IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SMART FACE DOOR LOCK USING ARTIFICIAL INTELLIGENCE

[1] Senthilkumar, [2] U Dhanya, [3] R Karthipriya, [4] N Praveenkumar, [5] M U Thirishaa

[1]Assistant Professor, [2,3,4,5]UG Student
[1]Computer Science and Engineering,
[1]Knowledge Institute of Technology, Salem, Tamil Nadu, India

Abstract : The Smart Face Door Lock utilizing Artificial Intelligence (CNN) is a cutting-edge security system designed to enhance access control through facial recognition technology. Leveraging Convolutional Neural Networks (CNN), the system provides robust face training capabilities, enabling seamless recognition of authorized individuals. Through continuous learning, the CNN algorithms adapt and refine their recognition accuracy, ensuring reliable performance over time. One of the key features of this system is its ability to detect unauthorized access attempts. By analyzing facial features in real-time, the CNN can promptly identify unfamiliar faces attempting to gain entry, triggering immediate security alerts. This proactive approach helps mitigate potential security breaches and safeguard the premises effectively. Furthermore, the Smart Face Door Lock incorporates a mail notification feature, enhancing user convenience and security monitoring. Upon successful access or any unauthorized detection event, the system sends instant notifications to designated email addresses, enabling users to stay informed about access activities remotely. Overall, the integration of Artificial Intelligence, specifically CNN, empowers the Smart Face Door Lock with advanced face training, unauthorized access detection, and mail notification functionalities. This comprehensive approach not only enhances security but also offers a seamless and user-friendly experience for access control in residential and commercial settings.

Keywords - Facial recognition technology;CNN;AI based face recognition; security alert; real-time analysis; user friendly feature; continuous learning

I. INTRODUCTION

A face analyzer is software that identifies or confirms a person's identity using their face. It works by identifying and measuring facial features in an image. Facial recognition can identify human faces in images or videos, determine if the face in two images belongs to the same person, or search for a face among a large collection of existing images. Biometric security systems use facial recognition to uniquely identify individuals during user onboarding or logins as well as strengthen user authentication activity. Mobile and personal devices also commonly use face analyzer technology for device security. Facial recognition technology, at its core, operates on the principle of identifying and verifying individuals based on their unique facial features. Leveraging sophisticated algorithms and machine learning techniques, this technology analyzes facial characteristics such as the distance between eyes, shape of the nose, and contours of the face to create a digital representation known as a facial template. These templates serve as the basis for comparison and authentication, enabling swift and accurate recognition of individuals in diverse settings. Facial recognition enhances surveillance capabilities, facilitating proactive threat detection and response. Deployed in public spaces, airports, border checkpoints, and high-security facilities, facial recognition systems enable real-time monitoring and identification of suspicious individuals, thereby preempting potential security breaches. Moreover, in the realm of law enforcement, facial recognition serves as a powerful investigative tool, aiding in the apprehension of criminals and the prevention of unlawful activities. By swiftly matching faces captured in surveillance footage with known offenders, law enforcement agencies can expedite investigations and ensure swift justice delivery.

II. EXISTING SYSTEM

Face recognition plays a pivotal role in security systems, offering robust identification and authentication capabilities. This system introduces the application of the Haar Cascade classifier in face recognition for security purposes. The Haar Cascade classifier is a popular method for face detection, particularly adept at detecting faces within images or video streams. By leveraging machine learning techniques, the classifier can identify facial features based on patterns of contrast. This system utilizing face authentication for various applications. Initially, the user faces are trained and labelled with their ID's in the database. Then verification processes, user face capture, identify the user. In security applications, this technology is instrumental in access control, surveillance, and authentication processes.

III. PROPOSED SOLUTION

Authorized access has come a long way from using keys, pin codes, cards, and fingerprints. We now find ourselves stepping into the era of face recognition. When you think of locks, traditional door locks are probably what comes to mind. These locks have a keyhole and a manual latch. Traditional locks have some issues like forgot their keys, door lock get stuck, easily break the lock etc. People feel that traditional lock is not safe so people get move to smart locks system but even smart lock systems also have some issues like forgot their codes, fingerprint can't get access etc. This project proposed a model, using Artificial Intelligence specifically utilizing Convolutional Neural Networks (CNN) for face recognition. The system consists of a camera-equipped door lock that captures and processes facial images for authentication. During setup, users enroll their faces into the system, allowing it to create a unique facial recognition profile. The CNN algorithm trains on these profiles, learning to distinguish between authorized and unauthorized individuals with high accuracy. When someone approaches the door, the camera captures their face, and the AI instantly compares it with the stored profiles. If a match is found, the door unlocks automatically. However, if an unrecognized face is detected, the system flags it as unauthorized. In the event of an unauthorized access attempt, the system triggers a mail notification to the homeowner or designated contacts, alerting them of the security breach. This notification includes the timestamp, captured image, and any relevant details for prompt action.

3.1 FACE CAPTURE

The face capture module utilizes camera technology to capture facial images of individuals approaching the door. It employs high-resolution cameras to ensure clear and detailed images, even in varying lighting conditions. The captured images serve as input data for subsequent processes such as training and authentication. Advanced algorithms are employed to ensure efficient face capture, minimizing errors and maximizing accuracy. This module forms the foundation for the intelligent functioning of the face recognition door lock system.

3.2 TRAINING

In the training phase, the captured facial images are processed to train the convolutional neural network (CNN) model. This involves feeding the images into the neural network, which learns to extract features and patterns unique to each individual's face. Through iterative training iterations, the CNN adjusts its parameters to improve its ability to accurately recognize faces. Training data is carefully curated to encompass a diverse range of facial expressions, angles, and lighting conditions, ensuring robustness and generalization of the model.

3.3 FACE DETECTION

Face detection is a crucial component of the system, responsible for identifying and locating faces within the captured images. Utilizing sophisticated algorithms, the system can accurately detect faces amidst varying backgrounds and environmental conditions. This module plays a pivotal role in preprocessing the input data for subsequent stages such as feature extraction and authentication.

3.4 FEATURE EXTRACTION

Feature extraction involves analyzing the detected facial images to extract discriminative features that uniquely represent each individual's face. Through the CNN model, relevant facial features such as the arrangement of eyes, nose, and mouth are extracted and encoded into a feature vector. This vector serves as a compact representation of the face, facilitating efficient comparison and matching during authentication.

3.5 AUTHENTICATION

The authentication module compares the extracted features from the captured face with those stored in the system's database. By employing similarity metrics or classification algorithms, it determines the degree of resemblance between the captured face and the enrolled faces. Upon successful authentication, the door lock mechanism is activated, granting access to authorized individuals. In the event of unauthorized access attempts, the system triggers alerts and notifications to designated recipients via email, ensuring robust security measures are upheld.

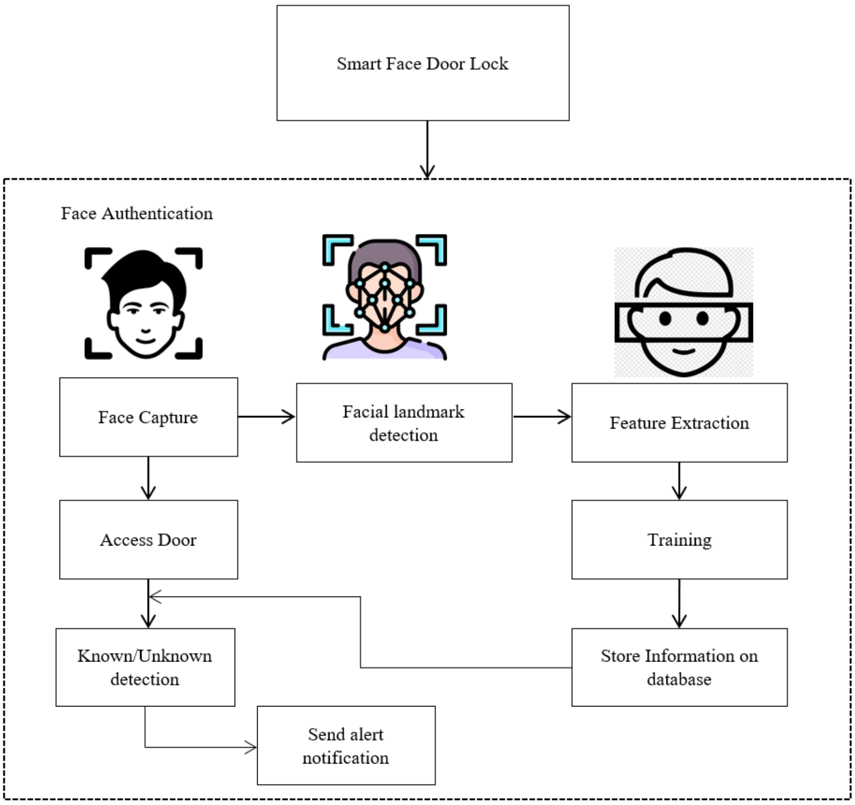

Fig 1: Workflow Of The System

The system architecture of a smart face door lock leveraging artificial intelligence, particularly Convolutional Neural Networks (CNNs), is fundamental to its functionality. Initially, the system involves face training, where individuals' facial features are captured and stored for recognition purposes. CNN algorithms are employed for efficient and accurate face recognition. Unauthorized detection mechanisms constantly monitor for unrecognized faces, triggering security protocols upon detection. Additionally, the system architecture incorporates mail notification capabilities, alerting authorized users of any attempted unauthorized access. This architecture seamlessly integrates hardware components such as cameras and sensors with software algorithms for real-time processing and decision-making. Through this interconnected system architecture, the smart face door lock ensures both security and convenience for users, epitomizing the potential of artificial intelligence in modern security systems.

IV Conclusion

The advent of smart face door locks powered by artificial intelligence, particularly utilizing Convolutional Neural Networks (CNN), represents a significant advancement in security technology. By employing face training algorithms, these systems can accurately identify authorized individuals, enhancing convenience and safety. Additionally, their capability for unauthorized detection ensures protection against potential security breaches. The integration of mail notification features further augments their functionality, providing users with real-time updates and peace of mind. As society continues to embrace smart technology, smart face door locks offer a sophisticated solution to modern security challenges. However, it's imperative to address concerns regarding privacy and data security in the deployment of such systems.

References

[1] Mun, Hyung-Jin, and Min-Hye Lee. "Design for visitor authentication based on face recognition technology using CCTV." IEEE Access 10 (2022): 124604-124618.

[2] Singh, Maneet, Shruti Nagpal, Richa Singh, and Mayank Vatsa. "Disguise resilient face verification." IEEE Transactions on Circuits and Systems for Video Technology 32, no. 6 (2021): 3895-3905.

[3] Zennayi, Yahya, Francois Bourzeix, and Zouhair Guennoun. "Analyzing the scientific evolution of face recognition research and its prominent subfields." IEEE Access 10 (2022): 68175-68201.

[4] Singh, Gurlove, and Amit Kumar Goel. "Face detection and recognition system using digital image processing." In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 348-352. IEEE, 2020.

[5] Wang, Xiang, Heyu Xue, Xuefeng Liu, and Qingqi Pei. "A privacy-preserving edge computation-based face verification system for user authentication." IEEE Access 7 (2019): 14186-14197.

[6] Ma, Yukun, Lifang Wu, Xiaofeng Gu, Jiaoyu He, and Zhou Yang. "A secure face-verification scheme based on homomorphic encryption and deep neural networks." IEEE Access 5 (2017): 16532-16538.

[7] Kaiming He; Xiangyu Zhang; Shaoqing Ren, “Deep Residual Learning for Image Recognition”, 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.