DESIGN OF EMBEDDED IDENTITY AUTHENTICATION SYSTEM

By

Anamonye U. G and Eyenubo O.J.
Delta State University Abraka
Oleh Campus
Email: gabriel.edu.ng@gmail.com, eyenubo63@yahoo.com

ABSTRACT

The project is aimed at the designing and implementing a stand-alone identity authentication device using fingerprint technique. The device does this by matching a user's fingerprint with the identity that the user claims. The design of this project is implemented with the SM630 optical sensor serially interfaced with a PIC16F876A microcontroller unit which is then interfaced with two 16x2 LCD units and a relay. A 5volts dc power supply (V_{cc}) was maintained throughout the circuit with the use of the IC7805 voltage regulator. A 7V rechargeable Li-ion battery provides back-up power for the system. The software design is based on mikroC with source code containing a total of 658 lines which provides control for the fingerprint sensor, LCD units and the relay circuit. When a fingerprint was detected, the biometrics information of the individual was revealed on one of the LCD displays, while the other LCD displayed operational instructions of the device.

INTRODUCTION

Biometrics is an automatic method of determining the identity of an individual based on some biological/physiological and behavioural traits or pattern. In 1882 Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, France, developed a detailed method of identification based on certain bodily measurements, physical descriptions, and photographs (Jain, 2011). Identity authentication is a security measure using data encryption that identifies and verifies the user, ensuring the user information is accurate and has not been tampered with. It restricts entrance and exit or usage of personal or collective resources. Electronic security systems using identity authentication for access control is now widely used in Nigeria within various sectors including Banking and finance, foreign exchange, housing, communication and defense. Other applications for various purposes require reliable and secure authentication techniques for access control. The User Identification Pin Number and Password protection are the most widely used authentication techniques. This method requires the user to create and remember a unique alphanumeric key combination for access control with the strength of the system dependent on the length and complexity of the password. However, a long and complex password can be forgotten or stolen in the case of user negligence. Another technique in identity authentication is the use of Radio Frequency Identification (RFID) tag.

The problem with RFID system is that the RFID card can be damaged and can also pose a security problem if the card gets lost or stolen as card can be used by an unauthorized proxy. To solve these problems, biometric authentication systems which identifies users by their unique biological information is now an area of interest. Biometrics involves the process of user recognition and verification based on physiological behaviour or pattern. Biometric authentication registers these behaviors and patterns on a database and is then

compared with subsequent attempts in order to grant or deny access. Biometrics uses fingerprint, face, iris, voice, signature, and hand geometry recognition and verification. Fingerprint based authentication system is one of the most important, well established and widely used biometric technology for access control and crime detection. Fingerprint authentication is based on the theory that human fingerprint is unique. Therefore, in this project fingerprint will be used as the medium in the authentication system which uses an optical fingerprint scanner interfaced with a microcontroller programmed to recognize and verify registered fingerprints. The mikroC is used to write the source code for fingerprint recognition and verification to the microcontroller. The C language is used because of its light weight and for faster processing speeds.

THEORETICAL BACKGROUND

Behavioural traits and characteristics are tools of identification, specific to each human-being, such traits include talking, or writing of signatures. On the other hand, we can also use physiological characteristics implying measurements of parts of the body such as fingerprint, hand geometry, facial structure and the iris pattern as method of identification. The mode of operation of biometric authentication systems comprises the verification method and the identification methods. These two methods are distinct. A verification system authenticates a person's claimed identity by comparing the particular biometric characteristic being used for identification against biometric measurements of the claimed identity that have been previously stored in the system (Jain, 2011). The identification system on the other hand compares the biometric characteristic against a database containing the identities of all authorized individuals. It is easier and more economical to implement the verification system but the identification method is more reliable.

The Concept of Biometric Technology

Various classes of biometric technique used for identity authentication exist. The earliest widely used are signature identification and fingerprint recognition. Signature identification is the analysis of the pattern in which an individual writes his signature. The process used by a biometric system to verify a signature is called dynamic signature verification (DSV) (Faundez, 2011). This process takes into account the angle at which the user holds the pen, the pressure exerted while writing, how many times the pen was lifted, the speed of writing and time taken to sign the entire signature.

Also, we have Face Recognition technique which uses visible physical structure of the face by analysing the three-dimensional geometry of the features that distinguish an individual. Since each human face is unique aside identical twins, the method is considered of relatively high accuracy.

Another method of identity authentication is the Iris Scan. The iris forms the coloured part of the eye and its pattern is unique to an individual. The shortcomings include its need for very expensive high-quality camera technology such as kiosk-based systems (Pavithra, Myna & Kavy, 2014). It also requires a high storage capacity for the large database. Other disadvantages include difficulty in aligning the eye with the scanner. The use of coloured contact lenses, and eye defects like cataracts can reduce its effectiveness.

Voice recognition is another form of identity biometric technique which uses acoustic features of the voice of an individual as a means of identification. These features include Short-term spectra features, Spectra-temporal features, Voice-source features, High level features, and prosodic features (Kinnumen and Li, 2009). In their work, entitled "Identity Authentication using Voice Biometrics Technique, Kamalu et al (2015) implemented a voice recognition system using the Gussian Mixture Model. The recorded voice signal was

matched to stored voice signal to identify the individual. All recorded voices were stored in an enrolment phase while the test voices were applied in the verification phase for comparison. Another very important biometric method is the finger print identity authentication system which is currently seen as most reliable. Fingerprints can be classified based on the ridge flow pattern (Lee, 2007). Based on this method of classification, the ridge pattern is tented arch, arch, right loop, left loop and whorl. A fingerprint consists of ridges and valleys. They together provide friction for the skin. The main identification of the skin is based upon the minutiae, which actually is the location and direction of the ridge endings and splits along a ridge path (Udih & Iweanya, 2016). There are basically two finger print matching methods namely minutiae matching and pattern matching. While Pattern matching compares checks similarity by comparing two fingerprint images, Minutiae matching relies on location and direction of each minutiae point. Experimental results have shown that the fingerprint based systems have very low False Rejection Rate (FFR) of 3 to 7% and False Acceptance Rate (FAR) of 0.001 to 0.01% (Ravi & Dattatreya, 2013).

DESIGN METHODOLOGY

The finger print authentication device is implemented through hardware design and embedded software algorithm. The hardware comprises of various components represented in the circuit diagram shown in figure 1. And embedded software development enables the SM630 optical sensor communication with the PIC16F876A microcontroller via the Universal Synchronous Receiver Transmitter (UART) communication protocol. Providing control for the microcontroller unit, fingerprints can be stored, added and deleted. It also controls outputs to both LCD units. The source code is written in mikroBASIC and simulated with Proteus. The software programme was loaded using top-win 6 programmer. The stand alone portable device can handle the processing of fingerprint image, extraction of feature point, classification and matching of fingerprint with user biometrics in the database.

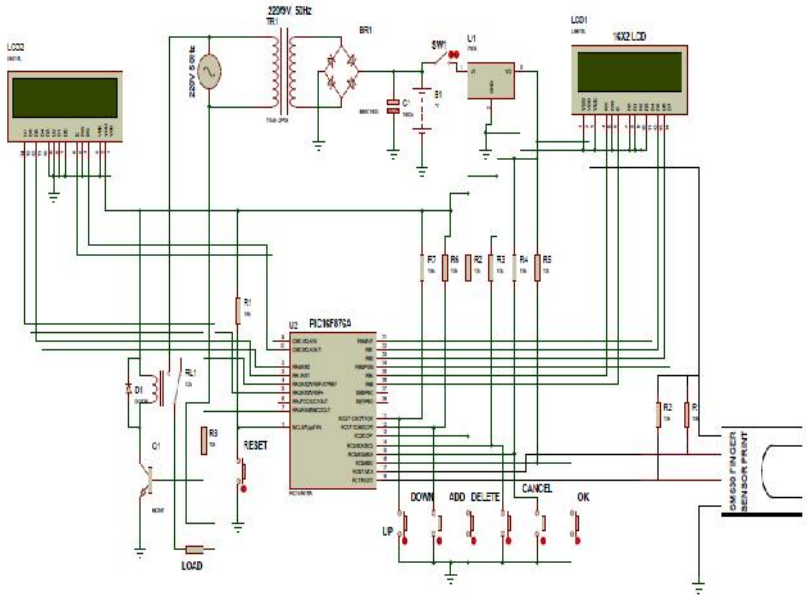

Figure 1: The Fingerprint Authentication Device

The bridge rectifier will give output voltage expressed in equation (1) (Gupta, 2007)

$$V_{dc} = 0.636V_m - 2V_F \quad (1)$$

Where V_m is the peak value (12v), V_F is diode forward drop (0.7v, IN4007) and $0.636 = 2/\pi$.

So, $V_{dc} = 6v$

Specifying capacitor value:

$$I = C\,{}^{dv}/_{dt} \quad (2)$$

$$C = I\,{}^{dt}/_{dv} \quad (3)$$

F = 50HZ

$dt = {}^{1}/_{2\times 50Hz}$ ie peak to peak time

So, dt = 0.01s

Where dv =2V ie ripple voltage, and I=1A,

$C = It/dv_{max}$ (4)

C = 1000μF

$$V_c = V(1 - e^{-t/Rc}) \quad (5)$$

As t tends to infinity $e^{-t/Rc}$ tends to zero

V_c = 12v

Since the working voltage of this capacitor should be such that it can hold at least 4/3 of the maximum charging voltage.

4/3 x 12 = 16v

Therefore, the capacitor C_1 rating used in this section is 1000uF/16v.

The Pull-up resistors R_2–R_7 of 10kΩ are connected such that when the button is depressed, a LOW appears at pins 11, 12, 13, 14, 15 and 16 of the microcontroller. And when the button is released a HIGH appears at the pins.

$$R_8 = (V - V_{BE})/I_b \quad (6)$$

V_{BE} = 0.7 V for silicon transistor, I_b =5mA

Then R_8 =860, 1KΩ was used as preferred value.

The LCD1 and LCD2 are driven by PORTA and PORTB respectively, while the keypad is driven by PORTC.

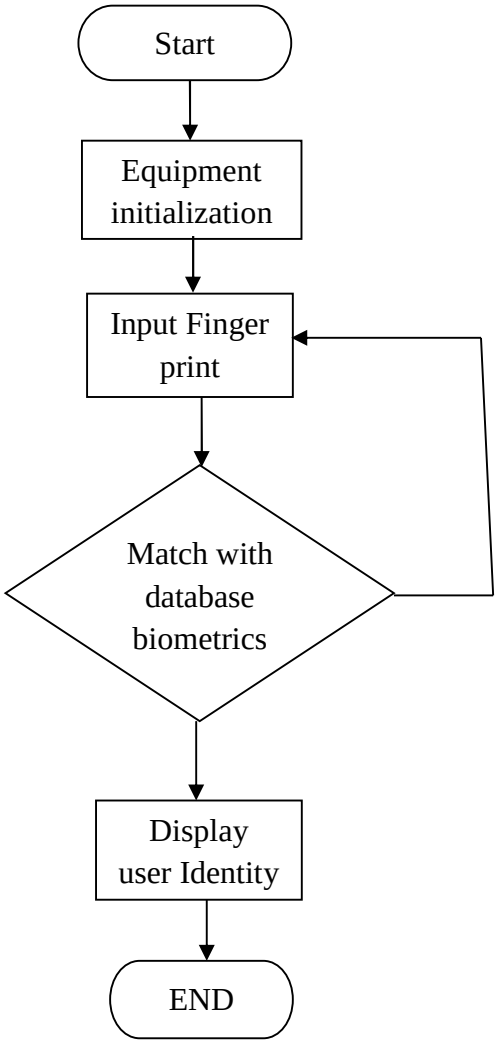

Fig. 2: Device Identity Authentication Sequence

CONCLUSION

The design and implementation of a portable stand-alone identity authentication device has been presented in this paper. The device can scan, capture and store user fingerprints automatically, perform authentication function and displayed appropriate messages on the two LCDs such as user information and operational guide. Test result showed that the device performance in the two basic modes, registration mode and authentication mode is satisfactory. It is recommended that the technology be expanded to handle image processing so as to provide real time identity verification for every user.

REFERENCES

Faundez-zanuy M. (2011), "Biometric Security Technology", Aerospace and Electronic Magazine, IEEE, 21(1), 15-21.

Gupta J.B. (2007), Electronic Devices and Circuits. S.K Katharia & Sons, Naisarak, Delhi.

Jain A, (2008), "Biometrics", Microsoft Encarta 2009 [DVD]. Redmond, WA: Microsoft Corporation.

Kamalu U.A, Raji A., & Nnebedum V.I. (2015). Identity Authentication Using Voice Biometric Technique. International Journal of

Research in Engineering and Technology (IJRET). Vol 4 Issue 12, 130-136.

Kinnumen T. And Li H. (2010). An overview of Text Dependent Speaker Recognition: from Features to Supervisors, Journal of Speech Communication, vol. 52, issue 1, 12-40.

Lee K.P, (2007), "Security System Using Biometric Technology: Using fingerprint", Student Thesis, Department of Industrial Electronics, University of Technology Malaysia.

Pavithra B.C, Myna B, and Kavy A, (2014), "Fingerprint Bank Locker System Using Microcontroller", IRF conference Proceedings India, April 2014.

Ravi S. and Dattatreya P.M (2013), A Study of Biometric Approach Using Finger Print Recognition. Notes on Software Engineering, Vol. 1, Issue 2.

Udih O. and Iweanya C. (2016), Design and Construction of a Fingerprint Authentication System, Student Project Delta State University, Oleh Campus.

