Electronic System for Personal Access Control for fingerprint recognition, Remote Authentication in database through a WLAN.

Jaime R. Michilena, ING, Estefanía G. Torres

Summary - **This document describes the process of design and implementation of Electronic System for Personnel Access Control for fingerprint recognition, Remote Authentication in Database to through a WLAN software using AVR STUDIO for programming AVR microcontrollers in C and assembler, PROTEUS simulator for debugging and graphical editor EAGLE layers, to design schematics and PCB.**

It provides an integrated security solution, the merger of the two technologies, it is feasible and interesting do implement a user authentication system by reading your fingerprint. The project to use WLAN in the transmission of data from multiple terminals into a single database, to allow the entry and exit of people through various access points.

.

I. INTRODUCTION

The Biometric authentication technologies today have become the main solution to avoid phishing. Among these, the reading of the fingerprint has established itself as a safe, fast and convenient for accreditation of users, regardless of the use of media as clonable coded badges or keys, its low power consumption, the high level of integration and mobility have become the best option for transmission of data.

In wireless communications, WLAN is the most convenient because of their widespread and standardization, bandwidth and security.

Implementing an Electronic System for Personnel Access control by fingerprint recognition, Remote Authentication in database through a WLAN in the Hostal la Garzas, security is an essential component. Biometric technologies to establish itself as teams that prevent spoofing can not allow to be cloned as cards or keys that were previously used, maintaining a constant monitoring of the network using the database for the early detection of alerts, to reports through providing the same. Thus, it prevents the resources involved main Inn.

II. CONCEPTS BASICS

A. Embedded Systems

They system is designed around a specific application and for that reason the develops very tailored to the needs, implying a low size, low cost and high replicated. [1]

These devices are used to control and operate equipment.

Term Embedded

Indicates that these circuits are essential and integral part of the system that are inherently integrate all the subsystems and elements needed to perform the work operation for proper operation. In embedded systems are distinguished: Hardware, software, operating systems and embedded systems access control. [1]

- **Systems Hardware Embedded.-**work on a wide range of hardware platforms and their selection depends exclusively on the final application.

- **Embedded Systems. -** Development programs are proprietary and closed, which generate binary codes are loaded in the system, are relatively costly because of license maintenance.

- **Operating Systems for Embedded Systems. -** Not all systems use an embedded operating system, is important to understand this because in many cases it is unnecessary. But if there are other systems that require an operating system to work which need less hardware to a standard PC.

- **Embedded Systems Access Control. -** It is important to have adequate security mechanisms to the environment to be protected, the purpose of identification systems not usually identify a person, but authenticate who he really is.

Authentication methods are divided into three categories: Password, Token, Biometric Authentication.

Document received August 31, 2012. This research was conducted as previous project to get the degree in the Engineering Electronics and Communication Network Engineering, Faculty of Applied Science (FICA), Technical University of the North.

J.R. Michilena, works at the Technical University of Northern Engineering Degree in Electronics and Communication Networks, July 17th Av sector El Olivo, Ibarra-Ecuador (Phone: 5936-2955-413, e-mail: jaimerobertomc @ gmail . com).

E.G. Torres, a graduate of the School of Electrical Engineering and Communication Networks (Phone: 5936-2602-725, e-mail: estefania_torres86@hotmail.com).

B. Biometrics

It is a security technology based on the recognition of a physical characteristic and non-transferable

Biometric Recognition

These devices consist of three main parts have an automatic mechanism that reads and captures a digital image, you have an entity to manage issues such as understanding, storing the captured data stored in the database, provides an interface to the applications that use them.

It consists of the following steps:

- **Capture or reading data to validate the user presents**
- **Removal of certain characteristics of the sample**
- **Decision on whether the user is valid or not**
- **Comparison of these characteristics with those stored in the database.**

Is the decision come into play where the two basic characteristics of the ability of any biometric system: the false rejection rate and false acceptance.

- **False rejection rate. -** Is the probability that the authentication system rejects a legitimate user because it is not able to identify it correctly.

- **False acceptance rate. -** Is the probability that the system correctly authenticate an illegitimate user.

Methods Biometrics

Physiological type methods include:

- **Fingerprint Identification**
- **Iris Recognition**
- **Recognition of the Retina**
- **Facial Recognition**
- **DNA Analysis**

Fingerprint recognition

Is biometric identification method par excellence due to its ease of use and has great acceptance by users. All fingerprint systems are based on four principles: continuity, Immutability, Infinite Diversity, watching the skin.

- **Durability. -** Fingerprints are present throughout the life until the decomposition of the corpse.
- **Immutability. -** The tracks are not affected by any disease or physical development of individuals.
- **Infinite Diversity. -** Fingerprints are unique and unrepeatable.
- **The skin** is not entirely smooth or uniform, is covered with ridges and depressions in the skin.

C. System Description

The device is a digital system for access control to buildings by people recognizing your fingerprint and checking if they are in the database with WLAN infrastructure. [2]

The various mechanisms implemented in the system allow:

- **Sensar accurately and at high speed, the parameters involved in access.**
- **Verify the legitimacy of biometric authentication of users by their fingerprint.**
- **Establish remote wireless communication with a personal computer.**
- **Use a user-friendly interface to manage the database.**

Requirements based on the work environment

Transmit power and receive sensitivity adequate capacity for coexistence with other wireless devices and immunity to electrical noise.

Requirements specifications based on power

Sufficient power handling, reduced power consumption in standby, efficient power delivery to support the safe operation of all devices and protection against reverse connection to prevent damage to the device.

Based on performance requirements requested

High speed data acquisition, processing and execution, graphical interface, explicit and readable for managing the database, wireless communication security to prevent intrusions and security biometric fingerprint reading. In Figure 1 displays the basic concept of the device subsystems grouped into blocks according to their general duties.

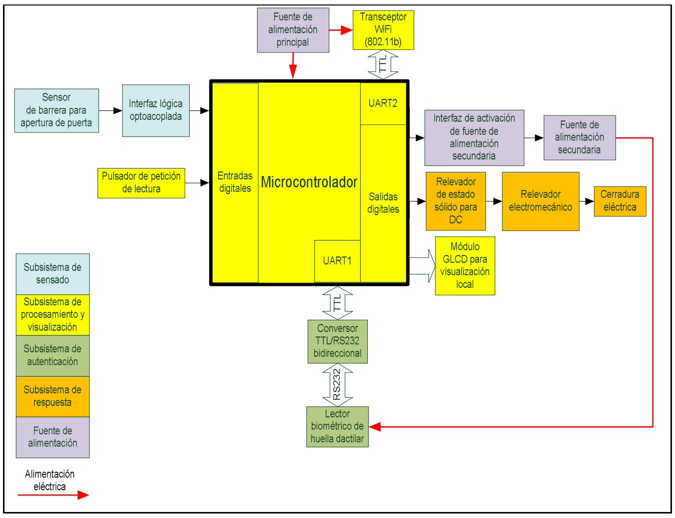

Fuente de alimentación principal
Transceptor WiFi (802.11b)
TTL
Sensor de barrera para apertura de puerta
Interfaz lógica optoacoplada
Pulsador de petición de lectura
Entradas digitales
Microcontrolador
UART2
Salidas digitales
UART1
Interfaz de activación de fuente de alimentación secundaria
Fuente de alimentación secundaria
Relevador de estado sólido para DC
Relevador electromecánico
Cerradura eléctrica
Módulo GLCD para visualización local
TTL
Conversor TTL/RS232 bidireccional
RS232
Lector biométrico de huella dactilar
Subsistema de sensado
Subsistema de procesamiento y visualización
Subsistema de autenticación
Subsistema de respuesta
Fuente de alimentación
Alimentación eléctrica

Fig 1. System Block Diagram

Sensing subsystem

Responsible for the acquisition and conditioning in the event of the opening and closing of the door.

Processing and Display Subsystem

The fundamental basis of the entire mechanism is the microcontroller handles two bidirectional serial communication ports for transferring information.

For remote communication with the PC is done with the IEEE802.11b transceiver.

The display module GLCD made by the user to verify the various functions that have been added to the mechanism.Para la comunicación remota con la PC se realiza con el transceptor IEEE802.11b.

Authentication Subsystem

It is basically a biometric fingerprint reader, the microcontroller simply sends commands to the biometric reader module and receive information.

The biometric reader can be connected to a PC to configure all parameters of the system.

Response subsystem

It is the interface used to manage power consumers, their main functional transform some digital output supply current to activate the electric lock.

III. IMPLEMENTATION AND TESTING SYSTEM

A. Physical Mounting

Biometric technologies have evolved continuously since its onset to prevent spoofing.

The resources used in the system to provide the control and analysis of different data, are listed below in the following graphs

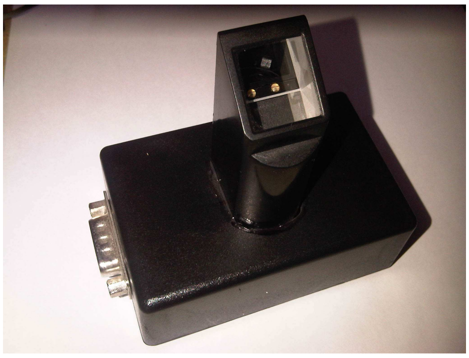


Figure 2: Biometric

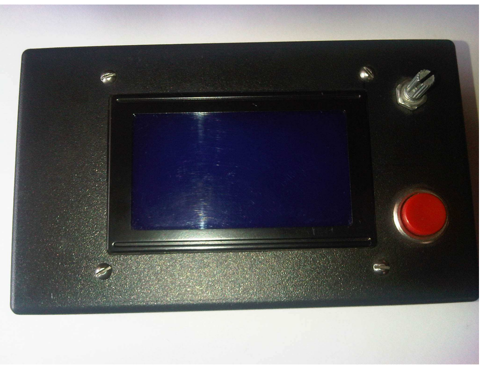


Figura 3: Access Control

Figure 4: Access Point

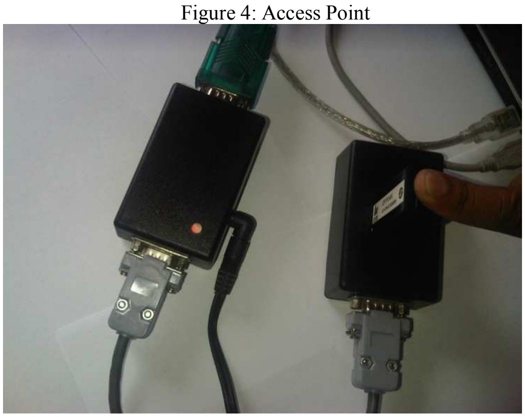


Figure 5: Connecting the PC to the biometric reader

B. Implementation

Implementation is seeking the least possible impact on the infrastructure of the Inn, the power connections are made so that they are not exposed to avoid possible violations to the system, the same care was taken to install the barrier and sensor electric lock.

Figure 5 presents the biometric reader configuration with the serial cable and the PC interface.

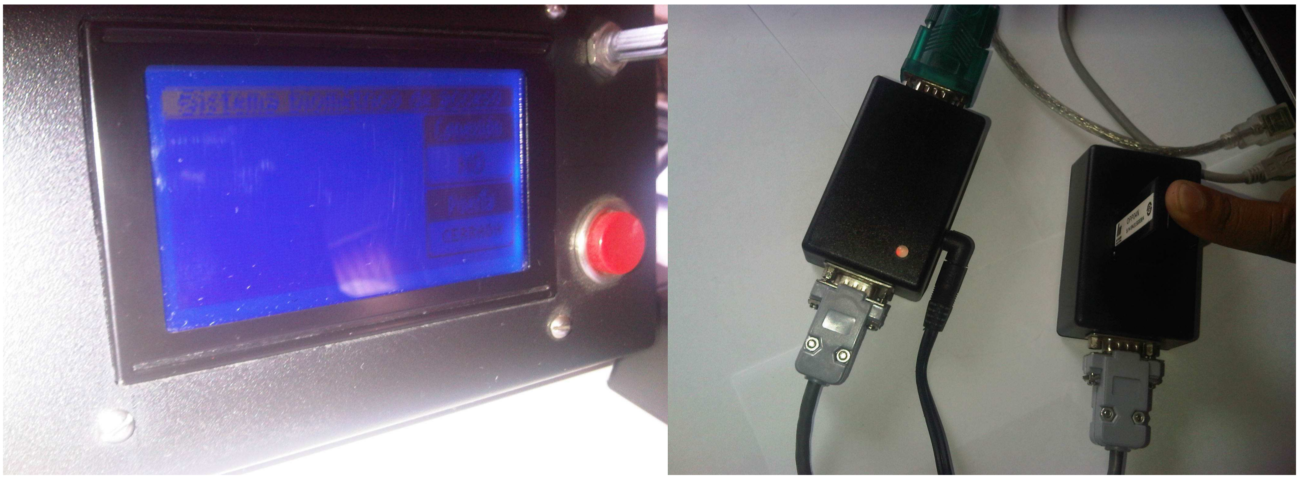
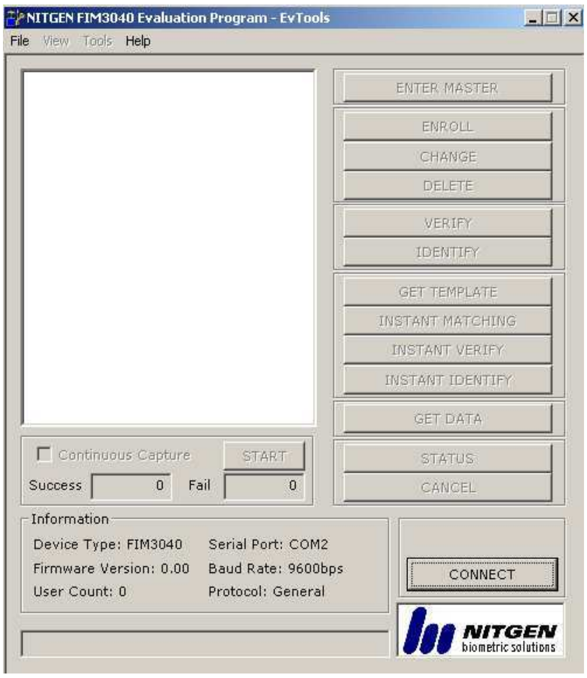


Figure. 5. Connecting the PC to the biometric reader

To configure the hardware of the reader and enter new users using the software of NITGEN EVTOOLS. This program has a serial communication with the biometric reader and identifies, add and delete fingerprints.



NITGEN FIM3040 Evaluation Program - EvTools

Success 0 Fail 0

Information

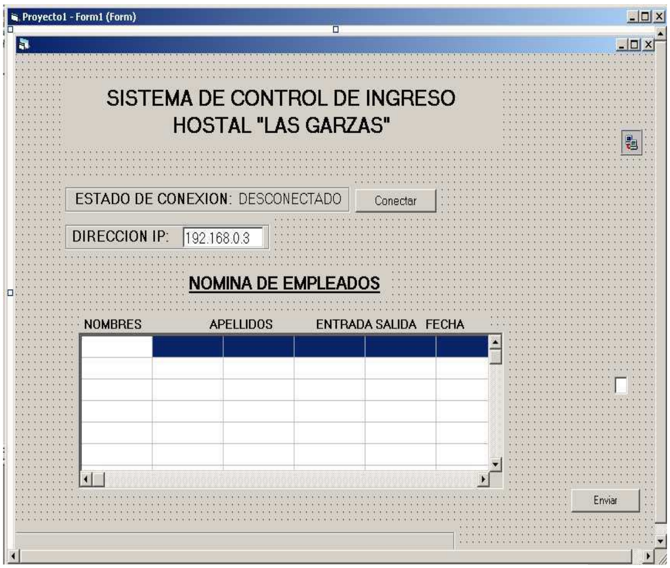
Device Type: FIM3040 Serial Port: COM2
Firmware Version: 0.00 Baud Rate: 9600bps
User Count: 0 Protocol: General

Figure 6: Software EVTOOLS of NITGEN

Another essential tool for the development of this project, is the database is done in Visual Basic 6.0, due to its ease of use and robustness. Which can be seen in Figure7.

The most important features of this application are:

- **Manages the Ethernet port on the PC via WINSOCK component. This element allows client / server connections through TCP / IP.**
- **Use the Microsoft Data Formatting Object references Library and Microsoft ActiveX Data Objects, allowing you to work with and manage MySQL database.**
- **The fields of the database that handle user information are: name, surname, check-in, check-out, turn initialization date**.



Proyecto1 - Form1 (Form)

SISTEMA DE CONTROL DE INGRESO
HOSTAL "LAS GARZAS"

ESTADO DE CONEXION: DESCONECTADO

DIRECCION IP: 192.168.0.3

NOMINA DE EMPLEADOS

NOMBRES APELLIDOS ENTRADA SALIDA FECHA

Figure 7: Main screen

C. *Testing*

Multiple tests were performed at both firmware and hardware; individual events and the whole system running. The single most important tests are:

• Proper operation of the interfaces used, likewise their interface with the microcontroller.
• Communication between the microcontroller and the WiFly module.
• Communication between the microcontroller and the biometric reader.
• Updating Data on the GLCD

We proceeded to verify the operation of the whole system together.

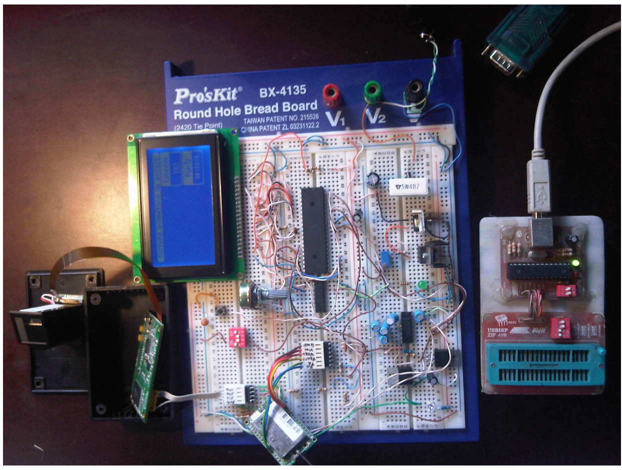


Figure 7: Pre-testing of the system board electronic test

D. Test scope

Regarding the distance there is a pattern that predominates in the quality of the wireless link, which indicates the following table: [3]

Table 2: Test range in different scenarios

OBSTACLE	SCOPE
Concrete Walls	50m
Metal doors	10m
Wooden doors	70m
Vehicles and trees	80m

E. INTERFERENCE TEST DRIVE IN THE MIDDLE

Testing was performed in confined spaces where there is massive presence of devices working in the system frequency (2.4GHz). [4]

Table 3: Tests of response in different scenarios

CANTIDAD DE INTERFERENCIA	RESPUESTA [seg]
None	1
Media	1.3
High	1.8

IV. OVERALL SYSTEM PERFORMANCE

From the above tests can indicate that all measurements yielded very satisfactory values.

With regard to the response time of the database, there are slight variations due to the free working computer (user applications are not open).

With regard to the values taken in the test range limitation exists due to the sensitivity and the type of radio equipment.

Furthermore, functional testing of the complete system, indicate that the device is safe. Its implementation is recommended.

V. CONCLUSIONS

The access control system that was implemented in the Hostal las Garzas is reliable, because it is a fast system that incorporates both high security hardware for storing data to perform encryption.

During system design, it is essential to establish strategically server location and capacity planning of computer hardware. From a good choice depend efficiency project to control the personnel working at the site and thus fulfill the purpose of implementation.

The electronics that were used were the correct implementation since these allow the proper functioning of the prototype with the aid of block diagrams and flow. We applied the acquired knowledge, especially information security, wireless networking, and database programming.

We analyzed the features they offer identification technology from their analysis concludes that, in most cases, are caused by the inappropriate use of resources of the place by users resulting in large losses in the Inn.

AWARDS

It expresses a special thanks to the hostal las garzas, especially Mr. Alejandro Pita for the support and collaboration provided for such work.referencias.

REFERENCES.

[1] REID Neil, 802.11 (Wi-Fi): Manual de Redes Inalámbricas, McGraw – Hill Interamericana, México, 2007.

[2] TANENBAUM Andrew, Redes de Computadoras, Prentice Hall Hispanoamericana, México, 2007.

[3] STALLINGS, W., Comunicaciones y Redes de Computadores, Prentice Hall, 2008.

[4] FISH Peter, Electronic Noise and Low Noise Design, McGraw – Hill, 2007.

Jaime R. Michilena C.

Was born on februry 19,1983 in Atuntaqui ,Imbabura.Engineer in Electronics and Telecommunications, National Polytechnic School in 2006. Currently teaches at the School of Engineering in Electronics and Communication Networks at the Technical University of the North, Ibarra-Ecuador, and studying for a Masters in Communication Networks (3do Semester), Pontifical Catholic University of Ecuador, Quito, Ecuador.

Estefanía G. Torres A.

Was born on october 14, 1986 in Ibarra-Ecuador. Daughter of Edgar Torres and Graciela Aza. He attended elementary school in Particular "Fe y Alegria". In 2004 received his Bachelor of Science degree in Physical Mathematical School "Ibarra National". Currently, he is a graduate of the School of Electrical Engineering and Communication Networks, Technical University of North Ibarra.