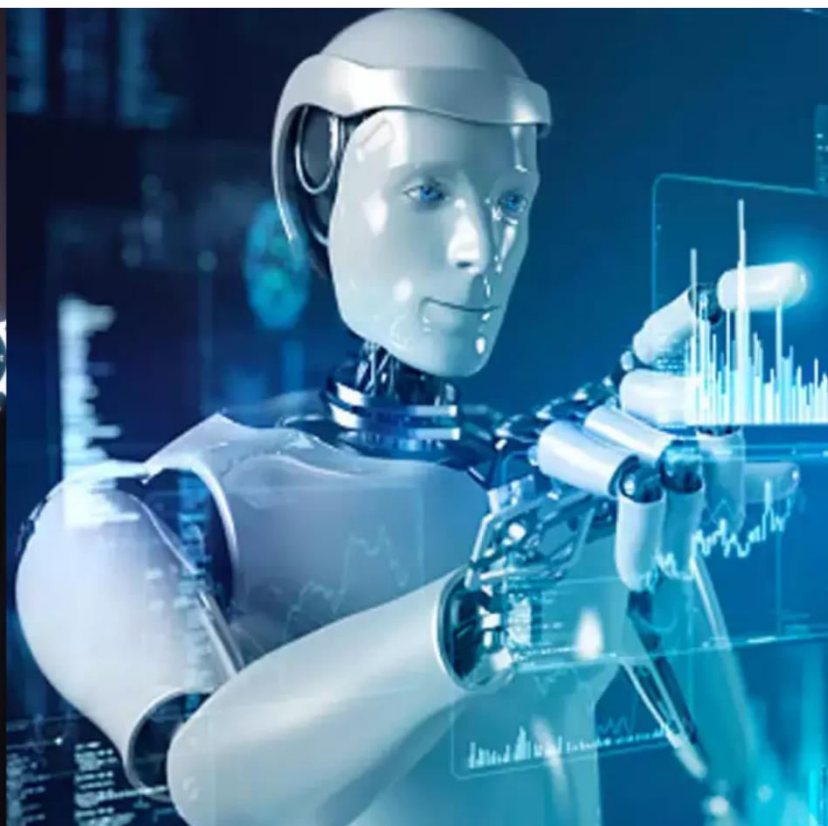




International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 7, July 2025

Face Pattern for Door Unlocking using CNN Framework

Munavar Jasim K, Ibrahim Salim M, Jihad Aboobaker, Jasir M P

Assistant Professors, Dept. of Computer Applications, MES College Marampally, Kerala, India

ABSTRACT: A face recognition system is a technology that identifies or verifies individuals by analysing and comparing their facial features. It typically involves capturing an image or video of a person's face using a camera, extracting facial features from the image, and then comparing these features against a database of known faces or templates. Face recognition systems can be used for various applications, including access control, surveillance, identity verification, and personalized user experiences in devices like smartphones and computers. They rely on advanced algorithms, often leveraging machine learning and deep learning techniques, to achieve accurate and reliable performance across different conditions and environments. This project is focusing to improve the efficiency and accuracy to recognize the faces. This paper includes several machine learning techniques such as Convolutional Neural Network (CNN), Random Forest Artificial Neural Network (ANN) which is used to unlock door by using face detection.

KEYWORDS: Face recognition, KNN, ANN, Machine Learning.

I. INTRODUCTION

Face recognition systems can be used for various applications, including access control, surveillance, identity verification, and personalized user experiences in devices like smartphones and computers. They rely on advanced algorithms, often leveraging machine learning and deep learning techniques, to achieve accurate and reliable performance across different conditions and environments. A face recognition system is a technology that identifies or verifies individuals by analysing and comparing their facial features. It typically involves capturing an image or video of a person's face using a camera, extracting facial features from the image, and then comparing these features against a database of known faces or templates. We use several techniques such as Support Vector Machine (SVM), K-Nearest Neighbours (KNN), Convolutional Neural Network (CNN), Random Forest Artificial Neural Network (ANN). The face recognition process uses the image dataset. This image dataset is collected from the Kaggle, it contains 5,124 images of 20 persons. This image dataset is divided into three parts: training, validation, and testing datasets. The training dataset consists of labelled images of faces, each tagged with an identifier that links it to a specific individual. This dataset is used to train the face recognition model. The validation dataset helps in tuning hyperparameters and making decisions about the model's architecture. It provides an intermediate check on the model's performance during the training process, helping to prevent overfitting. The testing dataset is used to assess the final performance of the trained model. It evaluates the model's accuracy, robustness, and generalization capabilities. The face recognition of door unlocking system presents a complex challenge within the fields of computer vision and human-computer interaction. Its main aim is to develop a dependable system capable of precisely identifying and classifying different faces from image or video feeds. This technology has broad applications, including enhancing virtual reality experiences, assisting robotics, and enabling touchless control systems. The difficulty arises from the wide variety of face expressions, positions, movements, as well as diverse lighting conditions and backgrounds. To tackle this challenge, advanced machine learning methods, particularly Support Vector Machine (SVM), are utilized to recognize and understand the intricate patterns and features of various faces, ensuring reliable real-time interaction between humans and technology.

II. BACKGROUND STUDY

Oghogho Ikponmwosa et al. [1] conducted research on "Face Recognition System for Automatic Door Access Control". The system employs machine learning and artificial intelligence, utilizing components such as the Raspberry Pi module, camera module, servo motor, and GSM module to create a prototype for facial biometric access control. User faces are captured by the camera module and stored in the Raspberry Pi's database. The system operates optimally

under good lighting conditions, where the camera module can effectively recognize faces. Upon recognition, the Raspberry Pi processes the images and activates the servo motor to open the door.

Ketty Siti Salamah¹ and Lutfi Arif Setiyawan, Imelda Uli Vistalina S [2] propose a method on “Design of Smart Home Security System with Face Recognition and Voice Command Based on Internet of Things”. An innovative concept for enhancing home security involves an IoT-based solenoid system with Telegram notifications. This idea leverages the Raspberry Pi minicomputer as the central processor, utilizing the webcam for facial detection and Voice Command for recognizing voice codes. The Raspberry Pi employs OpenCV to analyse facial features like eyes, nose, and mouth, along with the inputted code. Upon successful recognition of the face and correct voice code, the Raspberry Pi triggers the solenoid via a servo to unlock the door for the homeowner. Additionally, the system sends a notification through Telegram if an unauthorized access attempt is made. Tania Nurindini et al. [3] develop a study “Design of Smart Door Lock System Using Face Recognition and Mask Detection Based on Viola-Jones Algorithm with Android Integration”. In this study have both face recognition and facemask detection based on the Viola-Jones method will be used to process the webcam image. This algorithm has the advantages of a high detection rate for tracking faces in images with a low error rate. Istiqomah, Faqih Alam and dan Achmad Rizal [4] conducted a study on “Best Machine Learning Model for Face Recognition in Home Security Application”. This research explores various machine learning models for face recognition, employing the optimization tool Grid Search CV to refine these models. The machine learning methods utilized include AdaBoost, Stochastic Gradient Descent (SGD), Gradient Boosting, Random Forest, Decision Tree (DT), Gaussian Naïve Bayes, K-Nearest Neighbour (KNN), Support Vector Machine (SVM), and SoftMax Regression. Each of these methods is optimized using Grid Search CV to identify the best-performing model.

Rafly Athalla Farizan and Satria Mandala [5] develop a study on “Analysis of Smart Home Security System Design Based on Facial Recognition with Application of Deep Learning”. The Facial Recognition-Based Home Security System utilizes the Deep Learning Method, specifically employing the RNN algorithm for face recognition. The research involves evaluating the performance of RNN before and after tuning, focusing on metrics like accuracy, precision, recall, and F1 score. Keerthi Vuppula [6] conducted a study on “Smart Door Unlock System Using Face Recognition and machine learning”. It integrates a robotic locking mechanism comprising a 12V solenoid electronic lock, Raspberry Pi, and Pi camera with OpenCV. Human presence is detected using a PIR sensor. Upon detection, the Pi camera captures an image and sends it to the remote user via email. Face recognition is performed using the Haar cascade algorithm within OpenCV on the captured image. Mr. Rishabh Mantri et al. [7] develop research on “Door locking system using face recognition” To create a low-cost embedded facial recognition system for controlling an electromagnetic lock using deep learning techniques via Raspberry Pi and transferring data to the owner portal through GSM, the system utilizes the Local Binary Pattern Histogram (LBPH) algorithm for facial recognition. Morched Derbali et al. [8] presented a study on “Facial authentication based smart door lock system and anomaly detection using machine learning architectures integrated with IoT”. The facial authentication framework integrates an SDL system with IoT and machine learning-based intrusion detection methods to create a cost-effective and flexible system. Biometric authentication via facial recognition is employed to secure the smart door. Fadhillah Azmil, Insidini Fawwaz and Rina Anugrahwy [9] proposed a study titled “Smart Door System using Face Recognition Based on Raspberry Pi”. To develop a smart door system using Raspberry Pi-based facial recognition, the system integrates facial recognition algorithms with a webcam and solenoid lock controlled by the Raspberry Pi. Facial images processed through the Eigenface method are stored in a database. Raspberry Pi, acting as a mini-computer, manages image capture and storage, as well as door control based on facial recognition outcomes. Younes Akbari et al. [10] conducted a research study titled “A New Framework for Smart Doors Using mmWave Radar and Camera-Based Face Detection and Recognition Techniques” This paper introduces an innovative framework for smart doors, integrating face detection and recognition techniques using mmWave radar and camera sensors. The framework consists of four components: mmWave-based person detection, camera preparation and integration of sensor results, person identification, and door lock control for smart doors.

III. METHODOLOGY

For the face recognition process we use the image dataset. This image dataset is collected from the Kaggle, it contains 5,124 images of 20 persons. This image dataset is divided into three parts: training, validation, and testing datasets. The training dataset consists of labelled images of faces, each tagged with an identifier that links it to a specific individual. This dataset is used to train the face recognition model. The validation dataset helps in tuning hyperparameters and making decisions about the model's architecture. It provides an intermediate check on the model's performance during

the training process, helping to prevent overfitting. The testing dataset is used to assess the final performance of the trained model. It evaluates the model's accuracy, robustness, and generalization capabilities.

The proposed framework includes different steps such as input data, pre-processing, model selection, model training and face recognition. Proposed frame work is diagrammatically represented below.

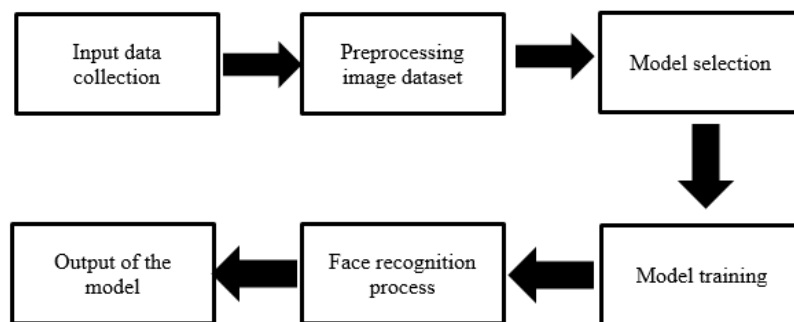


Fig 1: Proposed Framework

- Input data collection: collect the input dataset from the Kaggle, data in the form of image. Load the image dataset.
- Pre-processing the image dataset: The goal of preprocessing is to clean and format the data to improve the performance and efficiency of the model. It includes, Data Cleaning, Image Resizing, Normalization, Splitting the Dataset etc.
- Model selection: the model selection includes various machine learning algorithms Convolutional Neural Networks (CNN), K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Artificial Neural Network (ANN), Random Forest.
- Model training: Each model is trained using the training dataset.
- Face recognition process: The testing dataset is used to recognize the individual faces with the help of algorithm.
- Output of the model: It represents the evaluation of the model it includes accuracy, precision, f1 score, recall and confusion matrix.

There are 4 methods are used for face recognition. K-Nearest Neighbours (KNN) is a simple and powerful, machine learning algorithm used for classification and regression tasks. Convolutional Neural Networks (CNNs) are a class of deep neural networks specifically designed for processing structured grid data, such as images. They are particularly effective in tasks like image recognition, object detection, and other visual tasks.

The layers in a Convolutional Neural Network (CNN) are:

Input Layer: The raw input image, typically represented as a 3D matrix (width x height x channels).

Convolutional Layer: Applies filters (kernels) to the input image, creating feature maps that highlight specific features like edges or textures.

Activation Layer: Typically uses the ReLU function to introduce non-linearity and enhance the feature maps.

Pooling Layer: Reduces the spatial dimensions of the feature maps while retaining the most important information. Common pooling techniques include max pooling or average pooling.

Flattening: Converts the 2D feature maps into a 1D vector to be used as input for fully connected layers.

Fully Connected Layer: Uses the flattened vector to perform classification or regression tasks by connecting each neuron in the layer to every neuron in the previous layer.

Output Layer: Produces the final prediction or classification. For classification, this often uses a softmax function to provide probabilities for different classes.

Random Forest is an ensemble learning method used for both classification and regression tasks. It works by constructing multiple decision trees during training and outputting the class that is the mode of the classes (for classification) or the mean prediction (for regression) of the individual trees.

IV. EXPERIMENTAL RESULTS

The research study involves hardware and software for the experimental analysis to analysis the system performance. Hardware is a kind of microcomputer used by one person at a time. The research is conducted with the help of hardware equipped 11th Gen Intel(R) Core(TM) i3-1115G4 @ 3.00GHz 3.00 GHz. Software is a set of instructions, data, or programs used to operate computers and execute specific tasks. The software utilized in this experiment included development environment as Google Colab. The Google Colab (Google Collaboratory) is a free, cloud-based platform provided by Google that allows users to write and execute Python code in a web-based, interactive environment. It is particularly popular among data scientists, machine learning practitioners, and researchers for its ease of use and powerful features. It included scikit-learn for machine learning tasks, Scikit-learn (often abbreviated as sklearn) is a free and open-source machine learning library for the Python programming language. It is built on top of NumPy, SciPy, and Matplotlib and provides simple and efficient tools for data analysis and modelling.

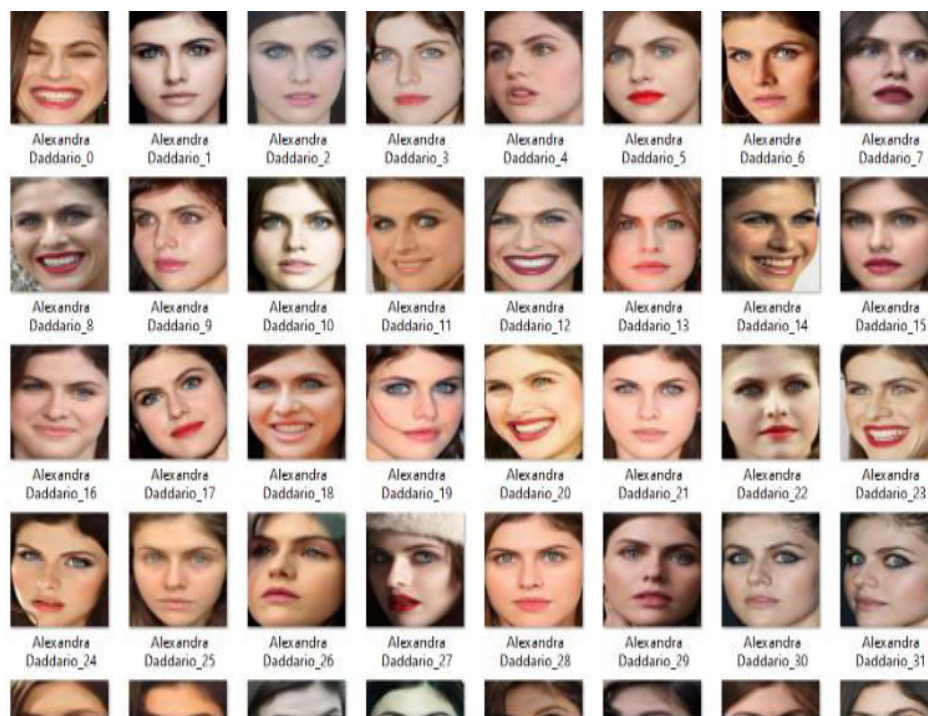


Fig 2. Image Dataset

Evaluation metrics of results include accuracy, precision, recall and F1 score.

A confusion matrix is drawn with obtained values. A confusion matrix is a table used to evaluate the performance of a classification model. It provides a summary of the prediction results by comparing the actual labels to the predicted labels. It helps in understanding not only the accuracy but also how well the model performs in distinguishing between different classes.

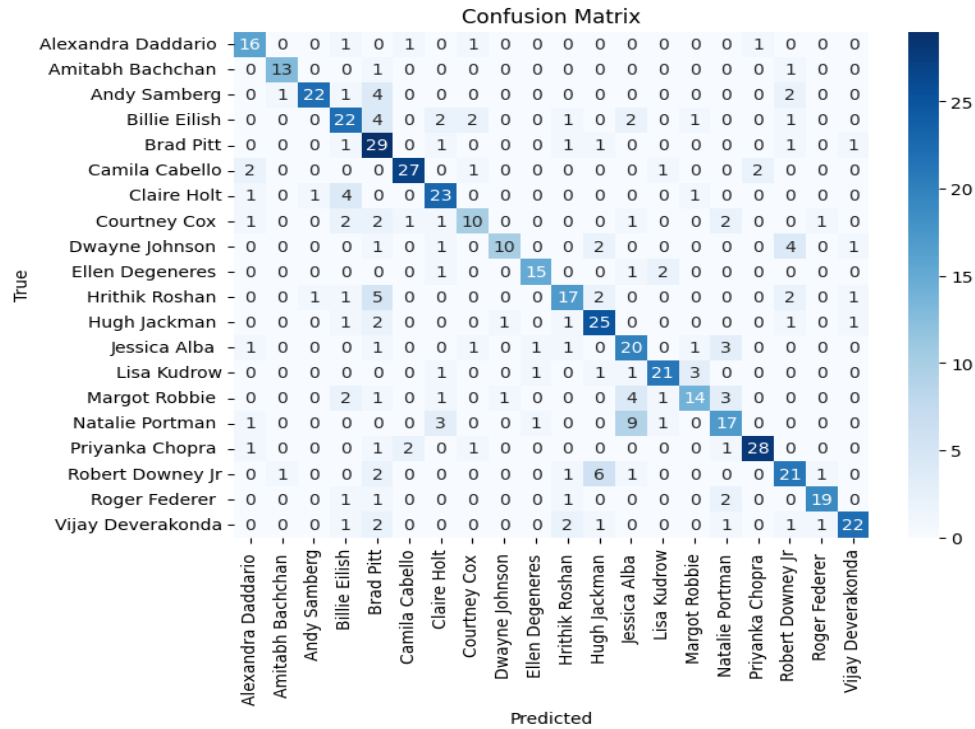


Fig 3. Confusion Matrix of CNN

Evaluation metrics such as accuracy, precision, recall and F1 score are calculated for different models for comparison. The values are represented in a tabular column below.

Model	Accuracy	Precision	Recall	F1 score
Convolutional Neural Network	0.813	0.87	0.842	0.849
Artificial Neural Network	0.766	0.835	0.766	0.758
Random forest	0.723	0.736	0.735	0.718
K-Nearest Neighbors	0.638	0.708	0.627	0.585

Table 1. Representation of Result Values

The table and confusion matrix shows that our proposed method has more accuracy, more precision, more recall and more F1 score than other methods taken for comparison.

V. CONCLUSION

In conclusion the system gets better accuracy compared with other models. The CNN model performed best, achieving an accuracy of 81.3%, precision (87%), recall and F1-score are (84%). The system aims to provide secure and hands-free access while reducing costs compared to traditional locks. Some limitations are accuracy depends on lighting and image quality, but future work could improve the system by adding a second camera for 3D analysis and increasing the recognition threshold.

REFERENCES

- [1]Oghogho Ikponmwosa, Otuagoma S, Ufuoma Jeffrey Okieke , Ebimene E. E. , Dania B. P. , Azubogu D. I. , Anamonye U.G. , Oyubu A. O. , Okpare A.O. , Eyenubo O.J. , Efenedo G. I. , Okpeki K. U., “Face Recognition System for Automatic Door Access Control”, Engineering and Technology Journal e-ISSN: 2456-3358 Volume 08 Issue 02 February-2023, Page No.-1981-1985.
- [2]Ketty Siti Salamah, Lutfi Arif Setiyawan, and Imelda Uli Vistalina, “Design of Smart Home Security System with Face Recognition and Voice Command Based on Internet of Things”, Jurnal Teknik Elektro, Vol. 15 No.1, April 2023, pp. 55 - 60 ISSN: 1858-1463 (print), 2580-6807(online).
- [3]Tania Nurindini , Mitodius Nicho Swacaesar , Rathalia Widita Astika , Hendrik Purwanto , Rieke Adriati Wijayanti , Mochammad Taufik, “Design of Smart Door Lock System Using Face Recognition and Mask Detection Based on Viola-Jones Algorithm with Android Integration”, Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi) Vol.13,No.1 (2023)
- [4]Istiqomah , Faqih Alam and dan Achmad Rizal, “Best Machine Learning Model for Face Recognition in Home Security Application”, JTIM: Jurnal Teknologi Informasi Dan Multimedia, 4(4), 300-307.
- [5]Raffly Athalla Farizan, Satria Mandala, “Analysis of Smart Home Security System Design Based on Facial Recognition with Application of Deep Learning”, KLIK: Kajian Ilmiah Informatika dan Komputer ISSN 2723-3898 (Media Online) Vol 3, No 6, Juni 2023, Hal 680-687.
- [6]Keerthi Vuppula, “Smart Door Unlock System Using Face Recognition and machine learning”, Journal for Innovative Development in Pharmaceutical and Technical Science Volume-2,Issue-3 (Mar-2019) ISSN (O) :- 2581-6934.
- [7]Mr. Rishabh Mantri, Mr. Rohit Kalveni, Mr. Mayur Vishwakarma, Prof. Amruta B. Kale , “Door locking system using face recognition”, International Research Journal of Modernization in Engineering Technology and Science Volume:05/Issue:04/April-2023.
- [8]Morched Derbali, “Facial authentication based smart door lock system and anomaly detection using machine learning architectures integrated with IoT”, King Abdulaziz University (KAU)- Jeddah.
- [9]Fadhilah Azmi, Insidini Fawwaz, Rina Anugrahwy, “Smart Door System using Face Recognition Based on Raspberry Pi”, Jurnal Infokum, Volume 10, No.1, Desember 2021 ISSN : 2302-9706.
- [10]Younes Akbari, Abdulaziz Al-Binali, Ali Al-Mohannadi, Nawaf Al-Hemaidi, Omar Elharrouss and Somaya Al-Maadeed, “A New Framework for Smart Doors Using mmWave Radar and Camera-Based Face Detection and Recognition Techniques”, Sensors 2024, 24, 172



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details