



**IJIRCCCE**

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 8, August 2023

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

**Impact Factor: 8.379**

 9940 572 462

 6381 907 438

 [ijircce@gmail.com](mailto:ijircce@gmail.com)

 [www.ijircce.com](http://www.ijircce.com)

# Face and Http Link Based Door Access Control System Using Facial Recognition Engine

**Dr. T. GEETHA, Ms. G. SIVAGAMI, SARAN.B**

Head, Department of MCA, Gnanamani College of Technology, Namakkal, India

Assistant Professor, Department of MCA, Gnanamani College of Technology, Namakkal, India

Student, Department of MCA, Gnanamani College of Technology, Namakkal, India

**ABSTRACT:** The Access control system is a security device that helps to provide safety to any offices, buildings, apartments, or shopping complex by giving flexible control over who is allowed to enter your premises. It can also control the “in and out” time of employees and students through a network. It is the most commonly used biometric system in electronic locks control doors using a Rafid card. An access control system is the most important device for security used in Residential, Offices and Hotels. 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. 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.

## 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. 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. We were all familiar with traditional door locks on our front door. However, it could pose a serious security risk if your kids or pets are locked inside. 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 and forms. Some are enhanced by security cameras, keypads, touchpads, others may simply be remotely controlled directly from a mobile app. So, people get to 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, NB-IoT, 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.

## II. 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 stuck 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.

### 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.

## III. PROPOSED SYSTEM

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 will send an SMS link to the owner of the system.

### Mask R-CNN model:

The proposed method is extended from the Mask R-CNN framework, which is the state-of- the-art object detection scheme and demonstrated impressive performance on various object detection benchmarks. As stated in Figure 3.1, the proposed G-Mask method consists of two branches, one for face detection and the other for face and background image segmentation. Face Feature Module is used to extract the facial features of the input image, and the Region of Interest (RoI) is rapidly generated on the feature map through the Region Proposal Network (RPN) You give it an image, it gives you the object bounding boxes, classes and masks. This is a major benefit to the end user, but it is also especially beneficial to multifamily buildings and offices by reducing their burden of managing key cards.

### Remote Control Access:

The registration process one can conveniently grant access to new users even remotely. And can also customize settings and easily give one-time or temporary access to your premises. It analyses the faces of every person trying to enter and allows entry only the persons pre-authorized by the user.

#### Face Verification Link:

Face Verification Link will be generated and sent to user to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification, which either authorizes the door to open appropriately or signals a security-violation alert to the security guard and enable the buzzer.

#### Blacklist:

It allows the user to create “blacklist” or banned individuals to detect and prohibit them from entering your business.

### IV. BLOCK DESCRIPTION

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. But there is a lack of issues in both traditional and smart lock systems such as fingerprint not access, forgot the key cards, security is low etc. So, to avoid the above issues this project proposes a facial recognition system for the door lock system.

#### 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.

#### 2.1.3. 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.

#### Face 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. In MR-CNN, the inputted image is first divided into nearly two thousand region sections, and then a convolutional neural network is applied for



each region, respectively. The size of the regions is calculated, and the correct region is inserted into the neural network. It can be inferred that a detailed method like that can produce time constraints. Training time is significantly greater compared to YOLO because it classifies and creates bounding boxes individually, and a neural network is applied to one region at a time. In 2015, Fast MR-CNN was developed with the intention to cut down significantly on train time.

## 2.2. 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

## 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 calculate the difference according to the result the door is open or generate face verification link and sent to the authorized person of the door access system for approval.

## 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.

## V. SYSTEM IMPLEMENTATION

The implementation of the Web-based Simulated System of Face Door Lock System using FRCNN and Face Verification Link Approval System can be broken down into several steps as follows:

### Set up the environment and required libraries:

Install the required libraries such as TensorFlow, Keras, OpenCV, Flask, Twilio API, etc.

Set up the web server for hosting the web application.

### Implement the SMS Notification System:

Use the Twilio API to send SMS notifications to the house owner's mobile phone.

Include a Face Verification Link in the SMS notification to allow the house owner to approve or deny access to the building or house.

### Create the Door Animation:

Implement a door opening animation that runs when a person is authorized to enter.

The animation should run for a specified duration before the door closes again.

### Testing and Debugging:

Test the system thoroughly to ensure that it works as expected.

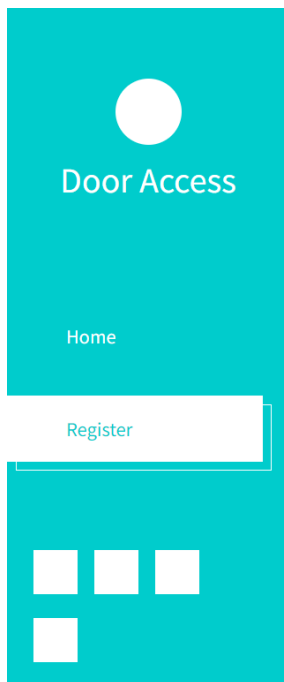
Debug any issues that arise during testing.

### Deployment:

Deploy the system on a web server accessible to the house owner and other authorized persons.

Ensure that the system is secure and protected against unauthorized access.

Overall, the implementation of this system requires expertise in deep learning, computer vision, web development, and software engineering. Careful attention must be paid to data privacy and security to ensure that the system is robust and reliable. The system should be thoroughly tested before deployment to ensure that it meets the requirements and expectations of the end-users.



### Family Head - Register

Name

Mobile No.

Email

Username

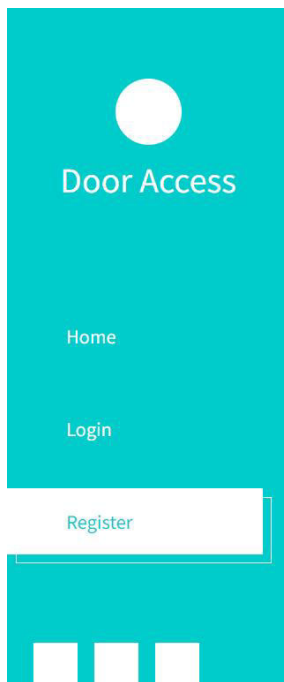
Password

Facial Recognition

Home Door Access

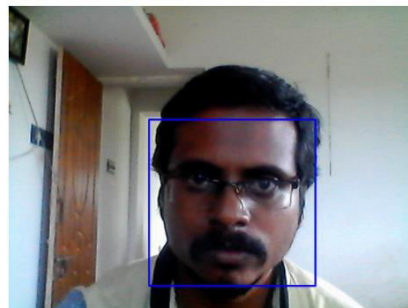
Email: info@security.com

However, we use Face ID to access our Home Door by secure way.



### Family Head - Register

#### Add Face Template



Facial Recognition

Home Door Access

Email: info@security.com

However, we use Face ID to access our Home Door by secure way.



Door Access

## VI. 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 accuracy of 82.71% for the entire Home Security system.

#### REFERENCES

1. B. Septian, A. Wijayanto, F. Utaminigrum, and I. Arwani, "Face Recognition Untuk Sistem Pengaman Rumah Menggunakan Metode HOG dan KNN Berbasis Embedded," Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 3, no. 3, pp. 2774–2781, 2019.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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
8. 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
9. Neelam Majgaonkar, Ruhina Hodekar, et al., "Automatic Door Locking System," International Journal of Engineering Development and Research, Vol.4, No.1, 2016.
10. Madhusudhan M and Shankaraiah, "Implementation of automated door unlocking and security system," International Journal of Computer Applications, pp. 5-8, 2015.



**INNO**  **SPACE**  
SJIF Scientific Journal Impact Factor  
**Impact Factor: 8.379**

**doi**<sup>®</sup>  
**CROSS** **ref**

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
**INDIA**



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 **9940 572 462**  **6381 907 438**  **ijircce@gmail.com**



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details