AMERICAN EXPRESS

hackerearth

×

Makeathon 2023

A HACKATHON FOR **WOMEN**

Idea Submission →

Pranjal Agarwal

Team Name

SleepyCoder ..zzz

Team Member

Pranjal Agarwal agarwalpranjal813@gmail.com /PranjalAgarwal04

Theme

Facial Recognition for Transactions and OTP

Problem Statement

To build a solution that uses facial recognition for approving digital transaction which is secure and also supports user privacy and confidentiality.
A system that balances the need for security with the user's convenience and privacy while ensuring the technology's accuracy and reliability.

Tasks

- To develop a working training model
- To design a detection and recognition system
- To deploy the project on Github

Solution

The solution provides a robust, secure web application for authenticating digital transactions using facial recognition.

I present to you,

FacePay, a web application that authenticates digital transactions using facial recognition. It uses Siamese Neural Network to perform facial recognition.

Current Issues

91.29 billion digital transactions have been carried out in the financial year 2022-23 in India. This adds up-to Rs. 2,050 trillion worth of money.
With growing digital payments, frauds are also on the rise. Around 80,000 frauds worth Rs 2 billion are committed through UPI every month, with 50% of financial frauds committed on UPI alone through various mechanisms like luring customer to making payment to unauthorized QR or gaining confidence to install malware and making the customer use the unauthorized app.
The currently used digital authentication methods are SMS - OTP or PIN, which have disadvantages like:

- risks of data breaches due to weak PINS
- low level of security for a second factor authentication method
- unsecure to Open Networks
- system must be capable of memorizing codes and password

Source: pib.gov.in
Source: economictimes.com

Technology Stack

Python - It is used to build the facial recognition Siamese Neural Network model.

OpenCV - It used to capture images of the subject in real-time to form the dataset.

Tensorflow - It is used to build the model and train it based on the dataset.

Kivy - It is used to build a python app to run and test the model in real-time.

Reactjs - It is used to build the frontend of the web application, where people will perform transaction and authenticate themselves using facial recognition.

Firebase - It is used to store all the user data, authenticate user.

Bootstrap - It is used to create the UI/UX of the web app.

Javascript - It is used to write the complete frontend.

Implementation

- The web app allows users to save their images in the database.
- While the transaction is being processed, the app prompts user to authorize the transaction using facial recognition.
- The app fetches images of user from the database and the current image from the webcam and feeds them into the neural network.
- The model compares the embeddings of the images and verifies the user

Scalability

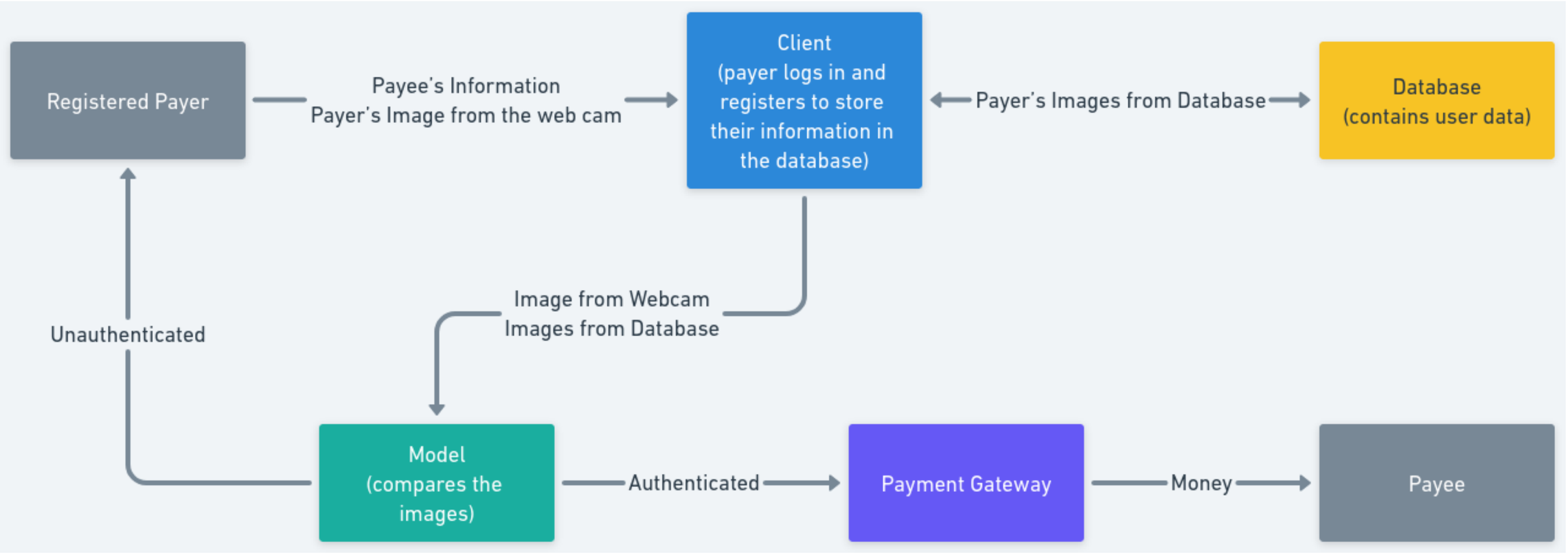
The app is built using the latest technology and is therefore highly scalable.

Usability

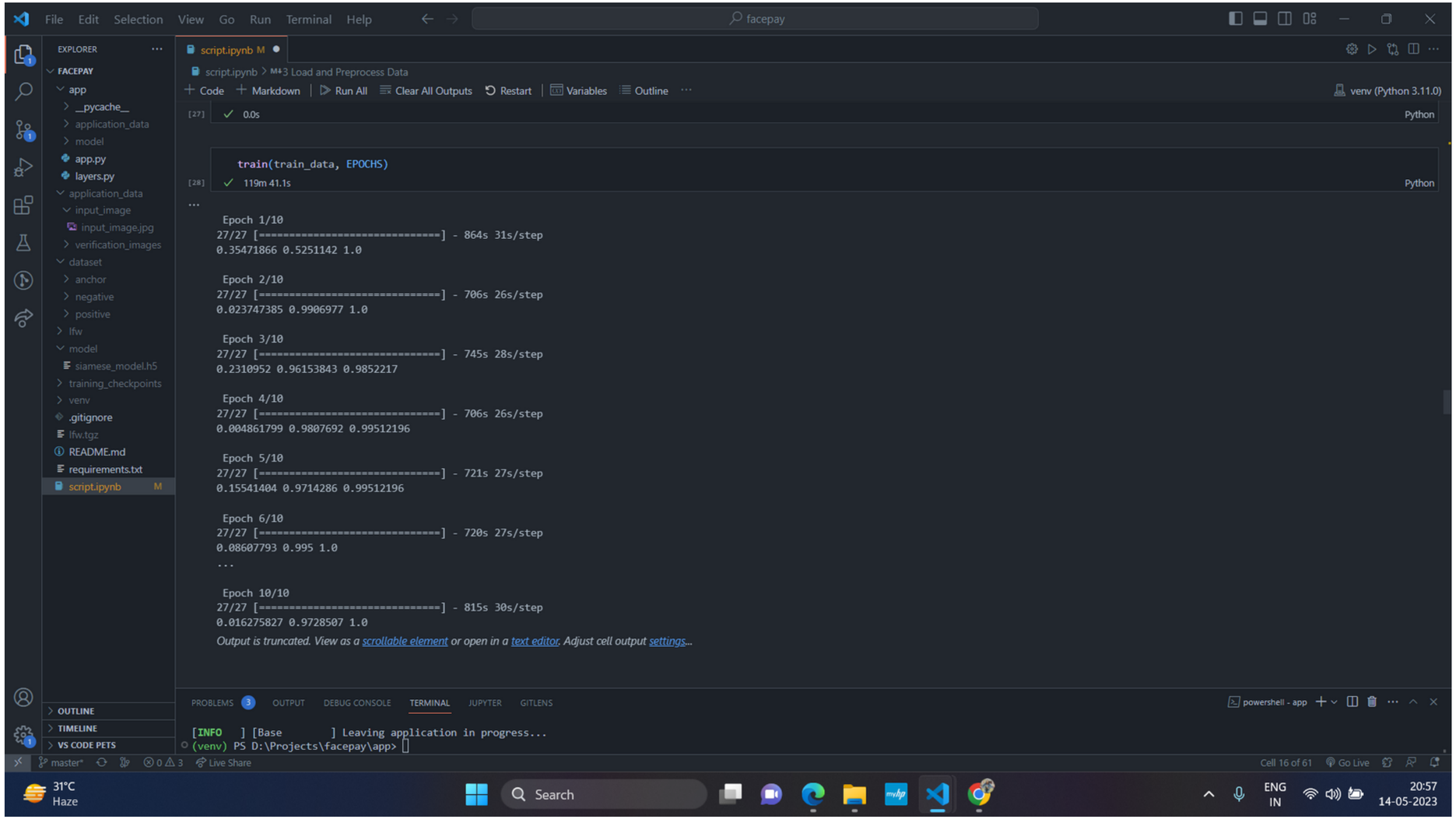
The app can be easily integrated with the existing businesses.

Flow Chart

hackerearth



Model Training Metrics



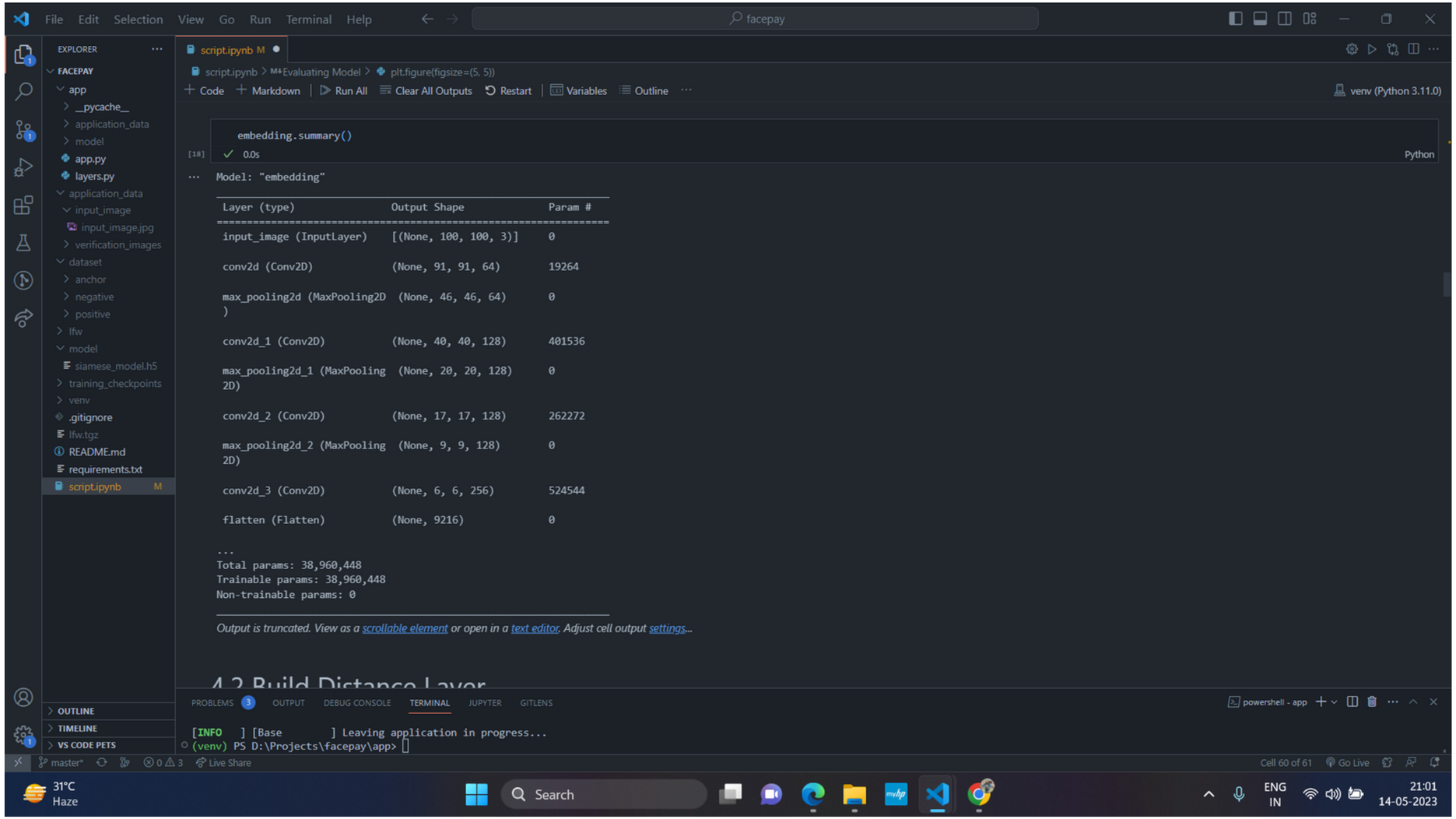
EPOCHS: **10**

Images Trained: **300**

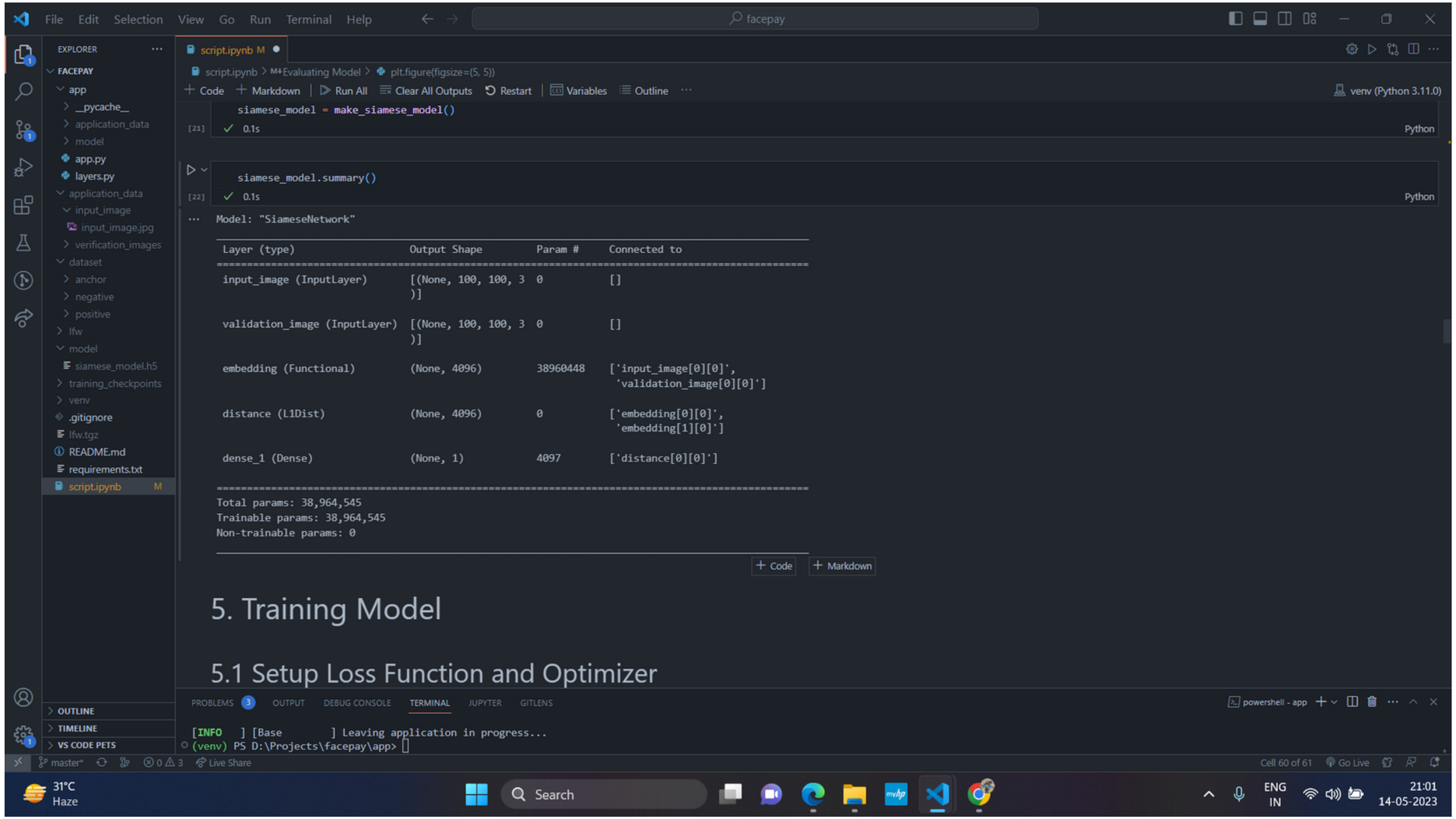
Loss: **0.016**

Accuracy: **97%**

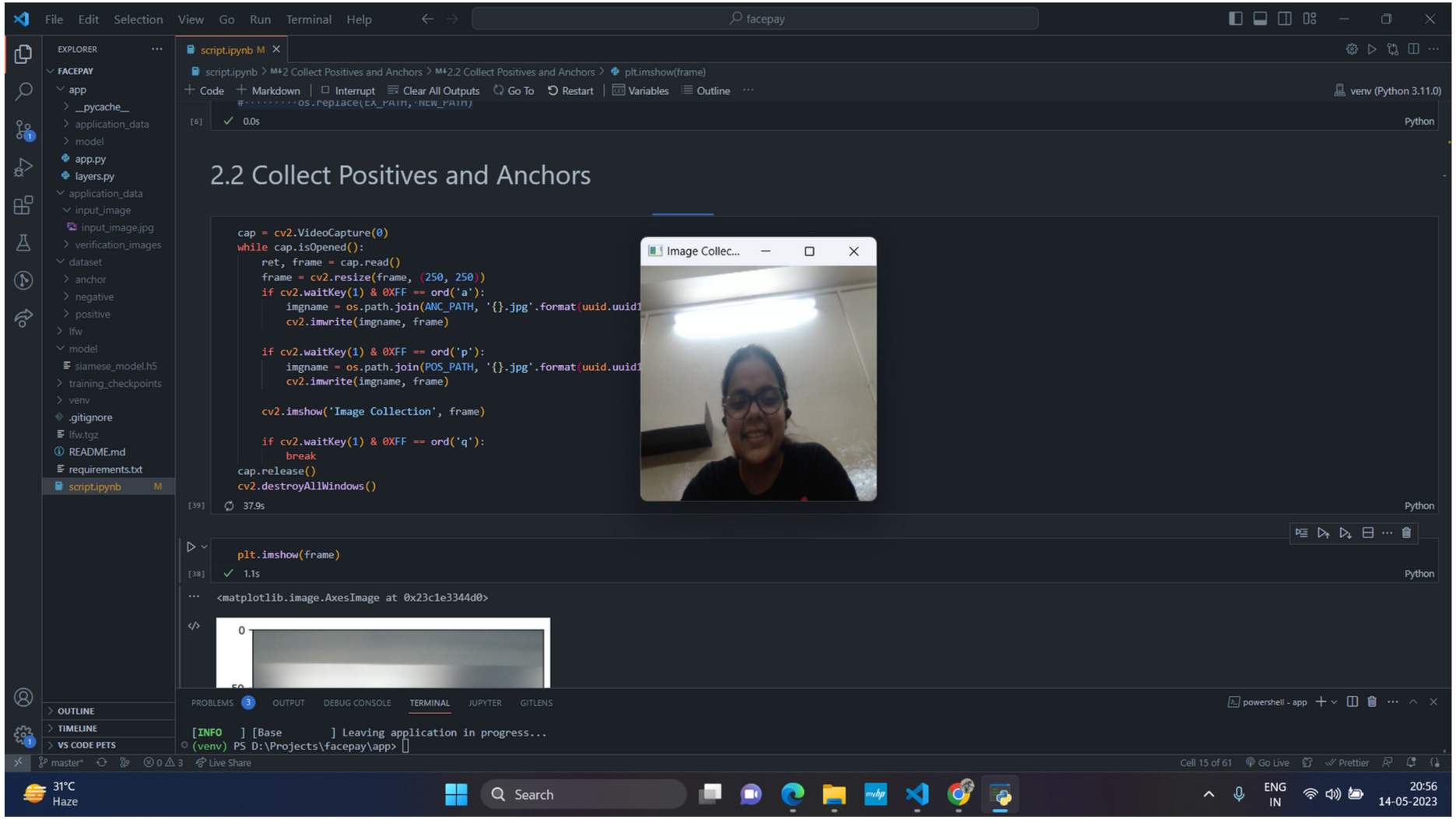
Embedding Summary



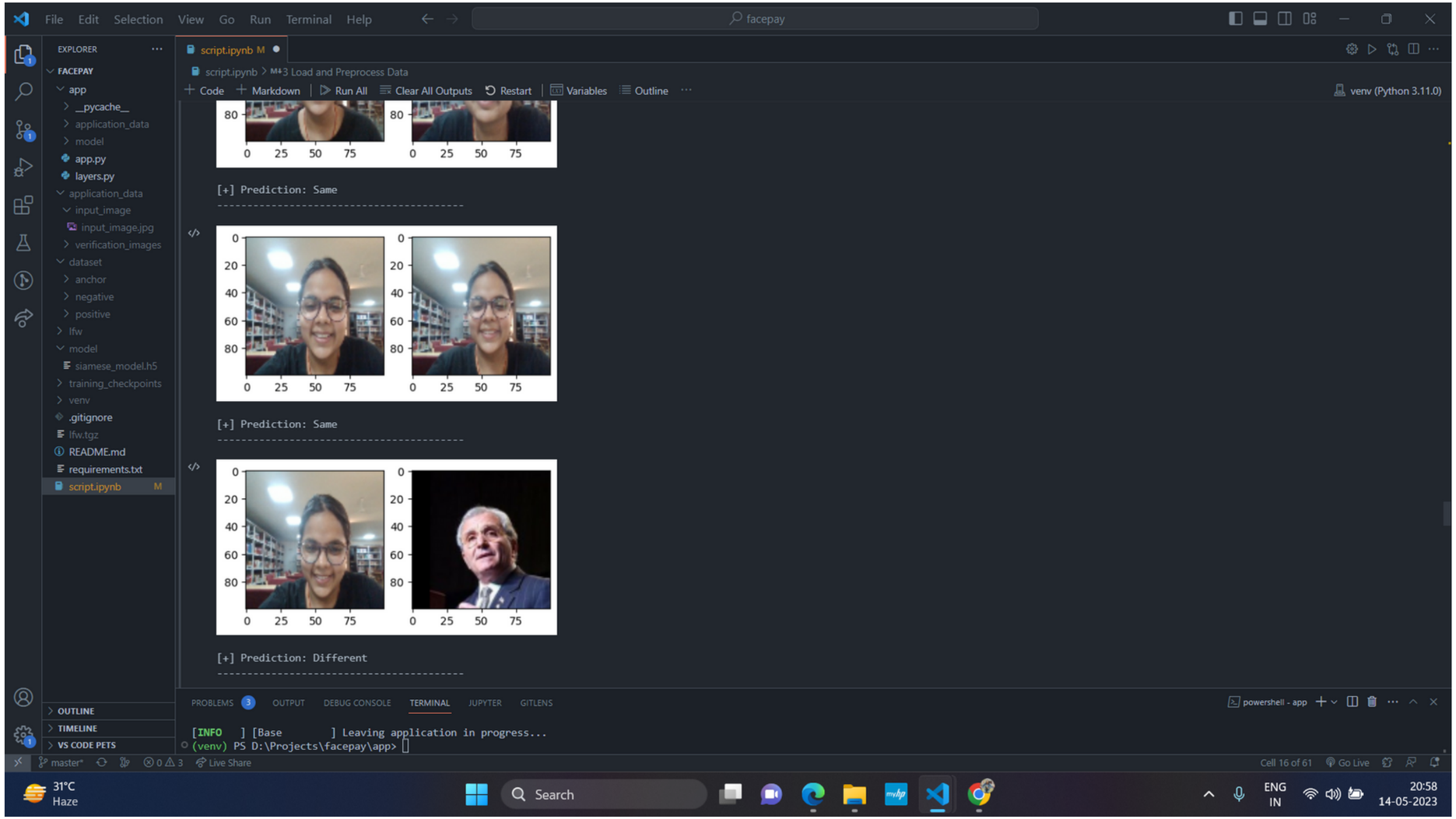
Model Summary



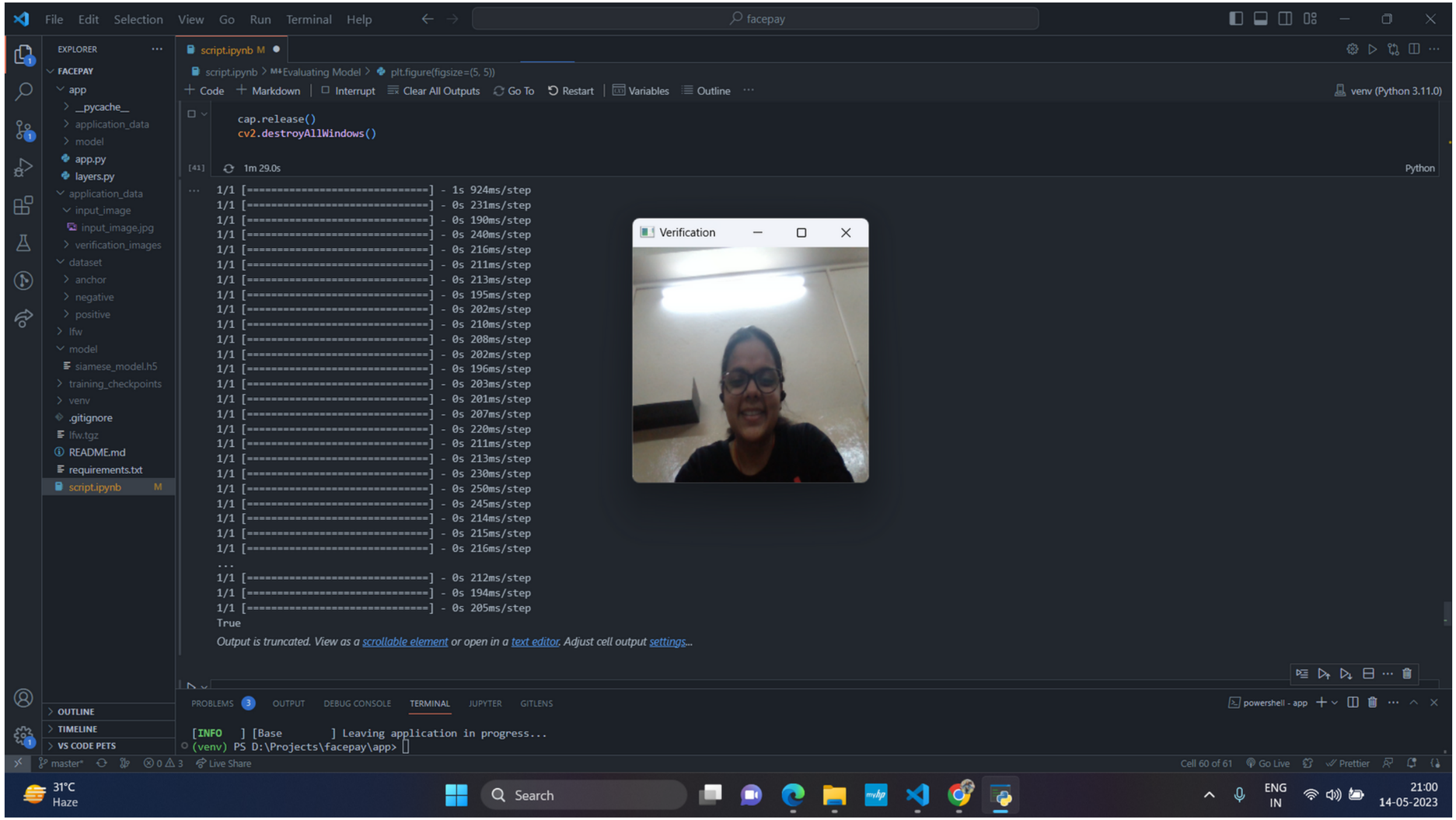
Creating Dataset



Results of the Comparison

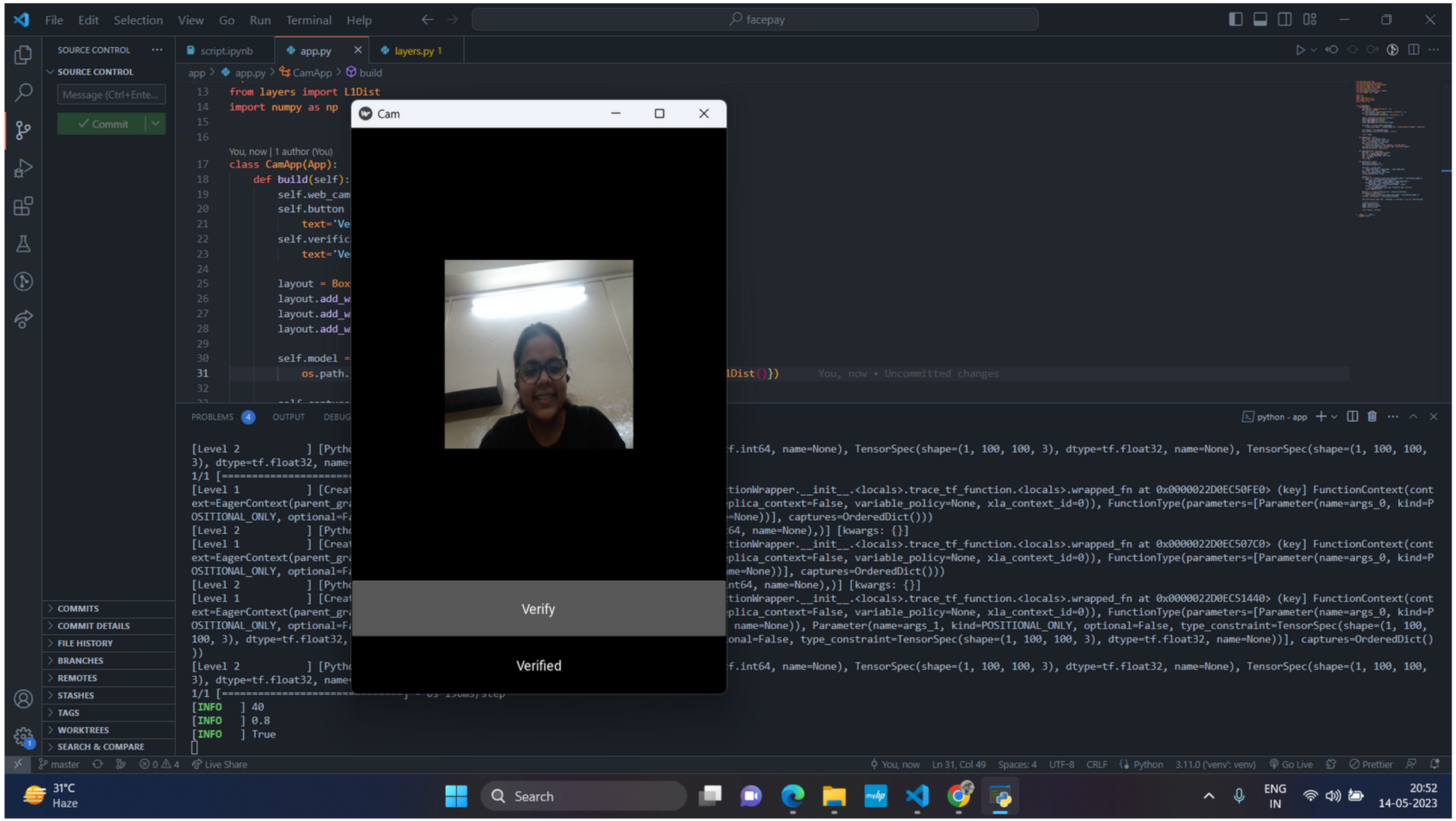


Model Output



Comapred one Input image with 50 test images and the model successfully recognized the person.

Kivy App Output



Successfully verified the user!

Societal Impact

hackerearth

1. Enhanced Security: Facial recognition technology can provide an additional layer of security to digital transactions by verifying the identity of the user based on their facial features. This can help prevent unauthorized access and fraudulent activities, improving the overall security of digital transactions.
2. Convenience and Efficiency: By using facial recognition for authorization, users may experience a more streamlined and convenient digital transaction process. It eliminates the need for traditional methods such as passwords or PINs, saving time and effort for users.
3. Privacy Concerns: Facial recognition technology raises privacy concerns as it involves capturing, storing, and analyzing personal biometric data. Users may worry about the potential misuse or unauthorized access to their facial data, leading to privacy breaches or identity theft. Hence, the web app has robust security measures and comply with relevant privacy regulations to address these concerns.
4. Improved User Experience: Facial recognition technology can enhance the user experience by providing a seamless and intuitive authentication process. Users no longer need to remember complex passwords or carry physical tokens, making transactions quicker and more convenient.
5. Enhanced Trust and Confidence: The use of facial recognition can help build trust and confidence among users, knowing that their transactions are secured using advanced biometric technology. This can encourage more users to adopt digital transactions, leading to increased participation in the digital economy.

Future Scope

1. Expansion to Various Industries: The app can expand its reach beyond specific sectors, such as banking or e-commerce, to other industries that involve digital transactions. This can include sectors like healthcare, travel, hospitality, and more. Each industry may have unique requirements and challenges, presenting opportunities to tailor the app's features and functionalities accordingly.
2. Integration with Mobile Devices: As facial recognition technology becomes increasingly integrated into mobile devices, the app can leverage this trend. Integration with smartphones and tablets can enable secure and convenient digital transactions directly from mobile devices, enhancing user experience and accessibility.
3. Advanced Authentication Methods: The app can explore additional biometric authentication methods alongside facial recognition, such as fingerprint or voice recognition. Multi-modal biometrics can provide even stronger security and authentication accuracy, further enhancing the reliability and trustworthiness of the app.
4. Continual Improvements in Accuracy and Speed: Facial recognition algorithms are continually evolving, with advancements in machine learning and computer vision techniques. The app can leverage these advancements to improve the accuracy and speed of facial recognition, enhancing the overall user experience and reducing false positives or negatives.

hackerearth

https://github.com/PranjalAgarwal04/facepay

Makeathon 2023