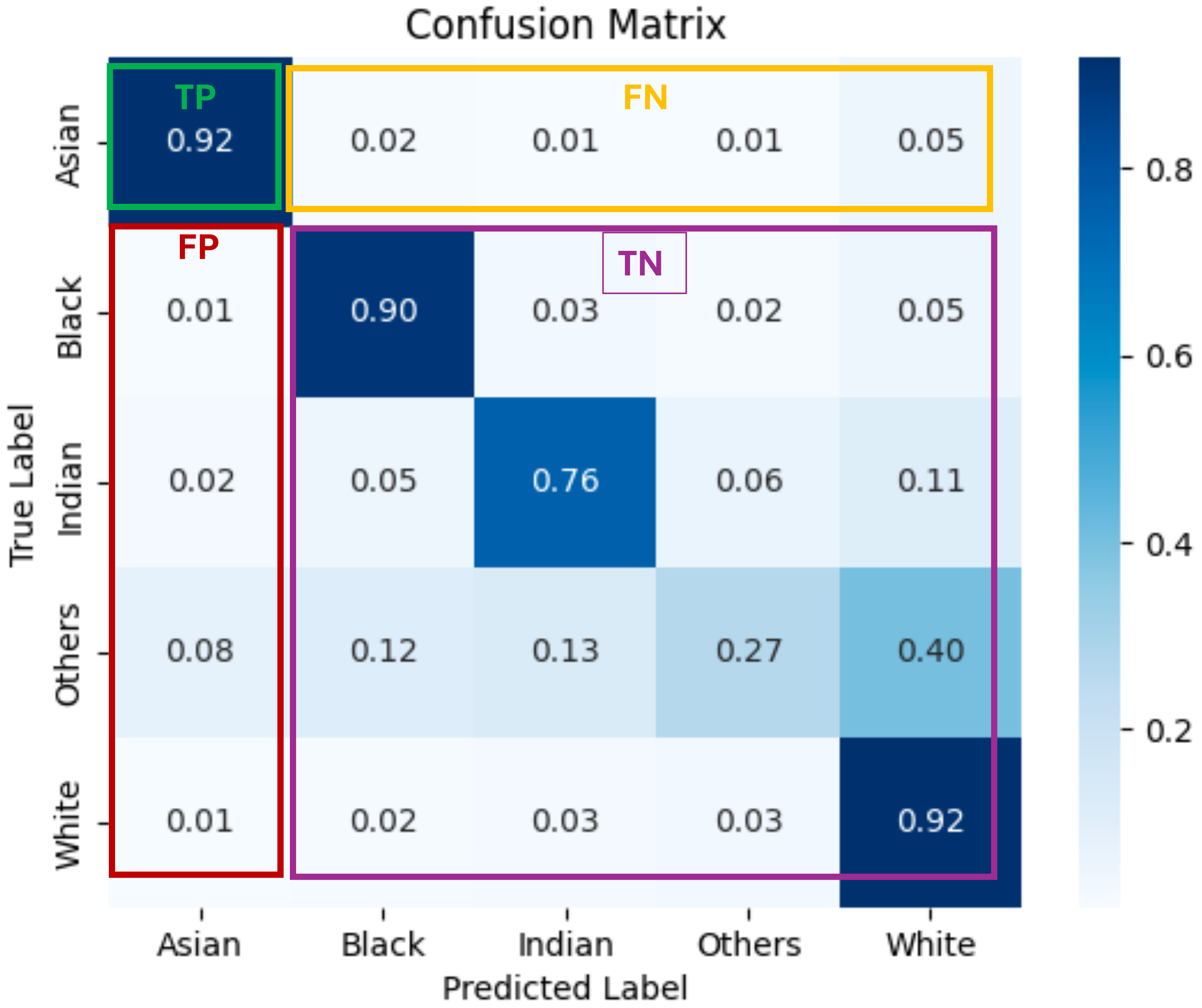
*% over total True Label

Confusion Matrix

Gender

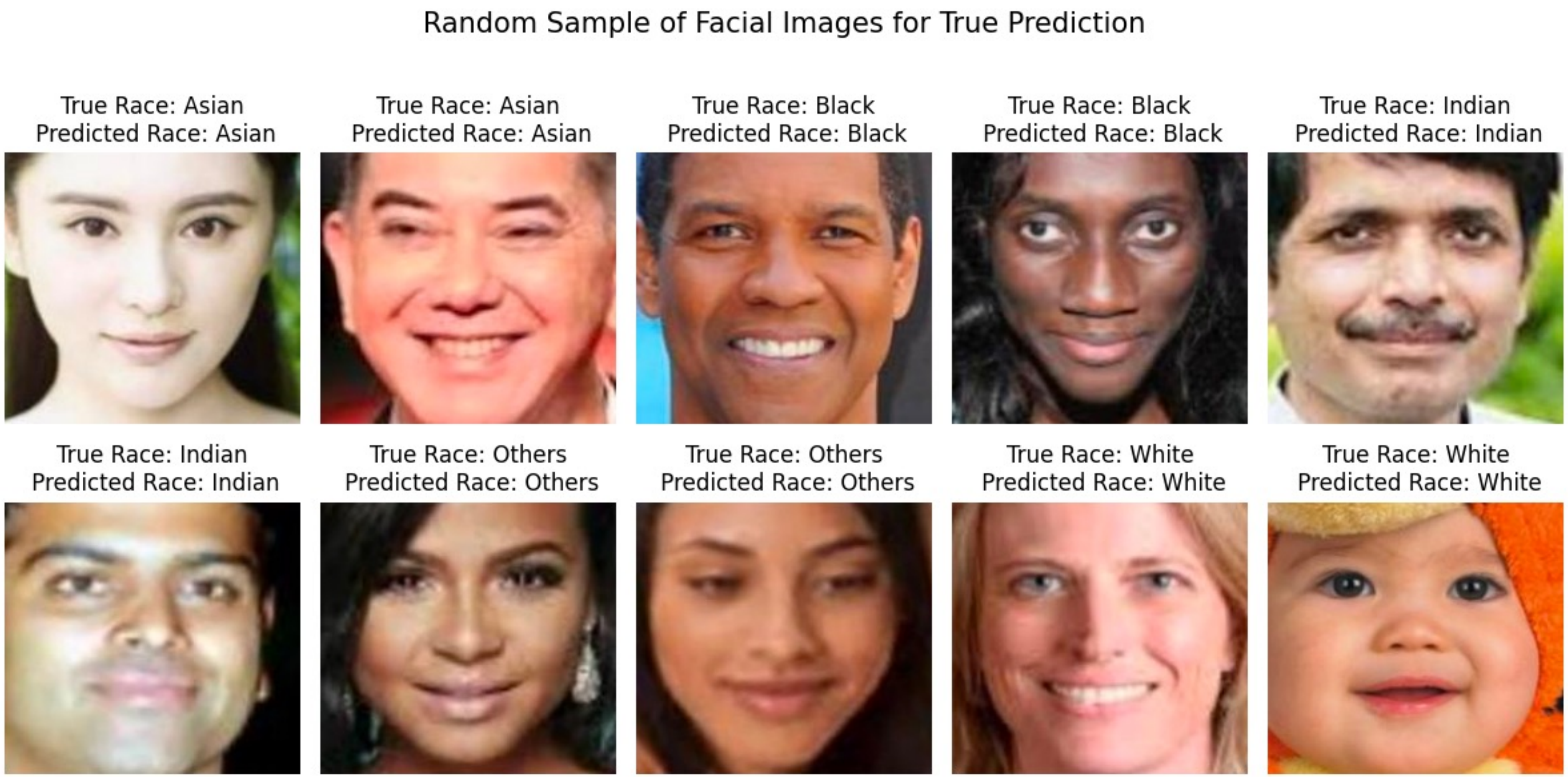
Race

Age

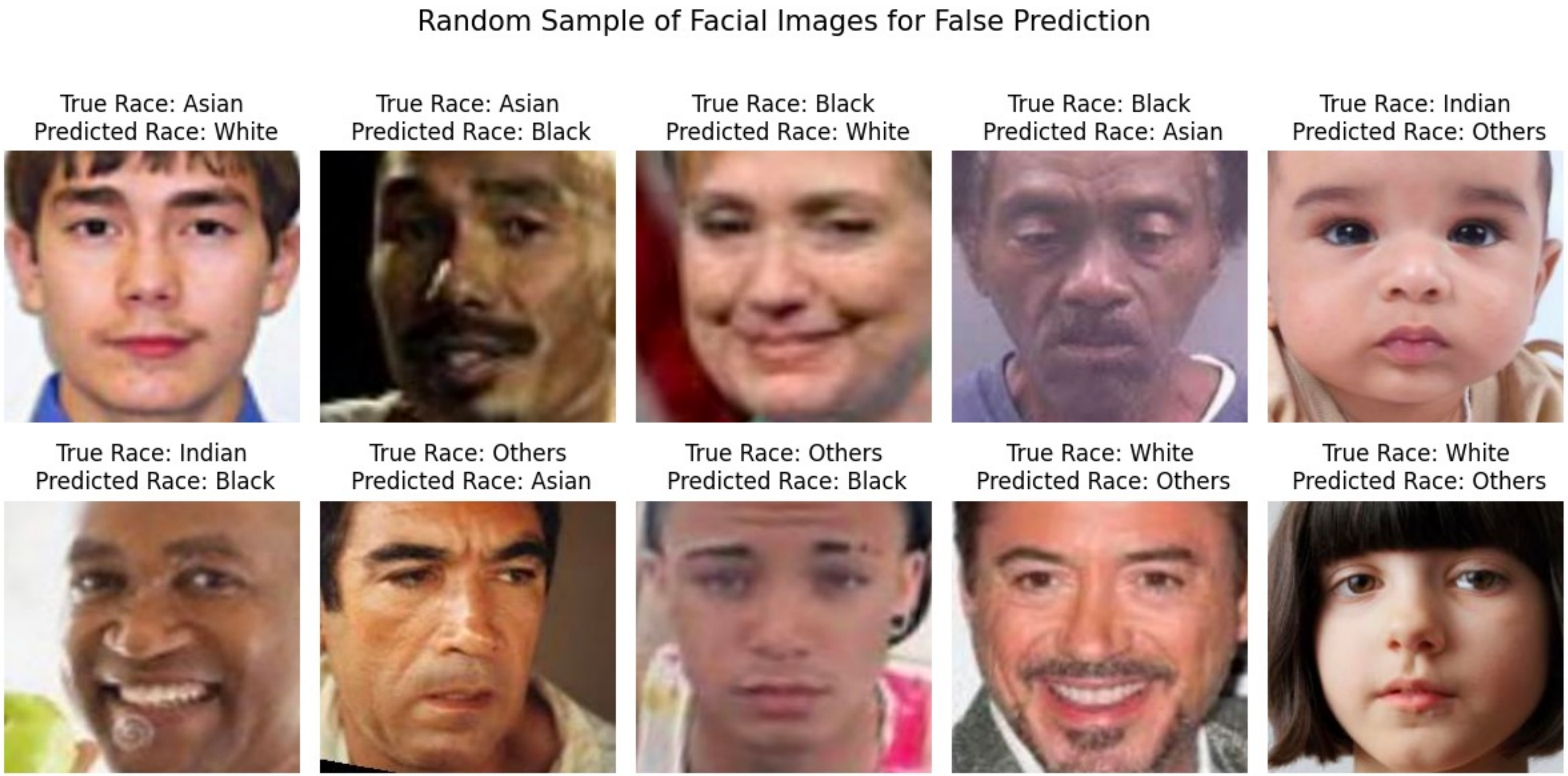


*% over total True Label

Samples of True Prediction



Samples of False Prediction

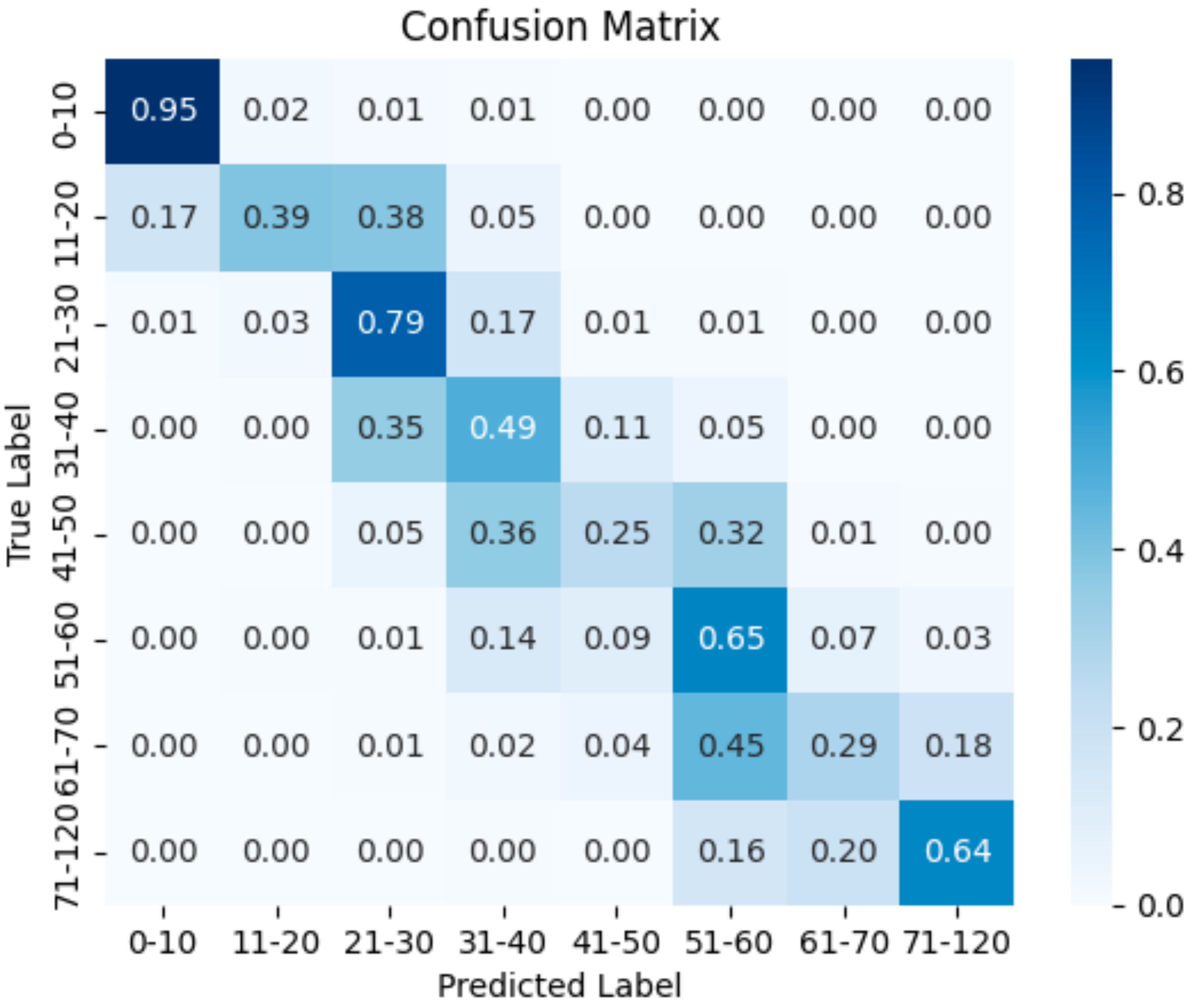


Confusion Matrix

Gender

Race

Age

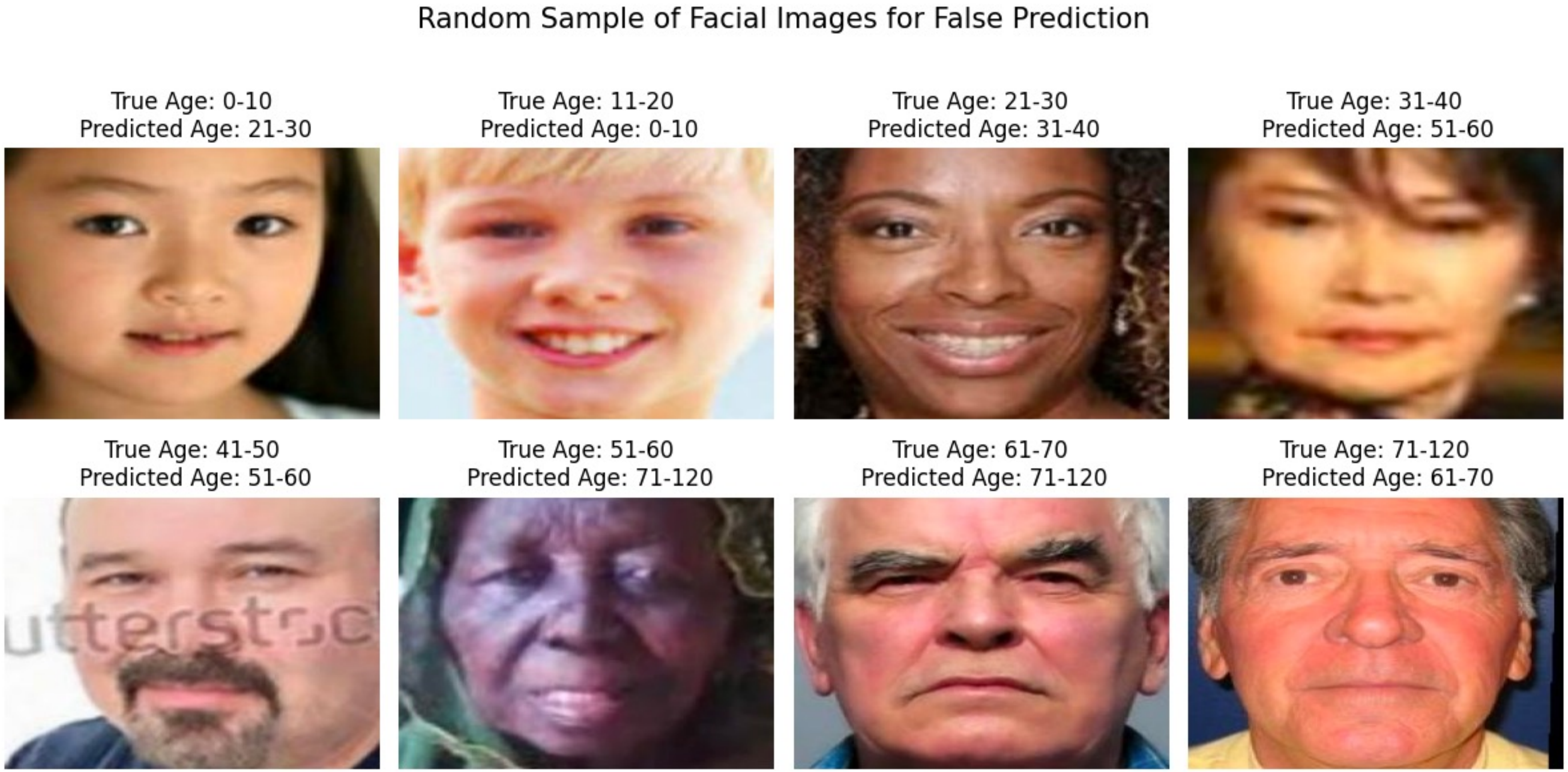


*% over total True Label

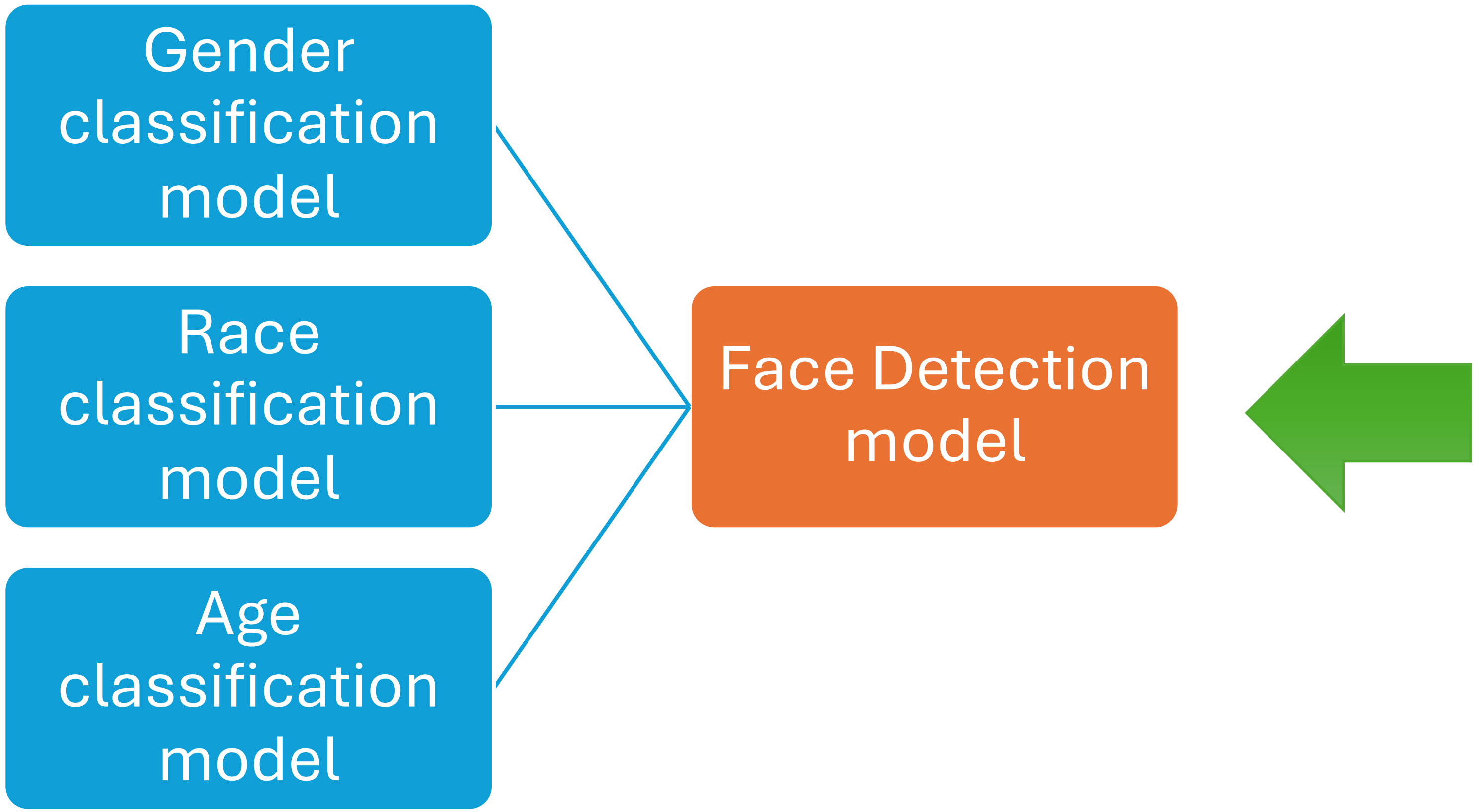
Samples of True Prediction

Random Sample of Facial Images for True Prediction

Samples of False Prediction

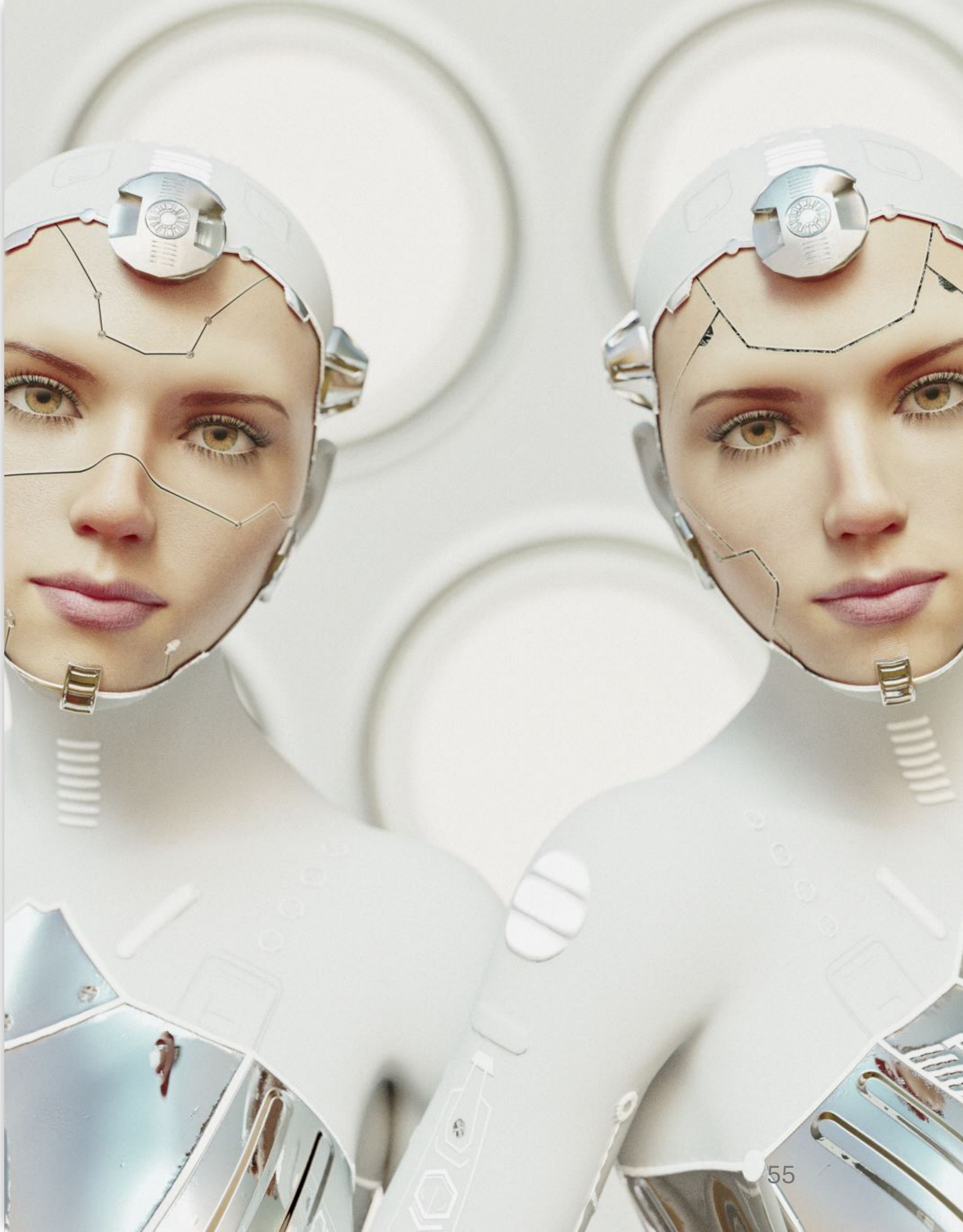


Machine learning models

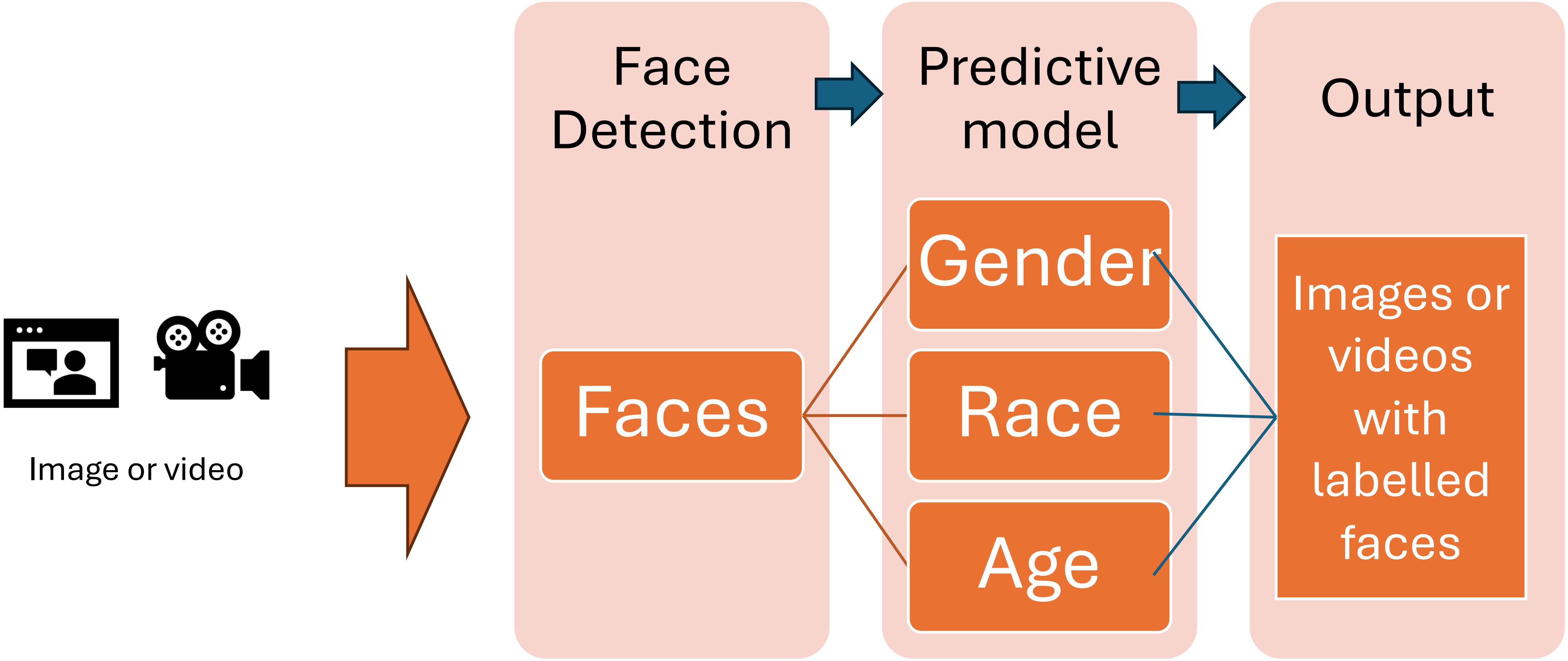


Face Detection model

- MTCNN is a powerful tool for finding faces in images and videos. It's accurate, fast, and works well even in challenging conditions. This makes it a popular choice for tasks like facial recognition, image annotation, and emotion detection in videos.



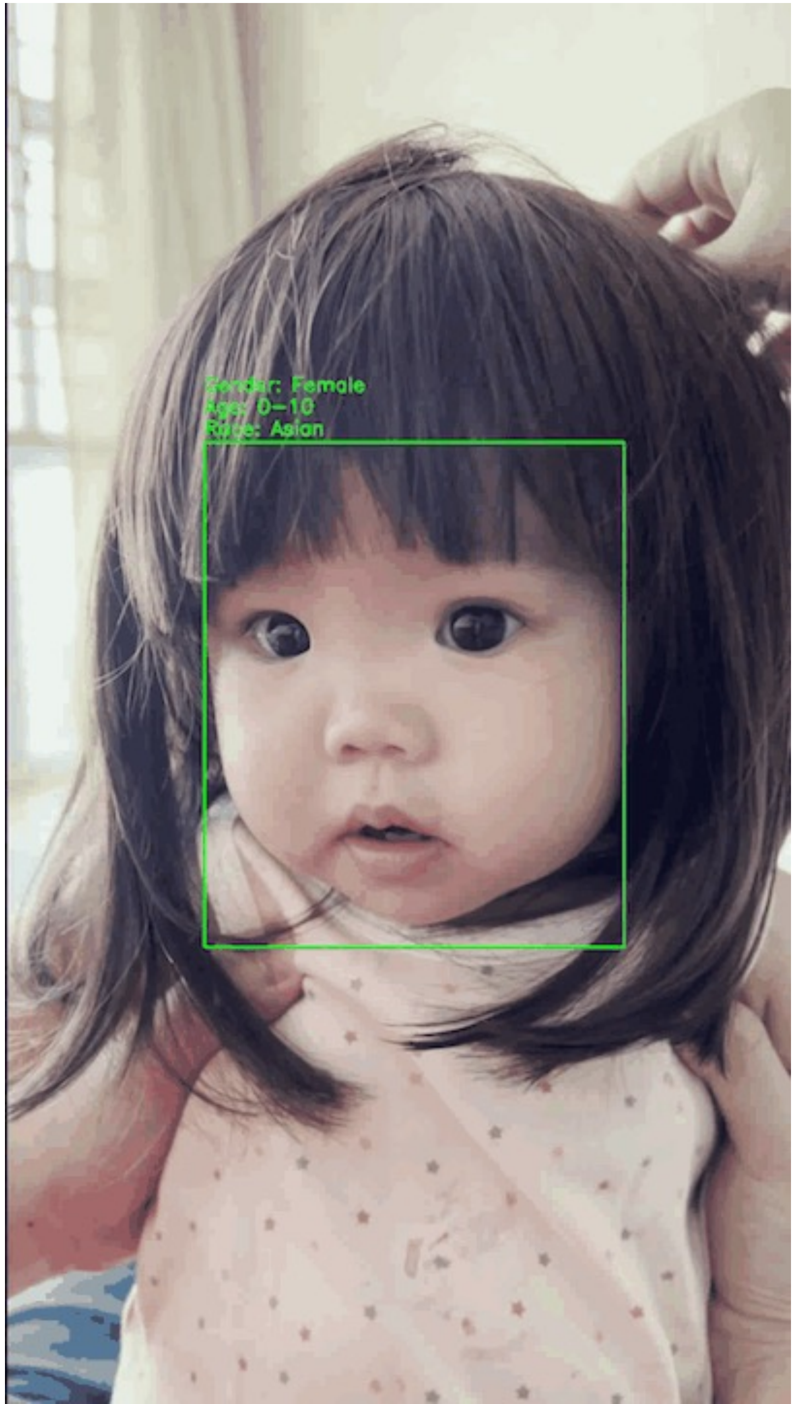
Face Detection model



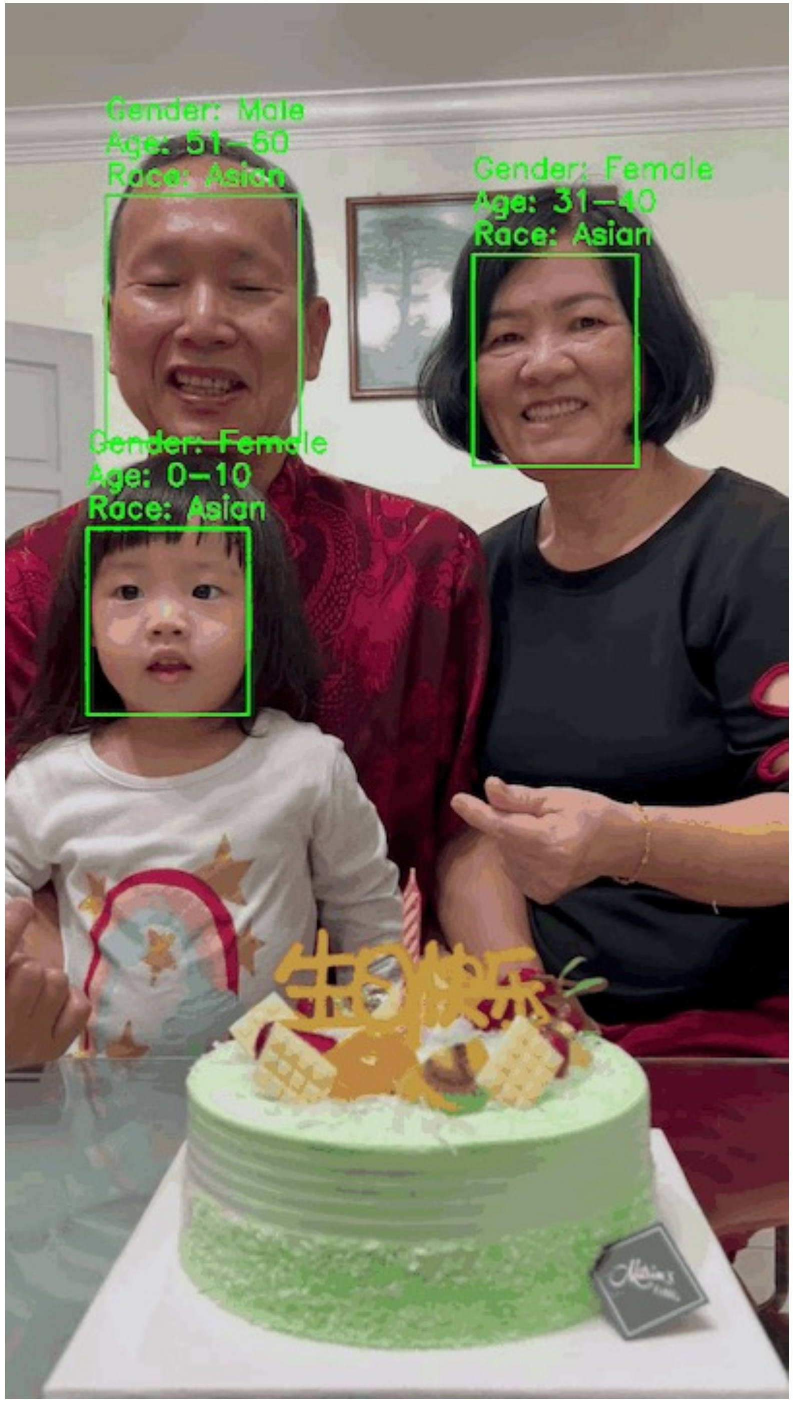
Face Detection on a single-face **image**

Face Detection on a multiple-faces **image**

Face Detection on a single-face **video**

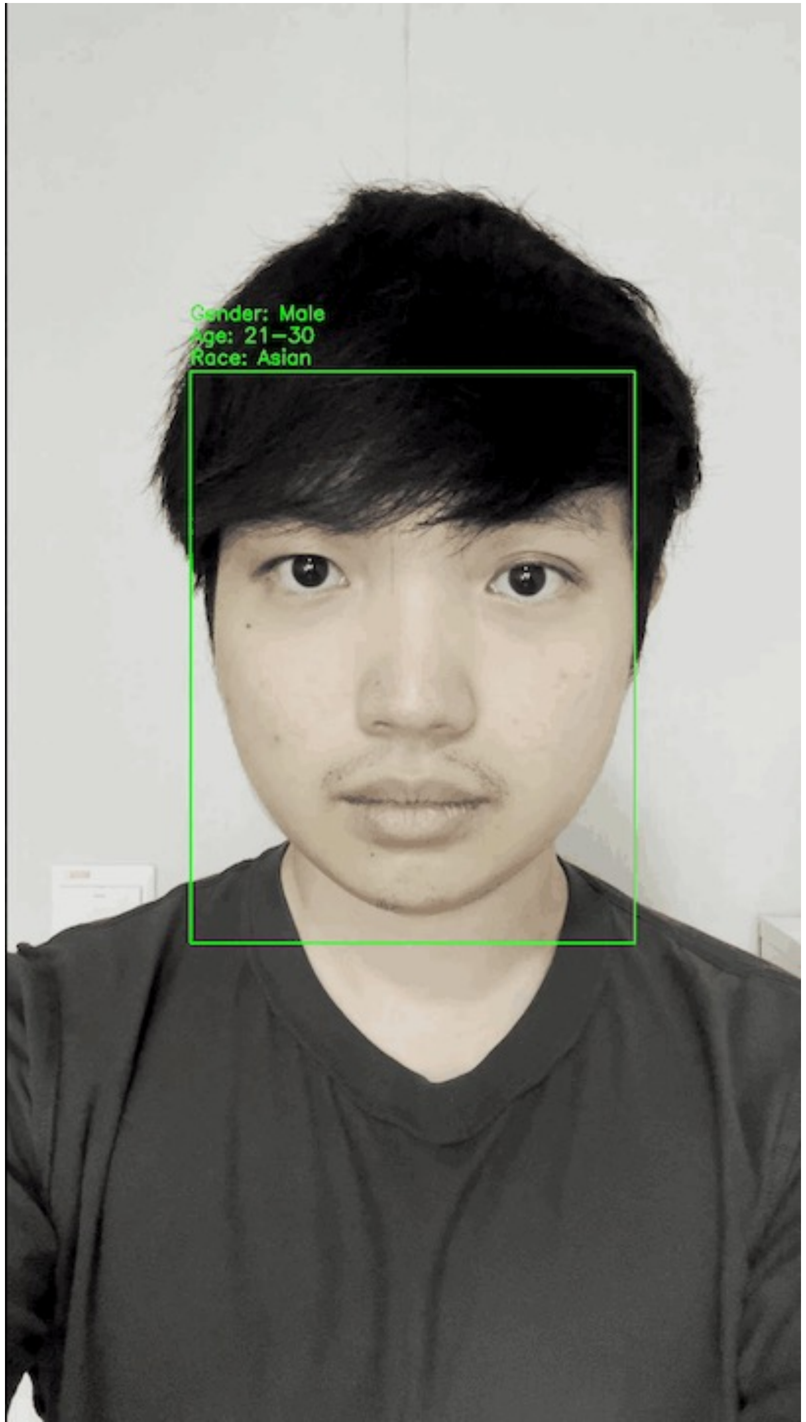


Face Detection on a multiple-faces **video**

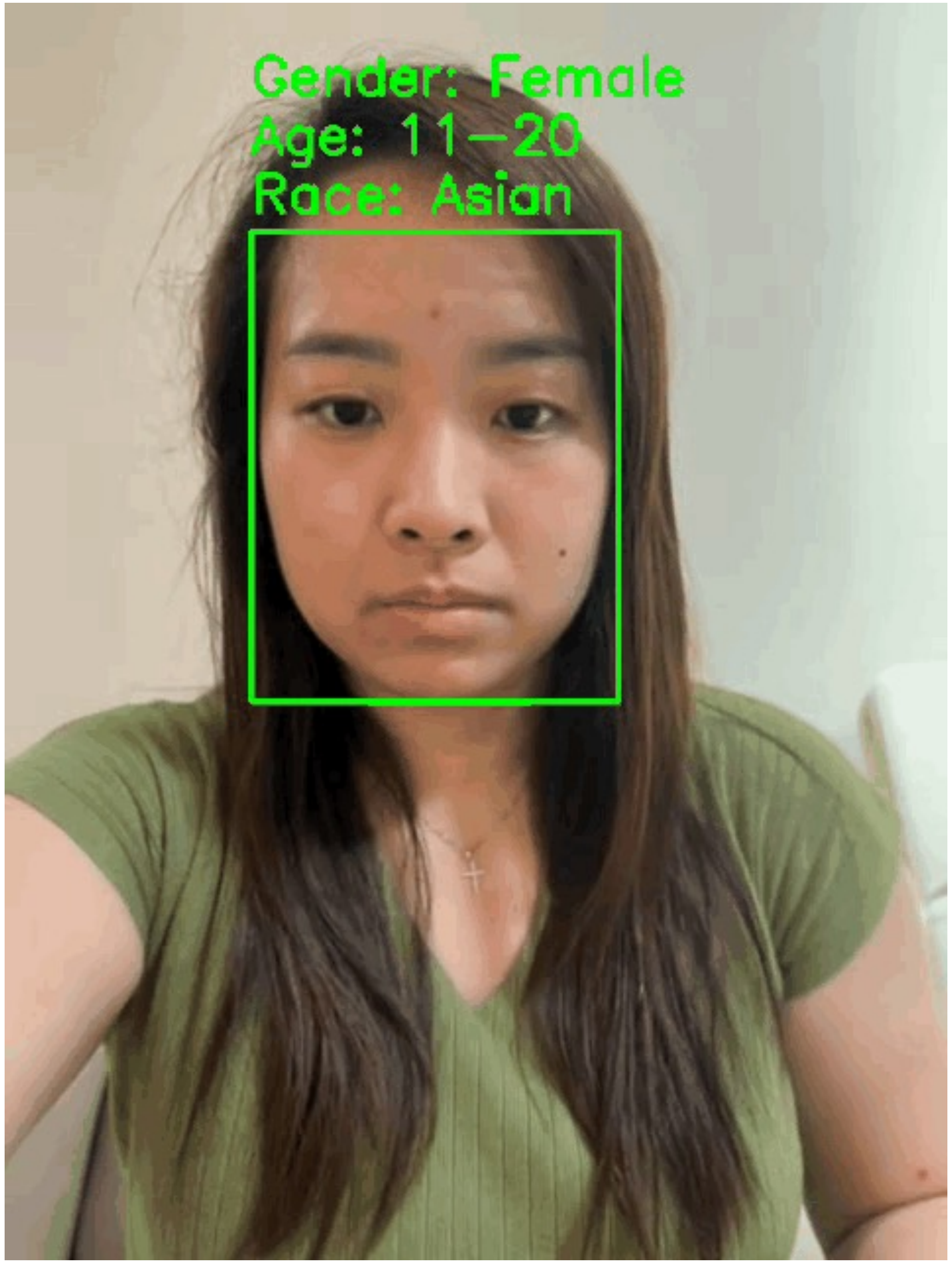


Demo – Face detection on ATM customers

Video 1

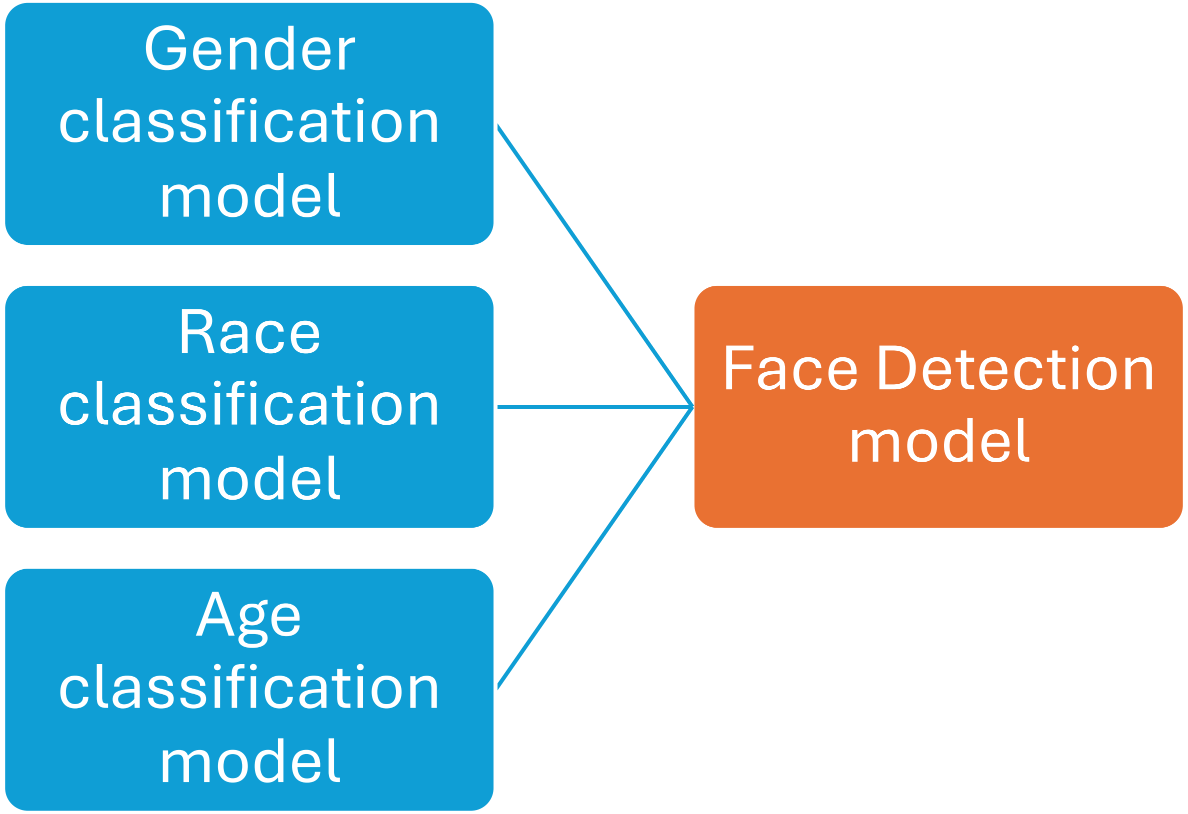


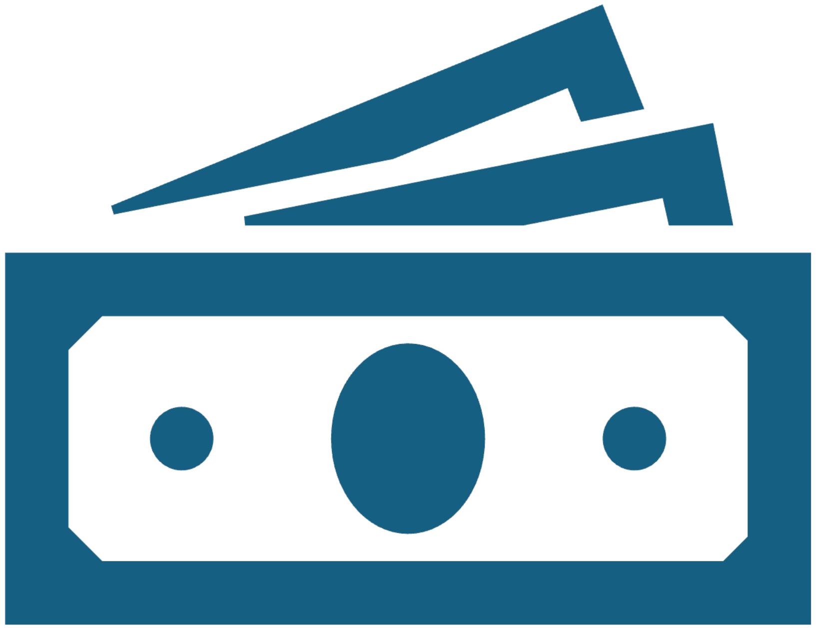
Video 2



Live demo

Machine learning models





Cost and benefit analysis

Costs to be incurred

Development cost

Personnel costs for data scientists and engineers.

Computational resources for training.

Implementation cost

Integration into existing ATM systems

Costs of installing camera or any related hardware onto ATMs

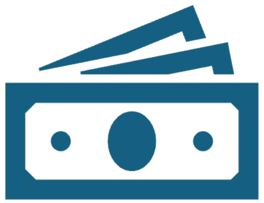
Maintenance

Regular face model updates to ensure accuracy with new data.

Benefits to be realized:

Increased customer trust

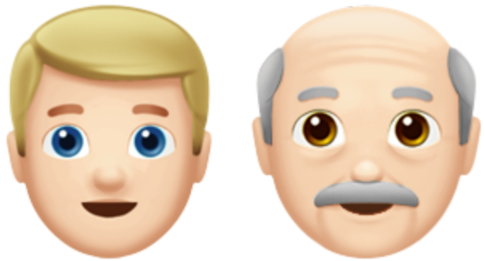
Compliance with regulations



Prevention of financial loss

Limitation of the models

1. Age model
   - The model has limited accuracy (0.6) when trying to determine age from facial features.
   - This is because judging age from appearance alone is difficult and subjective, as people can look much younger or older than their actual age.



Limitation of the models

2. Gender and Race model
   - ➢ Despite good performance in gender and race prediction, the model might be inaccurate due to limitations of facial features.
   - ➢ Just like age, appearance can vary significantly from a person's actual gender and race.

Limitation of the models

3. Face Detection model
   - The model cannot detect faces with face masks on.

What’s next?

- Appearance demographic
  - Due to the difference between appearance and actual demographics, banks might need to store additional data about a customer's perceived appearance.
  - In cases like a 30-year-old customer consistently appearing like a 20-year-old, the system should adapt to recognize their "appearance age".
  - This solves the problem of profiles mismatching a customer's visual presentation.
- Banks may consider mandatory mask removal for cash withdrawals at ATMs.
- Consider finding additional datasets to balance the training data for age and race.

Conclusion

- The models effectively tackle the problem statement by enhancing ATM security.
- The models improve ATM security by using face detection to flag suspicious withdrawals where the person doesn't match the cardholder. This builds customer trust in the bank's ATMs.

Q&A

Thank you!