Scientia Africana, Vol. 16 (No. 2), December 2017. Pp 147-151
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

MICROCONTROLLER BASED BIOMETRICS ACCESS CONTROL SYSTEM IN TERTIARY INSTITUTIONS

[1] K. O. Ojo and [2] T. E. Okuonghae

[1] Department of Science Laboratory Technology, University of Benin, Benin City, Nigeria
meetengrodu@mail.com, 08037999582

[2] Department of Physics, University of Benin, Benin City, Nigeria
timothy.okuonghae@uniben.edu, 08033188592

Received: 14-03-17
Accepted:19-04-17

ABSTRACT

In developing Nations as we have it today, access control is not given paramount attention in the higher institutions as it ought to be and this has led to retrogression of educational standard in the society in that examination malpractice is on the increase by way of impersonation of candidates. Physical security of both tutors and students of the institution is also a common challenge as seen in recent times. These challenges can be controlled by the use of a system that would grant access only to authorized persons to the institution. This paper presents the design and construction of a biometric control system using PIC16F877 microcontroller to give access to only staffs and students in the institution. Biometric technology offers a reliable and cost effective way to manage identities for security and authentication purposes.

Key words: Biometrics, Access control, Fingerprint, Microcontroller etc.

INTRODUCTION

With the high rate of crime, impersonation of candidates in examination hall in the higher institutions and physical security of personnel, security is necessary. Our higher institutions have over the years witnessed cultism, examination malpractices such as impersonation that have reduced our education standard by producing not well grounded graduates. To that end, improved security is the basic necessity of any individual or a system (Awasthi and Ingolikar, 2013).

Biometrics are automated methods of recognizing a person based on a physiological or behavioural characteristics such as fingerprints, face, signature etc (Awasthi and Ingolikar, 2013).

Depending on the application context, a biometric system may be called either a verification system or an identification system. A verification system verifies a person by comparing the captured biometric characteristic with his own biometric template pre-stored in the system. It conducts a one-to-one comparison to determine whether the identity claimed by the individual is true. A verification system either accepts or rejects the submitted claim of identity. Conversely, an identification system recognizes an individual by searching the entire database for a match. It conducts a one-to-many comparison to establish the identity of the individual (Ashraf , 2011).

Biometric Access control system has become necessary to overcome security and examination malpractice faced by almost every tertiary institution even in developed countries. By installing the system at every entrance of the institution, it would be possible to allow entry of only authorized persons. The primary purpose of an access control system is to secure access-controlled zones by restricting access to only those persons (assets) who are allowed access (Sadeque, 2012). The system can also be installed at various lecture halls, conference rooms, student's record rooms, sports facility, etc. In this way, suspicious person can be caught which will go a long way in improving the security level and more importantly prevent unauthorized candidates into the examination halls. Biometrics access control system uses a technology that captures individual finger print and the person's data is saved so that the entrance door opens for easy access. Unlike already developed biometric finger print for an automated access control in university hostels, it is very much possible to improve the security of the whole institution and with maximum control on examination.

Biometrics however has its limitations. It suffers perception problems in that most people consider biometrics to be somehow secret when they are just unique identifiers. Also biometrics cannot be used for people who do not possess the physiological characteristics such as amputees, disabled people or when the characteristics available are not of good quality (Jimoh et al, 2011). It is also important to understand that access control is not a complete solution for securing a system (Ravi and Pierangela, 1994). However, the selection of a particular biometric for use in a specific application involves a weighing of several factors like universality, uniqueness, permanence, measurability, performance, acceptability and circumvention (Jain et al, 1999).

MATERIAL AND METHOD

Software

The software is written in MikroC then compiled and burned into the PIC16F84A using mikroelectronika development board as the programmer.

Scientia Africana, Vol. 16 (No. 2), December 2017. Pp 147-151
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

Circuit Diagram

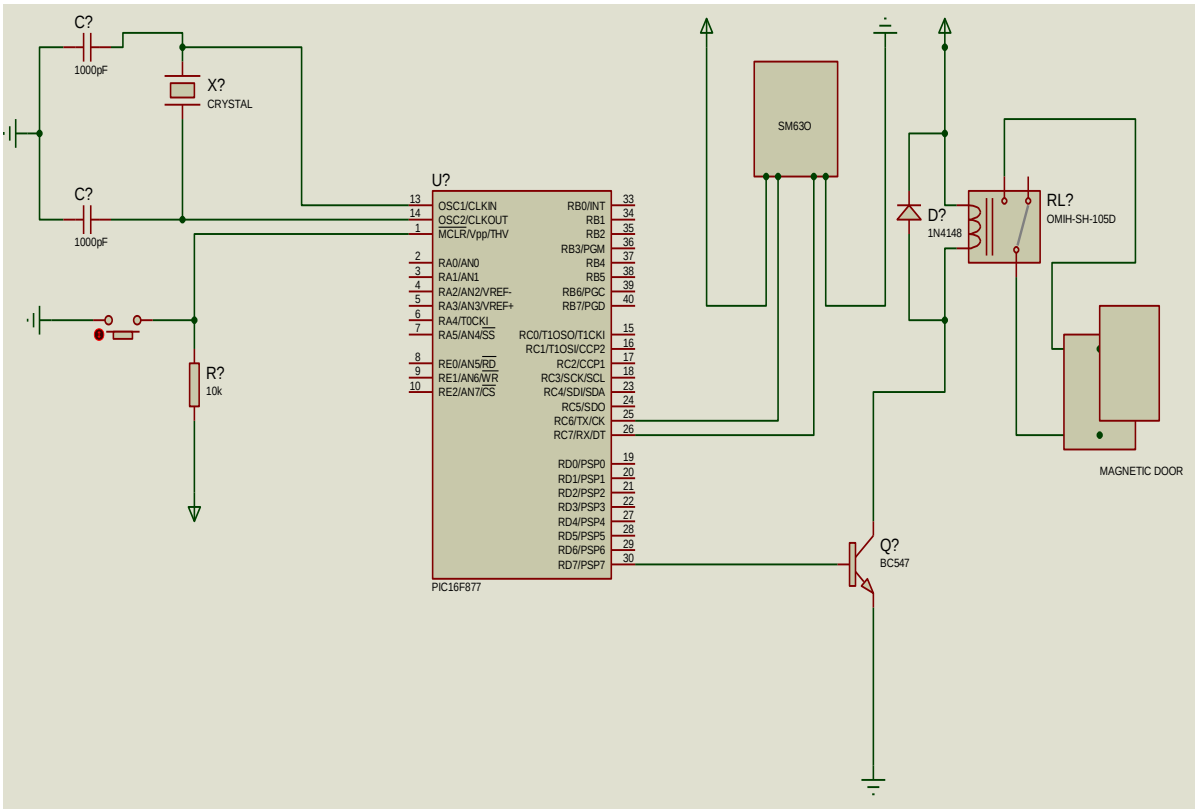

Figure 1: Circuit Diagram of the Biometrics System alone

General Circuit Operation

The schematic diagram shown in figure. 2 is the complete circuit diagram of the Biometrics Access Control System. The system has a transformerless circuit and a biometric system coupled together. It also comprise of both the power supply fully connected to the module. Just like every other automated system that detects, interpret and acts; this system detects the presence of human finger print, interprets as regards to the prior existence of the details and then finally carry out an action by either granting or denying access.

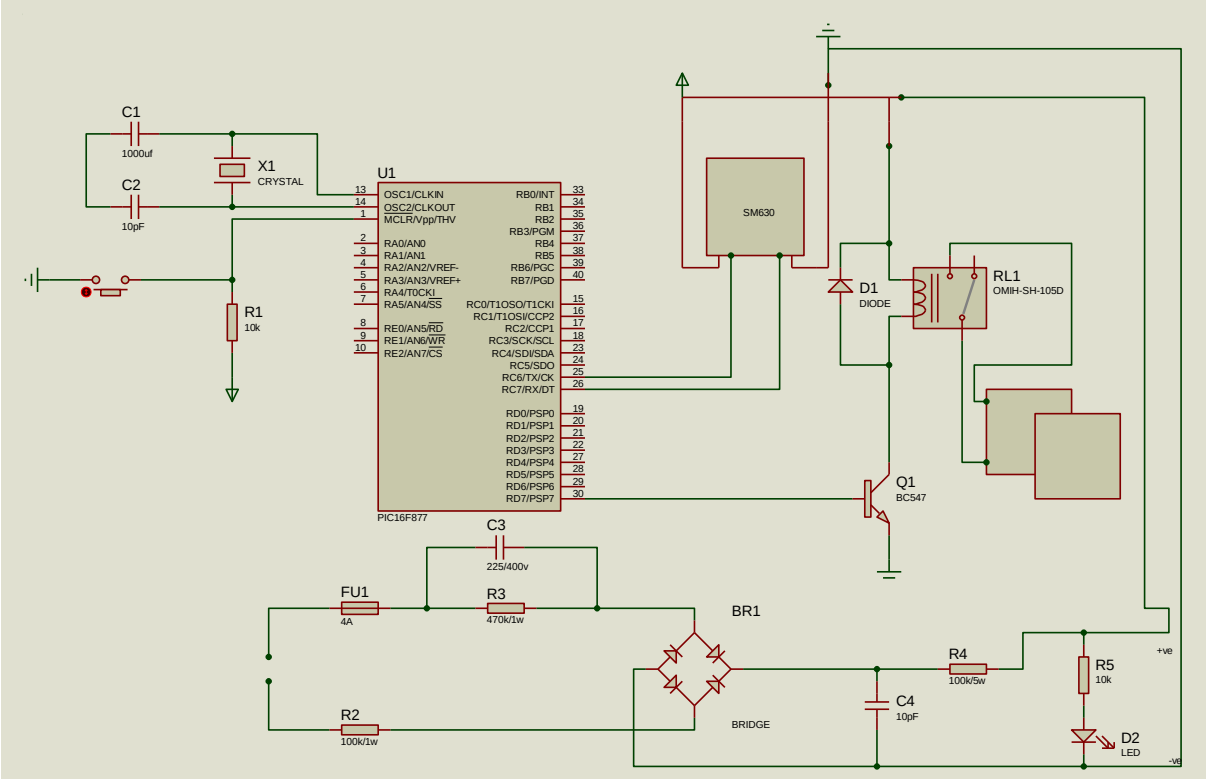

Figure 2: Complete Circuit Diagram of the Biometric System

Calculating for the voltage regulator value used, we have that

$$R = V_{in} - \frac{V_z}{I_z} \text{ - - - - - - - - (1)}$$

Where:
R = Resistance
V_{in} = Input Voltage
V_z = Output Voltage
I_z = Current through the Zener diode

A microcontroller based biometric access control system in tertiary institutions is presented in this paper. It will help us address several issued ranging from security, corruption, examination malpractices and illegal entry of unauthorized personnel among others.

Despite all of the interest in fingerprint-based biometric security systems, a number of serious concerns remain. The enrollment and matching performance can be poor. It may be significantly challenging to capture or verify proper fingerprint due to the presence of cuts and bruises. Face scanning may be hindered due to veils, eye patches, glasses, severe disfigurement and inability to keep still (Jimoh et al, 2011). Another challenge is the rate of entry and exit of persons in the institution on a daily basis, thereby over-stretching the facility and as

Scientia Africana, Vol. 16 (No. 2), December 2017. Pp 147-151
© Faculty of Science, University of Port Harcourt, Printed in Nigeria *ISSN 1118 – 1931*

such routine maintenance will be required within a stipulated period for optimum performance, which will definitely lead to cost implication. Moreso, stable power is required as this is a major challenge in the university community except using other source of power. Hence, the introduction of biometric access control system in the university will do more good than harm but only if the institution can bear the cost.

REFERENCE

Awasthi Reetu and Ingolikar, R.A. (2013) A Study of Biometrics Security System – International Journal of Innovative Research and Development.

Ashraf E. (2011) Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filter. Computer Science Department, Faculty of Computers and Information, Menofyia University, Egypt. The International Arab Journal of Information Technology, Vol. 8, No. 4.

Sadeque Reza Khan (2012) Development of low cost private office access control system International journal of embedded systems and applications Vol.2, No.2.

Jimoh, R. G., Abdulsalam, S.O. and Adewole K. S. (2011) Adoption of fingerprinting as an Automated Access Control Technique in University Hostels. ARPN journal of system and software. Volume 1, No. 4.

Ravi, S.S. and Pierangela, S. (1994). Access Control: Principles and Practice. IEEE Communications Magazine, September 1994.

Jain, A.K.; Bolle, R.; Pankanti, S. (1999). Biometrics: Personal Identification in Networked Society.