Indian Institute of Information Technology, Una [HP]
An Institute of National Importance under MoE
Saloh, Una (HP) - 177209

Website: www.iiitu.ac.in

Date:23.10.24

PRACTICUM-III
REVIEW-II
CSL306

Student Name	**UDAY DESHWAL**	**Roll No.**	23160
Batch No.	B8	**Semester**	3rd Semester
Branch	CSE	**Supervisor(s)**	Dr. Sanjit Ningthoujam

1. Title of the Project

Face Recognition-Based Login System.

2. Introduction

The Face Recognition-Based Login System project aims to enhance digital security and user convenience by using machine learning to authenticate users through facial recognition. By replacing traditional passwords with biometric verification, the system improves security and reduces login friction. It involves collecting and preprocessing facial image data, training advanced machine learning models like Convolutional Neural Networks (CNNs), and integrating the model into a user-friendly login interface. This approach addresses security vulnerabilities of conventional methods and promises a seamless, password-free user experience. The project also lays the groundwork for future innovations in biometric authentication technologies.

3. Problem Definition

Traditional login systems, typically based on passwords or PINs, face several significant problems:

1. **Security Vulnerabilities**: Passwords can be easily stolen, guessed, or cracked through methods like brute force attacks, phishing, or data breaches. Weak passwords or password reuse further exacerbate these risks.
2. **User Convenience**: Remembering multiple complex passwords can be challenging, leading to password fatigue. Users often resort to using simple or repeated passwords, which compromises security.
3. **Susceptibility to Social Engineering:** Users can be tricked into revealing their passwords through social engineering tactics, making it easier for attackers to gain unauthorized access.
4. **Management Overhead**: Managing and updating passwords, especially in large organizations, requires significant administrative effort and resources.

5. **Password Theft**: Physical or digital theft of password storage devices or written passwords can lead to unauthorized access.
6. **Limited Usability**: Traditional systems often require manual entry of passwords, which can be inconvenient and time-consuming.

   Face recognition-based systems address these issues by providing a more secure, user-friendly alternative that eliminates the need for passwords and reduces the risk of unauthorized access.

4. Objectives

The objectives of the Face Recognition-Based Login System project are as follows:

1. **Develop Accurate Facial Recognition Models**: Create and train advanced machine learning models, such as Convolutional Neural Networks (CNNs), to accurately identify and authenticate users based on facial features.
2. **Enhance Security**: Provide a more secure authentication method by replacing traditional passwords with biometric verification, reducing the risk of unauthorized access and mitigating vulnerabilities associated with password-based systems.
3. **Improve User Convenience**: Streamline the login process by eliminating the need for passwords, thereby simplifying user interactions and reducing login friction.
4. **Integrate Seamlessly**: Design and implement a user-friendly interface that integrates the facial recognition model with a login system, ensuring smooth functionality and ease of use for end-users.
5. **Evaluate Performance**: Assess the system's accuracy, efficiency, and robustness through rigorous testing, and refine the model based on performance metrics and real-world scenarios to ensure reliable operation.

5. Skillset additionally required to solve/address the problem

To successfully develop a Face Recognition-Based Login System, several additional skill sets are required beyond basic programming knowledge. These include:

1. **Machine Learning and Deep Learning**:

   Understanding of Algorithms: Knowledge of Convolutional Neural Networks (CNNs), transfer learning, and other relevant algorithms.

   Model Training and Evaluation: Experience in training, fine-tuning, and evaluating machine learning models, including handling overfitting, underfitting, and cross-validation.

2. **Data Science**:

   Data Collection and Preprocessing: Skills in gathering, cleaning, and preprocessing facial image datasets.

   Data Augmentation: Techniques to enhance the diversity of training data and improve model robustness.

3. **Computer Vision:**

   Image Processing: Expertise in techniques such as facial detection, feature extraction, and image alignment.

   Real-Time Processing: Knowledge of handling and processing images in real-time for live facial recognition.

4. **Software Development:**

   Programming Languages: Proficiency in languages such as Python, which is commonly used for machine learning and computer vision tasks.

   Frameworks and Libraries: Experience with libraries and frameworks like TensorFlow, Keras, PyTorch, OpenCV, and scikit-learn.

5. **User Interface (UI) and User Experience (UX) Design:**

   UI/UX Design: Skills in designing a user-friendly interface for the login system, including understanding user experience principles and ensuring accessibility.

6. Timeline to achieve the skillset

Month 1-2: Foundation and Core Skills

Programming Languages

Introduction to Machine Learning

Month 3-4: Deep Learning and Computer

Deep Learning Fundamentals

Computer Vision Basics

Month 5-6: Advanced Topics and Tools

Advanced Deep Learning

Frameworks and Libraries

Month 7-8: System Integration and Development

Software Development

User Interface (UI) and User Experience (UX)

7. Block schematic/algorithm/coding/testing metrics/experiments/result graphs/technical papers

Block Schematic

1. **Image Acquisition**: Capture images of students using a camera.
2. **Preprocessing:** Enhance and normalize images (e.g., resizing, noise reduction).
3. **Face Detection**: Detect faces in the images using algorithms like Haar Cascades or MTCNN.
4. **Face Recognition:** Identify students using pre-trained models like FaceNet or VGG-Face.
5. **Attendance Marking**: Update the attendance database with recognized faces.

Algorithm

1. **Data Collection**: a) Collect a labeled dataset of student images. b) Augment data to improve model robustness.
2. **Preprocessing:** a) Resize images to a standard dimension.
   b) Normalize pixel values.
3. **Model Training**: a) Split data into training and testing sets.
   b) Train a face recognition model (e.g., FaceNet) on the training set.
   c) Validate the model on the testing set to ensure accuracy.
4. **Implementation:**
   a) Integrate the trained model into the attendance system.
   b) Set up a camera to capture real-time images.

c) Use face detection to locate faces in each frame.

d) Recognize faces and match them against the database.

5. **Attendance Marking**:

a) For each recognized face, mark attendance in the database.

b) Generate attendance reports.

8. Weekly milestones

Week	Major Activities to be Completed
Week 1	Define objectives, scope, and requirements.
Week 2	Gather and read required resources
Week 3	Gather and read required resources
Week 4	Gather and read required resources
Week 5	Set up workstation
Week 6	Data Collection
Week 7	Clean and preprocess images (resizing, normalization).
Week 8	Research and select face detection and recognition models.
Week 9	Research and select face detection and recognition models.
Week 10	Train face detection and recognition models.
Week 11	Train face detection and recognition models.
Week 12	Evaluate the Model
Week 13	Testing phase
Week 14	Testing phase

9. Completed Milestones

1.Learning how to create a local host.
2.Passing value to a URL.
3.Dynamically creating URLs.
4.Video streaming on web using flask module.
5.Css integrated video streaming helpful for face detection.
6.Providing the data to the flask model.
7.Learning to use various modules under flask like face recognition,face decoding etc.
8.Providing the names with the images for recognition.
9.Using frames provided on the url for face recognition.
10.Matching the face and providing the name of the person if it is in the database.

10. Milestones to be Completed

1.Creating a web page for login

2.Authentication required.
3.If the username and the face matches in the database then giving access to the user.
3.Testing phase

11. Expected Challenges

1. Data Quality and Diversity

- **Challenge:** Collecting and ensuring high-quality, diverse facial image data is crucial for training an accurate model. Issues like varied lighting, different facial expressions, and diverse backgrounds can affect model performance**.**

2. Model Accuracy and Robustness

- **Challenge**: Achieving high accuracy in facial recognition, especially under different conditions (e.g., different angles, lighting, and facial expressions), can be difficult. The model must be robust against variations to minimize false positives and false negatives.

3. Real-Time Processing

- **Challenge:** Implementing real-time facial recognition requires efficient processing to ensure quick and accurate authentication. Lag or delays can impact user experience and system performance.

4. Privacy and Data Security

- **Challenge:** Handling biometric data raises significant privacy and security concerns. Unauthorized access or data breaches can have serious implications.

5. System Integration

- **Challenge:** Integrating the facial recognition model with the login system and ensuring seamless user interactions can be complex. Compatibility issues and integration errors may arise.

6. Handling Spoofing and Fraud

- **Challenge:** Face recognition systems are vulnerable to spoofing attacks (e.g., using photos or masks). Ensuring the system can distinguish between real faces and spoofing attempts is crucial.

12.References

1) "Face++ Cognitive Services: Face Recognition." Available at: https://www.faceplusplus.com/face-detection/. Accessed August 2024.

2) Krish naik (youtube)

3) OpenFace ,Available at: http://reports-archive.adm.cs.cmu.edu/anon/2016/CMU-CS-16-118.pdf.

Name and Signature of Student

Name and Signature of Supervisor