ISSN No:-2456-2165

Design of an Access Control Facial Recognition System Using Raspberry Pi

Dr. Bourdillon O. Omije[1], Udom Ukeme Saturday[2]
Senior Lecturer[1], ME Student[2]
Department of Electronics and Computer Engineering
University of Port Harcourt, Nigeria

Abstract:- This work introduces the development of a design of an access control facial recognition system with the use of a Raspberry pi controller, this design is meant for access to restricted areas. It consists of the camera which sends input to the microcontroller when a human face is being recognized and it grants access, the door in the output system then slides open; if the face is unrecognizable the system prompts the user to try again. This is an innovative design because it enables the automation of a door system.

***Keywords*:-** *RFID, IC, PCA Algorithm, ASCII*

I. INTRODUCTION

In recent times, there have been a lot of reported cases of robbery and burglary incident that occur frequently and also unwanted entrance to restricted areas has been on the rise. So the need for security cannot be overemphasized in our daily life. Traditional security system requires the use of a key, a security password, an RFID card, or ID card to have access to the system. However, these security systems have drawbacks; for example, they can be forgotten or stolen from unauthorized people. As a result, there is need to develop a software that guarantees a higher security level. The use of smart cards, plastic cards, PINS, tokens, keys for authentication and to get access in restricted areas like India space research organization (ISRO), national aeronautics and space administration (NASA), and defence research and development organization (DRDO) etc. is what is been used today. There are two types of biometric such as the physiological characteristics biometrics (face, fingerprint, finger geometry, hand geometry, palm, iris, ear and voice) and behavioural characteristics (gait, signature and keystroke dynamics).

II. LITERATURE REVIEW

Security systems are important in developing countries for the protection of lives and valuable resources. There are lots of advanced security systems that are used for providing security which have been developed and are still in use in the last few decades. These systems are studied in order to obtain some idea for the system that was designed

➢ *History of Lock*

The oldest known lock was found by archaeologists in the Khorsabad palace ruins near Nineveh (Scalon, 2018). The lock was estimated to be 4,000 years old. It was a forerunner to a pin tumbler type of lock, and a common Egyptian lock for the time. This lock worked using a large wooden bolt to secure a door, which had a slot with several holes in its upper surface. The holes were filled with wooden pegs that prevented the bolt from being opened.

Types of Locks:-Basically there are two types of locks

- Mechanical locks
- Electronic locks

- *Mechanical Locks*

This is a kind of lock whose key is a tangible object; the operation of such controlled mechanism is relatively simple. A key is inserted into an inlet part and withdrawn from that same part after turning or twisting to rotate a tumbler arrangement. The major disadvantage of such arrangement is that mechanical wearing set in after a long time of use of the key, also any user may formulate or have a master key to lock or unlock a door. There are three basic types of mechanical locks, each with variation and they are: warded lock, tumbler lock, combinational keyless electric mechanical lock (Anubala et al, 2014).

- Warded Lock
- Tumbler Lock
- Combinational Keyless
- Electric Mechanical Lock

- *Electronic Lock*

This is a type of lock whose key is a piece of information. It is used for activating mechanism to permit-entry to a secured area, by inputting code within the memory unit (Anubala et al, 2014).

Card Electronic Lock: In this type of Electronic lock, the electronic lock control assembly is mounted on the inside of the outer door of the enclosure and controls the operation of a solenoid for disengaging or releasing the mechanical lock from its locked condition. A transceiver is mounted in front of the door and when an IC card is slotted on the transceiver it instantly receives the equivalent code from the card and compares it with the present one, if they are same, the door opens, if not it remains locked. It has the disadvantages that, if the card gets lost, someone else might pick it up for use for the same purpose. We also have the Biometric Electronic lock and the Keypad access door control.

ISSN No:-2456-2165

III. DESIGN ANALYSIS

The design analysis focuses on the general configuration of the system. The design consists of four parts; the power supply unit, input unit, control unit and output unit.

➢ *The power supply unit*

The power supply unit is made up of the step down transformer (TR1), which step down the 220 Vac from PHCN supply to 12 Vac. The 12Vac is converted to 12Vdc by a bridge rectifier (BR1). The dc voltage gotten is filtered by using a filter capacitor (C4), the filter capacitor is used to filter off any ac ripples in the 12Vdc voltage. The voltage required by the circuit is 3.3Vdc and 5Vdc, three voltage regulators was used to supply constant voltage, 7805 (U1 and U2) supplies 5Vdc and lm317 (U3) supplies 3.3Vdc. The 3.3Vdc gotten from the U3 is from voltage divider network of the fixed 1k resistor (R2) and the 10k variable resistor (RV1). The capacitor c2 and c3 are used to provide stability to the voltage gotten from the LM317. A light emitting diode (d1) is used as a power indicator.

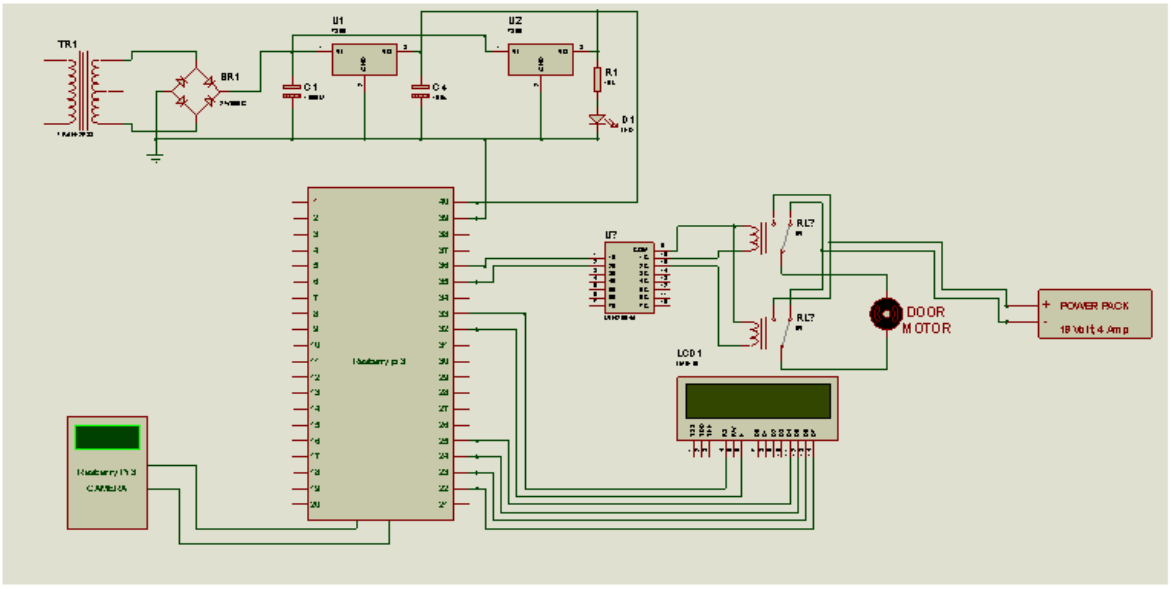

Fig 1:- Circuit Diagram of the Access Control System Using Raspberry Pi Camera and Controller

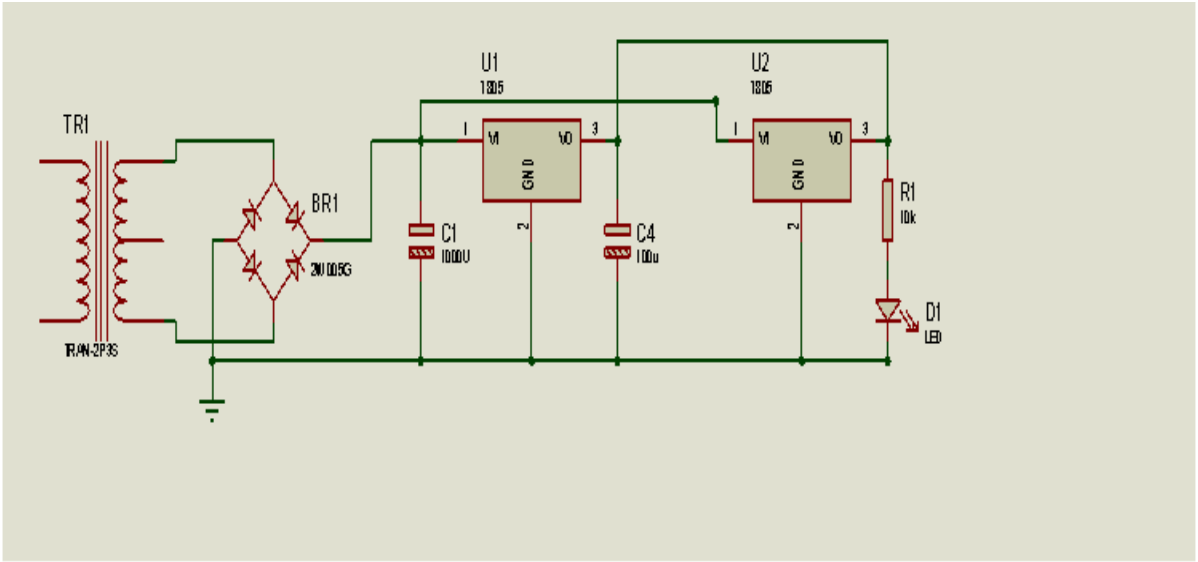

Fig 2:- Circuit Diagram of the Power Supply Unit

➢ *Power Supply Calculation*

The transformer used in the design is a 220vac to 12-0-12Vac transformer with a current capacitor of 500mA. The voltage that is supplied to the transformer is 220Vac from main supply; the voltage is step down to 12Vac.

The maximum voltage of the secondary side of the transformer can be calculated using equ 3.1.

$$V_m = \sqrt{2}V_{secondary}$$

1

V_m
$=$ The maxium voltage from the secondary of the transformer
V_s $=$ The voltage from the secondary of the transformer
$V_m = \sqrt{2} \times 12 = 17\ volt$
The maximum peak voltage is 17 volt.
The average dc voltage gotten is calculated from the formula given in Equ 3.2.
$V_{dc} = 0.636V_m$
2
V_{dc} $=$ Average dc voltage
V_m $=$ Maximum Voltage of the Transformer
From equation 1, the maximum voltage is 17 volts.
$V_{dc} = 0.636 \times 17 = 10.81\ volts$

From the calculation the average DC voltage is 10.81 volt. The bridge rectifier rectifies the voltage. The voltage gotten after the bridge rectifier is gotten from eqn. 3
$V_{dc} = V_m - 2(V_d)$
3
$V_d = forwardvoltagedropacrossthesilicondiodes$
$= 0.7$
$V_{dc} = V_m - 2(0.7) = 17 - 1.4 = 15.6\ volt$

The filter capacitor is use to filter off the ac ripples in the DC voltage, thereby reducing the ripple to a minimal level. The capacitor used in the design is 1000uf, with PIV of 50v, this meets the requirement of PIV of capacitor greater than the peak voltage from the bridge rectifier output. The capacitance of 1000uf was chosen to filter off AC ripples from the output voltage of the rectifier.

Two voltage regulators were used, two 7805 gives 5v. A light emitting diode is connected in the circuit this will notify that there is power in the circuit when plug to the socket. A limiting resistor is connected in series with the light emitting diodes. The limiting resistor reduces the current that that flows through the diode to prevent high current from flowing through the light emitting diode. The formula for calculating the current through the diode is shown in equation 4,

From kirchoff's voltage rule,
$V = V_r + V_d$
4
$V_d = Voltage\ drop\ across\ light\ emitting\ diode$
$V_r = Voltage\ drop\ across\ the\ resistor$
$V = Total\ Voltage$
$V_r = I \times R$
V_d is 2 volt, and the permissible current is 1mA to 30mA.
V is the voltage gotten from the voltage regulator (U2) (V = 5 volt).
Substituting this into the equation,
$5 = I \times 1000 + 2$
$5 - 2 = I \times 1000$
$3 = I \times 1000$
$I = \frac{3}{1000} = 3\ mA$

- *Input Unit*

The input unit is made up of the raspberry pi camera that captures the human face and sends the data to the micro controller. The raspberry pi camera board plugs directly into the raspberry pi. It is able to deliver a crystal clear 5mp resolution image to the raspberry pi.

- *Control Unit*

The control unit houses the Raspberry pi 3 controller which receives the image of the user and scans if the image is stored in the system, if it is stored, it allows access to the building, if not it alerts the user to stare at the camera again for facial input to be taken. The system uses an open CV library for the processing of the image of the individual. The open CV library makes use of the principal component analysis (PCA) algorithm. The controller sends a signal to the output unit, when a face is recognized. The output unit is made up of a transistor relay driver; the relays control the closing and opening of the door by forward biasing and reverse biasing of the relay. The user is able to communicate with the device via the use of a liquid crystal display which the microcontroller sends data to. The liquid crystal display is connected to the analogue pins (pin 22 to pin 28) of the microcontroller. The door system is controlled by the microcontroller via the two relays used in the system. The relays are connected to the uln2004 (transistor array chip) IC (U3), which is used to switch on and off the relay. The IC is used in the circuit, due to the current gain of the array of transistor used in the internal architecture of the IC. The IC (U3) turn the relay when a 5 volt is sent to it by the microcontroller and turns off when a 0 volt is sent to it by the microcontroller. The microcontroller is program using python language. The system worked base the algorithm and program used to control the control unit. This achieved by using python language program and the PCA algorithm. Principle Component Analysis (PCA) is an Eigen face based face recognition algorithm which uses feature vectors extracted from a frontal view of the face. The user face is inputted into the system via a camera, the PCA algorithm extracts the Eigen faces, Eigen vectors and mean from the image by performing a mathematical process on a set of trained images depicting different human faces. The training images are defined as a set of flattened vectors and these vectors are assembled together into a single matrix. The extracted Eigen vectors of the matrix are stored in a database. Eigen vectors are defined by the face spaces which are the training face images that are projected. This results in the variation between the set of faces without emphasis on any one facial region like the eyes or nose. The algorithm involves the training of the system to understand the pattern of the user face by taking pictures of the user and creating vectors for each image taken, the several vectors gotten from the images used in training the system are assembled together to form a single matrix that will be stored in the system memory (database).

ISSN No:-2456-2165

➢ *The Output Unit*

The output unit is made up of the sliding door, motor and gear system and the liquid crystal display. The liquid crystal displays if access is granted or denied. The sliding door system is made up of the gear and motor system and the aluminium framework of the door. The motor system is controlled by two relays connected to the microcontroller system via a transistor array IC ULN2003 (U3). The microcontroller controls the opening and closing of the door by forwarding and reverses biasing the motor system. The door will slide open if the face scan is stored in the database; this is achieved by the program burnt into the microcontroller. The program is shown in appendix A. The circuit diagram of the output unit is shown below. The liquid crystal display receives data from the micro-controller using the data pins d3-d7. The four terminals of the data pins are connected to the microcontroller pins 23-25. The communication between the microcontroller and the liquid crystal display is a nibble (four bit) parallel communication. It uses four bit to transfer information or ASCII character from the microcontroller to the liquid crystal display, this is done to only use four terminals of the microcontroller pin outs rather than using eight pins for eight bit. The RS (register select) and the EN (enable terminals) of the liquid crystal display are used in controlling the liquid crystal display to display the data received from the microcontroller or receive commands from the microcontroller. The uln2003 (U3) is connected to the microcontroller pin 3 and 6, the output of the IC (U3) is connected to the two relays (RL1 and RL2). The relays are switched on by the microcontroller via the IC (U3). When access is granted by the microcontroller, the microcontroller sends signal to the relay via the IC. Relay (RL1) is turn on and relay (RL2) is off the door slide open (the motor is reverse bias), when relay (RL2) is turn on and relay (RL1) is off the door slide close (the motor is forward bias).

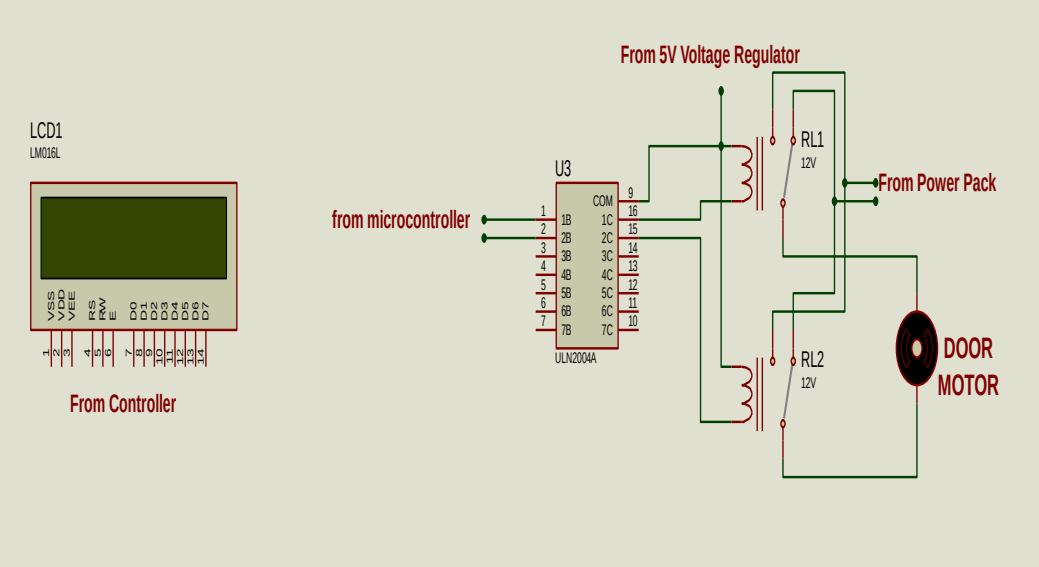

Fig 3:- Circuit Diagram of the Output Unit

IV. CONCLUSION

The design of the biometric access system using facial recognition was tested and the result showed that it worked perfectly. The facial system controlled the opening and the closing of the sliding door system. The ability to be able to control the access of the door to a building via biometric facial access system is of importance in technology, industry and Engineering to ensure secured access door system. Facial recognition system is an efficient security technology that promotes the use of identification in an establishment that cannot be manipulated. This system is efficient because it promotes the use of identification system as a security measure. This system could be recommended for homes, schools and hotels.

REFERENCES

[1]. Ahmad N., Butler S., and Ramachandran U., "GuardianAn- gel: An RFID base in door guidance and monitoring system," pp. 546 551, 2010.
[2]. Anubala B., Rahini M., and Bavithra T. Intelligent Door Locking System International Journal of Engineering Research and Applications (IJERA) ISSN:2248-9622 International Con- ference on Humming Bird. 2014.
[3]. Dorman, J. RFID devices: Journal of the Acoustical So- ciety of America. Vol. doi:10, No.1121/1.p.191 1801, 2013. Retrieved 12, September, 2016.
[4]. Huang K. S. and Tang S. M. "RFID applications strategy and deployment in bike renting system," in Proc. ICACT, pp. 660 663, 2008.
[5]. Lahiri S., RFID sourcebook, IBM Press, Westford, Mas- sachusetts, 2006.
[6]. Lourenco F. and Almeida C., "RFID based monitoring and access control system," in Proc. INFORUM, 2009

[7]. Meng X. L., Song Z. W., and X. Y. Li, "RFID-Based secu- rity authentication system based on a novel face-recognition structure," in Proc. WASE international Conference on Infor- mation Engineering, pp. 97-100, 2010.
[8]. Ostojic G., Stankovski S., and Lazarevic M., "Implementa- tion of RFID technology in parking lot access control system," in Proc. Annual RFID Eurasia Conference, pp. 1-5. 2007.
[9]. Umar Farooq, Mahmood ul Hasan, Muhammad Amar, Athar Hanif, and Muhammad Usman Asad. RFID Based Security and Access Control System. IACSIT International Journal of Engineering and Technology, Vol. 6, No. 4, 2014.
[10]. Raghu Ram.Gangi1 , Subhramanya and SarmaGollapudi. Locker opening and closing system using RFID, fingerprint, password and GSM. International Journal of Emerging Trends & Technology in Computer Science. (IJETTCS) Web Site:w ww.ijettcs.org, Volume 2, Issue 2, 2013.
[11]. Rohini R., Ravi S., Devi G. Efficient Home Security Sys- tem based on Biometrics and Keypad System. Department of CSE/ Vivekanandha College of Engineering for Women, layampalayam, Tiruchengode - TK,Namakkal District, India, 2010.
[12]. Scalon, L. Stokowski, Harvey Fletcher, and the bell labs experimental recordings. www.stokowsi.org. Vol.15, No. 112, p.191-195. Retrieved 4th, April 2018.
[13]. Wu D. L., Wing W. Y. NG, Yeung D. S., and Ding H. L., A brief survey on current RFID applications, in Proc. Inter- national Conference on Machine Learning and Cybernetics, Baoding, pp. 2330-2334, 2009.
[14]. Weinstein R., "RFID: A technical overview and its appli- cation to the enterprise," IT Professional, vol. 7, no. 3, pp. 2733, 2005.
[15]. Yan B., and Lee D. Y., "Design of spot ticket management system based on RFID," in Proc. International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 496-499, 2009.