FACE AND FINGERPRINT BASED PERSONIDENTIFICATIONSYSTEM

Mrs. Suchetha N V

Abstract

Biometric technologies are commonly used to upgrade the system security by allowing people to be recognized. It presents multimodal biometric system based on face and fingerprint biometric attributes. A camera is used to capture the pictures of the faces in the system. The fingerprint obtained from the fingerprint dataset is cross-checked once the input face is recognized to authenticate the identification. The characteristics of the fingerprint and face are retrieved using CNN approach.

Chapter 1

Introduction

1.1 Project Introduction

The use of various biometric indicators by personal identification systems to identify individuals is known as multimodal biometric. A face recognition system is a piece of software that can recognize a human face in a digital image. It's used to verify user's identities through ID verification services. One of the simplest ways to tell who someone is by looking at their face. It's not easy because there are so many variables in image appearance, such as stance, occlusion, image orientation, lighting condition, and face. One of the most significant applications of biometric technology is fingerprint identification. It is thought that each person's fingerprint is distinct from each of their fingers. Even identical twins who share DNA are thought to have unique fingerprints. Biometrics refers to the process of verifying a person's identity through the use of a physical or behavioural feature. Physical characteristics such as fingerprints, face, iris,and so on are based on inborn and stable physical qualities. For each of these biometric traits, unimodal biometric systems may fall short of the needed performance. The methodologies are broken down in order to combine the various elements into a multimodal biometric system.

1.2 Problem Description

A stolen biometric might do greater damage than a stolen credit card number because it discloses a portion of the user's identity and can be used to fabricate legal papers, passports, or criminal histories. Some of the issues with using biometrics include biometric enrollment security, data and network hacking, swiftly evolving fraud capabilities, familiar fraud (i.e., fraud perpetrated by a family member or acquaintance), deceived sensors, and sensor in accuracy. Data security is one of the biggest threats. There are two types of mistakes that biometric devices can make: the false accept, where the device mistakenly admits an unauthorized individual, and the false reject, where the device mistakenly rejects an authorized person. The accuracy of identification in multimodal biometric systems is anticipated to increase.

Chapter2

Literature Review

1.1 General Introduction

Literature Survey is an important activity, which we have to do while gathering information about a particular topic. It will help us to get required information or ideas to do work. The following paragraphs discuss the related work and issues in the area Prediction and Analysis of face and fingerprint based person identification system using machine learning algorithm.

1.2 Literature Survey

In the paper titled “Human Face Recognition using LBPH” [1], the authors Stitiprajna Panda, Swati Sucharita Barik have proposed new approach in Human Face Recognition. Initially they experimented with several datasets from the UCI library and Kaggle. They took tailored datasets later. They achieved an average accuracy level of 77 percent during training and assessment. When streaming video, they've also added a time module that allows you to verify the date and time.

In the paper titled "Face Recognition Based Attendance Marking System"[2], the authors Senthamil Selvi, Chitrakala, Antony Jenitha have proposed new approach in Face Recognition Based Attendance Marking System. The year 2014 is predicated on the discovery of facial recognition as a solution to the prior attendance system's problems. This system uses a camera to capture the photos of employees in order to do facial recognition. When a match is identified in the face database, the captured image is compared one by one to the face database to locate the labourer’s face, and presence is reported. The key benefit of this approach is that attendance is recorded on a robust security server, and no one else can view other people's attendance.

In the paper titled "RFID-based Student Attendance System" [3], the authors Hussain, Dugar, Deka, Hannan have proposed approach which is substantially identical to the first research article where RFID technology was utilized to improve the previous attendance system in 2014. In this arrangement, once again, a label and a scanner are used to track the student’s attendance. The difference between the first and this journals is that this one allows you to access attendance information via a web portal. It makes retrieving information more convenient.

In the paper titled “Human authentication systems”[4],the authors Fateme Saadat, Mehdi Nasr have proposed human authentication systems, biometric and multi biometric sciences play a significant role. Because of its invariability and lack of stealth, finger vein patterns are one of the most dependable and secure biometrics. The score level fusion of three different finger vein patterns is proposed in this research using a heuristic method.

In the paper titled "Fingerprint Recognition Using Robust Local Features," [5], the authors Madhuri and Richa Mishr have proposed a work titled claiming that fingerprints are used in many existing human recognition systems. For the most part, these strategies rely on tiny points. Fingerprints are matched. Because these procedures aren't rotation invariant, they're useless. When a person's enrolled image is compared to a rotated test image, and when only a fragment of a fingerprint image is matched, such techniques fail. This paper author introduces a fingerprint recognition method. Fingerprint representation and matching strategy that makes use of local robust features.

In the paper titled “software-based counterfeit detection technique” [6], the authors Galbally have described a which can be used in various biometric systems to discover different kinds of fraudulent login attempts for enhancing biometric recognition frameworks protection by having aliveness assessment in a quick, user-friendly, and nonintrusive manner. Using publicly available fingerprint, iris, and facial data sets, the suggested technique was tested and reviewed [6].

In the paper titled "Fingerprint Identification Using Image Segmentation," [7], the authors Sangram Bana and Dr.Davinder Kaur have proposed a work titled Fingerprint Identification Using Image Segmentation which details the research and deployment of minutiae-based matching techniques in a fingerprint identification system. This approach entails collecting minutiae points from reference fingerprint photos and matching fingerprints depending on the number of minutiae pairs.

1.3 Comparative Analysis of the related work

Table1:Performance Comparison of Face and Fingerprint

Biometric	**Algorithm**	**Database**	**Performance**	**Advantages**	**Disadvantages**
Face	PCA[11]	AR-Faces	70	Reduces the Number of dimensions [11].	The ability to distinguish Between classes remains unchanged.
	LDA[11]	AR-Faces	88	Reduce the Number of dimensions Increase the Separation of classes [11].	
	Kernel associated Memory Models[12]	FERET ORL XM2VTS	91.6 98 84	The computational complexity is low [12].	Large storage area
	3D Morphable Model	Real-time(live faces)	97	Even with pose And lighting variations, the performance Was excellent. Handling noise better	The level of Complexity is great.
	Virtual Frontal-View Face [13]	MIT face database	84.7	Pose variations Can be dealt with more quickly. High Rate of success [13]	A little difficult
Fingerprint	**Author**	**Year**	**Method Used**	**Accuracy/ Performance**	**Benefits and Restrictions**
	Xiang Fuet al[14]	2015	Minutia tensor matrix (MTM), Spectral matching.	EER – 2.47% Average Matching time-1.02 (ms)	Improved description Capability and non-linear robustness Deformation and Real noise/matching pairs of little Details show little resemblance compatibilities And remain a

					mystery[14].
	Rodrigues R.Met al[15]	2015	Planar graph, Delaunay triangulation, Characteristic vector model	EER – 1.14%	Fingerprint representation that is efficient, Rotation and tiny distortions don't affect it. Reduces the difficulty of computing [15]
	Priyanka Das et.al[16]	2012	Minimum Distancegraph, Correspondence Search algorithm	EER – 2.27%	Nopre-alignment is necessary. Insensitive to rotation and translation aberrations, Computational complexity is low [16].

1.4 Summary

Before actually planning and carrying out the study, the assessment of the literature provides a clear image of the issue that has to be solved. The researchers are guided by the review of prior research since it helps them avoid doing the same thing twice. Knowing what has already been done in the field of study about the data collection techniques A researcher's personal endeavors are kept organized by the collections and conclusions of their analysis. Consequently, a crucial stage in research is the examination of relevant literature. In biometrics, a human must be recognized based on a few distinctive physiological markers. The identification of a person requesting their services is either confirmed or determined using a wide range of recognition systems.

Chapter3

Problem Formulation

3.1 General

We must first establish or characterize an issue before attempting to solve it. It's critical to clearly state the issue you want to resolve. The process of identifying an issue, its source, and its solution is known as problem formulation.

3.2 Problem Statement

The accuracy of a system is influenced by the sort of biometric feature used in it. The unimodal biometric system has certain inherent problems, including as non-universality, similarities between classes, and spoofing. To go past the restrictions, develop multimodal biometric systems that use many variations of the same identifying evidence.

3.3 Objectives of the Present Study

The following are the objectives of the proposed project:

1. To develop person authentication system by having multiple biometric traits.
2. To develop secured and efficient multimodal biometric system.
3. To make the system performance unaffected by noisy input data, intra class variation.

3.4 Summary

The necessity to verify and identify persons for security reasons is constantly expanding in the modern high-tech environment. To either validate or establish the identification of a person seeking their services, a wide range of current technologies require consistent personal recognition techniques. The goal is to specifically identify people in corporate areas, deter fraud, improve security, and make sure that only authorized users can access the offered services. Person identification techniques are often divided into three groups.

Biometric based approach makes advantage of physiological traits that are unique to each person and cannot be taken or lost. The biometric identification method entails three steps: first, a biometric sample of the person is taken and converted into a digital representation; next, using a feature extract or, unique features are extracted from the digital representation; and finally, using a matcher, the extracted feature set is compared to a template set in the database. Features are combined at the score level. Softmax classifier is then used to classify the features.

Chapter4

Requirements and Methodology

4.1 Hardware Requirements

The table below shows the hardware specifications needed for the proposed project:

Table4.1:Hardwarer equirements

Sl.No	Hardware/Equipment	Specification
1.	Graphic Card	Intel621graphic cardor 2 GB
2.	RAM	4GB and above

4.2 Software Requirements

The table below shows the software specifications needed for the proposed project.

Table4.2:Software requirements

Sl.No	Software	Specification
1.	Anaconda	Anaconda64bit
2.	Python	Python 3 and above

4.3 Methodology Used

The three primary processes of the multimodal biometric system are input acquisition, feature extraction, and classification. The system accepts face pictures from a face dataset and fingerprint images from a fingerprint dataset, and then using CNN architecture, discrete face and fingerprint characteristics are retrieved. After the facial and fingerprint characteristics have been retrieved, features are combined at the score level. Softmax classifier is then used to classify the features.

The proposed Face and Fingerprint Based Person Identification system involves following steps:

1. Collecting the realtime dataset of face and fingerprint images from the dataset.
2. Processes the data.
3. Splitting the data into training and testing data.
4. Using the training data to train the model.
5. Testing the performance of the model with the testing data.

Chapter5

System Design

5.1 System Design

One crucial stage of software or system development is system design. The process of identifying the various modules needed for software or a system to satisfy all criteria is known as system design.

5.1.1 Architecture of proposed system

The proposed face and fingerprint-based person identification system's general design is represented in figure 5.1, which is shown below.

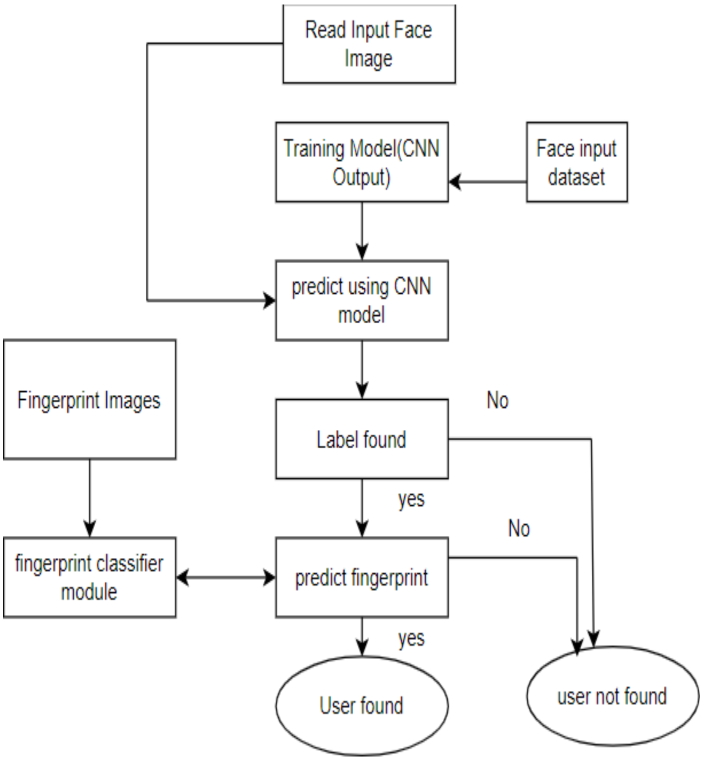


Figure5.1: Design of the proposed system

Using supervised learning, the Face and Fingerprint Based Person Identification System is trained using real-time face photos and fingerprint datasets. The system starts with training and testing phase before acquiring images, detecting faces, analyzing those images, extracting features, and classifying them. From face and fingerprint photographs, face detection and feature extraction are performed. The facial and fingerprint features are then combined at the score level. Softmax classifier is then used to classify the features.

5.1.2 System Flow chart

The flow chart of the proposed system is depicted in figure5.2shown below:

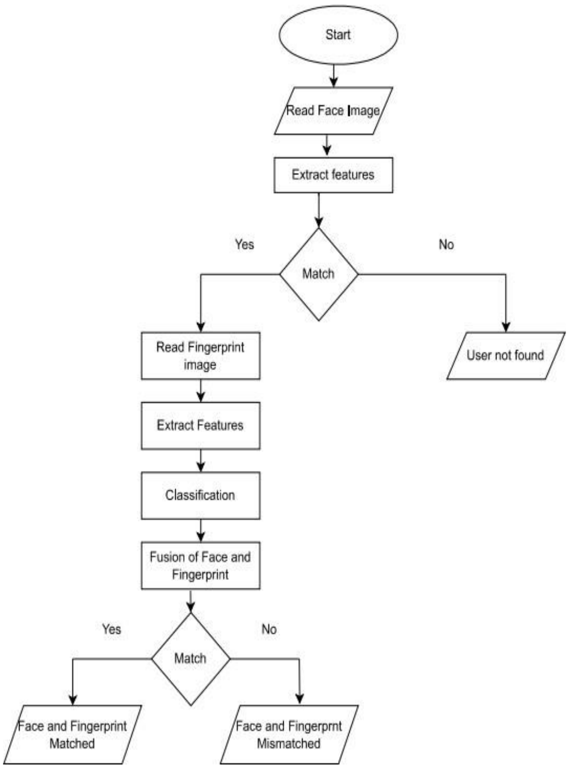


Figure5.2:Flow chart of the proposed system

Chapter 6

System Testing, Results and Discussion

6.1 System Testing

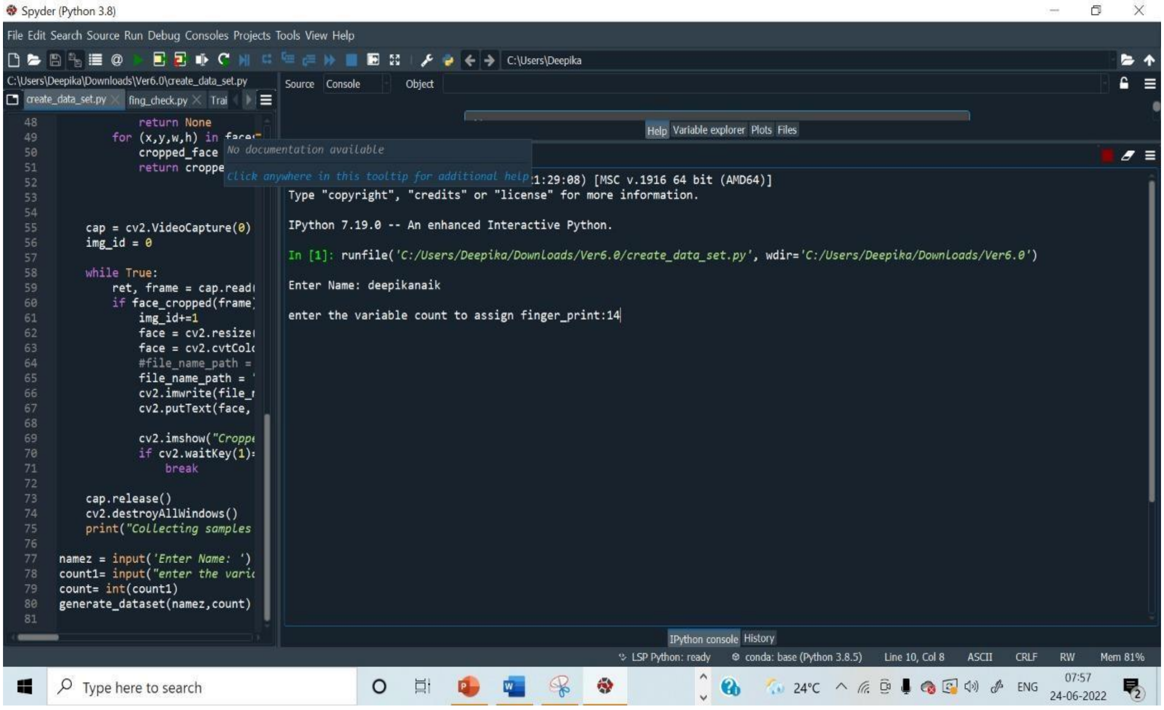
Testing is done to look for mistakes. Testing is the process of looking for any flaws or weaknesses in a piece of work. It offers a means of examining the operation of parts, subassemblies, assemblies, and/or a final product. It is the process of testing software to make sure that it satisfies user expectations and meets requirements without failing in an undesirable way.

Table6.1Results of Unit Testing

Test Case Number	Input	Expected Result	Observed Result	Status P=Pass F=Fail
1	Face	Face Recognition	Face Recognized	P
2	Fingerprint	Fingerprint Recognition	Fingerprint Recognized	P

6.2 Result Analysis

Maximum classification accuracy was observed when both the face and fingerprint modules were fused at the score level, which is the project's goal for the Face and Fingerprint Based Person Identification System. The algorithm was first trained using different random samples from every dataset using supervised learning. Each dataset has it's own data divided into training and testing portions. Samples for each dataset are consistently picked at random from a pool of the corresponding dataset and are each completely unique. Real-time photos are being utilized to demonstrate the suggested approach. The multimodal system performs better than the unimodal system with 97% accuracy, according to the performance table and accuracy curve.

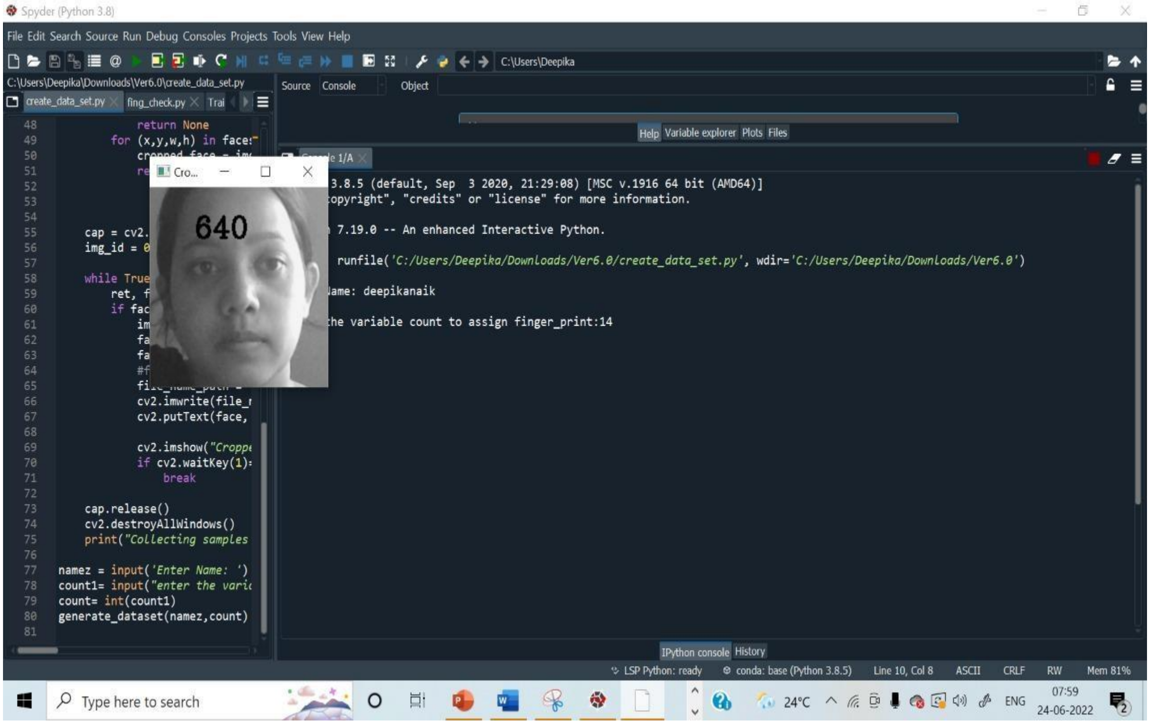


```
            return None
        for (x,y,w,h) in faces
            cropped_face
            return croppe



    cap = cv2.VideoCapture(0)
    img_id = 0

    while True:
        ret, frame = cap.read(
        if face_cropped(frame)
            img_id+=1
            face = cv2.resize(
            face = cv2.cvtColo
            #file_name_path =
            file_name_path = '
            cv2.imwrite(file_n
            cv2.putText(face,

            cv2.imshow("Croppe
            if cv2.waitKey(1)=
                break

    cap.release()
    cv2.destroyAllWindows()
    print("Collecting samples

namez = input('Enter Name: ')
count1= input("enter the varia
count= int(count1)
generate_dataset(namez,count)
```

```
1:29:08) [MSC v.1916 64 bit (AMD64)]
Type "copyright", "credits" or "license" for more information.

IPython 7.19.0 -- An enhanced Interactive Python.

In [1]: runfile('C:/Users/Deepika/Downloads/Ver6.0/create_data_set.py', wdir='C:/Users/Deepika/Downloads/Ver6.0')

Enter Name: deepikanaik

enter the variable count to assign finger_print:14
```

Figure 6.1: Entering the Name and Variable Count of the Person

Figure 6.1 Shows the Entering the name of the person and variable count to assign fingerprint. A camera is used to capture the pictures of the faces in the system.



```
            return None
        for (x,y,w,h) in faces:
            cropped_face = im
            re


    cap = cv2.
    img_id = 0

    while True
        ret, f
        if fac
            im
            fa
            fa
            #f
            fi
            cv2.imwrite(file_
            cv2.putText(face,

            cv2.imshow("Croppe
            if cv2.waitKey(1):
                break

    cap.release()
    cv2.destroyAllWindows()
    print("Collecting samples

namez = input('Enter Name: ')
count1= input("enter the varia
count= int(count1)
generate_dataset(namez,count)
```

```
3.8.5 (default, Sep  3 2020, 21:29:08) [MSC v.1916 64 bit (AMD64)]
opyright", "credits" or "license" for more information.

 7.19.0 -- An enhanced Interactive Python.

 runfile('C:/Users/Deepika/Downloads/Ver6.0/create_data_set.py', wdir='C:/Users/Deepika/Downloads/Ver6.0')

Name: deepikanaik

he variable count to assign finger_print:14
```

Figure 6.2: Capturing Real Time Face Dataset

Figure 6.2 shows the capturing real-time face dataset. Camera is used to capture the pictures of the Face images. It takes upto 1000 images.

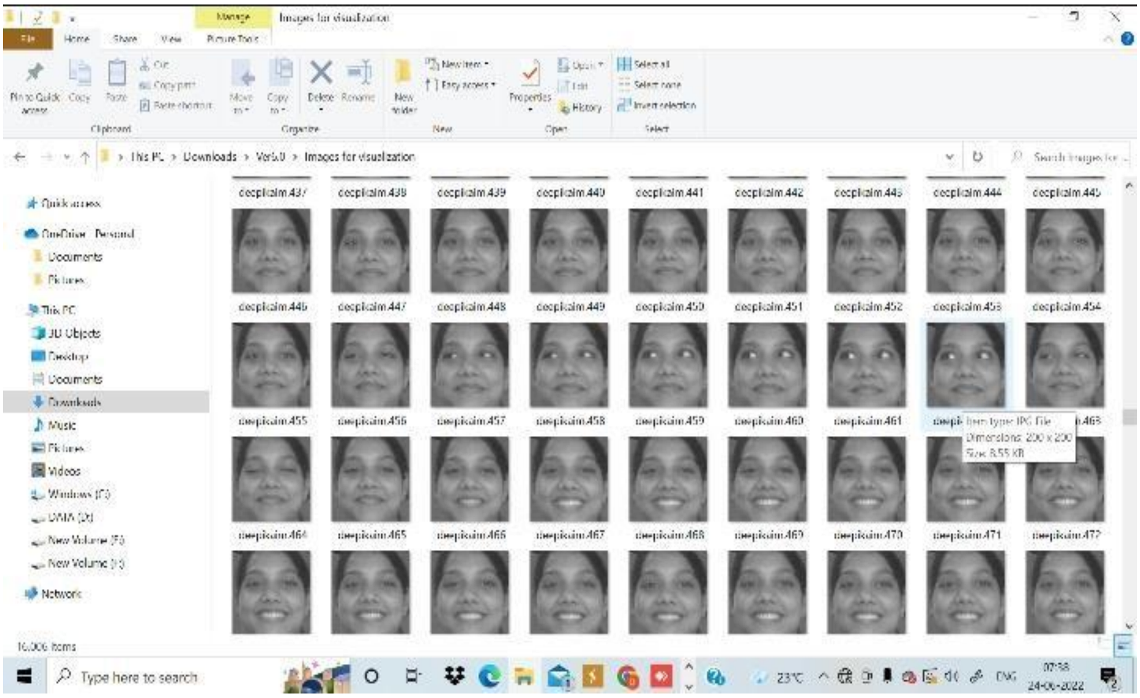


Figure 6.3:Sample Face Images

Figure 6.3 shows the Sample Face Images. For each person it takes1000 images of face and store in the dataset.

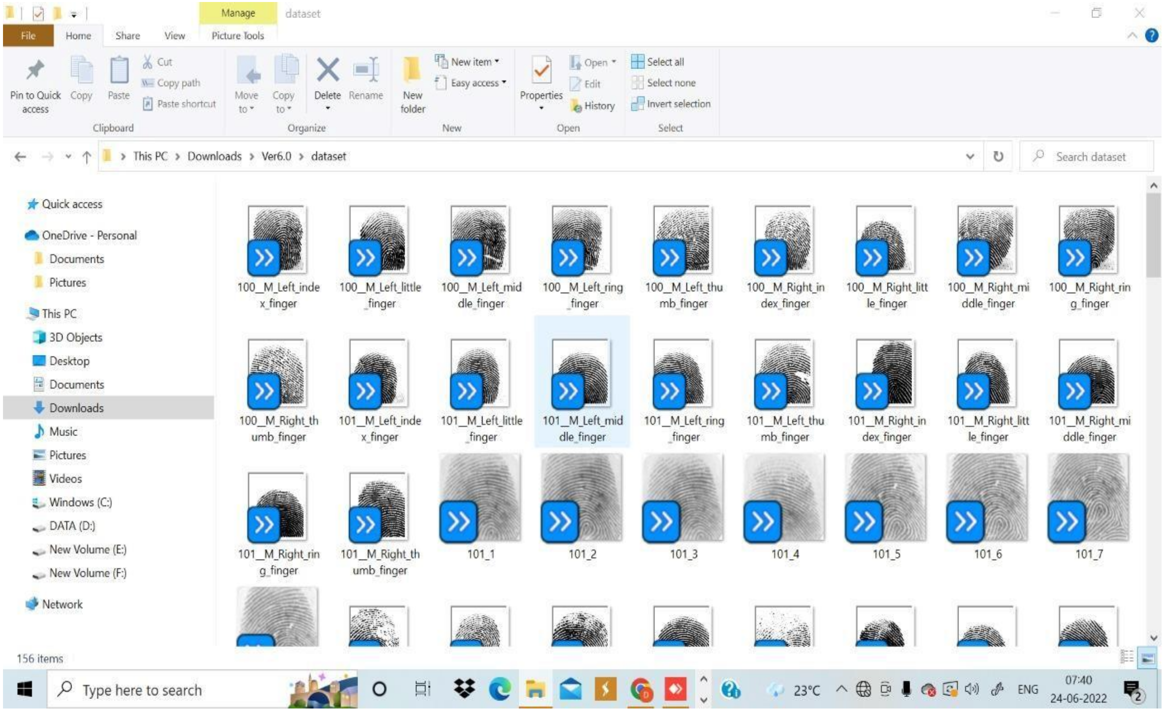
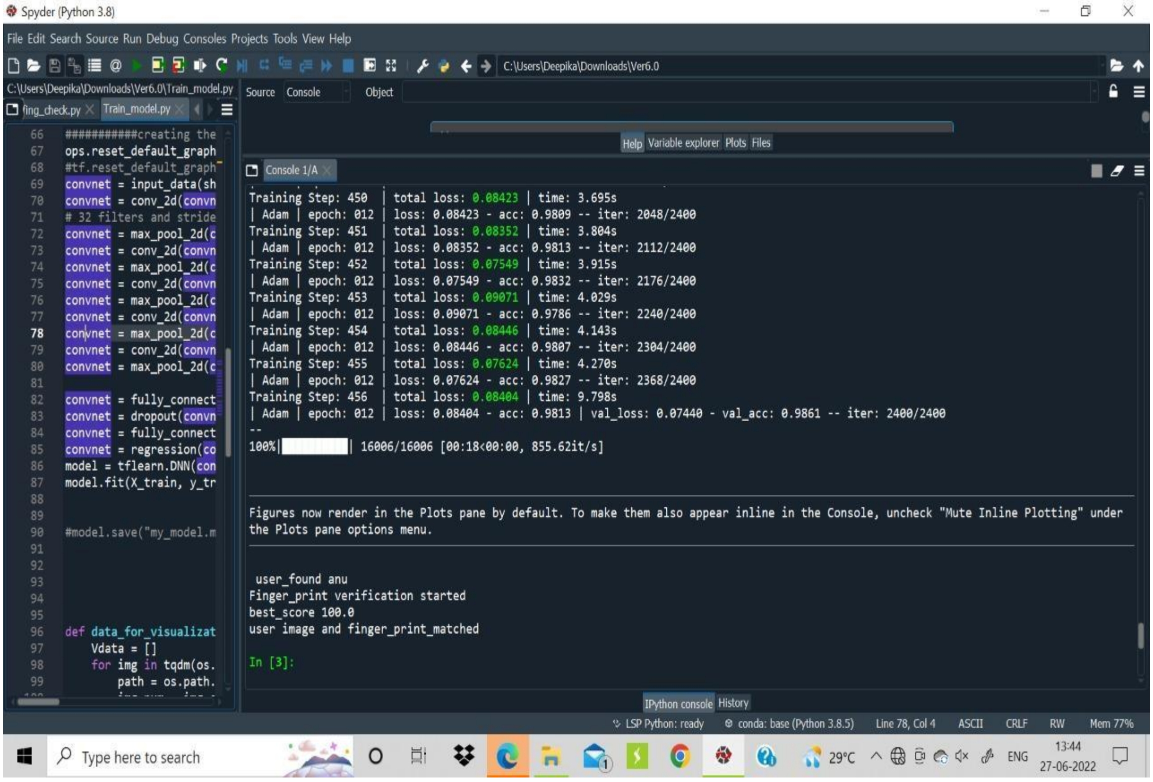

dataset
This PC > Downloads > Ver6.0 > dataset
100__M_Left_index_finger
100__M_Left_little_finger
100__M_Left_middle_finger
100__M_Left_ring_finger
100__M_Left_thumb_finger
100__M_Right_index_finger
100__M_Right_little_finger
100__M_Right_middle_finger
100__M_Right_ring_finger
100__M_Right_thumb_finger
101__M_Left_index_finger
101__M_Left_little_finger
101__M_Left_middle_finger
101__M_Left_ring_finger
101__M_Left_thumb_finger
101__M_Right_index_finger
101__M_Right_little_finger
101__M_Right_middle_finger
101__M_Right_ring_finger
101__M_Right_thumb_finger
101_1
101_2
101_3
101_4
101_5
101_6
101_7
156 items
Type here to search
23°C
ENG
07:40
24-06-2022

Figure 6.4: FVC Finger print Dataset

Figure 6.4 Shows the FVC Fingerprint dataset. Enter the variable count to assign fingerprint and each person it takes 10 fingerprint images from the fingerprint dataset.



```
###########creating the
ops.reset_default_graph
#tf.reset_default_graph
convnet = input_data(sh
convnet = conv_2d(convn
# 32 filters and stride
convnet = max_pool_2d(c
convnet = conv_2d(convn
convnet = max_pool_2d(c
convnet = conv_2d(convn
convnet = max_pool_2d(c
convnet = conv_2d(convn
convnet = max_pool_2d(c
convnet = conv_2d(convn
convnet = max_pool_2d(c

convnet = fully_connect
convnet = dropout(convn
convnet = fully_connect
convnet = regression(co
model = tflearn.DNN(con
model.fit(X_train, y_tr


#model.save("my_model.m





def data_for_visualizat
    Vdata = []
    for img in tqdm(os.
        path = os.path.
```

```
Training Step: 450  | total loss: 0.08423 | time: 3.695s
| Adam | epoch: 012 | loss: 0.08423 - acc: 0.9809 -- iter: 2048/2400
Training Step: 451  | total loss: 0.08352 | time: 3.804s
| Adam | epoch: 012 | loss: 0.08352 - acc: 0.9813 -- iter: 2112/2400
Training Step: 452  | total loss: 0.07549 | time: 3.915s
| Adam | epoch: 012 | loss: 0.07549 - acc: 0.9832 -- iter: 2176/2400
Training Step: 453  | total loss: 0.09071 | time: 4.029s
| Adam | epoch: 012 | loss: 0.09071 - acc: 0.9786 -- iter: 2240/2400
Training Step: 454  | total loss: 0.08446 | time: 4.143s
| Adam | epoch: 012 | loss: 0.08446 - acc: 0.9807 -- iter: 2304/2400
Training Step: 455  | total loss: 0.07624 | time: 4.270s
| Adam | epoch: 012 | loss: 0.07624 - acc: 0.9827 -- iter: 2368/2400
Training Step: 456  | total loss: 0.08404 | time: 9.798s
| Adam | epoch: 012 | loss: 0.08404 - acc: 0.9813 | val_loss: 0.07440 - val_acc: 0.9861 -- iter: 2400/2400
--
100%|██████████| 16006/16006 [00:18<00:00, 855.62it/s]


Figures now render in the Plots pane by default. To make them also appear inline in the Console, uncheck "Mute Inline Plotting" under
the Plots pane options menu.

 user_found anu
Finger_print verification started
best_score 100.0
user image and finger_print_matched

In [3]:
```

Figure 6.5: Final output of Person Identification using Face and Fingerprint

Figure 6.5 shows the final output of the Face and Fingerprint Based Person Identification. If the Face Image and Fingerprint image is of the same person then it will display user image and fingerprint matched otherwise it displays user image and fingerprint mismatched.

6.3 Summary

Faces and fingerprints are utilized in this biometric technology to verify a person's identification. The proposed technique addresses the drawbacks of both finger print verification and face recognition. Securities Breaches, Software Issues, Scanner Issues, etc. are a few drawbacks of face and fingerprint verification systems. Performance can be improved according to the system's Score level fusion approach, which combines a number of stimuli with different confidence measures. Experiment results show how efficiently technology operates. The accuracy criteria were met.

Chapter 7

Conclusion and Scope for Future Work

7.1 Conclusion

In this biometric system, personal identification is authenticated using the user's face and fingerprint. Low image quality or bad lighting conditions can have an influence on facial recognition systems. Due to obstructed camera angles, the data may not match the person's nodal points, which results in an error when a matching face cannot be confirmed in the database. Problems with facial identification and fingerprint authentication verification are resolved by the solution. The integrated system operates in identification mode. The score level fusion strategy used by the system enhances performance by combining a large number of cues with several confidence metrics. The findings show that this system works superbly in testing. It complies with the demands for accuracy.

7.2 Scope for Future Work

Many people now use biometric authentication systems to overcome the drawbacks of traditional authentication techniques. The current project will require more time to create the dataset. Future improvements to the proposed technology could include real-time fingerprint implementation for the fingerprint dataset and multi-layered biometric authentication.

References

[1] Stitiprajna Panda, Swati Sucharita Barik proposed on March 2020 IJRTE, system called Human Face Recognition using LBPH.

[2] Senthamil Selvi, Chitrakala, Antony Jenitha 2014“Face Recognition Based Attendance Marking System”.

[3] Hussain, Dugar, Deka, Hannan.et.al[6],the proposed “RFID based Student Attendance System” Information and communication Technology-2014.

[4] Fateme Saadat, Mehdi Nasri proposed Biometric and multi biometric sciences play an important role in human authentication systems.501-507, 2015.

[5] Madhuri and Richa Mishr,”Fingerprint Recognition using Robust Local Features”, IJARSSE, Volume 2, Issue 6, June 2012, INDIA.

[6] Galbally, J.; Marcel, S.; Fierrez, J. 2014. Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition. IEEE Trans. Image Process. 23(2), 710–724.

[7] Sangram Bana1 and Dr.Davinder Kaur2,” Fingerprint Recognition using Image Segmentatio”, IJAEST,Vol No. 5, IIT Roorkee, Roorkee.