Sistema Electrónico para Control de Acceso de Personas por Reconocimiento de Huella Dactilar, con Autenticación Remota en Base de Datos a través de una WLAN.

Jaime R. Michilena, ING, Estefanía G. Torres

***Resumen*— El presente documento expone el proceso de diseño e implementación de un Sistema Electrónico para Control de Acceso de Personas por Reconocimiento de Huella Dactilar, con Autenticación Remota en Base de Datos a través de una WLAN empleando el software AVR STUDIO para la programación de microcontroladores AVR en lenguaje C y ensamblador , el simulador PROTEUS para la depuración de errores y el editor gráfico de capas EAGLE, para el diseño de diagramas esquemáticos y placas de circuito impreso.**

Se proporciona una solución de seguridad integrada, con la fusión de las dos tecnologías, resultando factible e interesante implementar un sistema de autenticación de usuarios por lectura de su huella dactilar. El proyecto se orienta a utilizar WLAN en la transmisión de datos desde varios terminales hacia una sola base, a fin de permitir la entrada y salida de personas a través de diversos puntos de acceso.

.

I. INTRODUCCIÓN

Las tecnologías de autenticación biométrica hoy en día se han convertido en la principal solución para evitar la suplantación de identidad. Dentro de éstas, la lectura de la huella dactilar se consolida como un medio seguro, rápido y práctico para la acreditación de usuarios, prescindiendo del uso de medios clonables como las tarjetas codificadas o llaves, por su bajo consumo de potencia, el gran nivel de integración y la movilidad se han convertido en la mejor opción para la transmisión de datos.

Dentro de las comunicaciones inalámbricas, WLAN es la más conveniente debido a su gran difusión, estandarización, ancho de banda y seguridad.

Documento recibido el 31 de agosto de 2012. Esta investigación se realizó como proyecto previo para obtener el título profesional en la carrera de Ingeniería Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte.

J.R. Michilena, trabaja en la Universidad Técnica del Norte, en la Carrera de Ingeniería en Electrónica y Redes de Comunicación, Av. 17 de Julio sector El Olivo, Ibarra-Ecuador (teléfono: 5936-2955-413; e-mail: jaimerobertomc@gmail.com).

E.G. Torres, egresada de la Carrera de Ingeniería Electrónica y Redes de Comunicación (teléfono: 5936-2602-725; e-mail: estefania_torres86@hotmail.com).

La implementación de un Sistema Electrónico para control de Acceso de Personas por Reconocimiento de Huella Dactilar, con Autenticación Remota en Base de Datos a través de una WLAN en la Hostal la Garzas, constituye un componente de seguridad indispensable. Las tecnologías biométricas al constituirse como equipos que evitan la suplantación de identidad no permiten que puedan ser clonadas como las tarjetas o llaves que anteriormente se usaba, se mantiene un constante monitoreo de la red mediante la base de datos para la detección temprana de alertas, a través de reportes que proporciona la misma. De esta manera, se evita que se involucren los recursos principales de la Hostal.

II. CONCEPTOS BÁSICOS

A. Sistemas Embebidos

Son sistema que se diseñan pensando en una aplicación concreta y por esa razón se los desarrolla de manera muy ajustada a las necesidades, implicando un bajo tamaño, reducido costo y alta replicidad. [1]

Estos dispositivos son utilizados para controlar y operar equipos.

Término Embebido

Indica que estos circuitos son parte esencial e integral del sistema en el que se encuentren se integran intrínsecamente, todos los subsistemas y elementos necesarios para realizar la labor de operación para el correcto funcionamiento. Dentro de los sistemas embebidos se distinguen: Hardware, Software, Sistemas Operativos y Sistemas embebidos de control de acceso. [1]

- **Hardware de Sistemas Embebidos.-**Trabajan sobre una amplia gama de plataformas de hardware y su selección depende exclusivamente de la aplicación final.

- **Software de Sistemas Embebidos.-** Los programas de desarrollo son propietarios y cerrados, generan códigos binarios los cuales son cargados en el sistema, son de costo relativamente elevado debido a su mantenimiento de licencia.

- **Sistemas Operativos de Sistemas Embebidos.-** No todos los sistemas embebidos usan un sistema operativo, es importante tener en claro esto porque en muchos casos es innecesario. Sin embargo existen otros sistemas que si requieren de un sistema operativo para trabajar los cuales necesitan un hardware menor a un PC normal.
- **Sistemas Embebidos de Control de Acceso.-** Es importante disponer de mecanismos de seguridad adecuados al medio que se intenta proteger, el objetivo de los sistemas de identificación no suele ser identificar a una persona, sino autenticarla es decir quién es realmente.
  Los métodos de autenticación se dividen en tres categorías: Password, Token, Autenticación Biométrica.

B. Biometría

Es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible.

Reconocimiento biométrico

Estos dispositivos constan de tres partes principales disponen de un mecanismo automático que lee y captura una imagen digital, dispone de una entidad para manejar aspectos como la comprensión, almacenamiento de los datos capturados con los guardados en la base de datos, ofrece una interfaz para las aplicaciones que los utilizan.

Consta de los siguientes pasos:

- **Captura o lectura de los datos que el usuario a validar presenta**
- **Extracción de ciertas características de la muestra**
- **Decisión de si el usuario es válido o no**
- **Comparación de estas características con las guardadas en la base de datos.**

Es en la decisión en donde entran en juego las dos características básicas de la habilidad de todo sistema biométrico: las tasa de falso rechazado y las de falsa aceptación.

- **Tasa de falso rechazo.-** es la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente.
- **Tasa de falsa aceptación.-** es la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo.

Métodos Biométricos

Los métodos de tipo fisiológico incluyen los siguientes:

- **Identificación de huellas dactilares**
- **Reconocimiento de Iris**
- **Reconocimiento de la Retina**
- **Reconocimiento Facial**
- **Análisis de ADN**

Reconocimiento de Huella Dactilar

Es el método de identificación biométrica por excelencia debido a su facilidad en el uso y tiene gran aceptación por parte de los usuarios.
Todos los sistemas dactiloscópicos se basan en cuatro principios: Perennidad, Inmutabilidad, Diversidad Infinita, Observación de la piel.

- **Perennidad.-** Las huellas dactilares están presentes a lo largo de toda la vida hasta el momento de la descomposición del cadáver.
- **Inmutabilidad.-** Las huellas no se ven afectadas por ningún tipo de enfermedad ni por el desarrollo físico de los individuos.
- **Diversidad Infinita.-** Las huellas dactilares son únicas e irrepetibles.
- **La piel** no es enteramente lisa o uniforme, está cubierta de rugosidades y depresiones en la piel.

C. Descripción del Sistema

El dispositivo es un sistema digital de control de acceso de personas a edificaciones mediante reconocimiento de su huella dactilar y verificando si se encuentran en la base de datos con conexión WLAN de infraestructura. [2]

Los diversos mecanismos implementados en el sistema permiten:

- **Sensar de manera precisa y con alta velocidad, los parámetros implicados en el acceso.**
- **Verificar la legitimidad de los usuarios mediante autenticación biométrica de su huella dactilar.**
- **Establecer comunicación inalámbrica remota con una computadora personal.**
- **Utilizar una interfaz amigable con el usuario para administrar la base de datos.**

Requisitos en base al ambiente de trabajo

Potencia de transmisión y sensibilidad de recepción adecuada, capacidad de coexistencia con otros dispositivos inalámbricos e inmunidad al ruido eléctrico.

Requisitos en base a especificaciones de potencia

Manejo de potencia suficiente, consumo eléctrico reducido en estado de espera, entrega de potencia eficiente para permitir el funcionamiento seguro de todos los dispositivos y protección contra conexión invertida para evitar daños en el dispositivo.

Requisitos en base al desempeño solicitado

Alta velocidad de adquisición, procesamiento y ejecución, interfaz gráfica, explícita y legible para el manejo de la base de datos, seguridad en la comunicación inalámbrica para evitar intrusiones y seguridad en la lectura biométrica de huella dactilar.

En la Fig. 1 se visualiza la concepción básica del dispositivo en bloques agrupados en subsistemas de acuerdo a sus funciones generales.

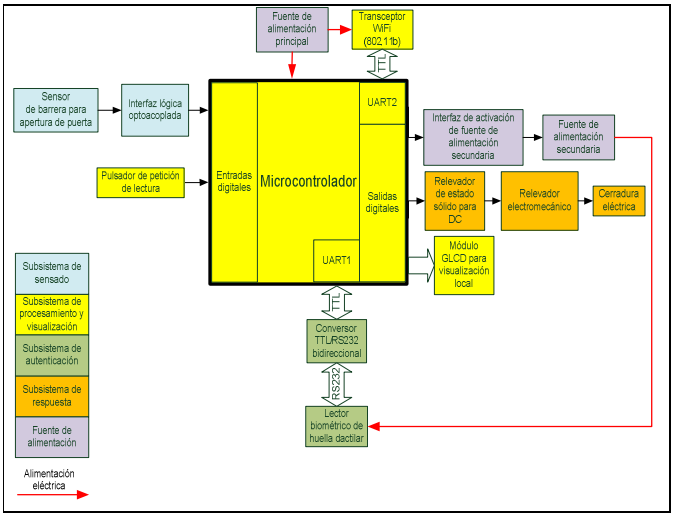

Fig. 1. Diagrama de bloques de sistema

Subsistema de Sensado

Se encarga de la adquisición y acondicionamiento en el evento de la apertura y cierre de la puerta.

Subsistema de procesamiento y Visualización

La base fundamental de todo el mecanismo es el microcontrolador, maneja dos puertos de comunicación serial bidireccional para la transferencia de la información.

Para la comunicación remota con la PC se realiza con el transceptor IEEE802.11b.

El modulo de visualización realizado por la GLCD permite verificar al usuario las diferentes funciones que han sido agregadas al mecanismo.

Subsistema de Autenticación

Consiste básicamente en un lector biométrico de huella dactilar, el microcontrolador se limita a enviar comandos hacia el módulo de lectura biométrica y recibir información de este.

El lector biométrico se puede conectar a un computador personal para configurar todos los parámetros de funcionamiento del sistema.

Subsistema de Respuesta

Es la interfaz que se usa para manejar los consumidores de potencia, su funcional principal es transformar cierta salida digital en un suministro de corriente para activar la cerradura eléctrica.

III. IMPLEMENTACIÓN Y PRUEBAS DEL SISTEMA

A. Montaje Físico

Las tecnologías biométricas han ido evolucionando continuamente desde su aparición para evitar la suplantación de identidad.

Los recursos empleados en el sistema para proporcionar el control y análisis de los diferentes datos, se detallan a continuación en los siguientes gráficos.

Figura 2: Lector biométrico

Figura 3: Control de Acceso

Figura 4: Punto de acceso

B. Implementación

La implementación se realiza procurando el menor impacto posible en la infraestructura de la Hostal, las conexiones de la alimentación se realizaron de tal manera que no queden descubiertas para evitar posibles violaciones al sistema, el mismo cuidados se tuvo al instalar el sensor de barrera y la cerradura eléctrica.

La Fig. 5 expone la configuración del lector biométrico con el cable serial y la interfaz de la PC.

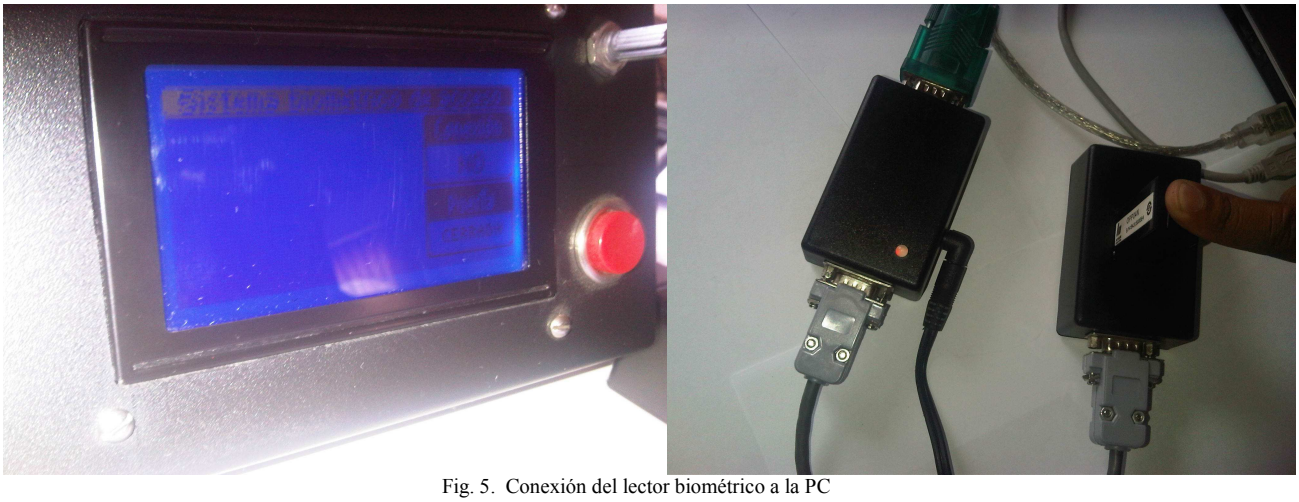

Fig. 5. Conexión del lector biométrico a la PC

Para configurar el hardware del lector e ingresar nuevos usuarios se utiliza el software EVTOOLS de NITGEN. Este programa mantiene una comunicación serial con el lector biométrico y permite identificar, agregar y borrar las huellas dactilares.

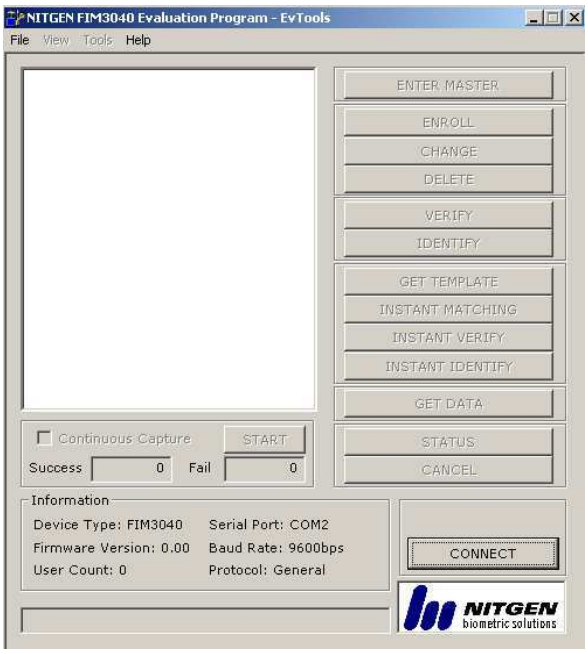

Figura 6: Software EVTOOLS de NITGEN

Otra de las herramientas imprescindibles para el desarrollo de este proyecto, es la base de datos está realizado en Visual Basic 6.0, debido a su simplicidad de uso y gran robustez. La cual se puede observar en la figura7.

Las características más importantes de esta aplicación son:

- **Maneja el puerto Ethernet de la PC a través del componente WINSOCK. Este elemento permite realizar conexiones cliente / servidor a través del protocolo TCP/IP.**
- **Utiliza las referencias Microsoft Data Formatting Object Library y Microsoft ActiveX Data Objects, lo que le permite trabajar en conjunto con MYSQL y administrar la base de datos.**
- **Los campos de la base de datos que manejan la información del usuario son: nombres, apellidos, hora de entrada, hora de salida, fecha de inicialización del turno.**

Figura 7: Pantalla principal del programa

C. *Pruebas*

Se realizaron múltiples pruebas tanto a nivel de firmware como de hardware; pruebas individuales y con todo el sistema funcionando. Las pruebas individuales más importantes son las siguientes:

- **Funcionamiento correcto de las interfaces utilizadas; así mismo la interacción de éstas con el microcontrolador.**
- **Comunicación entre el microcontrolador y el módulo WIFLY.**
- **Comunicación entre el microcontrolador y el lector biométrico.**

- **Actualización de datos en la GLCD.**

D. PRUEBAS

Se realizaron múltiples pruebas tanto a nivel de firmware como de hardware; pruebas individuales y con todo el sistema funcionando las cuales son las siguientes:

- **Funcionamiento correcto de las interfaces utilizadas; así mismo la interacción de éstas con el microcontrolador.**
- **Comunicación entre el microcontrolador y el módulo WIFLY.**
- **Comunicación entre el microcontrolador y el lector biométrico.**
- **Actualización de datos en la GLCD.**
- **Pruebas con las diferentes tramas manejadas en la transmisión inalámbrica de datos.**
- **Manipulación de datos por parte del software en la PC, observando la correcta codificación de las tramas enviadas e interpretación de las tramas recibidas.**

Se procedió con la verificación del funcionamiento de todo el sistema en conjunto.

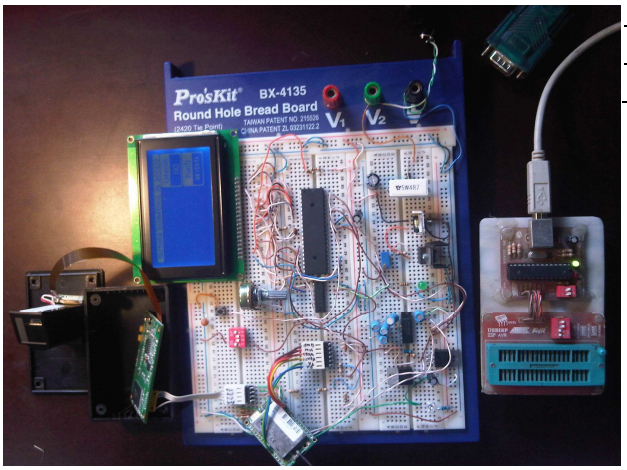

Figura 7: Pruebas previas del sistema en tablero de ensayo electrónico

E. PRUEBA DE ALCANCE

En cuanto a la distancia hay un patrón que predomina en la calidad del enlace inalámbrico, los cuales indica la siguiente tabla: [3]

Tabla 2: Pruebas de alcance en diferentes escenarios

OBSTÁCULO	ALCANCE
Paredes de concreto	50m
Puertas de metal	10m
Puertas de madera	70m
Vehículos y árboles	80m

F. PRUEBA DE INTERFERENCIA EN EL MEDIO DE TRANSMISIÓN

La prueba se realizó en espacios reducidos donde existe presencia masiva de dispositivos que trabajan en la frecuencia del sistema (2.4Ghz). [4]

Tabla 3: Pruebas de respuesta en diferentes escenarios

CANTIDAD DE INTERFERENCIA	RESPUESTA [seg]
Ninguna	1
Media	1.3
Alta	1.8

V. CONCLUSIONES

El sistema de control de acceso que se implementó en la Hostal las Garzas es confiable, debido a que se trata de un sistema rápido que incorpora hardware de alta seguridad tanto para almacenar datos como para realizar funciones de cifrado.

Durante el diseño del Sistema, es primordial establecer estratégicamente la ubicación del servidor y planificar la capacidad de hardware del equipo. De una buena elección dependerá la eficiencia del proyecto para controlar al personal que labora en el lugar y así cumplir con el propósito de implementación.

IV. DESEMPEÑO GENERAL DEL SISTEMA

De las anteriores pruebas se puede indicar que todas las mediciones arrojaron valores muy satisfactorios.

En lo referente al tiempo de respuesta de la base de datos, se tienen mínimas variaciones debido a que el computador está trabajando libre (no existen aplicaciones de usuario abiertas).

En cuanto a los valores tomados en las pruebas de alcance existe una limitación debido a la sensibilidad y la clase de radio de los equipos.

Por otro lado, las pruebas de funcionamiento del sistema completo, indican que el dispositivo es seguro. Su implementación es recomendable.

Los elementos electrónicos que fueron utilizados en la implementación fueron los correctos ya que estos permitieron el buen funcionamiento del prototipo con ayuda de diagramas de bloques y de flujo. Se aplicaron los conocimientos adquiridos, especialmente los de seguridad de la información, redes inalámbricas, base de datos y programación.

Se analizaron las características que ofrecen las tecnologías

de identificación las cuales pudieron ser aplicadas a las comunicaciones inalámbricas en los sistemas microcontrolados.

De su análisis se concluye que, en su mayoría, se originan debido al uso inapropiado de los recursos del lugar por parte de los usuarios dando lugar a grandes pérdidas en la Hostal .

RECONOCIMIENTOS

Se expresa un especial reconocimiento a la Hostal las Garzas, en especial al Ing. Alejandro Pita por el apoyo y colaboración brindada para desarrollar este trabajo.

REFERENCIAS

[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.

Nació en Atuntaqui provincia de Imbabura el 19 de Febrero de 1983. Ingeniero en Electrónica y Telecomunicaciones, Escuela Politécnica Nacional en 2006. Actualmente es docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra-Ecuador, y cursa la Maestría en Redes de Comunicación (3do Semestre), Pontificia Universidad Católica del Ecuador, Quito-Ecuador.

Estefanía G. Torres A.

Nació en Ibarra-Ecuador el 14 de octubre de 1986. Hija de Edgar Torres y Graciela Aza. Realizó sus estudios primarios en la Escuela Particular “Fe y Alegría”. En el año 2004 obtuvo su título de Bachiller en Ciencias con especialización Físico Matemático en el Colegio “Nacional Ibarra”. Actualmente, es egresada de la Carrera de Ingeniería Electrónica y Redes de Comunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.