



A Face Recognition-Based Intruder Detection System for Automatic Door Control

*¹Daniyan, A. & ¹Michael O. M.

¹Electrical And Electronics Engineering Department, Federal University of Technology, Minna, P.M.B. 65, Niger State, Nigeria

*Corresponding author email: a.daniyan@futminna.edu.ng +234 806 420 3455

ABSTRACT

In recent years, theft and unauthorized access to private areas in homes and communities has become a growing concern, leaving individuals feeling insecure about their lives and properties. To address this problem, this paper proposes a solution that features a facial recognition system to prevent entry by unauthorized individuals.

The system uses an ESP32 Camera module and the Arduino Integrated Development Environment (IDE) to capture and store facial biometric details through facial recognition techniques. The data is saved in a database that is accessible through a web interface enabled by HOTSPOT connection. The camera's Internet Protocol (IP) address also allows for live streaming as an added feature.

An ATmega328 microcontroller on the Arduino IDE receives signals from the ESP32 camera, process the data and operate the door accordingly. When the ESP32 Camera recognizes a face, it sends a signal to the microcontroller to open the door. If the face is not recognized, the door is kept locked to prevent entry by intruders.

The proposed solution effectively identifies intruders and those with authorized access but grants access only to authorized individuals in its database. This ensures a secure environment for homes and communities, providing peace of mind to individuals who have long been worried about theft and unauthorized access.

Results demonstrate that the proposed facial recognition system is has been able to provide a secure environment for homes and communities by denying entry to intruders and granting access only to recognized individuals.

Keywords: *Biometric, Database, Face detection, Facial, Intruder detection, Security*

1 INTRODUCTION

Intrusion, the act of an unauthorized person gaining access to a restricted zone without your permission, is on the rise. A human intrusion detection system is designed to detect an unauthorized entry into a building or a protected area and deny such unauthorized access to protect personnel and property from damage or harm (Kumar, *et al.*, 2013b). Security systems are mainly used in residential, commercial, industrial, and military properties for protection against burglary (theft) or property damage, as well as personal protection against intruders. The human presence of security guard may not be completely trustworthy (Kumar, *et al.*, 2013b). In such cases, this system provides proper detection of intruder and provides security. By using this system, we can reduce robbery by detecting the intruder and deny access to unauthorized entry so we can ensure that no harm takes place in our home (Sampson, 2011). In the designed system, the camera is kept outside the room and the continuous video is captured by the camera. The system is designed in such a way that as soon as someone enters the room, the processing takes place at the instance of time (Sampson, 2011). The proposed system thus should be efficient in all aspects

including the cost as the ESP32 camera is employed. Most countries are gradually adopting smart door security system. A major part of any door security systems are identifying accurately the persons who enter through the door. Face recognition is probably the most natural way to perform authentication between human beings (Sampson, 2011). With theft and robbery amongst some of the most dangerous threats across the globe in recent times and with home security systems constantly failing to safeguard houses and offices, Facial Recognition has gained prominence as a result of its effectiveness in identifying intruders. A survey conducted by FBI, perfectly illustrates why facial recognition is ever more important as it shows that all the intrusion problems occurred in absence of the owners at home. In the year 2012, a house is being invaded by the intruders for every twenty seconds (Sampson, 2011). Among these, only 10% of them end up in arrests, and rest of them are still suffering from intruders. Whilst there are other solutions for this problem like home automation systems, alarm detection systems etc; there is a chance of producing false alarms by these systems. This is the main reason for those systems to have a higher rate of failure (Sampson, 2011). Thus, there is a need to design a system that can detect the intruder who tries to enter the home or



office. This research aims to design a security system that will detect intruders based on facial recognition and will only give access into the building to recognized faces by automatically opening a motorized door.

An efficient and accurate home security and access control to the doors system which is based on face recognition is very important for wide range of security application. Security is an important aspect or feature in the smart home applications (Karri, *et al.*, 2015). Most of the countries are gradually adopting smart door security system. The most important major part of any door security systems is identifying accurately the persons who enter through the door. Face recognition is probably the most natural way to perform authentication between human beings (Karri, *et al.*, 2015). Additionally, it is the most popular biometric authentication trait, after fingerprint technology. Most of the security system was implementing a Principal Component Analysis (PCA) algorithm for face recognition on hardware platform for its dimensionality reduction and simplicity. Wireless technologies for example and ZigBee, radio frequency identification (RFID) and etc are used in access control systems (Karri, *et al.*, 2015). This proposed system also act as home security system for both Intruder detection and provide security for door access control by using facial recognition for home environment. Human body is identified as an intruder within a home environment achieved by capturing live video from web camera and processing will be done on captured video frames to identify the motion detection of the intruder (Khan, *et al.*, 2012). The web camera capture the series of images as soon as the intruder motion is detected in certain area of the home premises and also it send automatic e-Mail alerts along with captured images and other contact details to the nearby police station or control room's e-mail about the intruder detected to take further immediate necessary actions (Khan, *et al.*, 2012). The advantage of this system is for accessing the door such that face detection and recognition is performed by using face detection technique and the entire face recognition is completed by pressing single and tiny push button switch. Face recognition includes feature extraction from the facial image, recognition or classification and feature reduction (Khan, *et al.*, 2012). PCA is an effective feature extraction method used based on face as a global feature. It effectively reduces the dimension of captured images and at the same time holds the primary information (Khan, *et al.*, 2012). In this project, face recognition system is implemented based on standard PCA (Principal component analysis) algorithm. Classification or Recognition is done by the measure method such as Euclidean distance technique, which is used to classify the feature of images stored in the database and captured test images (Khan, *et al.*, 2012).

In 2018, (ARL, 2018) developed a technique that would allow them to match facial imagery obtained using a thermal camera with those in databases that were captured using a conventional camera. Known as a cross-spectrum synthesis method due to how it bridges facial recognition from two different imaging modalities, this method synthesizes a single image by analyzing multiple facial regions and details. It consists of a non-linear regression model that maps a specific thermal image into a corresponding visible facial image and an optimization issue that projects the latent projection back into the image space. ARL scientists have noted that the approach works by combining global information (i.e., features across the entire face) with local information (i.e. features regarding the eyes, nose, and mouth). According to performance tests conducted at ARL, the multi-region cross-spectrum synthesis model demonstrated a performance improvement of about 30% over baseline methods and about 5% over state-of-the-art methods (ARL, 2018).

Lwin, *et al.*, (2015) proposed a door lock access system which comprised mainly of three subsystems: namely face detection, face recognition and automatic door access control. Face recognition is implemented by using the Principal Component Analysis (PCA). The door will open automatically for the known person due to the command of the microcontroller. On the other hand, alarm will ring for the unknown person. Drawback of this system is input images are taken through a web camera continuously until the 'stop camera' button is pressed (Lwin, *et al.*, 2015). Someone is required at the location to check unauthorized person's images or status of the system and take further action. Personal computer (PC) is connected with the microcontroller, The whole system will not work if PC is crashed or Non-Function.

Kumar, *et al.*, (2013a) presented the implementation of a low-cost wireless home security system using ZigBee protocol and remote access through internet. A ZigBee based star network with two nodes had been established employing Xbee radio, ARM7, PIC, and MBED microcontroller. The detection of the intruder motion, gas leakage detection and visual surveillance of the home were provided with the help of Passive Infrared Sensor (PIR), Gas sensor (GH-312) and Camera (LS_Y201). Problem is here multiple micro controllers are used; usage of ZigBee based network to communicate with the base station is limited to 100-150 meters long distance only. Base station is dependent on only Ethernet for internet connectivity.

Kartik, *et al.*, (2013) proposed two systems are proposed, one is based on GSM technology and other uses web camera to detect the intruder. The first security system uses a web camera, installed in house premises, which is

operated by software installed on the PC and it uses Internet for communication. The camera detects motion of any intruder in front of the camera dimensions or camera range. The software communicates to the intended user via Internet network.

In 2003, (Mae, *et al.*, 2003) presented a system that monitors everything by moving cameras. The system can increase the efficiency of monitoring and can eliminate the blind spots of fixed cameras. In this system, a mobile manipulator is developed which is equipped with cameras at the arm end for purpose of monitoring.

2 METHODOLOGY

2.1 MATERIALS

In order to build our proposed system, the following hardware components were used: ESP32-Camera Module, Micro-Controller Unit (ATmega328), power supply unit (transformer, rectifier diode, voltage regulator, filter capacitor), dvd mini, servo motor, JQC-3F-12VDC relay, and BJTs.

2.2 METHODS

The approach used in realizing a functional prototype of this work is grouped into two categories which are: software design and hardware design.

2.2.1 Software Design

The ATmega328 microcontroller was connected to the computer system via Universal Serial Bus (USB) data-cable. The Arduino Integrated Development Environment (Arduino IDE) which is a programming software installed on a computer system was used to upload the codes written in C++ to the ATmega328 microcontroller. The ESP32-CAM was mounted on its Future Technology Device International (FTDI) programmer's board and connected to the computer system using USB data Cable. The Arduino IDE program software is compatible with the ESP32-Cam FTDI programmer's board and written codes in C++ was uploaded to the ESP32-CAM module.

2.2.2 Hardware Design

This section shows snapshots of the connections together with the final soldering work done on the Vero-Board and the fully designed Prototype. Bread board was not used for preliminary connections and testing because the ESP32 camera pins does not match the holes on the bread board. Figure 1 is a snapshot of the fully built prototype.



Figure1: Fully Built Prototype

3 RESULTS AND DISCUSSION

In this section, results obtained during testing and evaluation of the proposed system are presented and discussed. During the software design, compatibility between software application and programming language to be used analysed and a suitable programming language was chosen, in this case, C++. Furthermore, Arduino software (IDE) was selected as the platform to write, edit, and upload written codes to the ESP32-camera module and ATmega328 microcontroller. The major challenge encountered during the software design was that the Arduino software had to be downgraded in order to access the face recognition of ESP32-camera module each time the module is being worked upon. The fully built prototype was connected to power supply and turned on, major tests based on its intended function were carried out and information gotten forms part of the results which is the next category.

3.1 RESULTS

Obtained from the working prototype were the visual outputs captured as screenshots on the Web-interface provided by the ESP32-Camera module which has a Wi-Fi-HOTSPOT connection embedded in its system that provides real time visual streaming and snapshots of the prototype's door as it is being operated automatically in the process.

Figure 2 shows the web-interface that serves as an input as it prompts you to enroll face after activating face detection and recognition

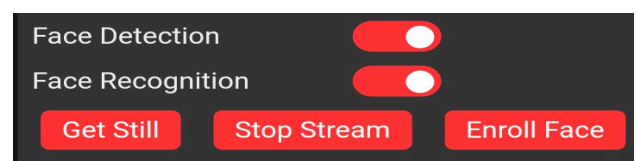


Figure 2: Command Prompt

The screenshot in Figure 3 shows when the face of an individual is being captured, enrolled and saved to database

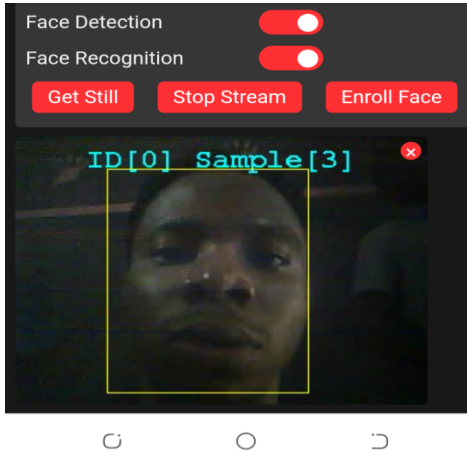


Figure 3: Registering Facial Data

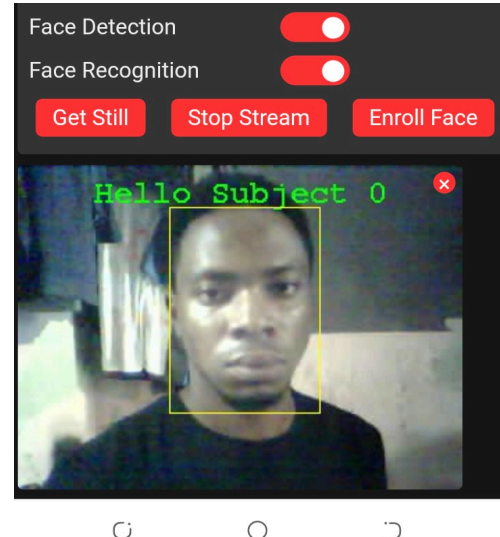


Figure 5: Recognized Face

The snapshot in Figure 4 shows the normally closed door of the prototype



Figure 4: Prototype Showing Closed Door

The screenshot in Figure 5 shows when the individual whose image is saved in the database come in front of the camera mounted on the door

Figure 6 shows when the prototype's door opened for the recognized face



Figure 6: Door Opens to Allow Entry of The Recognized Person

Figure 7 shows when another individual whose image is not in the database comes in front of the prototype's camera

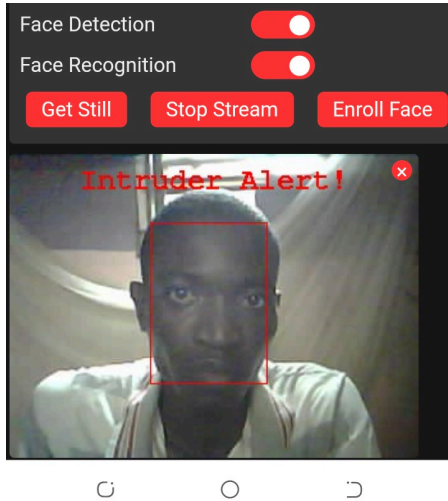


Figure 7: Unrecognized Face

In Figure 8 below, the prototype's door remains locked as it does not open for the intruder



Figure 8: Door Stayed Locked as It Detected an Intruder

3.2 DISCUSSION OF RESULTS

The system as whole functioned as expected performance was achieved so need to check for its reliability became a necessity. The procedures used to achieve the results were then repeated ten (10) times in other to determine the reliability of the system. For the ten test which was carried out in fifty (50) minutes, seven (7) were successful as the system operated smoothly while the system failed to operate three (3) times due to malfunction of the visual user interface failing to record and save the images to its database, so it had to be restarted by re-booting. Using the data obtained, the reliability of the system was calculated as shown below.

Number of test carried out = 10

Number of success = 7

Number of failure = 3

Operated time (t) = 50 mins = 0.833 hrs

$$\text{Failure rate } (\lambda) = \frac{3}{10} = 0.3 \quad (1)$$

$$\text{Reliability } (R) = e^{-\lambda t} \quad (2)$$

$$R = e^{-(0.3 \times 0.833)} = 0.7789 \quad (3)$$

For a system with reliability of 0.7789, the system is said to be reliable. Since the prototype was operated ten time for a specific period, hence the need to check its consistency became necessary. The table below shows the time taken for each of the ten operations.

TABLE 1: SPECIFIC TIME TAKEN FOR TEN DIFFERENT TESTS

Number of Operations	Time Taken (Minutes)
1	5
2	4
3	6
4	5
5	7
6	5
7	4
8	5
9	5
10	4

For the ten test operations carried out, an average time of five (5) minutes was spent on each test hence, the prototype proved to be consistent in its operation.

Figure 9 below shows the graph of number of operations plotted against time using the values of Table 1.

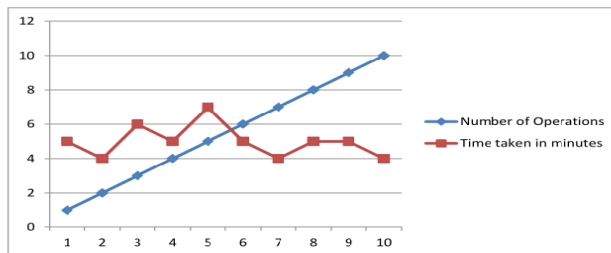


Figure 9: Graph of Number of Operations Plotted Against Time Taken for Each Operation

From the graph, the point of interception of “Number of Operations” and “Time taken in minutes” is 5 which is equal to the Average Time calculated, hence, it confirms consistency.

CONCLUSION

In this work, a security system that detects intruders based on facial recognition and only grant access to recognized faces by automatically opening a motorized door was proposed. To achieve this, an ESP 32 camera module of 2 mega-pixel as the prototype correctly identifies the intruder. Also, the prototype was successfully able to control a motorized door automatically by the instructions it receives from the Arduino ATmega328 microcontroller. The prototype was able to control the door automatically when the ESP32-camera recognizes the face of a person whose image is on its database by activating the Arduino NANO micro-controller into action. The system can establish a software-hardware relationship by allowing the prototype’s web-interface visualizes inputs to be processed. The system designed has the capacity to function as a security unit for our homes, offices, schools and so on. ance.

REFERENCE

- ARL, P. (2018). *Army Develops Face Recognition Technology that Works in the Dark*. Retrieved February 3, 2023, from https://www.army.mil/article/203901/army_develops_face_recognition_technology_that_works_in_the_dark
- Bramer, M. (Ed.). (2006). *Artificial Intelligence in Theory and Practice: IFIP 19th World Computer Congress, TC 12: IFIP AI 2006 Stream, August 21-24, 2006, Santiago, Chile* (Vol. 217). Springer Science & Business Media.
- Chen, S. K., & Chang, Y. H. (2014). *2014 International Conference on Artificial Intelligence and Software Engineering (AISE2014)*. DEStech Publications, Inc.
- Hamann, K., & Smith, R. (2019). Facial Recognition Technology. *Criminal Justice*, 34(1), 9-13.
- Jain, A. K., & Li, S. Z. (2011). *Handbook of Face Recognition* (Vol. 1). New York: Springer.
- Karri, V., & Lim, J. D. (2005). Method and Device to Communicate via SMS after a Security Intrusion. In *1st international conference on sensing technology, Palmerston North, New Zealand* (pp. 21-23).
- Kartik, J. S., Kumar, K. R., & Srimadhavan, V. S. (2013). Security System with Face Recognition, SMS Alert and Embedded Network Video Monitoring Terminal. *International Journal of Security, Privacy and Trust Management (IJSPTM) Vol, 2*.
- Khan, S. R., Al Mansur, A., Kabir, A., Jaman, S., & Chowdhury, N. (2012). Design and Implementation of Low-Cost Home Security System Using GSM Network. *International Journal of Scientific & Engineering Research*, 3(3), 1.
- Kumar, B. U., Murty, D. S., & Kumar, C. R. P. (2013a). Implementation of Low-Cost Ethernet Based Home Security Using Wireless Sensor Network. *Journal published at Algorithms Research*.
- Kumar, B. U., Murty, D. S., & Kumar, C. R. P. (2013b). Implementation of Low-Cost Ethernet Based Home Security Using Wireless Sensor Network. *Journal published at Algorithms Research*.
- Lwin, H. H., Khaing, A. S., & Tun, H. M. (2015). Automatic Door Access System Using Face Recognition. *International Journal of scientific & technology research*, 4(6), 294-299.
- Mae, Y., Sasao, N., Inoue, K., & Arai, T. (2003). *Person Detection by Mobile-Manipulator for Monitoring*.



4th International Engineering Conference (IEC 2023)
Federal University of Technology, Minna, Nigeria



In SICE 2003 Annual Conference (IEEE Cat. No. 03TH8734) (Vol. 3, pp. 2801-2806). IEEE.

Sampson, R. (2011). *False Burglar Alarms*. US Department of Justice, Office of Community Oriented Policing Services.

Socolinsky, D. A., & Selinger, A. (2004). *Thermal Face Recognition in an Operational Scenario*. In Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2004. *CVPR 2004*. (Vol. 2, pp. II-II). IEEE.

Wechsler, H. (2007). *Reliable Face Recognition Methods: System Design, Impementation and Evaluation*. Boston, MA: Springer US.

Williams, M. (2008) "*Better Face-Recognition Software*". Retrieved 2008-06-02.