IOT Powered Smart Doorbell System For Enhanced Home Security And Communication

Mrs.Donepudi Priyanka[1], Peddagamalla Kavitha[2], Naragam Vineela[3], Muthireddy Naga Sai Deepika[4], Molleti Aanoor Venkata Mahesh[5]

[1]Assistant Professor, [2,3,4,5] UG Scholar

Department of Computer Science and Engineering,
Seshadri Rao Gudlavalleru Engineering College,
Gudlavalleru, Andhra Pradesh, India.

ABSTRACT

This project aims to enhance security using facial recognition technology. By comparing captured facial images with stored ones, the system unlocks a door for authorized users. Facial recognition is increasingly popular for its effectiveness in identifying intruders and restricting unauthorized access, outperforming other methods like fingerprints or passwords. However, achieving quick and accurate recognition poses a challenge. This project addresses this by simplifying images, storing them, and rapidly comparing new images for matches. When a match is found, a controller unlocks a door. If an unknown face is detected, it alerts designated individuals for a decision on granting access. This project demonstrates how facial recognition tech can swiftly enhance security measures.

INTRODUCTION

In the era of expanding interest in smart home systems driven by the Internet of Things (IoT), security remains a paramount concern. Traditionally, security experts have recommended approaches like biometrics and passwords to fortify home security. However, as technology evolves, the focus has shifted markedly towards face recognition systems, seen as a pivotal advancement in safeguarding homes.

The proposed project centres on leveraging a Raspberry Pi micro-controller board, a Pi camera module for face recognition, and a programmable stepper motor to enhance home security. The foundational step involves installing a suitable Linux-based operating system onto the Raspberry Pi micro-controller board. The core mechanism for unlocking the door involves positioning a stepper motor at the door latch, programmed to respond when the system authenticates a person in front of the camera. The innovation lies in the integration of image processing technology, utilizing the Pi camera module for facial recognition. This module interfaces with the Raspberry Pi, facilitating the storage of various facial profiles within the database. When an individual approaches the home, they stand before the camera. The system employs image recognition to compare the captured face with those stored in the database, granting automatic door access upon a match. In cases of mismatch, an alert message promptly notifies the homeowner.

This project represents a convergence of IoT, image processing, and Raspberry Pi technology, offering a sophisticated yet user-friendly means to reinforce home security through facial recognition, ensuring seamless access while maintaining robust protective measures.

LITERATURE REVIEW

The literature survey explores several facets of face recognition systems implemented within IoT-based security setups. Kulkarni, Bagul, and Dukare (2017) introduced a system adaptable for various connections, such as cascade, parallel, or series, offering flexibility for system expansion. However, its limitation lies in the absence of a secondary unlocking method if facial recognition fails for authorized users. The system's dual functionality in online and offline modes adds versatility, utilizing internet connectivity based on operational requirements.

Vamsi, Sai, and Vijayalakshmi (2019) highlighted the efficiency of the LBPH algorithm for face recognition due to its representation of local features, especially in controlled environments. Yet, its sensitivity to scale requires pre-processing for normalization. While robust against grayscale transformations, LBPH's performance diminishes with variations in pose and illumination.

Gsponer (2018) aimed to create a cost-effective security system utilizing facial recognition, emphasizing three core elements: data gathering, machine learning, and facial recognition. Similar to the previous systems, the absence of an alternative unlocking method poses a limitation.

Deshmukh, Nakrani, Bhuyar, and Shinde (2019) utilized Haar classifiers for face detection, highlighting its advantage in calculating features rapidly due to integral image usage. However, while it offers swift detection, Haar classifiers tend to sacrifice accuracy compared to techniques like CNN.

In examining the literature and proposed systems, a notable aspect absent from both is the incorporation of email alerts and IoT-driven responses when an unauthorized user attempts access. The reviewed systems primarily focus on facial recognition as the primary authentication method for door unlocking, but they lack provisions for immediate alerts or actions when unauthorized entry is detected.

The proposed system, in contrast, introduces a novel layer of security enhancement. Apart from facial recognition-based door unlocking, it incorporates an alert mechanism via email notification to the homeowner or administrator when an unrecognized individual approaches. Furthermore, the system harnesses IoT capabilities to enable responsive actions upon unauthorized access attempts. This could involve triggering alarms, capturing images of the intruder, or logging the event for future reference, enhancing the system's security by providing real-time alerts and potential deterrents against unauthorized entry. This addition elevates the proposed system beyond the scope of the reviewed literature, addressing a crucial aspect of security by integrating proactive

measures in response to unauthorized access attempts, thereby enhancing the overall robustness of the IoT-based facial recognition security system.

PROPOSED METHOD

Constructing The proposed system shown in figure1 centers on utilizing Raspberry Pi in conjunction with a USB camera to establish a comprehensive security setup. Upon program activation, the Pi camera assumes the role of a surveillance system. When the authorized owner stands before the camera, facial recognition triggers the unlocking of the door, granting access. However, if the facial features do not match those stored in the system's database, an alert is promptly dispatched to the administrator. Simultaneously, an image of the individual attempting access is captured and stored in a designated folder within the Raspberry Pi. This feature serves as a security measure, enabling the system to document unauthorized access attempts for subsequent review and analysis.

To further enhance user convenience and remote access control, the system integrates a door unlock app. This app empowers the user to remotely unlock the door for authorized individuals even when they are not physically present at home. This functionality adds a layer of flexibility and control, allowing homeowners to manage door access conveniently from a distance, ensuring secure and controlled entry even in their absence.

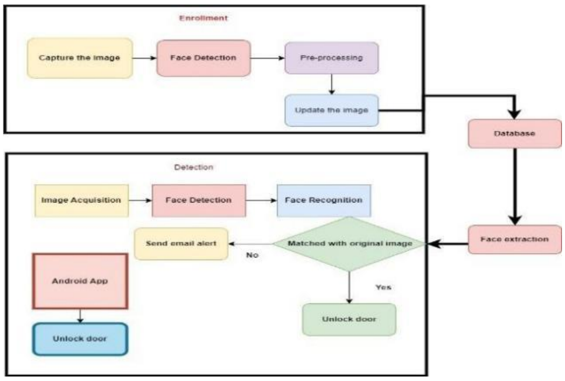


Figure 1: Proposed system architecture.

SYSTEM ARCHITECTURE

The system architecture is explained in following sections.

A. Enrolment:

Capture and Pre-Process Images: The system utilizes a camera module to capture images of individuals. These images undergo pre-processing, enhancing their suitability for face detection.

Face Detection: The system employs accurate face detection algorithms, specifically a Convolutional Neural Network (CNN), to identify faces. If a face isn't detected correctly, the system restarts for accurate processing.

Pre-Processing: Prior to feature extraction using PCA (Principal Component Analysis), the face images undergo additional pre-processing to enhance recognition rates.

Update Database: Processed images of authorized users are stored in a designated folder for recognition during access attempts.

B. Face Detection and Recognition:

CNN for Detection and Recognition: CNN, known for high accuracy, detects the homeowner's face. The system then matches it against stored face data in the database. Upon a successful match, the Raspberry Pi signals the solenoid lock to unlock the door.

C. System Implementation:

Hardware Setup: The system utilizes a modified Pi Camera module connected to a Raspberry Pi 4 Model B via WLAN for real-time face recognition.

Objective: Implement a face recognition system based on CNN (OpenFace) within a real-time embedded system like Raspberry Pi, showcasing practical use through Automated Door Access.

Enhancements: Future system improvements include implementing anti-spoofing measures like eye-blink detection and sending an intruder alert email containing a visitor's picture.

Convolutional Neural Networks (CNNs):

CNN Operations: CNNs perform four main operations: convolution, non-linearity (ReLU), pooling or subsampling, and classification. These operations facilitate efficient feature extraction and recognition.

The proposed system showcases a comprehensive approach to face recognition, emphasizing real-time application and security enhancements through CNN-based detection, with future considerations for anti-spoofing measures and intruder alerts.

REQUIREMENTS

Raspberry Pi 4 Model B:

The selection of the Raspberry Pi 4 Model B as the core hardware for this project was meticulous, considering its exceptional features and versatility. In an extensive evaluation of microcontrollers, the Raspberry Pi stood out for its robust processing capabilities, affordability, and adaptability across diverse programming environments. Running on the Linux OS, it offers access to an extensive array of compatible libraries and applications.

Figure 2: Raspberry-pi 4

Key Features of Raspberry Pi 4 Model B:

Connectivity: Featuring an Ethernet port for network connectivity within the same subnet, it allows device access and management. With four USB ports, it facilitates connections for peripherals like keyboards, mice, cameras, and other USB-compatible devices.

Interface and GPIO Pins: Equipped with an HDMI port providing an interface to access the installed operating system, it aids initial device setup. The GPIO (General Purpose Input/Output) pins, divided into 3V and 5V groups, enable signal reception and transmission, crucial for interfacing with external components.

Software and OS Compatibility: Upon acquisition, the Raspberry Pi doesn’t come with a pre-installed operating system, which can be downloaded from the Raspberry website and transferred onto an SD card for installation. Supported by Debian and Arch Linux ARM distributions, it primarily uses Python as its main programming language, supplemented by BBC BASIC, C, and Perl.

USB Camera Module: The USB Camera module seamlessly interfaces with the Raspberry Pi through its USB ports. Offering compatibility with various USB cameras, it enhances flexibility in choosing camera models based on project requirements and supports different image and video resolutions efficiently.

Figure 3: USB camera

Additional Components: Apart from the USB Camera module, the system integrates a Solenoid Lock, offering power-on unlocking and locking modes, ensuring secure access based on the solenoid's power status. Additionally, a Buck Converter efficiently steps down voltage from the input supply to the load, ensuring optimal power management within the system.

Figure 4 :Solenoid lock

Each hardware component, from the Raspberry Pi as the central controller to the USB camera module, solenoid lock, and buck converter, plays a vital role in ensuring functionality, connectivity, and security within the system.

RESULTS AND DISCUSSION

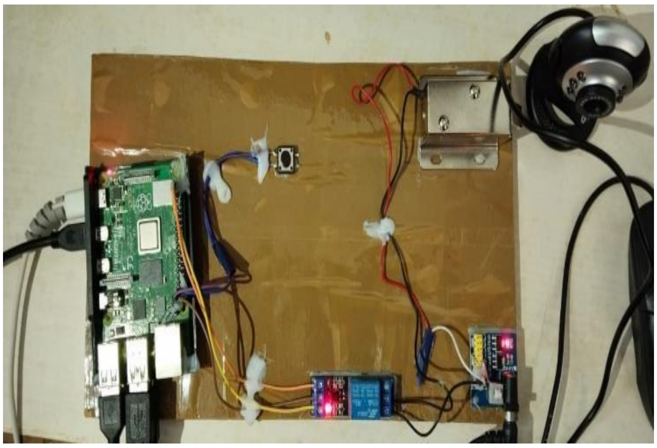
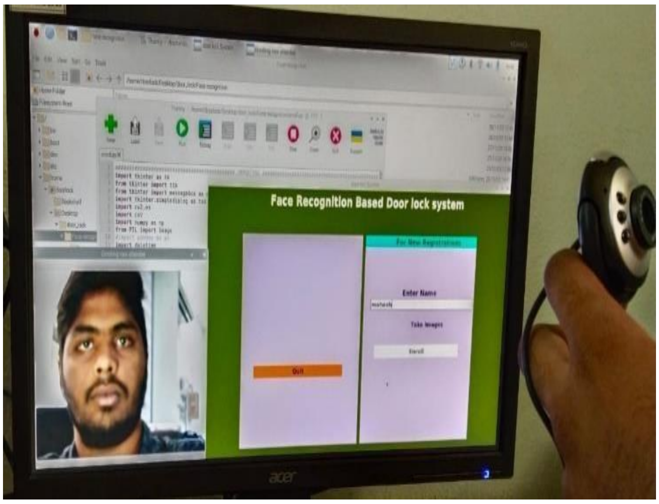


Figure 5: Project kit.

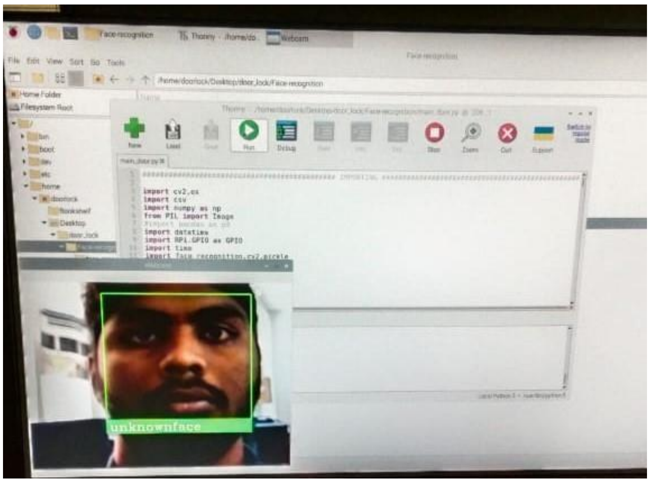
The above figure represents the kit used along with a special camera module that can take pictures and a solenoid lock. The main component used is raspberry pi-4. Moreover, it keeps you connected to your doorstep from anywhere.



```
import tkinter as tk
from tkinter import ttk
from tkinter import messagebox as
import tkinter.simpledialog as tsd
import cv2,os
import csv
import numpy as np
from PIL import Image
#import pandas as pd
import datetime
```

Figure 6: Enrolling a person’s face.

Fig.6 depicting capturing and storing facial features for potential recognition in the future is part of the face enrollment procedure for the smart doorbell system. When a user uses the Blynk app to enroll, the system gathers a set of photos in order to do facial mapping on a large scale and showing when a known person is effectively recognized by the smart doorbell system. After analyzing facial recognition data, the system automatically activates the access control mechanism, opening the door and allowing permitted access.



```
import cv2,os
import csv
import numpy as np
from PIL import Image
#import pandas as pd
import datetime
import RPi.GPIO as GPIO
import time
import face_recognition,cv2,pickle
```

Figure 7:Identifying the registered person’s face

CONCLUSION

The Raspberry Pi 4 Model B serves as the linchpin of this project, meticulously chosen for its robust processing prowess, adaptability across programming environments, and extensive connectivity options. Its integration with a USB Camera module offers versatile image capture, while GPIO pins facilitate seamless interfacing with peripherals. Complemented by a Solenoid Lock and a Buck Converter, this hardware ensemble ensures security, efficient power management, and seamless functionality. Each component’s synergy within the system, from the Raspberry Pi to the USB Camera, solidifies the project's foundation, enabling a robust and adaptable platform for the envisioned face recognition system.

REFERENCES

[1] S. Kulkarni, M. Bagul, and A. Dukare, "Face recognition system using IoT," IJARCET Publications, 2017.

[2] T.K.Vamsi, K.C. Sai, and V. M, "Face recognition based door unlocking using Raspberry Pi," IJARIIT Publications, Feb. 2019.

[3] D. Gsponer, "Building a Raspberry Pi security system using facial recognition," Haaga-Helie publications, 2018.

[4] K.M. Mande and N. Bhansali, "Smart door using face recognition," IRJET Publications, May 2018.

[5] A.D. Deshmukh, M.G. Nakrani, D.L. Bhuyar, and U.B. Shinde "Face recognition using OpenCV on IoT for smart door," Elsevier SSN publications, Feb.2019.