VIETNAM GENERAL CONFEDERATION OF LABOR
TON DUC THANG UNIVERSITY
FACULTY OF INFORMATION TECHNOLOGY

FINAL REPORT

INTRODUCTION TO INFORMATION SECURITY

Instructor: **HUYNH NGOC TU**

Executor: **VO NHAT HAO – 522H0090**

PHAM VAN PHUC – 522H0068

NGUYEN THANH NHAN – 522H0051

Class **: 22H50202**

Course **: 26**

HO CHI MINH CITY , YEAR 2024

VIETNAM GENERAL CONFEDERATION OF LABOR
TON DUC THANG UNIVERSITY
FACULTY OF INFORMATION TECHNOLOGY

FINAL REPORT

INTRODUCTION TO INFORMATION SECURITY

Instructor: **HUYNH NGOC TU**

Executor: **VO NHAT HAO – 522H0090**

PHAM VAN PHUC – 522H0068

NGUYEN THANH NHAN – 522H0051

Class **: 22H50202**

Course **: 26**

HO CHI MINH CITY, YEAR 2024

THANK YOU

- We are deeply grateful to Ms. Huynh Ngoc Tu for her constant support and enthusiastic direction throughout our investigation and final report.
- We also like to thank Ton Duc Thang University's Faculty of Information Technology for providing us with an enriching academic environment. The faculty's willingness to share vital expertise and reference materials has not only aided our research endeavor, but has also improved our overall educational experience at the university.
- As we wrap up our study project, we reflect on the vital lessons and insights learned from our educators. Regardless of our limitations and areas for improvement, we are willing to learn and grow. We really seek further assistance to improve our work and appreciate the critical input from our professors and classmates. With their continuous assistance, we are determined to improve our research talents in future initiatives.
- We wish all of our teachers and friends ongoing health and happiness, as their support and care have been invaluable to us on our path.

WE THANK YOU!

THE PROJECT IS COMPLETED
AT TON DUC THANG UNIVERSITY

I hereby declare that this is my own project product and is guided by Ms. Huynh Ngoc Tu. The research content and results in this topic are honest and have not been published in any form before. The data in the tables for analysis, comments, and evaluation were collected by the author from different sources and clearly stated in the reference section.

In addition, the project also uses a number of comments, assessments as well as data from other authors and other organizations, all with citations and source notes.

If any fraud is discovered, I will take full responsibility for the content of my project. Ton Duc Thang University is not involved in copyright violations caused by me during the implementation process (if any).

Ho Chi Minh City, 20 May 2024

Author

(sign and write full name)

Vo Nhat Hao

Pham Van Phuc

Nguyen Thanh Nhan

INSTRUCTOR VERIFICATION AND EVALUATION SECTION

Confirmation from the instructor

_____

_____

_____

_____

_____

_____

Ho Chi Minh City, day month year

(sign and write full name)

The teacher's evaluation part marks the test

_____

_____

_____

_____

_____

_____

Ho Chi Minh City, day month year

(sign and write full name)

TABLE OF CONTENTS

CHAPTER – 1: SECURITY SCENARIOS

❖ Website Security Script Using Face Authentication Context: The web uses facial authentication to ensure user safety when logging in and accessing services. The scenario below describes the process of users registering and logging in using face authentication.

- **New user registration page:**

- Goal: Allow new users to sign up for an account and set up face authentication.
- Step 1: Enter personal information The user visits the registration page. They fill in personal information fields such as full name, email, password.
- Step 2: Register your face After filling in the personal information, the user will be redirected to the face registration section. They click on the "Register face" button, the system will activate the camera to capture the face and take 5 times then the user presses the save button.

- **Abbreviate**

- The above script provides two main parts: registration and facial login. Users need to take a picture of their face to register and then can use their face to log into the system. The steps include using the camera to take pictures and sending the image data to the server for processing.

CHAPTER – 2: TECHNOLOGY USED

- **OpenCV (OpenCV Library):**

- OpenCV, which stands for Open Source Computer Vision, is considered one of the leading open source libraries for real-time image processing.
- First officially launched in 1999, OpenCV is a free and open source library for both academic and commercial use.
- OpenCV supports multiple platforms including Windows, Linux, Mac OS, iOS and Android.
- OpenCV supports C/C++, Python and Java programming languages.
- OpenCV is written in C/C++ and integrates OpenCL. The library has more than 2500 optimized algorithms.

- **Dlib:**

- Dlib is a modern C++ toolkit containing machine learning algorithms and tools for creating complex software in C++ to solve real-world problems. It is used in both industry and academia in many fields including robotics, embedded devices, mobile phones and large high-performance computing environments. Dlib's open-source license allows you to use it in any application for free.
- Dlib is a program of the OpenCV library, which assists users in identifying faces. The algorithm that Dlib uses is HOG (Histogram of Oriented Gradients) and SVM (Support Vector Machine), which is why Dlib has a very small runtime and can be used in real-time systems. More recently, however, Dlib has also provided additional CNN-based face-recognition functions.

- **Flask:**

- What is Flask Python?
- Flask is a micro web framework written in Python. "Micro" means that Flask does not require any additional third-party tools or libraries to work. This makes the

framework flexible and easy to get started with while ensuring it provides enough features to build web applications from small projects to more complex systems.

- Flask offers basic features such as URL routing, user interface creation, request handling, and HTTP responses. In addition, it also supports extended features through Flask extensions libraries to add functions such as user authentication, database connections, session management, and many others.
- Python Flask was created and developed by Armin Ronacher when he was a student at the Technical University of the Bremen Institute, Germany. Flask was first released in 2010 and has become one of the most popular Python web frameworks ever since.
- In the context of face recognition, Flask can be used to create a web application that allows users to upload images and recognize faces from those images. This is a basic example of how to use Flask in conjunction with face_recognition facial recognition library in Python.

CHAPTER – 3: INSTALLATION STEPS

1. **Install dlib library:**

```
C:\Users\Admin>pip install dlib
```

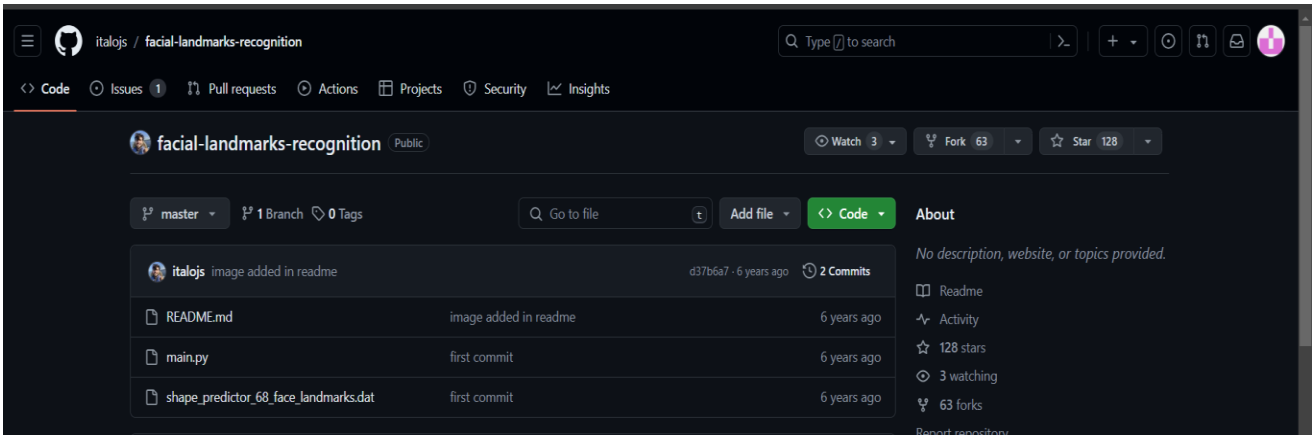
2. **Install OpenCV library:**

```
C:\Users\Admin>pip install opencv-python
```

3. **Install Flask:**

```
C:\Users\Admin>python -m pip install flask
```

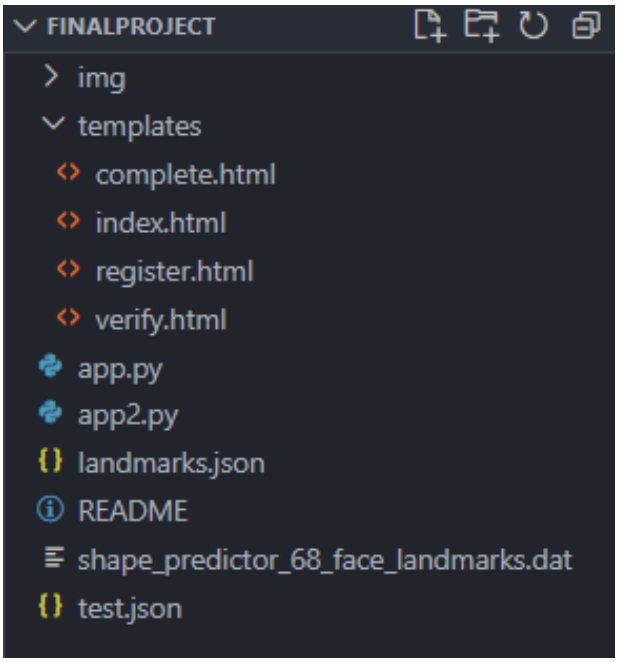
4. **Download file shape_predictor_68_face_landmarks.dat**



5. **Build source code**

   Details are provided in the accompanying source code zip file.

6. **Complete directory**

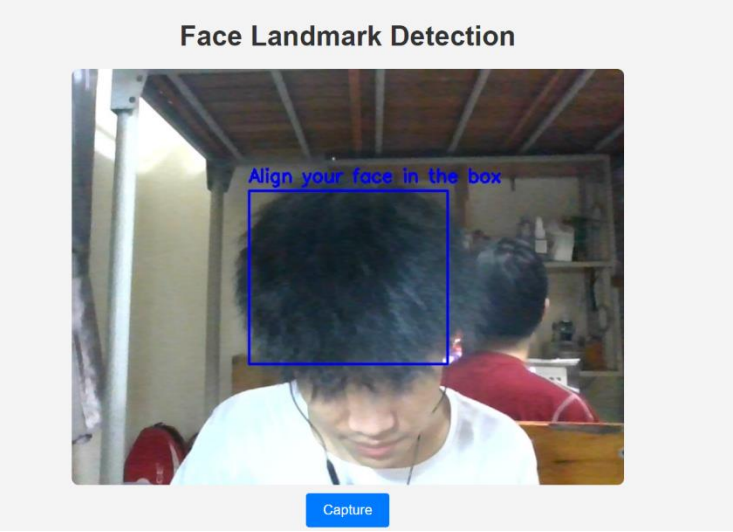

FINALPROJECT
img
templates
complete.html
index.html
register.html
verify.html
app.py
app2.py
landmarks.json
README
shape_predictor_68_face_landmarks.dat
test.json

CHAPTER – 4: INPUT, OUTPUT OF EACH STEP

Step 1: Registration

- **Face Scanning:**

- The system activates your device's camera to capture your face.
- A blue overlay (frame) appears on the screen, guiding you to position your face squarely within the frame. This ensures optimal image capture for accurate feature extraction.



- **Facial Feature Extraction:**

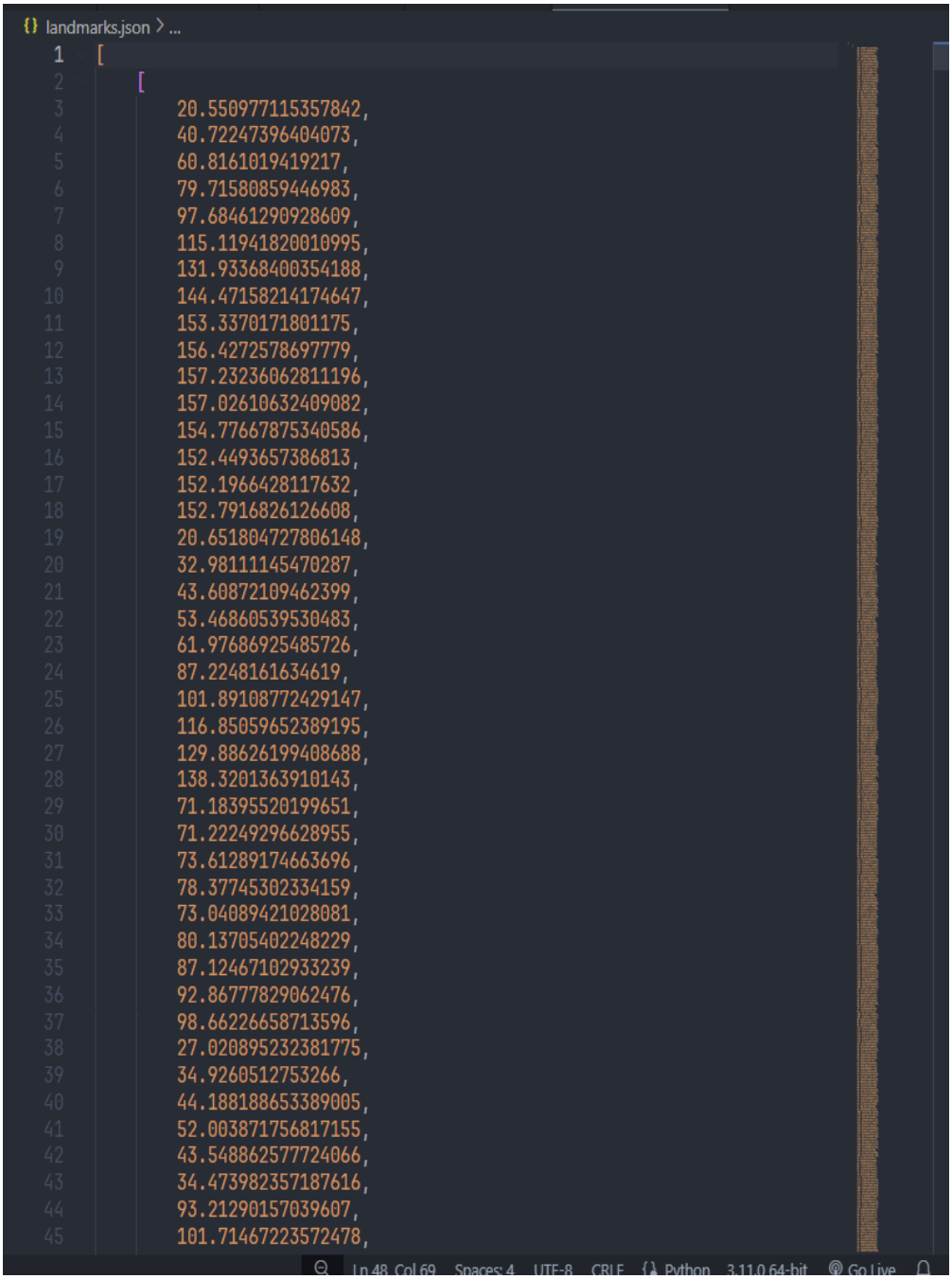
- The cv2 library (typically used for computer vision tasks in Python) efficiently detects your face in the captured image.
- The powerful dlib library comes into play to extract a set of key facial features (e.g., distance between your eyes, shape of your eyebrows, etc.). These features form a unique representation of your face.

Output :

Step 2: Calculating Average Distance

- The system calculates the average distances between various key facial features in the extracted data. This creates a single value that summarizes the overall geometry of your face.

Output:



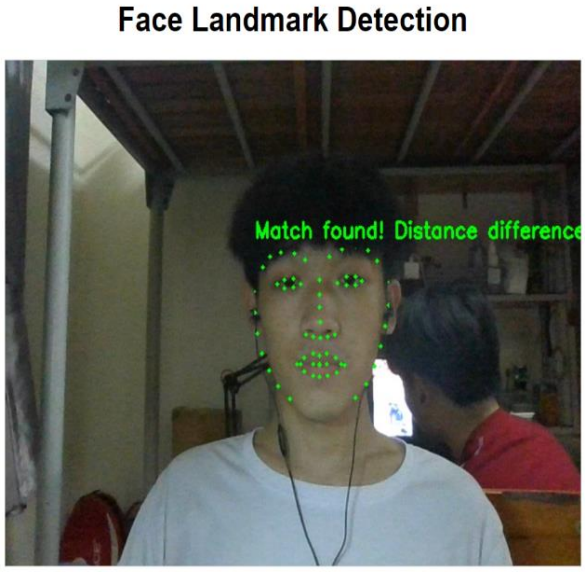
Step 3: Face Authentication

- **Face Scanning:**

- Similar to Step 1, the system scans your face using the camera.

- **Feature Extraction and Comparison:**

- The cv2 and dlib libraries are used once more to extract a new set of facial features from the captured image.
- The system compares the newly extracted features with the average distance value stored from your registration process (Step 2).
- After the process of testing and checking, we decided to set the benchmark for determining whether a match or a mismatch is 150.

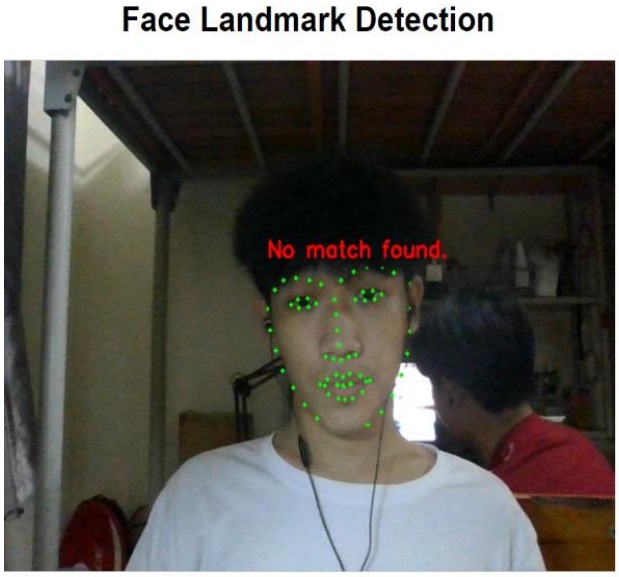


- **Authentication Success:**

- If the comparison reveals a close match (i.e., the average distances between features are similar), the system authenticates you and grants access (skips to the "complete page").

- **Authentication Failure:**

- If the comparison indicates a significant difference (i.e., the average distances deviate substantially), the system denies access, potentially prompting you to re-register or contact an administrator for assistance.



CHAPTER – 5: DEMO

CHAPTER – 6: EVALUATION AND CONCLUSION

❖ **Advantages:**

- Convenience: Quick and easy to use, no need to remember passwords or carry authentication devices.
- No contact: Reduces the risk of spreading bacteria and disease, especially useful during epidemics.
- High accuracy: Advanced facial recognition technology can achieve high accuracy, especially when used in combination with other biometric methods.
- Difficult to copy: Each person's face is unique and difficult to copy, increasing security compared to methods using passwords or cards.

❖ **Disadvantages:**

- Risk of data breach: Facial data is considered sensitive information, which if leaked can lead to serious consequences such as identity theft or fraud.
- Being fooled: Some facial recognition systems can be fooled using techniques such as using fake photos or videos.
- Privacy issues: Collecting and storing facial data can impact individual privacy.
- Cost: Implementing facial recognition systems can be expensive, especially for highly accurate systems.