IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11649

FACE RECOGNITION SMART HOME DOOR LOCK SYSTEM USING ARTIFICIAL INTELLIGENCE

Vaijayanthimala J[1], Ramya A[2], Rubasri G[3], Rupanjani S[4]

Assistant Professor, Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology, Salem, Tamil Nadu, India[1]

Student, Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology, Salem, Tamil Nadu, India[2,3,4]

Abstract: Security is at most concern for anyone nowadays, whether it's data security or security of their own home. With the advancement of technology and the increasing use of IoT and AI, digital door locks have become very common these days. Face recognition system is broadly used for human identification because of its capacity to measure the facial points and recognize the identity in an unobtrusive way. The application of face recognition systems can be applied to surveillance at home, workplaces, and campuses, accordingly. The problem with existing face recognition systems is that they either rely on the facial key points and landmarks or the face embeddings from FaceNet for the recognition process. Deep convolutional neural networks have been successfully applied to face detection recently. Despite making remarkable progress, most of the existing detection methods only localize each face using a bounding box, which cannot segment each face from the background image simultaneously. To overcome this drawback, this project present a face detection and identification method based on improved Mask R-CNN, named G-Mask, which incorporates face detection and recognition into one framework aiming to obtain more fine-grained information of face. This paper also investigates the robustness of the face recognition system when an unknown person is being detected, wherein the system will send an SMS Web link to the owner of the house through edge computing. The door lock can also be accessed remotely from any part of the world by using a door lock integrated server account.

Keywords: IOT, AI, Deep Convolutional Neural Networks,Mask R-CNN

I. INTRODUCTION

Locks have been around for thousands of years. Probably as long as there have been valuables that people wanted to protect, locks — in some form — have been there to keep things secure. One can probably encounter all sorts of locks every day. From combination locks on school lockers to deadbolt locks on front doors, locks are all around us. Today there are many different kinds of locks. Some are very simple locks that open with a key or a combination of numbers. Others are extremely complicated locks that open with fingerprints or special electronic key cards. Today's locks feature many different types of mechanical and technological systems to increase security Effects of Traditional door locks . We were all familiar with traditional door locks on our front door. And we surely cannot forget the most frustrating thing come across in our life is practically walking out the front door suddenly recognized that you've locked the door and left your keys on the kitchen table. However, it could pose a serious security risk if your kids or pets are locked inside. Pin-and-tumbler locks are different, because they require a key to unlock them. Basic pin-and-tumbler locks have several spring-loaded pins inside a series of small cylinders. If you don't have the right key, one or more of the pins will remain in the way of the shear line. This will prevent the cylinder from turning and the lock will remain closed. Designed to ensure privacy and securing access, nowadays you'd find a lock on almost everything - from home's front door to your smartphone. This goes to show how we, as a society, have come to value privacy and safety more and more over time. Choosing the right kind of door lock for yourself is, in our view, more important than ever. Let's first clarify the distinction between 'smart' and 'traditional' locks. Most people are not used to the term 'traditional' locks - we simply call them 'locks', essentially referring to the average door lock that is non-automated and has to be manually engaged. You rotate the key and a deadbolt locks your door - easy! On the other hand smart locks (in their simplest form) are automated versions of traditional locks or retrofitting accessories, which can be integrated into smart home systems. They too usually operate a traditional deadbolt - but the mechanism can be engaged and controlled remotely, which can bring many improvements to the overall home security experience. Just like traditional locks, smart locks come in different shapes

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.11649

and forms. Some are enhanced by security cameras, keypads, touchpads, others may simply be remotely controlled directly from a mobile app. So, people gets move from traditional door lock systems to electronic door lock systems. Smart locks (like all smart-home devices), in order to exchange data between other smart home electronic devices, commonly use protocols such as Bluetooth, ZigBee, LoRa, NBIoT, and WiFi. Therefore anyone with a smart lock should definitely keep their apps and system updated and phone and passwords secured (I think we'd agree that a screen lock is pretty much a must these days). The electronic locks do not eliminate the risk of someone sweeping the key from under your doormat, picking your lock, or smashing their way in through your door Traditional locks - not as safe as we think. Despite what all of us would like to believe, most common locks are highly vulnerable to picking - an experienced burglar could snap a deadbolt and stage a break-in in only a matter of seconds. Unfortunately, your front door is not as secure as you'd think - it will, pretty much, only keep out the 'honest' criminals who are either not quite willing to push their luck or simply inexperienced beginners.

Effects of technological door locks systems Forgetful - You may be the one to forget your keys now and then, and it can be easy to forget your PIN code for the lock and when you're in a rush to get into the room or building or it is night time and dark, you don't want to be changing the code in the middle of the night or when it's raining!

II. SYSTEM STUDY

A. Existing System

In existing system various types of techniques have been applied for door lock systems. Few approaches are shown here

- **Traditional lock system:**

The key is stock or broken inside the lock Your key may be stuck due to misaligned door latch or that some components of the lock are not properly lubricated. If the key is stuck, forcing it to turn may lead to breaking the key inside the locks. Understand that you are low on time and in a hurry to meet up with an appointment. However, if you notice that the key is stuck on the lock, do not force it to open or close; you may end up aggravating the problem.

- **Slow door locks:**

Stiffened or slow door locks may occur as a result of the accumulation of dirt or grime in your locks. If you notice that the handle of your lock is slow or it is difficult inserting the key into the lock.

- **Histogram of Oriented Gradients (HOG) and Support Vector Machines (SVM):**

Detect a human face using texture analysis which includes computing a Histogram of Gradients (HOG) over a region of the face and then uses Support Vector Machines (SVMs) to recognize a face. It is resulted of 82.68 % accuracy for face recognition when the lighting conditions are optimum. During the night time the system efficiency drops by the maximum number and is unable to detect blinks.

- **Haar cascade classifier:**

Recognizing of faces is done by using Haar cascade classifiers. For this testing, it used 40 images only. Computer vision is used in the IOT. For security purpose, it implemented real time face detection by Haar classifier. It is resulted of 89 % accuracy for face recognition.

- **One time password (OTP) and SMS:**

Android application for the premise owner and Chatbot for the guest to automate the process of door locking and replacing the need of lock key with PIN. It fully exploits the capacity of the IoT environment to monitor and grant access to also unlike the other systems present in the market, our system doesn't require the guest to install any application.

Disadvantages:

- ✓ Stiffened or slow door locks.
- ✓ Forgot the keys, key cards.
- ✓ Increasing the burden of managing key cards person.
- ✓ A serious security risk if your kids or pets are locked inside.
- ✓ Accuracy is low.
- ✓ Time consuming process.
- ✓ Fingerprint lock can have problems reading fingerprints due to various reasons such as sensitivity to moisture,dryskin,oil and sweats
- ✓ It difficult shutting or locking your door properly.

B. Proposed Method

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 gets 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 Mask R-CNN, named G-Mask for accessing the door lock systems. Thus this project designed the method of the face recognition system when an unknown person face is being detected or captured, where in the system

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11649

will send an SMS link to the owner of the system.Using Mask R-CNN, named G-Mask model, that model detects an unknown person face gets captured then the system will send an SMS link to the owner that link have that unknown or unauthorized person captured face and ask permission for the owner if the owner or user gives permission then only the door gets opened otherwise not.

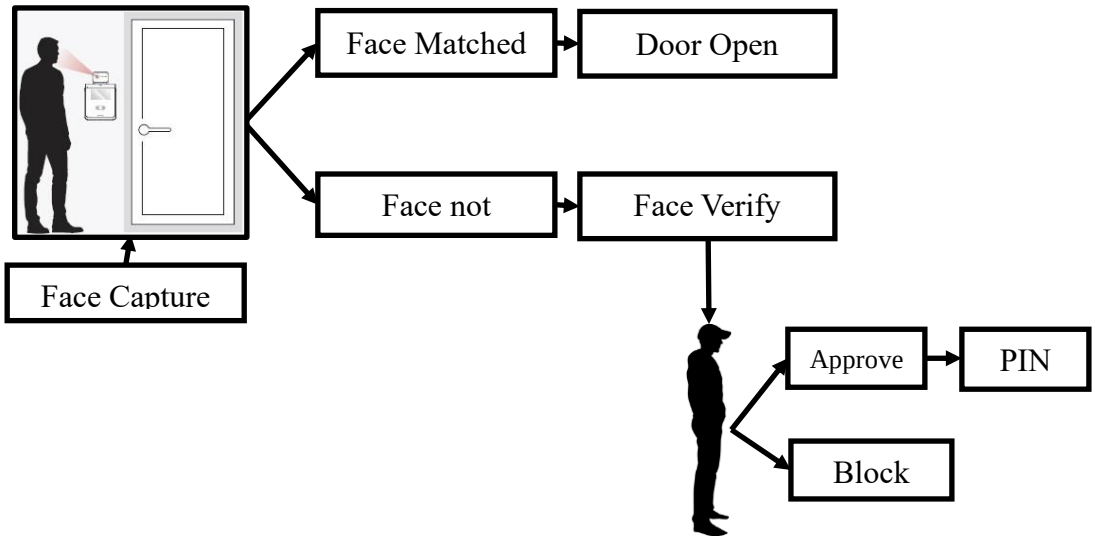

Figure: Block Diagram

III. SYSTEM SPECIFICATIONS

A. HARDWARE SPECIFICATION

- Processors: Intel® Core™ i5 processor 4300M at 2.60 GHz or 2.59 GHz (1 socket, 2 cores, 2 threads per core), 8 GB of DRAM
- Disk space: 320 GB
- Operating systems: Windows® 10, macOS*, and Linux*

B. SOFTWARE SPECIFICATION

- Server Side : Python 3.7.4(64-bit) or (32-bit)
- Client Side : HTML, CSS, Bootstrap
- IDE : Flask 1.1.1
- Back end : MySQL 5.
- Server : WampServer 2i
- OS : Windows 10 64 –bit or Ubuntu 18.04 LTS “Bionic Beaver “

IV. MODULE DESCRIPTION

A. Smart Door Access System Dashboard

A dashboard for background data management provides administrators at-a-glance information about building access by family members and friends can use. Individuals can be classified and graded into different categories and warning level in the facial information database, so customers can perform corresponding actions and processing after face recognition. For example, individuals can be classified into a whitelist, special list, temporary deployment and other warning targets. Customers can connect different systems such as door opening, door closing, and notification of security guards according to their needs.

Face Recognition in Access Control & Door Intercoms. To register, each individual to be added to the access system (eg. residents in an MDU/apartment building or multi-tenant office workers) requires an initial face scan or photograph of their face. The access control system uses AI algorithms to convert the image of the face into what is effectively a series of 'co-ordinates' - accurately pinpointing the distances between eyes, nose, mouth, ears, etc. - to create a unique identifying string of numbers which is stored in the system's database. In doing so, the access control system does not actually store an image/photograph of the individual's face stored as class label with encrypted format. A face recognition-based system will use access control end-points featuring integrated, web cameras which will provide a live face scan of the individual

DOI: 10.17148/IJARCCE.2022.11649

at the door or gate. To authenticate each individual's identity and, therefore, allow access, the system will accurately match the unique face 'co-ordinates' to those stored on the database.

B. Face Registration Module

Face Enrollment:

This module begins by registering a few frontal face of family members, friends or other know person. These templates then become the reference for evaluating and registering the templates for the other poses: tilting up/down, moving closer/further, and turning left/right.

Face Image Acquisition:

Cameras should be deployed in door to capture relevant video. Computer and camera are interfaced and here webcam is used.

Frame Extraction :

Frames are extracted from video input. The video must be divided into sequence of images which are further processed. The speed at which a video must be divided into images depends on the implementation of individuals. From we can say that, mostly 20-30 frames are taken per second which are sent to the next phases.

RNN Face Detection:

Therefore, in this module, Region Proposal Network (RPN) generates RoIs by sliding windows on the feature map through anchors with different scales and different aspect ratios. Face detection and segmentation method based on improved RPN. RPN is used to generate RoIs, and RoI Align faithfully preserves the exact spatial locations. These are responsible for providing a predefined set of bounding boxes of different sizes and ratios that are going to be used for reference when first predicting object locations for the RPN.

Feature Extraction:

After the face detection, face image is given as input to the feature extraction module to find the key features that will be used for classification. With each pose, the facial information including eyes, nose and mouth is automatically extracted and is then used to calculate the effects of the variation using its relation to the frontal face templates.

MRCNN Face Classification:

Mask Region-based convolutional neural networks or regions with CNN features (MR-CNNs) are pioneering approaches that apply deep models to object detection. MR-CNN models first select several proposed regions from an image (for example, anchor boxes are one type of selection method) and then label their categories and bounding boxes (e.g., offsets). These labels are created based on predefined classes given to the program. They then use a convolutional neural network to perform forward computation to extract features from each proposed area.

C. Face Identification

After capturing the object or face image from the Smart Glass Camera, the image is given to face detection module. This module detects the image regions which are likely to be human. After the face detection using Region Proposal Network (RPN), face image is given as input to the feature extraction module to find the key features that will be used for classification. The module composes a very short feature vector that is well enough to represent the face image.

D. Door Access

In this module the matching process is done with trained classified result and test Live Camera Captured Classified file. Hamming Distance is used to verification link and sent to the authorised person of the door access system for approval.

E .Surveillance System

If a visitor enters a prohibited area, the system will send a notification to the security guard. The fast and accurate facial image analysis engine can instantly differentiate family members, friends or other visitors and individuals in specific lists in the surveillance image and automatically provide notifications to authorized user. Our AI Security Solution also provides anti-trailing, intrusion detection and other functions to ensure asset protection and personnel safety.

F.Performance Analysis

In this module we able to find the performance of our system using SENSITIVITY, SPECIFICITY AND ACCURACY of Data in the datasets are divided into two classes not pedestrian (the negative class) and pedestrian (the positive class). Sensitivity, specificity, and accuracy are calculated using the True positive (TP), true negative (TN), false negative (FN), and false positive (FP). TP is the number of positive cases that are classified as positive. FP is the number of negative cases that are classified as positive. TN is the number of negative cases classified as negative and FN is the number of positive cases classified as negative.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.11649

$$Sensitivity = \frac{TP}{TP + FN}$$

$$Specificity = \frac{TN}{TN + FP}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

V. CONCLUSION

This paper presents a solution for Smart Home Security. Models for facial and speaker recognition have been proposed for user authentication. Mask- Region Convolutional neural network with Face Net based on one-shot learning is used for facial authentication-processing is done for the captured image of the user. Based on the features extracted, the minimum distance for facial recognition. Using these parameters, the user is classified as either a member in the database or unidentified. Apart from this, the model not only recognizes the identities of unmasked faces but also recognizes masked faces. For a masked user, their eye and nose region should be clearly visible. The proposed model reports a final ac- curacy of 82.71% for the entire Home Security system.

FUTURE ENHANCEMENT

Facial recognition access control systems can also be integrated with other logistical and system platforms, such as time & attendance, automatic payment systems or building management systems, helping to develop smart building environments.

REFERENCES

[1] R. A. Isaac, A. Agarwal, and P. Singh, “Face Recognition Security Module using Deep Learning,” J. Netw. Commun. Emerg. Technol., vol. 8, no. 10, pp. 10–13, 2018.
[2] J. Nasir and A. A. Ramli, “Design of Door Security System Based on Face Recognition with Arduino,” vol. 3, no. 1, pp. 127–131, 2019.
[3] F. Faisal and S. A. Hossain, “Smart security system using face recognition on raspberry Pi,” 2019 13th Int. Conf. Software, Knowledge, Inf. Manag. Appl. Ski. 2019, no. August, 2019.
[4] M. F. A. Hassan, A. Hussain, M. H. Muhamad, and Y. Yusof, “Convolution neural network-based action recognition for fall event detection,” Int. J. Adv. Trends Comput. Sci. Eng., vol. 8, no. 1.6 Special Issue, 2019.
[5] A. R. Syafeeza, M. K. Mohd Fitri Alif, Y. Nursyifaa Athirah, A. S. Jaafar, A. H. Norihan, and M. S. Saleha, “IoT based facial recognition door access control home security system using raspberry pi,” Int. J. Power Electron. Drive Syst., vol. 11, no. 1, pp. 417–424, 2020.
[6] Meera Mathew, Divya R S, "Survey on Various Door Lock Access Control Mechanisms," International Conference on circuits Power and Computing Technologies (ICCPCT), pp.1-3, 2017. DOI: 10.1109/ICCPCT.2017.8074187
[7] Pradnya R. Nehete, J. P. Chaudhari, et al., "Literature survey on door lock security systems," International Journal of Computer Applications, Vol.153, No.2, pp.13-18, 2016. DOI: 10.5120/ijca2016911971
[8] Neelam Majgaonkar, Ruhina Hodekar, et al., "Automatic Door Locking System," International Journal of Engineering Development and Research, Vol.4, No.1, 2016.
[9] Madhusudhan M and Shankaraiah, "Implementation of automated door unlocking and security system," International Journal of Computer Applications, pp. 5-8, 2015.
[10] Hteik Htar Lwin, Aung Soe Khaing, Hla Myo Tun, "Automatic Door Access System Using Face Recognition," International Journal Of Scientific Technology Research, Vol.4, No.6, 2015.
[11] Anuradha R.S, Bharathi R, et al., "Optimized Door Locking and Unlocking Using IoT for Physically Challenged People," International Journal of Innovative Research in Computer and Communication Engineering, Vol.4, No.3, 2016. DOI: 10.15680/IJIRCCE.2016. 0403120
[12] Chi-Huang Hung, Ying-Wen Bai, Je-Hong Ren, "Design and Implementation of a Door Lock Control Based on a Near Field Communication of a Smartphone," IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2015. DOI: 10.1109/ICCE-TW.2015.7216992
[13] Am-Suk Oh, "A Study on Automatic Doorway Access Control System Including Server Based On Bluetooth Local Communication," International Journal of Control and Automation Vol.8, No.11, 2015. DOI: 10.14257/ijca.2015.8.11.07

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11649

[14] IEEE Standards, IEEE 802.15.7-2011. "IEEE Standard for Local and Metropolitan Area Networks-Part 15.7: Short- Range Wireless Optical Communication Using Visible Light," September 2011 [Online]. Available: https://standards.ieee.org/standard/802_15_7-2011.html. DOI: 10.1109/IEEESTD.2011.6016195

[15] IEEE Standards, IEEE 802.15.7-2018. "IEEE Standard for Local and metropolitan area networks--Part 15.7: Short- Range Optical Wireless Communications," April. 2019 [Online]. Available: https://ieeexplore.ieee.org/servlet/opac?punumber=8697196. DOI: 10.1109/IEEESTD.2019.8697198

[16] Jaesang Cha, Minwoo Lee, Vinayagam Mariappan, "VTASC - Light based Flexible Multi-Dimensional Modulation Technique for OWC," IEEE COMSOC MMTC Communications - Frontiers, Vol.13, No. 2, pp.39-43, 2018.

[17] Jaesang Cha, Vinayagam Mariappan, Sukyoung Han, Minwoo Lee, "Smartphone Color-Code based Gate Security Control," International Journal of Advanced Smart Convergence, Vol.5, No. 3, pp.66-71, 2016. DOI: 10.7236/IJASC.2016.5.3.66

[18] He, K., Zhang, X., Ren, S., Sun, J., "Deep residual learning for image recognition," In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 770-778, 2016. DOI 10.1109/CVPR.2016.90

[19] Sutskever, I., Vinyals, O., et al., "Sequence to sequence learning with neural networks," In Proceedings of the 27th International Conference on Neural Information Processing Systems, pp.3104-3112, 2014.

.