Face Recognition- Based Security for Social Media Login

Name:-Snehal Raju Taware
Email-id:-snehaltaware421@gmail.com
Department of Computer Engineering

Name:-Sourabh Vilas Nawale
Email-id:-sourabhnawale5154@gmail.com
Department of Computer Engineering

Name:-Rupesh Murlidhar Khairnar
Email-id:- rupeshmk2003@gmail.com
Department of Computer Engineering

Name:-Swapnil Mohan Shinde
Email-id:- swapnilshinde2327@gmail.com
Department of Computer Engineering

Guide Name: Prof. Nanda Kulkarni

SIDDHANT COLLEGE OF ENGINEERING SUDUMBARE, TAL- MAVAL DIST-PUNE – 412109.

----------***----------

Abstract: Social Networking has become today's lifestyle and anyone can easily receive information about everyone in the world. It is very useful if a personal identity can be obtained from the device and also connected to social networking.
Therefore, we proposed a face recognition system. Our system is designed in the form of an application developed on desktop. We also applied the Machine learning as an information viewer to the users.

The result of testing shows that the system is able to recognize face samples with the average percentage of 85 percentage with the total computation time for the face recognition system reached 7.45 seconds, and the average augmented reality translation time is 1.03 seconds to get someone's information.

Face authentication has emerged as a prominent method for identity verification, leveraging the unique biometric features of individuals to enhance security and user convenience. This paper presents the design and implementation of a face authentication system that utilizes advanced machine learning algorithms and image processing techniques to accurately and efficiently verify user identities. The system captures facial images in real-time and processes them to extract distinguishing features, which are then compared against a secure database of registered users.

Key Words: Face recognition, biometric authentication, machine learning, image processing, feature extraction, Secure login system

INTRODUCTION

With the rise of social networking, security concerns like identity theft and unauthorized access have become major issues. Traditional password-based authentication is vulnerable to attacks, making secure login methods essential. This project proposes a Face Recognition-Based Security System for Social Media Login**,** utilizing biometric authentication for enhanced security.

The system captures real-time facial images, processes them using machine learning algorithms, and verifies user identities with an 85% accuracy

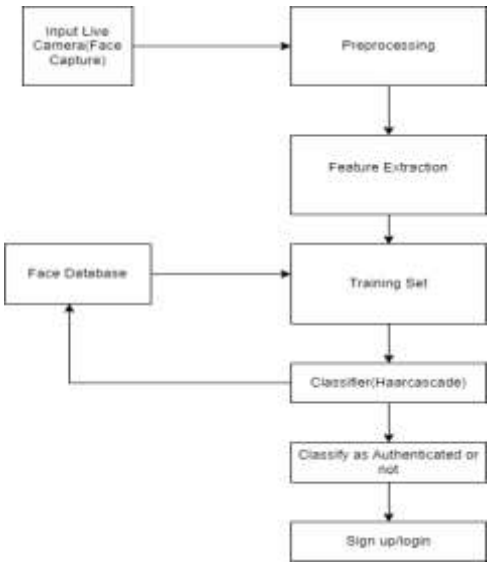
rate. Developed as a desktop application, it ensures secure and efficient authentication while integrating augmented reality (AR) for quick information retrieval. This approach enhances social media security by reducing unauthorized access and improving user convenience.

Background of the Industry:

With rising security threats in social media, traditional passwords are no longer reliable. Face recognition powered by AI and machine learning is emerging as a secure alternative for user authentication. Tech companies are adopting biometric authentication to enhance security, protect user data, and provide a seamless login

Proposed Working

The proposed system is designed to login social media using biometric that is live face capturing. If person is registered itself and then try to login then he will be authenticate else unauthenticate. Only authenticate people can login to Social media.
This flowchart represents a face authentication system using Haar cascade for classification.



Fig[1] System Architecture

1. Input Live Camera (Face Capture)

A live camera captures the face of the user in real-time.

2. Pre-processing

The captured face image undergoes pre-processing, which may include gray scale conversion, noise reduction, normalization, and face alignment.

3. Feature Extraction

Important facial features are extracted from the pre-processed image using feature extraction techniques like edge detection or histogram-based methods.

4. Training Set

The extracted features are used to create a training dataset, which consists of known facial data for comparison.

5. Face Database

The system maintains a database of authenticated faces, which are used for comparison and classification.

6. Classifier (Haar cascade)

The Haar cascade classifier processes the input face image and compares it with stored features in the database.

7. Classify as Authenticated or Not

Based on the classifier's output, the system determines whether the detected face is authenticated or not.

8. Sign up/Login

If the face is authenticated, the user is granted access (login).If the face is not recognized, the system may prompt the user to sign up by storing

their facial features in the database for future authentication.

Methodology

CNN Algorithm

Convolutional Layers: These layers apply filters (kernels) to input images, extracting low-level features like edges, textures, and patterns. They slide over the image (convolve), detecting different visual patterns at various spatial lo cations.

Pooling Layers: After convolution, pooling layers (e.g., max pooling) reduce the dimensionality of the feature maps, retaining the most important information while reducing computational complexity.

Fully Connected Layers: After several convolution and pooling layers, the CNN has fully connected layers that aggregate learned features and make a final classification decision (e.g., distinguishing forged from authentic images).

Activation Functions: These functions (usually ReLU) introduce non-linearities, allowing the network to learn more complex patterns in the data.

Architecture Selection: Choose an appropriate CNN architecture (e.g., CNNfor image data, feedforward networks for structured data).

Training:Use a portion of the dataset for training while reserving data for validation and testing. Implement techniques like cross-validation to prevent over fitting

Tools and Technology used

Python: An interpreted, high-level programming language emphasizing readability. Supports multiple paradigms and has a rich standard library.

NumPy: A fundamental library for numerical computing in Python, offering support for arrays, linear algebra, and matrix operations.

Pandas: A data manipulation and analysis library built on NumPy, ideal for handling structured data and time series.

OpenCV (cv2): An open-source computer vision library. Includes pre-trained Haar cascade classifiers for object detection.

Pillow: A friendly fork of the Python Imaging Library (PIL) used for opening, manipulating, and saving images.

Anaconda: A distribution of Python and R for data science and machine learning, includes Conda for package/environment management.

Spyder: A Python IDE for scientific development with features like code editor, IPython console, debugger, and documentation viewer.

Supervised Machine Learning: A method where models are trained on labeled datasets to make accurate predictions based on input data.

Results

Fig[2] Main page

The main page of the Face Authentication System provides a user-friendly interface with an "Open an Account" option, designed for secure social media

login using facial recognition. A banner highlights the system's goal of enhancing account security and user experience through biometric authentication.

Fig[3] Home page

This interface allows users to register, input their ID, capture their face, train the facial data, and log in securely using face recognition.

Fig[4] Registration page

This page allows new users to create an account by entering personal details such as name, address, email, contact number, and gender, with options to submit or display the entered data.

Fig[5] Success page

This page displays a popup message confirming that the user account has been successfully created after filling out and submitting the registration form.

Fig[6] Capturing face

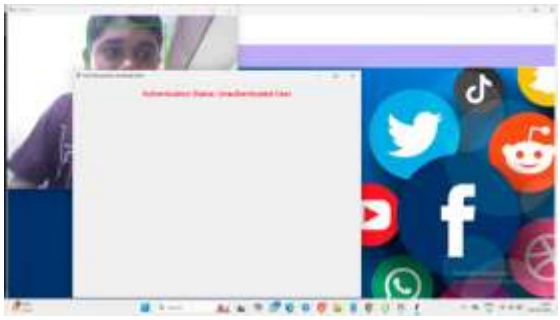
This is a face capture window showing the user's detected face within a bounding box, used for authentication or registration.

Fig[7] Training face data

This page captures and trains facial data linked to a user ID for secure login, enabling face recognition-based authentication.

Fig[8] Authentication

This screen confirms successful face recognition, displaying the message "Authenticated User", indicating the user's identity has been verified.



Fig[9] Unauthentication

This screen confirms successful face recognition, displaying the message "Authenticated User", indicating the user's identity has been verified.

Fig[10] login page

Success page shown after face is verified, allowing user to open an Instagram.

Objectives

The objective is to design and implement a face authentication system that enhances security by using facial recognition technology. The system captures live facial images, processes them, and authenticates users based on a stored face database. The primary goals include:

1. Automated User Authentication : Provide a seamless and secure login/signup process using facial recognition instead of traditional credentials like passwords.

2. Real-Time Face Recognition: Process live camera input to identify users quickly and accurately.

3. Feature Extraction & Classification :Extract key facial features and classify users using a trained Haar cascade classifier.

4. Secure Access Control: Restrict unauthorized access by ensuring only registered users can authenticate successfully.

5. Face Database Management: Store and manage facial features of authorized users for future authentication.

6. Enhanced User Experience : Provide a convenient, contact less, and efficient authentication method for improved security and ease of use.

This system can be applied in various domains such as biometric security, banking, office access control, and mobile authentication.

CONCLUSION

The development of a face authentication system presents a significant advancement in the field of biometric security, offering a robust and user-friendly method for verifying identities. By leveraging state-of-the-art machine learning techniques and image processing methods, this system addresses key challenges such as accuracy, speed, and security.

ACKNOWLEDGEMENT

This is a great pleasure and immense satisfaction to express my deepest sense of gratitude and thanks to everyone who has directly or indirectly helped me in completing my seminar work successfully.

I express my gratitude towards project guide Prof. Nanda Kulkarni and Coordinator Prof. Apeksha Pande and , Prof. Nanda Kulkarni Head of Department of Computer Engineering, Siddhant College of Engineering, Pune who guided and encouraged me in completing the seminar work in scheduled time. I would like to thanks our Principal

Dr L.V.Kamble, for allowing us to pursue my seminar in this institute.

REFERENCES

[1] S. Krishna, G. Little, J. Black, and S. Panchanathan," A wearable face recognition system for individuals with visual impairments," in Proceedings of the 7th international ACM SIGACCESS conference on Computers and accessibility, Baltimore, MD, USA, 2005, pp. 106-113.

[2] R. Jafri and H. R. arabinan," A Survey of Face Recognition Techniques," Journal of Information Processing Systems, vol. 5, pp. 41-68, 2009.

[3] I. J. Cox, J. Ghosn, and P. N. Yianilos," Feature-based face recognition using mixture-distance," presented at the Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, 1996.

[4] L. Wiskott, J.-M. Fellous, N. Kru¨ger, and C. von der Malsburg," Face Recognition by Elastic Bunch Graph Matching," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, pp. 775-779, July 1997.

[5] M. Turk and A. Pentland, "Eigenfaces For Recognition," Journal Of Cognitive Neuroscience, vol. 3, pp. 71-86, Winter 1991

[6] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman," Eigenfaces vs. Fisher faces: Recognition using class specific linear projection," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, pp. 711-720, July 1997.

[7] R. Jafri and H. R. arabinan," PCA-Based Methods for Face Recognition," in The 2007 International Conference on Security and Management (SAM'07), Las Vegas, USA, 2007, pp. 534-541.

[8] S. Zhou and R. Chellappa," Beyond a single still image: Face recognition from multiple still images and videos," in Face Processing: Advanced Modelling and Methods, ed: Academic Press, 2005.

[9] D. Pascaline and S. P. Mariotti," Global estimates of visual impairment: 2010," British Journal Ophthalmology, 2011.