ISSN: 3065-0437

Columbia Journal of Engineering and Technology

Research Article

PIONEERING THE FUTURE OF SECURITY: FACIAL RECOGNITION IN ELECTRONIC GATE SYSTEMS FOR ATTENDANCE AND PROTECTION

Olumide Abiola Akintoye

Department of Electrical and Electronic Engineering, Federal University of Technology Owerri, Imo State, Nigeria

Abstract

Effective attendance monitoring is essential for the smooth running of any organization. Manual methods of attendance monitoring are time-consuming and prone to errors, leading to poor staff attendance and adverse impacts on the organization. Automated methods have been introduced, ranging from paper-based systems to biometric identification using fingerprints, face, and voice. This paper proposes an electronic gate system that can control access and monitor staff attendance using facial recognition technology to address the issues of other identification methods. The system identifies staff members by recognizing their faces from a camera mounted at an access point and interfaces with a database containing their details and images. An automated penalization system was introduced to encourage punctuality, and weight verification was employed to reduce tailgating. The system also has a provision for registering visitors on-site, using a database independent of the main staff database. The proposed system employs less intrusive and more convenient identification methods, enhancing privacy concerns, and contributes significantly to access control functions. The system can efficiently monitor attendance, leading to improved staff attendance and productivity.

Keywords: Attendance monitoring, Automated identification, Biometric identification, Facial recognition technology, Access control, Staff attendance.

INTRODUCTION

Poor staff attendance is detrimental to any organization and can be curbed by proper attendance monitoring. Different automated methods of attendance monitoring have been in place to alleviate the cumbersome effort involved in employing a manual approach. These methods range from paper-based manual methods to radio frequency identification (RFID) tags, and recently the use of biometrics for marking attendance. Scanner devices were developed which made use of these underlying biometric features, such as fingerprints, face, voice etc., to capture biometric information specific to an individual which are stored and used in the event of an identification process [1]. Other forms of biometrics related to behavioral attributes have also been exploited [2]

This paper aims to develop an electronic gate system that can control access as well as monitor staff attendance within an organization using facial recognition technology. Facial recognition offers less privacy concerns and provides a good enough accuracy [3]. The system identifies staff members by recognizing their faces from a camera mounted strategically at an access point. It interfaces with a database which contains the details of each staff and their associated picture. This database also serves for recording attendance data. An automatic penalization system was also introduced as a way of discouraging lateness. This involve making fixed deductions from a staff's salary each time they default in terms of punctuality. Moreover, we also employed weight verification to reduce the occurrence of tailgating. In order to cater for visitor and strangers, a way to register visitors onsite will be made available. This will use a database independent of the main staff database.

Problem Statement

Paper-based attendance systems were manual, time-consuming and also prone to human errors and biases. Automating them eliminates the above problems but requires the use of electronic means of identification. One way this was achieved was through the use of RFID tags. However, RFID tags offer no means of preventing impersonation. Thus, a better and unique form of identification was required, this came in the form of biometrics [4].

Biometric features such as fingerprints, iris and voice are quite advantageous in the area of identification. But they are not so convenient since the user has to present themselves in some form. This is usually intrusive, inconvenient, time-consuming, and offer less privacy. For example, to capture a fingerprint, users will have to place their fingers on a scanner which performs the authentication. This can be seen as intrusive to some users, and others may worry about the security of their fingerprint details especially with the ongoing digital revolution where fingerprints are now being frequently used in authenticating financial transactions. Furthermore, most attendance systems do not provide means for performing access control. While arguably this may be handled by a separate unit, but for an enterprise where access control might be needed, this gives a considerable economical advantage since the same components that collect attendance information can also be used for access control functions.We propose an efficient attendance management system that relies on facial recognition technology. Facial recognition is a non-intrusive method of identification and has less privacy concerns.

LITERATURE REVIEW

Various methods of taking attendance have been suggested by different authors. In [5], the authors proposed an effective attendance solution based on the Internet of Things (IOT) paradigm. Fingerprints were used to identify students and the system was provided with cloud connectivity to allow real time access, processing and analysis of the results. The attendance capturing device which consisted of Raspberry Pi Rev 3 microcomputer interfaced with a fingerprint scanner GT 511C3 and a 4x4 keypad, communicated with both the cloud engines and a mobile application developed for the system. The authors in [6] took a different approach by leveraging on face recognition for identifying students. A camera captures the classroom containing the students and sends it to an image processing module which then identifies each student from the capture. Capturing is done twice daily to

ISSN: 3065-0437
Columbia Journal of Engineering and Technology
Research Article

reduce inconsistencies. Viola-Jones object detection framework was used for face detection while Product Component Analysis (PCA) was used for face recognition.

Also, in [7] an automated system for human face recognition was presented for an organization or institute to mark the attendance of their students or employees. They also introduced face detection method using the Voila and Jones algorithm and recognition using correlation technique. The authors performed a set of experiments to demonstrate the efficiency of the proposed method. Images of different persons were used in training set. In order to obtain the efficiency of proposed methodology, training images were taken. The detected faces from the image were compared with the database. This is called the selection of region of interest. In this way faces of students were verified one after the other with the face database using the correlation method and attendance is marked along with the login time and date. Here, faces recognition rate achieved by proposed methodology was 81.875%. While the high computational analysis and database management processes required to authenticate and authorize users may be performed on high performance systems, a dedicated form of intelligence is required to communicate with the low-level interfaces that actualize the access control action. This can take the form of activating a relay when an authorized user is detected or receiving input feed from sensors. Usually, this is achieved by using a microcontroller such as Arduino Uno as seen in [8] and [9]. Communication between the microcontroller and the central computer may be achieved using wireless technologies such as Wireless Fidelity (Wi-Fi) as in [8] or Bluetooth as in [9]. Alternatively, wired communication may also be used.

METHODOLOGY

This paper involves the development of Staff and Visitors Management System which comprises access control, staff payroll and staff attendance systems using incremental software model for developing facial recognition software and waterfall model for the Arduino software programming. It incorporates an access control system which uses facial recognition technology to ensure that only authorized personnel are granted access into the building. The functional block diagram and general block diagram showing the interrelationship among the whole components is as shown in figure 1 and 2 respectively.

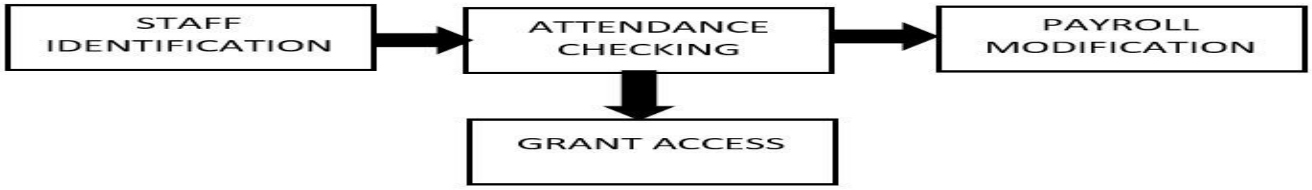

Figure 1. Functional block diagram of the system

ISSN: 3065-0437
Columbia Journal of Engineering and Technology
Research Article

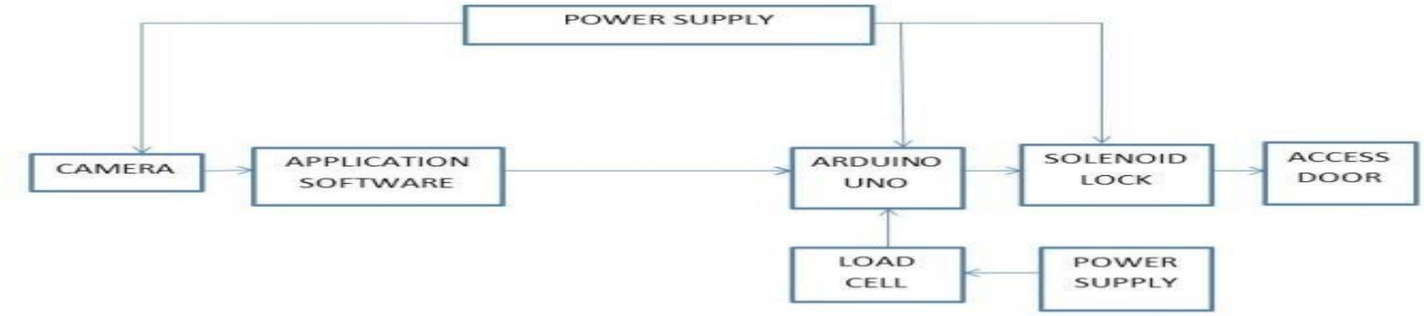

Figure 2. Block diagram showing interrelationship among components

HOW THE SYSTEM WORKS

First the system identifies staff members as they approach the access point (door) using facial recognition. The facial recognition software feeds live images from the camera mounted at the access point and performs the comparison, as shown in figure 3, for identification.

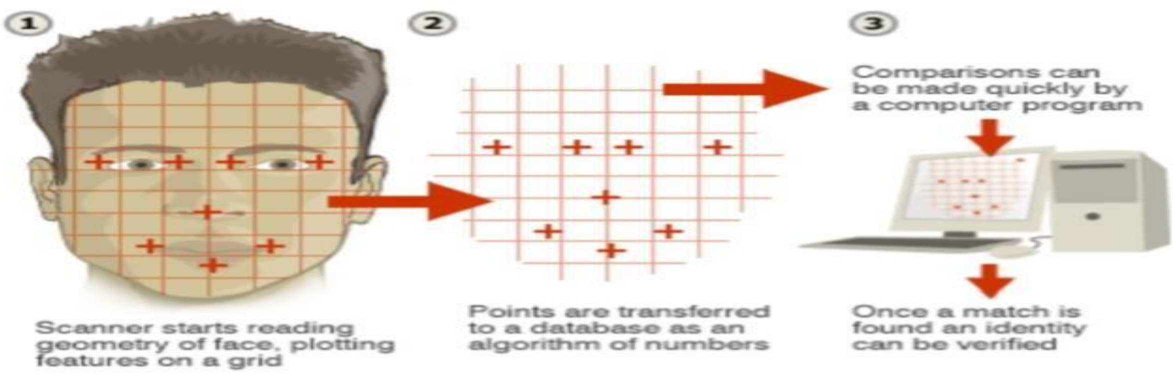

Figure 3. Facial recognition process [E9]

With the staff identified, the system records his/her time of arrival and directly compares this time to the predefined resumption or departure time. If it exceeds this time, the system increments the deductions field of the staff's entry in the database. The SQL database can easily be queried to provide data of the cumulative deductions over a time period (for example, a month) and this can be effected through a dedicated financial platform, which will be at the discretion of the administrators.

Simultaneously, the software sends signal to the microcontroller to activate the solenoid locks granting the identified staff access to the premises.

SYSTEM REQUIREMENTS

PROTOTYPING BOARD: Arduino Uno board, containing Atmega328 microcontroller was used for access control. The microcontroller was programmed with Arduino C language using the Arduino software.

12Volt SOLENOID LOCK: 12V Solenoid locks are basically electromagnets: they are made of a big coil of copper wire with an armature (a slug of metal) in the middle. They are of two types: energize to lock types and energize to unlock types. In this paper, energize to unlock type was used.

HD CAMERA: Two high-definition 1080P camera were used. Resolution was 2MP with a viewing angle of 108.5º. The cameras were selected to match lighting condition for both indoor and outdoor purposes. These cameras were used to capture and transmit the streams of picture elements onto the facial recognition software.

A/V TO USB CONVERTER: This was used to feed the video output from the camera to the laptop computer via USB.

PROTOTYPE DOOR: The door used was made of plywood material. The door was split into two. The first door opens after facial recognition process while the second opens after weight verification process.

LOAD CELL: A load cell is a force sensing module enclosed within a carefully designed metal structure. It contains strain gauges mounted at precise locations within the structure. Strain gauges convert mechanical strain to a change in resistance. Usually, the four strain gauges are placed on each arm as in a Wheatstone bridge configuration. At equilibrium with no applied load, the voltage output is zero or very close to zero when the resistances of the four strain gauges are closely matched in value.

HX711 LOAD CELL AMPLIFIER: Load cells produce very small variations in the output voltage over the range of reading. This creates a problem as it requires either a highly sensitive analog-to-digital converter (ADC) or amplification. This can be achieved using the HX711 load cell amplifier. Figure 4 shows the circuit diagram for the access control system

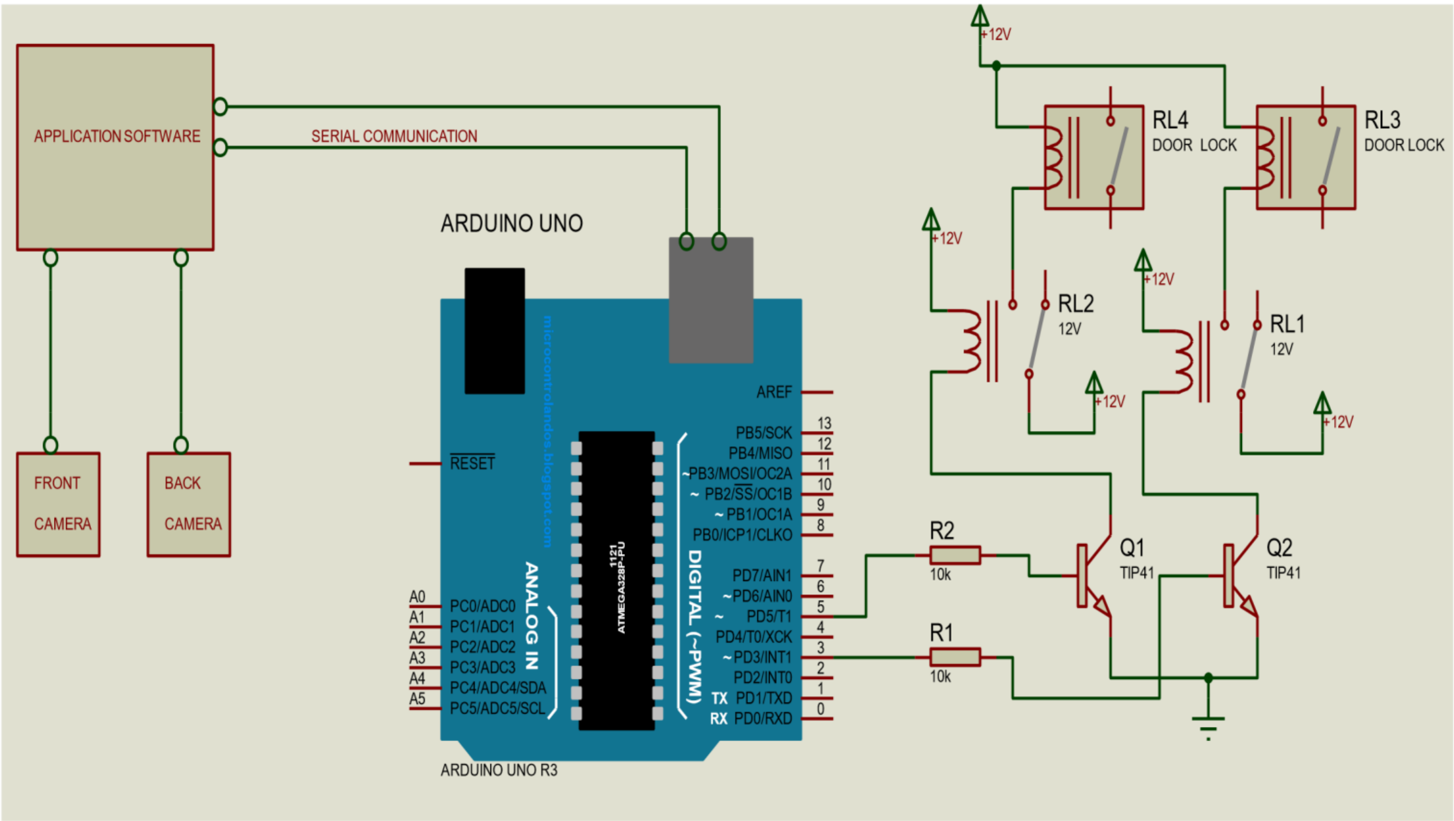

Figure 4. Access control circuit diagram

POWER UNIT: We used a 12V battery to power the prototype. In order to ensure reliability of the system, mains supply can be augmented with backup batteries which are activated when there is a disconnection. A mini solar power system is a good alternative.

Flowchart for Staff Access

As a staff approaches the access point which is the door, the camera which is streaming live images to the computer, picks up the staff's face. The facial recognition software then tries to identify the staff using his/her facial features. If successful, the staff will be allowed into the cubicle for weight verification. This verification reduces the possibility of tailgating. For facial recognition, the system tries to compare the captured image against images of staff in the database to find a match.

A match indicates that the staff has been identified, therefore the system retrieves the details pertaining to the identified staff. Particularly, the system retrieves the staff's weight and send same to the microcontroller to carry out weight verification. In weight verification, the microcontroller receives the measured weight from the sensor and compares it to the value obtained from the database. Ideally, they should be same with some tolerance. This system allows a tolerance of 10kg over and under. This tolerance accommodates the issue of weight loss. However, if the weights differ by more than 10kg, the system treats it as an error and denies access to the staff. This is done in order to checkmate the possibility of an illegitimate person being sneaked in to the premises. We assume that the combined weight of the illegitimate person and that of the staff should be more than the staff's weight and given tolerance. The flowchart of the process is illustrated in figure 5.

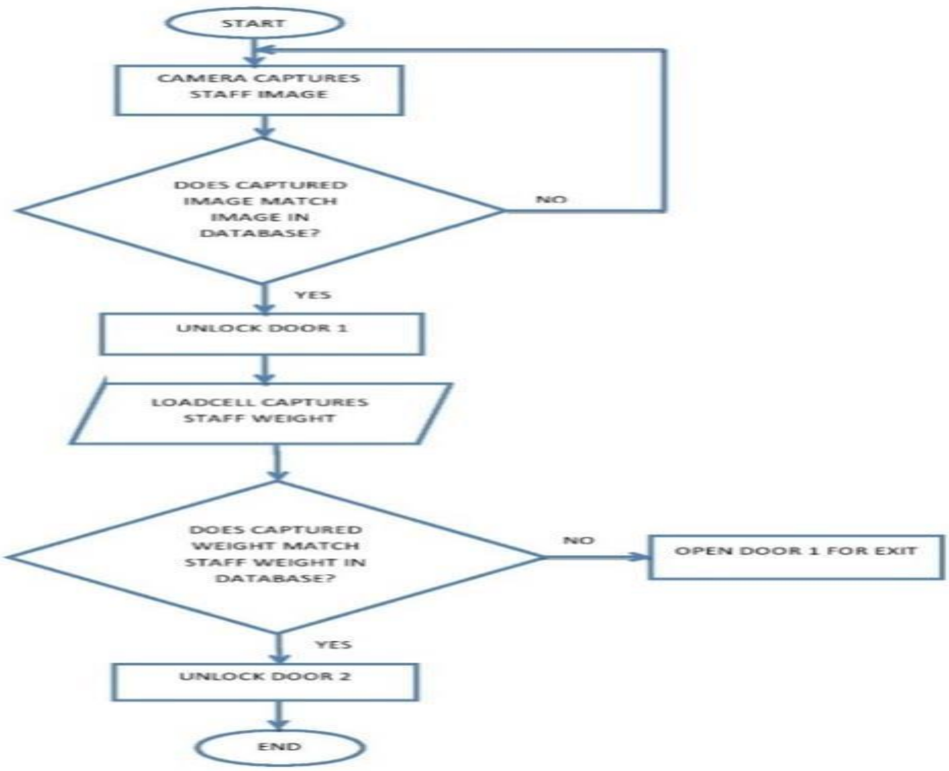

Figure 5. Flowchart for access control process

RESULTS

A. **UNIT TESTING**

HARDWARE TESTING

Each component was tested individually to verify that they are working properly. The solenoid locks were powered separately with 12V DC from a battery. The plunger retracted as expected on application of the voltage. This is shown in figure 6.

ISSN: 3065-0437
Columbia Journal of Engineering and Technology
Research Article

Figure 6. Testing the solenoid locks

The load sensing unit was set up by connecting the load cell to the amplifier, HX711 as shown in figure 7. The HX711 was connected to Arduino Uno following the pin labels. Ground from the HX711 went to Arduino Ground and VCC went to 5V power pin of the Arduino. Two digital pins for DT and SCK were arbitrarily selected. After that, a calibration sketch which was downloaded from the web to derive the calibration factor and zero factor was run, in order to setup our digital scale. Finally, the accuracy of the load sensing unit was further tested and found to be 96.6%.

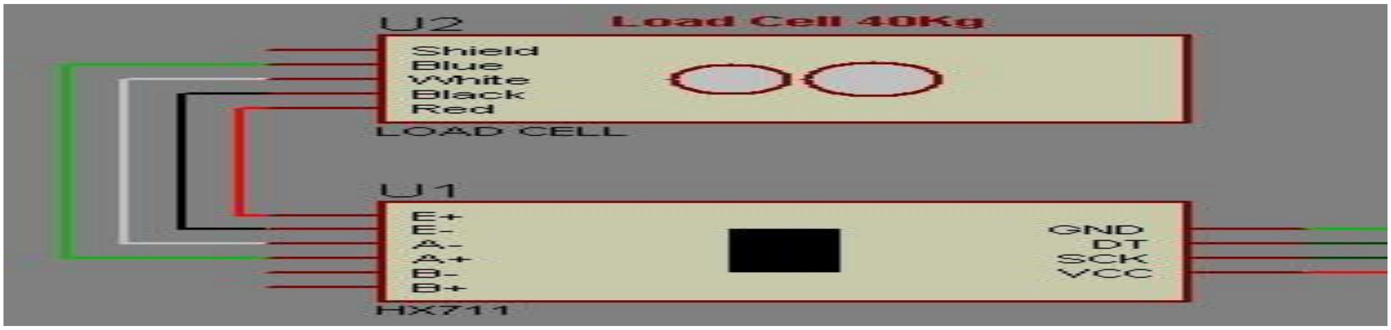

Figure 7. Load cell to HX711

The camera also functioned properly when connected 12V battery and its output was monitored using a PC. The AV-to-USB converter was used to receive the video output from the camera via USB port.

2. SOFTWARE TESTING

Figures 8 – 11 shows the system response to various activities

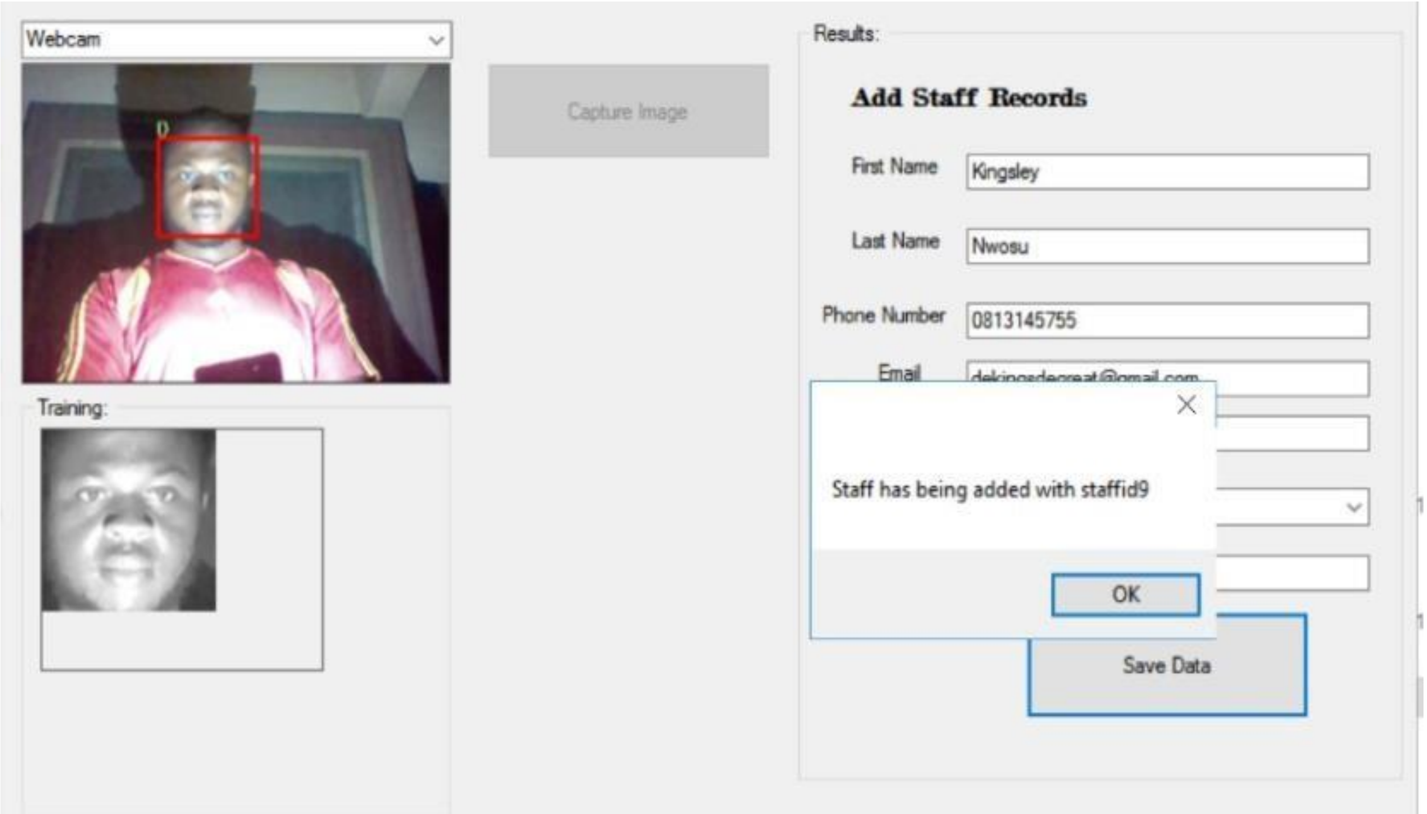

Figure 8. Enrolling a staff to the database

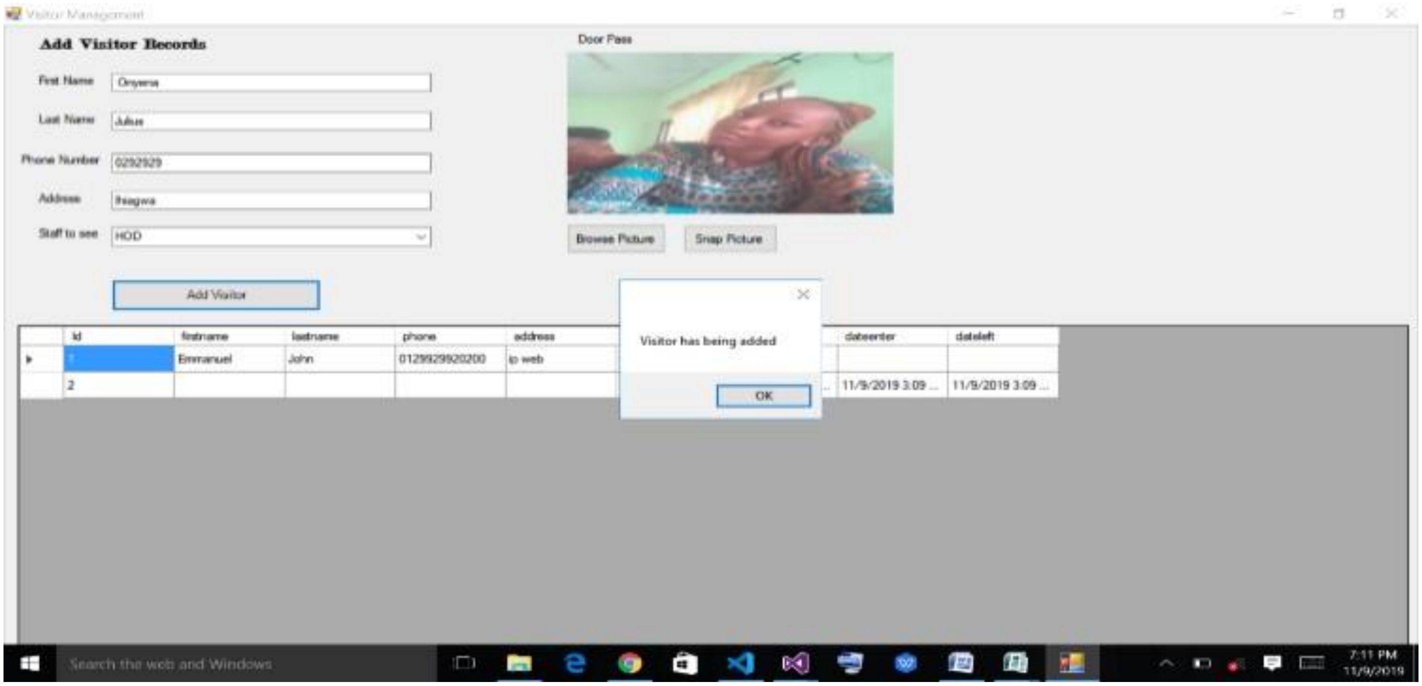

Figure 9. Adding a visitor to the database

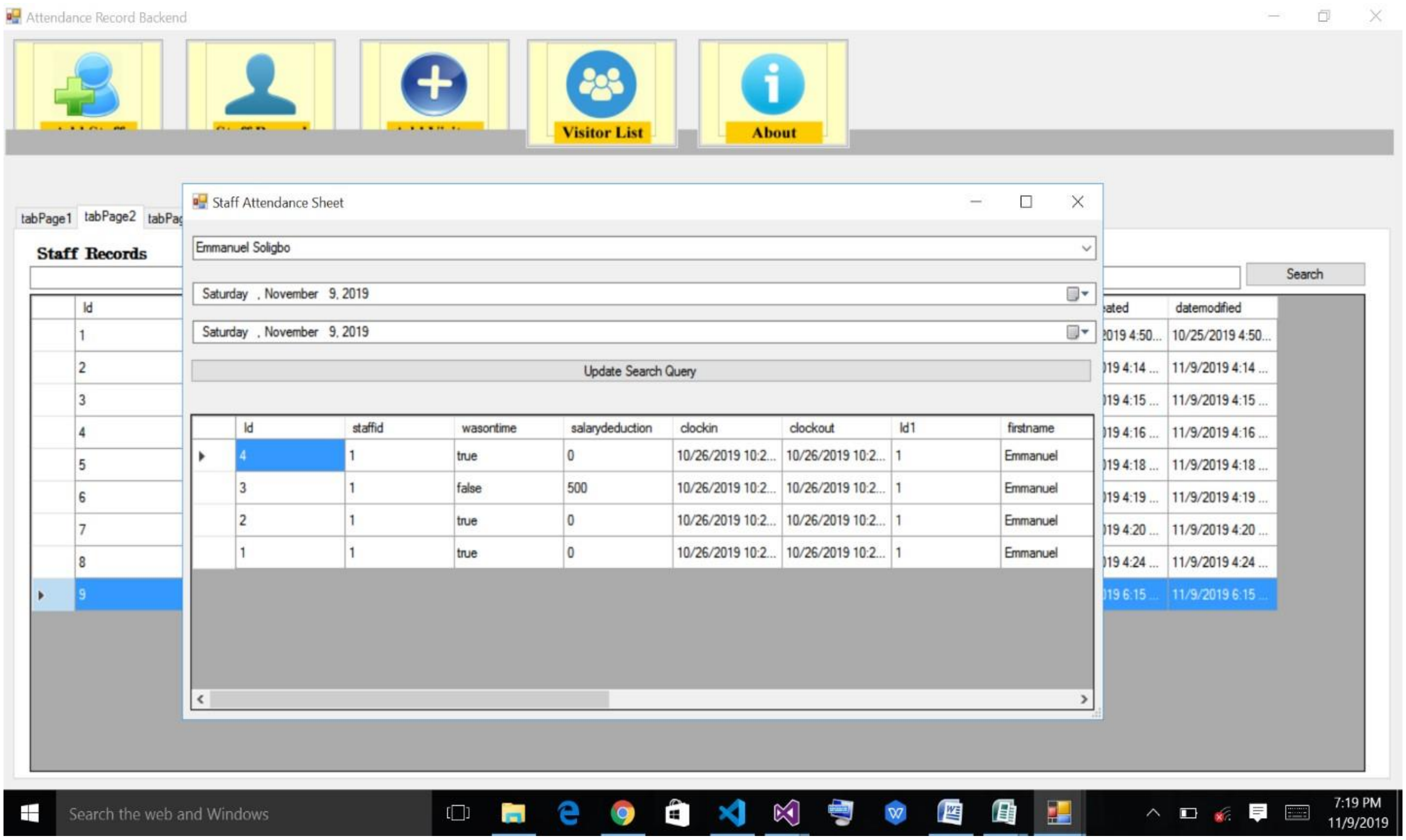

Figure 10. Reading attendance records

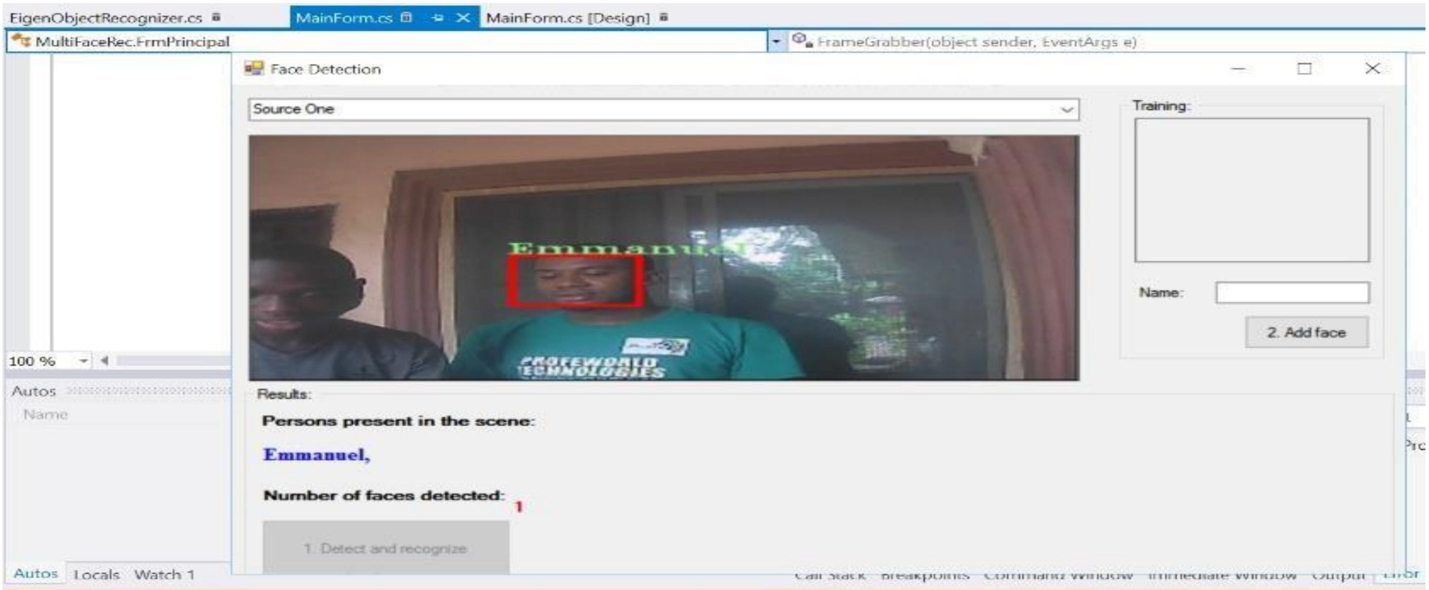

Figure 11. System detects a face

B. **SYSTEM TESTING**

Finally, all subunits were integrated together and tested using a sample size of 10. The results are shown in table 1. Recognition time was less than 2secs for each valid user.

Table 1. Results from final system testing

USER	FACE DETECTED	FACE RECOGNIZED	STATUS
STAFF 1	YES	YES	ACCEPT
STAFF 2	YES	YES	ACCEPT
VISITOR 1	YES	YES	ACCEPT
VISITOR 2	YES	YES	ACCEPT
VISITOR 3	YES	YES	ACCEPT
VISITOR 4	YES	YES	ACCEPT
VISITOR 5	YES	YES	ACCEPT
STRANGER 1	YES	NO	REJECT
STRANGER 2	YES	NO	REJECT

STRANGE R 3	YES	NO	REJECT

C. **DISCUSSION**

From the results, the system showed a perfect accuracy. Having a true acceptance rate (TAR) of 100%, a false rejection rate (FRR) of 0% and a false acceptance rate (FAR) of 0%. The accuracy however depends on the following:

- Quality of camera: Poor resolution cameras will increase FRR or FAR.
- Quality of template pictures: Poor template pictures will also increase FRR or FAR.
- Number of users: The recognition time will be longer as the number of users increases. This is because we used a one-to-many matching process. Accuracy also might be less since facial recognition technique is not 100%, so the chances of mistaken identities will increase.

CONCLUSION

An electronic gate system capable of monitoring attendance and also performing access control was successfully designed and implemented. This method of preventing tailgating works quite well for situations where staff may be sensitive about the weight. Although a more accurate method can be used to compare a staff's weight directly against their actual weight as recorded in the database. More so, wireless communication can be introduced in order to make the system capable of remote operation.

REFERENCES

L. Cruz, "5 things you didn't know about facial recognition but should," [Online] Available: https://www.newsroom.cisco.com, Sept. 4, 2018 [Accessed June 25, 2019].

M. Maguire, "The Birth of Biometric Technology," Anthropology Today, Vol. 25, no. 2, April 2009. [3] ex-sight. (2009) "Facial recognition technology overview," [Online] Available: https://www.exsight.com/technology.html [Accessed August 14, 2019]

Wikipedia contributors, "Biometrics," [Online]. Available: https://en.wikipedia.org/wiki/Biometrics, [Accessed June 30, 2019].

V. Yadav, G. P. Bhole, "Cloud Based Smart Attendance System for Educational Institutions," International Conference on Machine Learning, Big Data, Cloud and Parallel Computing, February 2019.

A. Choudhary, A. Tripathi, A. Bajaj, M. Rathi, B. M. Nandini, "Automatic Attendance System Using Face Recognition," International Journal of Modern Trends in Engineering and Research (IJMTER), vol. 03, issue 04, April 2016.

K. Suhel, Z. Hussain, K. Shoeb, P. Nazim, M. Khan, "Automated Attendance System Using Face Recognition," International Journal of Innovative Research in Computer and Communication Engineering, vol. 4, issue 4, April 2016.

P. Srivastava, M. Bajaj, and A. S. Rana, "Irrigation System using IoT," 2018 Fourth Int. Conf. Adv. Electr. Electron. Information, Com. Bio-Informatics, pp. 1–5, October 2018.

M. Kumar, M. Hanumanthappa, T. V. S. Kumar, and A. K. Ojha, "Android Based Smart Door Locking System with Multi User and Multi Level Functionalities," International Journal of Advanced Research in Computer and Communications Engineering (IJARCCE), vol. 5, no. 2, pp. 3–6, 2016.