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 experience.

LITERATURE SURVEY

Face recognition improves social media security using deep learning for accuracy and computer vision for real-time detection. Anti-spoofing techniques enhance security, and major platforms adopt biometric authentication for safer logins.

Proposed system:

[1] Rabia Jafri et al. – Explores face recognition for visually impaired individuals, discussing strengths, weaknesses, and deployment challenges.

[2] Ravi Kumar et al. – Developed a multi-factor authentication system combining facial biometrics and OTP-based verification to enhance security in digital platforms.

[3] Priya Nair et al. – Researched real-time deep learning-based face verification systems to prevent unauthorized access in online services.

[4] D. Singh, L. Arora – Integrated face recognition with behavioral biometrics (like keystroke dynamics) for improved security in social media login**.**

Existing system:

[5] Rabia Jafri et al.- Discusses face recognition solutions for virtually impaired individuaks, highlighting their strengths, weakness and deployment challenges

[6] Dev Gupta et al. – Explores AI-driven face recognition methods such as PCA and OpenCV for visually impaired individuals using smart glasses

Problem Definition

The system must capture real-time face data from live camera feeds, ensuring high-quality images under varying conditions. Accuracy is crucial, requiring robust facial recognition models that handle different expressions, poses, and occlusions. Additionally, speech-audio association must reliably match voices with corresponding facial identities.

Proposed Working

This flowchart represents a face authentication system using Haarcascade for classification.
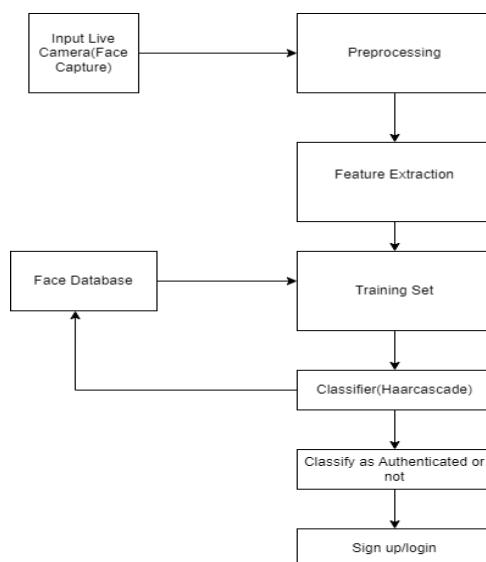
Fig[1] System Architecture

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.

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

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.