https://doi.org/10.46335/IJIES.2025.10.3.7 **e-ISSN: 2456-3463**
Vol. 10, No. 3, 2025, PP. 30-32

International Journal of Innovations in Engineering and Science, www.ijies.net

Secure Access Control Using Face Recognition

Anagha Borkar[1], Sakshi Deote[2], Saloni Nimje[3], Vaishnavi Dandekar[4], Vaishnavi Gomase[5] , Dr. S.S. Golait [6], Ms. Ashwini Lokande[7]

[1,2,3,4,5,] Students ,[6,7] Professor, Dept. Artificial Intelligence and Data Science. C. E. Nagpur, India.

Email of corresponding Author: ***vaishnavigomase1112@gmail.com***

Received on: 19 April, 2025 *Revised on: 05 May ,2025* *Published on: 07 May,2025*

Abstract *– Face recognition has emerged as a leading biometric technique for secure and efficient person authentication, offering a user-friendly alternative to traditional password-based systems. Th is project, titled "Face Recognition for Person Authentication Using Deep Learning," aims to develop a highly accurate and robust face recognition system for user authentication. Leveraging state-of-the-art deep learning models such as ResNet50, Efficient Net, VGG16, VGG19, and VGG Face, the system will recognize and authenticate users based on their facial features. The project workflow begins with the collection and cleaning of a facial dataset, followed by preprocessing steps such as image resizing, noise removal, and histogram equalization to enhance image quality. The dataset will be split into training, validation, and testing sets in an 80:10:10 ratio. Multiple deep learning models will be trained and evaluated to select the optimal architecture and hyperparameters, with key performance metrics like precision, recall, F1-score, and accuracy used to gauge model effectiveness. The system is designed to offer a multi-step authentication process. Users will log in using their credentials, followed by an OTP verification. Once authenticated, registered users will undergo face recognition to confirm their identity, while new users will be prompted to register by providing their email and real-time facial data. The web interface, developed using HTML, CSS, and JavaScript, is integrated with the backend via Flask to ensure seamless interaction between the user and the deep learning model. The system provides a secure, real-time authentication process, ensuring that only legitimate users gain access while alerting account owners of unauthorized access attempts. This project delivers a comprehensive solution combining advanced deep learning techniques with practical real-world applications in secure authentication.*

Keywords- Face Recognition, Deep Learning, Secure Authentication, Biometric System.

INTRODUCTION

In today's digital era, secure and reliable user authentication has become a necessity across various domains, from online banking to access control in physical spaces. Traditional methods of authentication, such as passwords or PINs, are prone to vulnerabilities like phishing attacks, password guessing, and unauthorized access.

As a result, there is a growing demand for more robust, user friendly, and secure authentication systems. Face recognition, powered by deep learning, has emerged as a leading solution to this problem due to its non-intrusive nature and high accuracy. This project, titled "Face Recognition for Person Authentication Using Deep Learning," aims to develop a cutting-edge face recognition system for user authentication. The goal is to provide a secure and seamless user experience by leveraging deep learning models to authenticate users based on their facial features. This solution will not only enhance security but also improve user convenience, eliminating the need to remember passwords or carry authentication tokens.

The project will follow a systematic approach, starting with the collection and cleaning of facial datasets, followed by extensive preprocessing to ensure the quality of the data. Advanced deep learning models, including

https://doi.org/10.46335/IJIES.2025.10.3.7 e-ISSN: 2456-3463
Vol. 10, No. 3, 2025, PP. 30-32

International Journal of Innovations in Engineering and Science, www.ijies.net

ResNet50, Efficient Net, VGG16, and VGG Face, will be employed to perform face recognition with high accuracy.

These models will be trained, validated, and tested using various performance metrics such as confusion matrices, recall, precision, and F1 score, ensuring that the final model achieves optimal performance. To provide an intuitive and user-friendly interface, a web-based system will be developed using HTML, CSS, and JavaScript for the frontend, with Flask serving as the backend framework to integrate the trained deep learning model. The system will feature a robust multistep authentication process, where users first log in with their credentials and undergo OTP verification before being asked to provide face recognition. For registered users, the system will instantly verify their identity, while for new users, an easy registration process will capture their face and email details to securely onboard them. By combining the power of deep learning with a seamless user interface, this project aims to deliver an efficient and highly secure face recognition system for person authentication, addressing both the convenience and security needs of modern applications.

Face recognition has emerged as a leading biometric technique for secure and efficient person authentication, offering a user-friendly alternative to traditional password-based systems.

This project, titled "Face Recognition for Person Authentication Using Deep Learning," aims to develop a highly accurate and robust face recognition system for user authentication Leveraging state-of-the-art deep learning models such as ResNet50, Efficient Net, VGG16,VGG19, and VGG Face, the system will recognize and authenticate users based on their facial features.

METHOLOGY

The face recognition system is developed using a deep learning approach that involves several structured steps to ensure accuracy and real-world applicability. The process begins with collecting a diverse facial dataset from sources like LFW or custom data, capturing variations in lighting, angle, and expression. Preprocessing is then applied, including image resizing, normalization, noise reduction using Gaussian filters, and histogram equalization to improve image quality.

Feature extraction is performed using Histogram of Oriented Gradients (HOG) for initial detection and Convolutional Neural Networks (CNNs) for deeper feature learning. The dataset is split into training, validation, and test sets (80/10/10) to optimize and evaluate model performance.

Various deep learning architectures such as ResNet50, EfficientNet, VGG16/19, and VGG-Face are employed for classification. The system is trained using Python with frameworks like TensorFlow and Keras. Performance is evaluated using standard metrics like accuracy and robustness under challenges like occlusion and lighting variation. Finally, the system is deployed with real-time functionalities including face-based login, access control, and live surveillance integration.

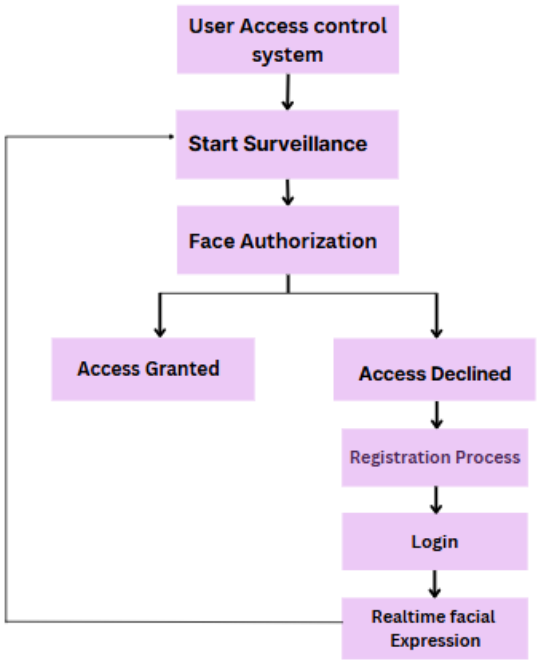

Fig. 1- Block Diagram

This fig.1. block diagram represents a face recognition-based access control system. It starts with surveillance, detecting faces in real time. If the face is authorized, access is granted. If not, the system initiates a registration process where the user logs in and their facial data is recorded. Real-time facial expression analysis may follow. The process then loops back to integrate the new user into the system for future recognition and access control.

CONCLUSION

This project successfully developed a robust and secure face recognition system for user authentication. By leveraging advanced deep learning models like ResNet50, EfficientNet, VGG16, and VGG Face, the system

achieved high accuracy in recognizing and authenticating users based on their facial features. The implementation of a multi-step authentication process, combining user ID/password login, OTP verification, and face recognition, significantly enhanced security. The user-friendly web interface, powered by HTML, CSS, and JavaScript, provided a seamless user experience. The Flask-based backend ensured efficient communication between the frontend and the deep learning model, while also safeguarding user data. The system's ability to capture and process real-time facial data further streamlined the authentication process. By comparing multiple deep learning models and fine-tuning the best-performing one, the project achieved optimal accuracy and real- time performance. The integration of security measures, such as encryption and unauthorized access alerts, protected sensitive user information. Overall, this project demonstrates the potential of deep learning in revolutionizing user authentication and providing a more secure and convenient user experience.

ACKNOWLEDGMENT

This paper is made possible through the help and valuable support of our Guide Dr. S.S.Golait. Finally, we sincerely thanks to my parents and God. Authors are very much thankful to management for providing the facilities to conduct the research work in the institution’s laboratory. Also thankful to the department for approving our research proposal and providing us the grants to conduct research activities.

REFERENCES

[1] *O. A. Al-Shareef and N. M. Gaboua, "Face Recognition Using Deep Learning," 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Benghazi, Libya,2023, pp. 159-165,doi: 10.1109/MISTA57575.2023.10169331. keywords: {Training ; Performance evaluation ; Industries ; Convolution ; Face recognition ; Neurons ; Artificial neural networks ; Face Recognition ; Biometrics ; Deep Learning ; CNN ; Python.*

[2] *V. C. R, V. Asha, B. Saju, S. N, T. R. Mrudhula Reddy and S. K. M, "Face Recognition and Identification Using Deep Learning," 2023 Third International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India,2023, pp. 1-5, do i: 10.1109/ICAECT57570.2023.10118154. keywords: {Deep learning ;Training ;Image recognition ; Face recognition ; Surveillance ; Neural networks ; Training data ; Face Recognition ; Deep Learning ; Convolutional neural network ;OpenCV ; Algorithm}*

[3] *P. J. Thilaga,B. A. Khan, A. A. Jones and N. K. Kumar, "Modern Face Recognition with Deep Learning," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 1947-1951, do i: 10.1109/ICICCT.2018.8473066. keywords:{Face ; Face recognition ; Conferences; Machine learning ; Databases ;Training ;Feature extraction ;Histograms of Oriented Gradients ;Deep Learning ;classifiers}*

[4] *S. Sharma, M. Bhatt and P. Sharma, "Face Recognition System Using Machine Learning Algorithm," 2020 5th International Conference on Communication and Electronics Systems(ICCES), Coimbatore, India, 2020, pp. 1162-1168, do i: 10.1109/ICCES48766.2020.9137850. keywords: {Support vector machines ; Machine learning algorithms ; Social networking (online);Face recognition ; Lighting ; Multilayer perceptron ; Linear discriminant analysis ; Machine learning ;face recognition ; support vector machine ; principal component analysis ;Naïve Bayes}*