

## TÍTULO DEL INFORME TÉCNICO

REPORTE TÉCNICO SISTEMA DE  
REGISTRO DE ASISTENCIA POR  
MEDIO DE HUELLAS DACTILARES

### Reporte Final

**Área:** Ciencias de la Ingeniería

### Línea de generación y aplicación del conocimiento:

Estudios en Sistemas Digitales  
Instrumentación

### Autores del informe técnico:

MTRO. GABRIEL BRAVO MARTÍNEZ  
MTRO. FRANCISCO JAVIER ENRÍQUEZ AGUILERA  
DR. JESÚS MARTÍN SILVA ACEVES  
DR. RAFAEL ELIECER GONZALEZ LANDAETA  
MTRO. ARNULFO CASTRO VAZQUEZ

## REPORTE TÉCNICO SISTEMA DE REGISTRO DE ASISTENCIA POR MEDIO DE HUELLAS DACTILARES

### **Resumen del informe técnico:**

Hoy en día existen sistemas computacionales de reconocimientos de huellas dactilares, por otro lado, también estamos comenzando a ver cada vez más su uso en un rango mucho más amplio de situaciones cotidianas

Es un sistema desarrollado en base de datos, un microprocesador de tipo Arduino que está integrado por huellas biométricas del alumno. Vivimos en una sociedad en constante y acelerado cambio que nos exige el desarrollo de un compromiso social en nuestra comunidad, generando conciencia en nuestros alumnos para su incorporación a la sociedad. Las huellas dactilares son un medio confiable de identificación de personas; es por ello que el reconocimiento de huellas dactilares por medio de sistemas informáticos es el auxiliar para la confiabilidad y certeza de nuestros usuarios.

El proyecto contempla tres etapas: la primera se realizarán explicaciones y ejercicios sobre el tema de huella dactilar, sensores (tecnología en general). La segunda etapa contempla un registro previo en la herramienta llamado (Arduino) en el que se darán de alta las huellas dactilares de toda la comunidad educativa. La tercera etapa contempla un pequeño análisis para decidir donde es el lugar más adecuado para la implementación de nuestro sistema de registro de asistencia, y así poner en funcionamiento a nuestro sistema. También en esta etapa se pretende realizar una pequeña platica que haga conciencia sobre las tecnologías, uso y cuidado que requieren para un buen funcionamiento.

**Palabras clave:** biometría, huella dactilar, seguridad, reconocimiento.

**Justificación:**

El alto costo de los sensores especializados en el registro de asistencias a través del escáner de la huella biométrica, hacen que ocasionalmente se encuentren fuera del alcance de los campos de investigación, a diferencia del campo industrial, donde se encuentra con un nivel más económico y amplio. Sin embargo, las empresas se limitan solo a la utilización de los medios brindando por los investigadores del campo y no al desarrollo, contar con un software elaborado en LabVIEW que no solo beneficia en costo, sino además en tiempo y esfuerzo empleado para obtener los datos necesarios beneficiaria a las empresas o personas dedicadas a la investigación del tema.

## Índice de contenido

1. Introducción .....	4
2. Desarrollo .....	5
2.1 Obtención del registro de la base de datos .....	5
2.2 Inserción de la información y validación .....	6
2.3 Bases de datos .....	8
2.4 Almacenamiento y comparación de datos .....	9
3. Resultados .....	9
4. Discusión .....	9
5. Código en Arduino .....	11
5.1. Código implementado en IDE Arduino .....	11
6. Interfaz de usuario en LabVIEW .....	17
7. Programación de LabVIEW .....	21
8. Conclusiones .....	22
9. Referencias .....	22

## Índice de figuras

Figura 1. Interfaz de usuario primaria .....	6
Figura 2. Sensor de huellas biométricas .....	7
Figura 3. Interfaz del programa Arduino (software y hardware) .....	7
Figura 4. Tablilla de desarrollo con microcontrolador .....	7
Figura 5. Dispositivo hardware en funcionamiento (pruebas piloto) .....	8
Figura 6. Base de datos .....	8
Figura 7. Diagrama de metodología propuesta .....	9
Figura 8. Software utilizado para la creación de la base de datos encargada de almacenar la información .....	10
Figura 9. Registro de base de datos 1 (prueba) .....	10
Figura 10. Registro de base de datos 2 (prueba) .....	11
Figura 11. IDE de Arduino .....	12
Figura 12. Asignación de ID .....	15
Figura 13. Inicio de registro de huella .....	16
Figura 14. Segunda solicitud de huella para comparar .....	16
Figura 15. Resultado del registro de huella .....	17
Figura 16. Interfaz principal del usuario .....	18
Figura 17. Mensaje de asistencia y de bienvenida .....	18
Figura 18. Usuarios previamente registrados .....	19
Figura 19. Opción de registrar en la base de datos .....	19

Figura 20. Datos personales de la persona .....	20
Figura 21. Un caso particular .....	20
Figura 22. Base de datos con información del ejemplo .....	21
Figura 23. Código completo del programa en LabVIEW .....	21

## Introducción

La detección de huellas dactilares es un procesamiento digital de imágenes, como parte fundamental en la aplicación de registro de asistencia, ya que puede ser utilizada para proporcionar datos personales generales, tales como nombres, fecha de nacimiento, apellidos, lugar de nacimiento, estado civil, sexo, y estatura [1]. Se han desarrollado varios sistemas para la detección biométrica, se especula que son más de 40 rasgos los que se clasifican y analizan para la impresión dactilar para sentar una base de una identificación personal [2].

Una de las mayores desventajas es el uso de un dedo de silicona con la huella de una persona para tener acceso a dicha información por otro lado no se puede comprobar si el dedo está vivo para acceder [3]. Con este control de accesos que reconoce a usuarios admite o restringe la entrada, se conoce también quien ha accedido a las instalaciones, a qué hora lo ha hecho. El nivel de seguridad que ofrece es alto [4]. Este método está vigente y desarrollado desde 1883 por Juan Vucetch. Considerado un sistema fiable y el más desarrollado entre los sistemas biométricos.

Esta investigación toma como idea principal el resguardo de información y el acceso limitado dependiendo de la confiabilidad otorgada a cada uno de los usuarios [5].

Muchas empresas y organizaciones usan hoy en día identificación biométrica con el objeto de asegurar sus instalaciones o su información confidencial. Hay muchos tipos de escáneres biométricos.

Algunos de ellos escanean el iris, mientras otros escanean las huellas dactilares de los usuarios, la forma de sus manos e incluso la manera en que las personas escriben en un teclado. Aunque la identificación biométrica es más segura que los métodos tradicionales, tiene ciertas desventajas [6].

La identificación biométrica es una técnica que usa las características físicas y de comportamiento únicas de cada individuo, para identificarlo. Por ejemplo, cuando un dispositivo biométrico escanea las huellas dactilares y las compara con cada una de las huellas autorizadas en su base de datos, es la manera por la que un investigador puede comparar huellas dactilares.

Si las huellas escaneadas coinciden con un usuario autorizado, el dispositivo le concede el acceso a esa persona. Pero la identificación biométrica no está sólo limitada

a las características físicas. Algunos patrones de comportamiento, como el habla o la forma en que la persona escribe en el teclado, pueden ser también analizados [7].

Los dispositivos de identificación biométrica están instalados normalmente en puertas de lugares asegurados. Permiten al personal autorizado entrar a las instalaciones e impiden el acceso a los individuos no autorizados.

También hay otros usos de la identificación biométrica, algunas empresas usan la biometría para asegurar sus redes de computación, en tanto que algunas escuelas utilizan los escáneres de huellas dactilares para controlar la asistencia de los estudiantes [8].

Las máquinas de identificación biométrica son más costosas que las tradicionales. Además, algunos usuarios pueden rechazar la biometría en su conjunto, viéndola como una invasión de la privacidad.

Otra desventaja es que las máquinas de identificación biométrica no siempre son totalmente precisas, es probable que un individuo con un resfriado no pueda identificarse por un dispositivo de uso de la voz y la gente que aumenta o baja de peso puede, de repente, perder el acceso a un lugar protegido por un sistema de identificación de rasgos faciales [9].

## **2. Desarrollo**

En esta sección se presenta el sistema basado en el reconocimiento de huellas digitales mediante un sensor de identificación biométrica de la persona.

El cual funcionara registrando la asistencia de la comunidad educativa del plantel por otro lado el registro se llevará en una base de datos la cual almacenara el nombre y apellidos de quienes utilizaran el sistema. El sistema será utilizado en un plantel educativo por motivos de inseguridad a la hora de ingresar, otorgando una mayor seguridad en el plantel educativo y los alumnos

### **2.1 Obtención del registro de la base de datos.**

El primer paso es obtener la información personal de los usuarios, para esto es necesario contar una identificación oficial.



Después de obtener la información personal se realiza el llenado correspondiente en la base de datos de tal manera que el usuario estaría registrado dentro de la institución.

Posteriormente se pide apoye el dedo índice de la mano derecha para realizar el registro de la huella dactilar en el sistema de tal manera que la base de datos contenga almacenada la información vinculada con la huella del usuario [5].

Al finalizar todo este proceso el alumno deberá ingresar nuevamente el dedo previamente registrado para obtener una asistencia correcta, este proceso deberá ser llevado a cabo durante un máximo periodo de 2 días en los cuales el primer día serán los semestres de 1ero, 2do y 3ero, posteriormente en el día 2 serán los semestres 4tos, 5tos y 6tos.

En caso contrario de que el usuario no esté registrado, no podrá ser dado de alta y tampoco se llevara la asistencia correspondiente dispositivo para el registro de las huellas dactilares figura 1.

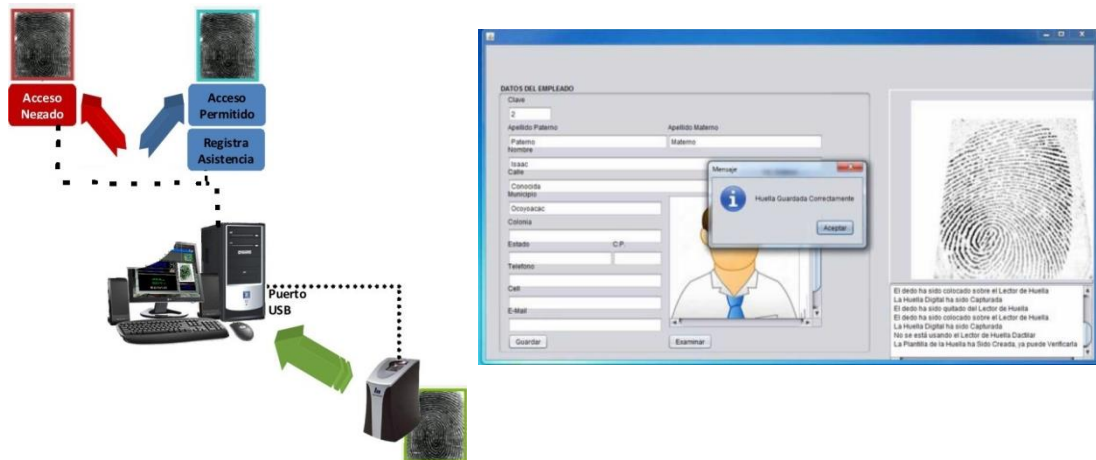


Figura 1. Interfaz de usuario primaria

## 2.2 Inserción de la información y validación

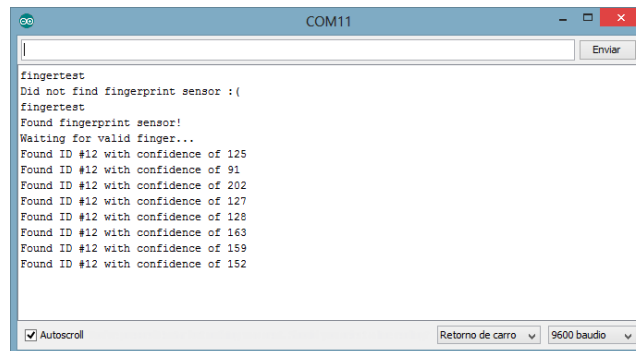
El siguiente paso después de realizar el llenado de la base de datos y realizar el registro de la huella dactilar es generar el registro ya que al ser un usuario nuevo no tendrá asistencia por lo cual deberá apoyar el dedo indicado en el scanner por segunda vez consecutiva.

Después de realizar por segunda vez el paso anterior el usuario ya tendrá un registro y una asistencia perteneciente al día al que fue registrado, en caso

contrario de no tener un registro previo en la base de datos y en el sensor se le deberá de asignar un id el cual es intransferible.

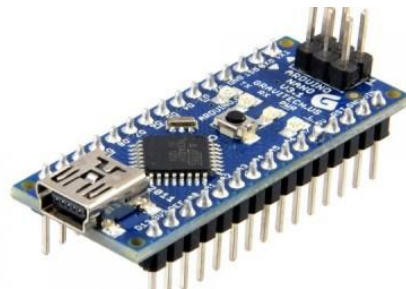


**Figura 2. Sensor de huellas biométricas**



**Figura 3. Interfaz del programa Arduino (software y hardware)**

Microprocesador Arduino nano. (ver Fig. 4) microcontrolador que controla el sensor y permite la conectividad entre el dispositivo y la computadora.

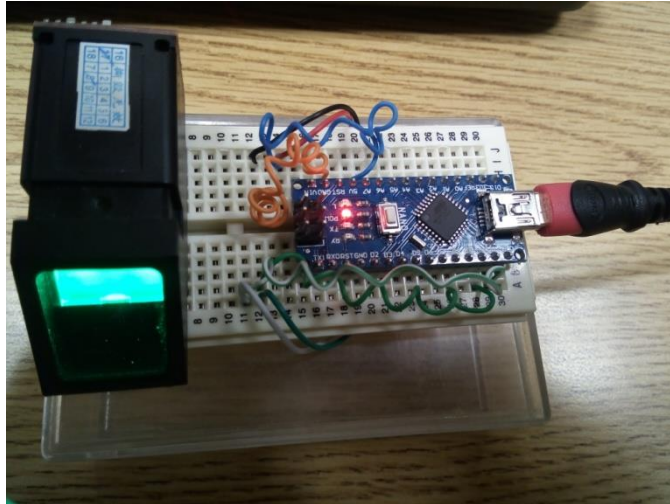


**Figura 4. Tablilla de desarrollo con microcontrolador**

### 2.3 Bases de datos.

Se utiliza para almacenar o guardar información de forma organizada para que después pueda ser utilizada fácilmente.

Algunas características son:



**Figura 5. Dispositivo hardware en funcionamiento (pruebas piloto)**

- Independencia lógica y física de los datos.
- Redundancia mínima.
- Acceso concurrente por parte de múltiples usuarios.
- Integridad de los datos.
- Consultas complejas optimizadas.
- Seguridad de acceso y auditoría.
- Respaldo y recuperación.
- Acceso a través de lenguajes de programación estándar.

La base de datos la cual se encarga de almacenar y mostrar los datos solicitados se muestra en la figura 6.



**Figura 6. Base de datos**

## 2.4 Almacenamiento y comparación de datos

Si se cumplen las condiciones que pide el sistema podrá ser registrado en la tabla de asistencia, así como en la tabla de alumnos. En la figura 7 se muestra el diagrama de metodología propuesta.

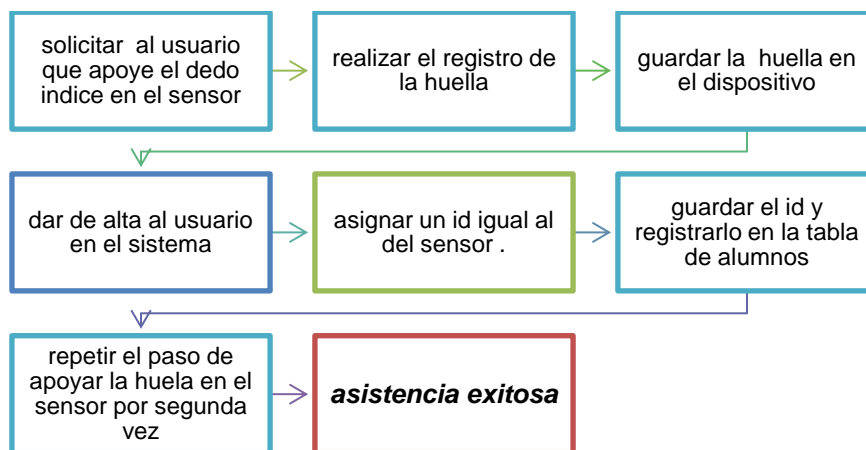


Fig. 7. Diagrama de metodología propuesta.

## 3. Resultados

Para probar el sistema propuesto se utilizarán aproximadamente 10 huellas dactilares, en las que cada una de las huellas va a contener datos reales. Todos los registros se realizaron en una computadora portátil con procesador de 1.6. GHz

El primer registro consistió en dar de alta los 5 dedos de la mano izquierda tanto como en el sensor como en el sistema y la base de datos.

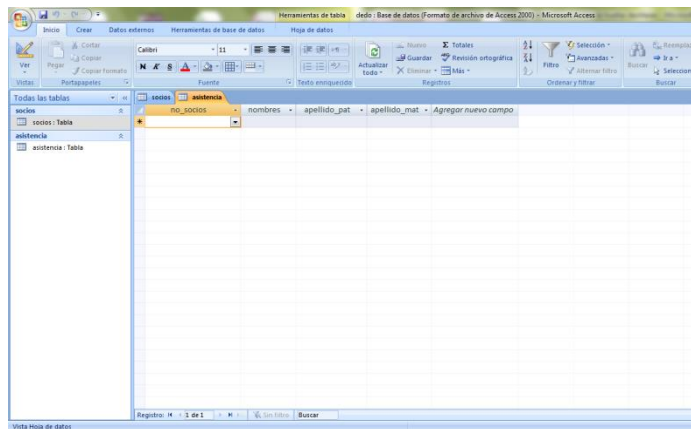
## 4. Discusión

En esta sección se analiza la forma de realización haciendo una comparación con algunos gestores de bases de datos, programas para interfaces graficas etc. [9].

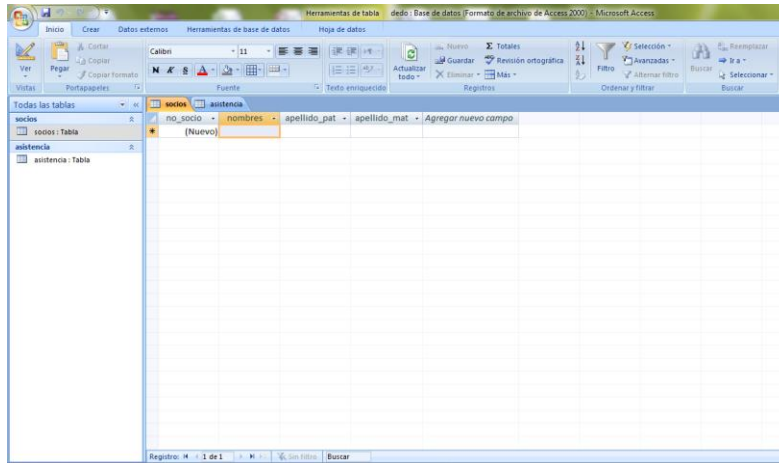
Existen otros gestores de bases de datos que ayudan a realizar de una manera más profesional una base de datos, pero la complejidad de esos sistemas requiere un poco más de conocimiento a la hora de utilizarlos. Por otro lado, el software de ambiente grafico son un poco más complejos y con un costo más alto a comparación del software utilizado en este proyecto. En la figura 8 se muestra el logo del software utilizado.



**Figura 8. Software utilizado para la creación de la base de datos encargada de almacenar la información.**



**Figura 9. Registro de base de datos 1 (prueba)**



**Figura 10. Registro de base de datos 2 (prueba)**

Para obtener un buen funcionamiento de la base de datos es recomendable tener un orden a la hora de diseñar las tablas que contendrán la información sobre nuestro sistema.

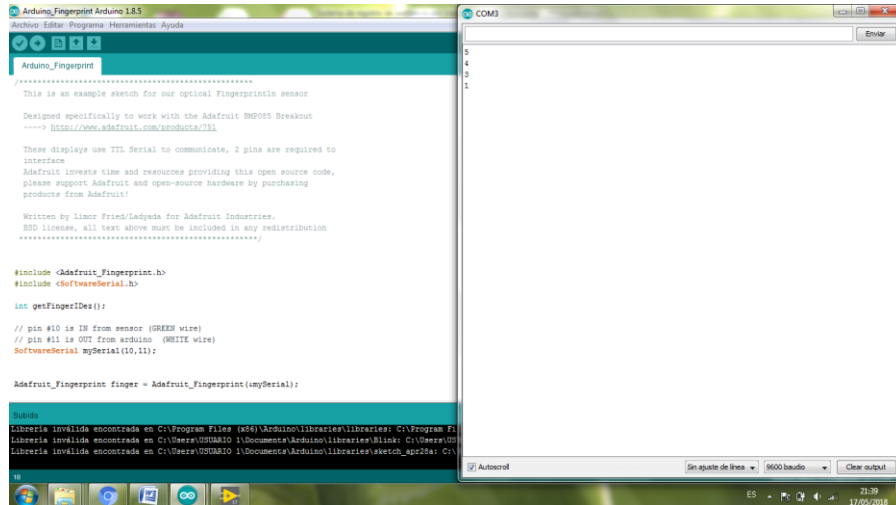
Otros puntos que juegan un papel importante a la hora de realizar un trabajo con las herramientas propuestas es tener conocimiento de un lenguaje de programación en ambiente grafico como labview y por otro lado conocimientos en c++, de lo contrario se podría llegar a obtener resultados no favorables o datos no necesarios generando un mal funcionamiento de todo el sistema.

## 5. Código implementado en Arduino

Esta parte del código es el encargado de mostrar los id de las huellas que han sido registradas. Estas podrán ser ingresadas en la base de datos para otorgar el registro y acreditar la asistencia.

El código proporcionado en esta parte es el encargado de mostrar la información previamente almacenada

El código está en implementado en C++



**Figura 11. IDE de Arduino**

```

#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>

int getFingerIDez();

// pin #10 is IN from sensor (GREEN wire)
// pin #11 is OUT from arduino (WHITE wire)
SoftwareSerial mySerial(10,11);

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

void setup()
{
  Serial.begin(9600);
  // Serial.println("fingertest");

  // set the data rate for the sensor serial port
  finger.begin(57600);

  if (!finger.verifyPassword())
  while (1)
  {

```

```

Serial.println("@");
delay(2000);

}
//Serial.println("Waiting for valid finger...");
}

void loop()          // run over and over again
{
  getFingerprintIDez();
  delay(50);        //don't ned to run this at full speed.
}

uint8_t getFingerprintID() {
  uint8_t p = finger.getImage();
  switch (p) {
    case FINGERPRINT_OK:
      //Serial.println("Image taken");
      break;
    case FINGERPRINT_NOFINGER:
      Serial.println("A");
      return p;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("C");
      return p;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("D");
      return p;
    default:
      Serial.println("E");
      return p;
  }

  // OK success!

  p = finger.image2Tz();
  switch (p) {

```



```

case FINGERPRINT_OK:
    //Serial.println("Image converted");
    break;
case FINGERPRINT_IMAGEMESS:
    Serial.println("D");
    return p;
case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("C");
    return p;
case FINGERPRINT_FEATUREFAIL:
    Serial.println("C");
    return p;
case FINGERPRINT_INVALIDIMAGE:
    Serial.println("C");
    return p;
default:
    Serial.println("E");
    return p;
}

// OK converted!
p = finger.fingerFastSearch();
if (p == FINGERPRINT_OK) {
    //Serial.println("Found a print match!");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("C");
    return p;
} else if (p == FINGERPRINT_NOTFOUND) {
    Serial.println("C");
    return p;
} else {
    Serial.println("E");
    return p;
}

// found a match!
/* Serial.print("Found ID #"); Serial.print(finger.fingerID);

```

```

/* Serial.print(" with confidence of ");Serial.println(finger.confidence); */
}

// returns -1 if failed, otherwise returns ID #
int getFingerprintIDez() {
  uint8_t p = finger.getImage();
  if (p != FINGERPRINT_OK) return -1;

  p = finger.image2Tz();
  if (p != FINGERPRINT_OK) return -1;

  p = finger.fingerFastSearch();
  if (p != FINGERPRINT_OK) return -1;

  // found a match!
  /*Serial.print("Found ID #");*/ Serial.println(finger.fingerID);
  /*Serial.print(" with confidence of "); Serial.println(finger.confidence);*/
  // return finger.fingerID;
}

```

## 5.1 Código implementado en IDE Arduino

Esta parte del código es el encargado de registrar con un id las huellas nuevas las cuales será registrada en la base de datos.

En la figura 12 del código se muestra cómo se pide asignes un id para después apoyar el dedo en el lector y así almacenar la huella con el id.

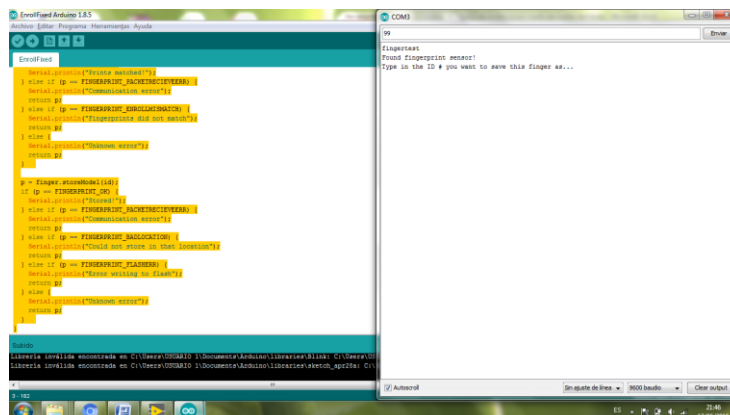


Figura 12. Asignación de ID

En la figura 13 se muestra el código inicial pidiendo que apoyes el dedo en el lector para poder comenzar con la digitalización de la huella.

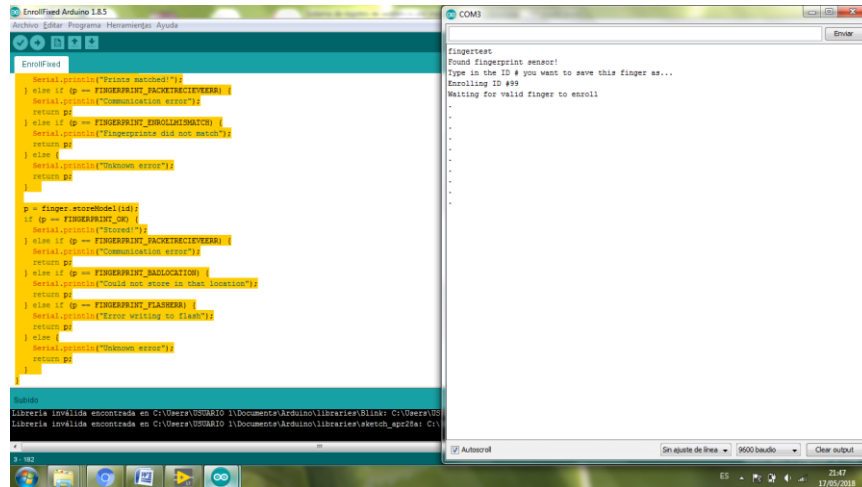


Figura 13. Inicio de registro de huella

En la figura 14 del código después de que ingresaste por primera vez el dedo en el lector de huellas pide que retires el dedo para luego pedirlo una vez más y así realizar un segundo escáner de huella proporcionando una comparación.

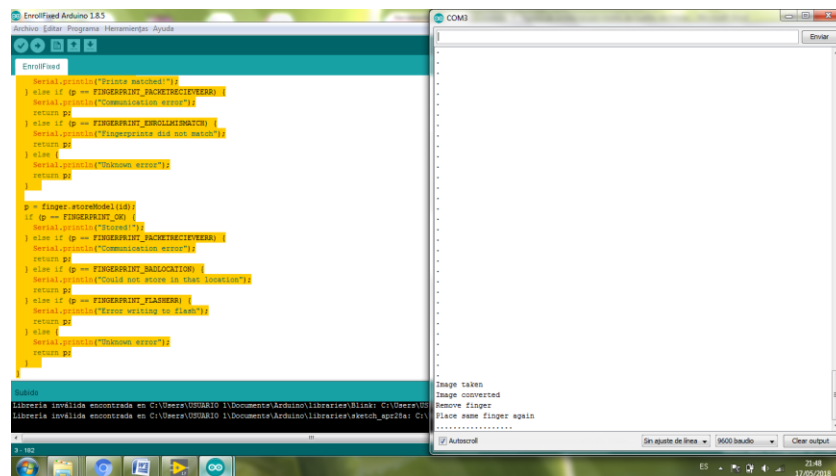
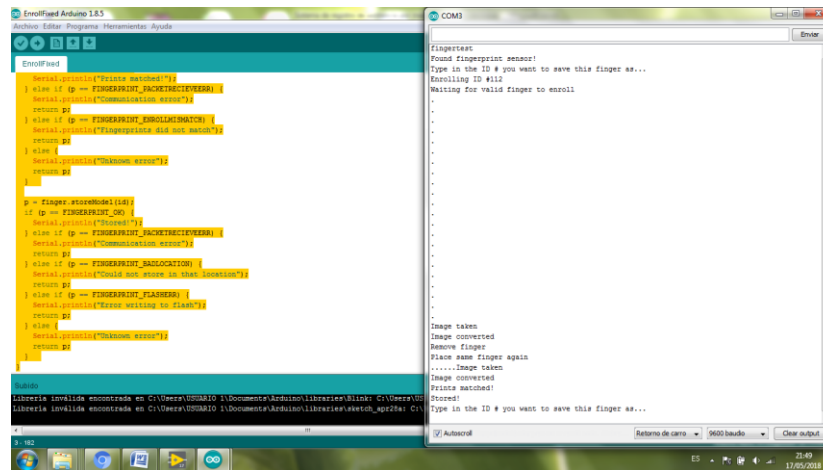


Figura 14. Segunda solicitud de huella para comparar

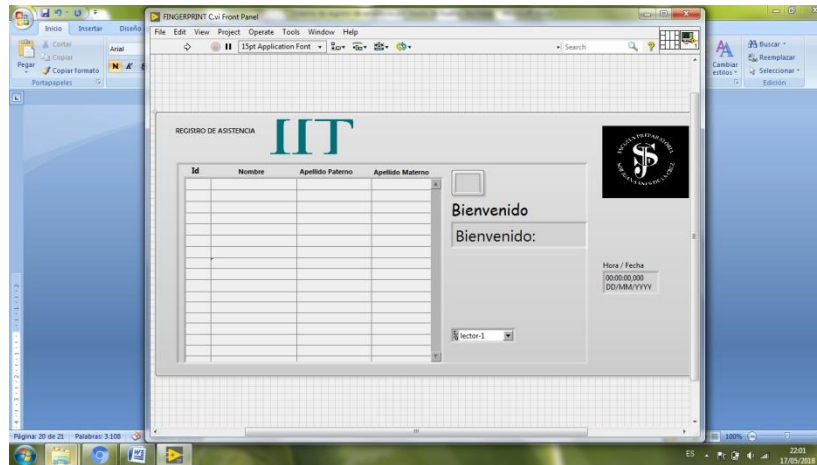
En la figura 15 del código se muestra que después de ingresar la por segunda vez el dedo en el lector realiza la comparación y muestra un mensaje indicando si la huella es igual o no, en caso de ser igual pedirá que se ingrese una nueva huella en el lector biométrico de ser necesario se tendrá que repetir una vez más el proceso de registro de huella biométrica.



**Figura 15. Resultado del registro de huella**

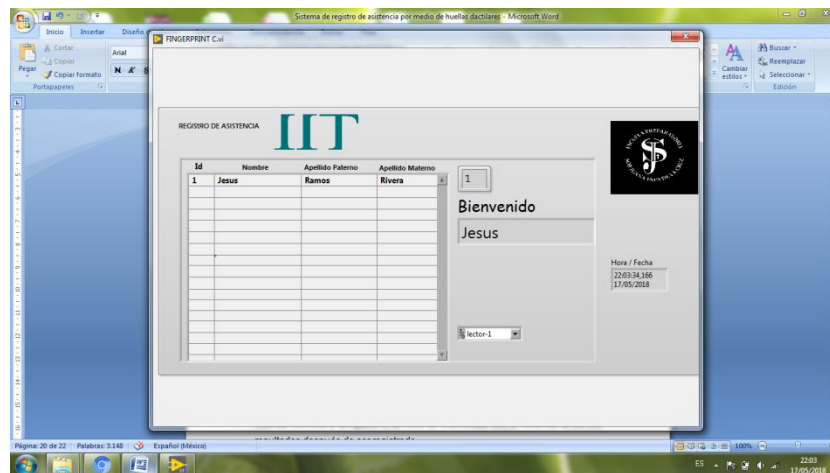
## 6. Interfaz de usuario en LabVIEW

En la figura 16 mostramos la interfaz principal que el usuario utilizara la interfaz está desarrollada en LabVIEW la cual muestra únicamente los campos de id, nombre, apellido paterno, apellido materno, el número de registro, fecha y el mensaje de bienvenido.



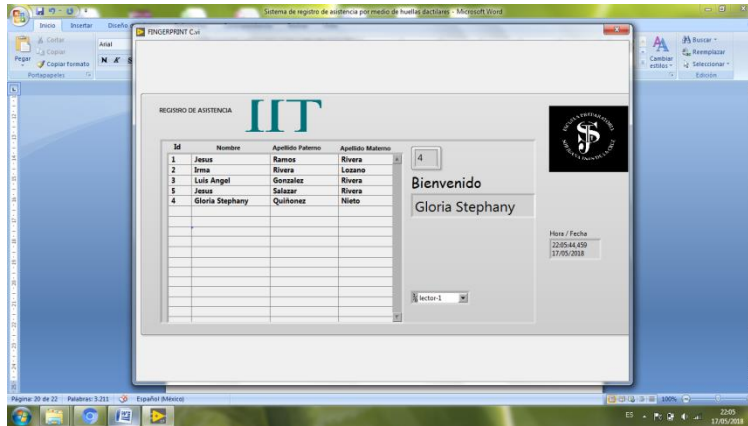
**Figura 16. Interfaz principal del usuario**

En la figura 17 se muestra la asistencia y el mensaje de bienvenida, eso se muestra ya que el usuario con el id 1 ya estaba registrado previamente en el programa de Arduino y registrado en la base de datos, de tal manera que proporciona una asistencia al usuario, muestra la hora y fecha en la que el usuario ingreso la asistencia.



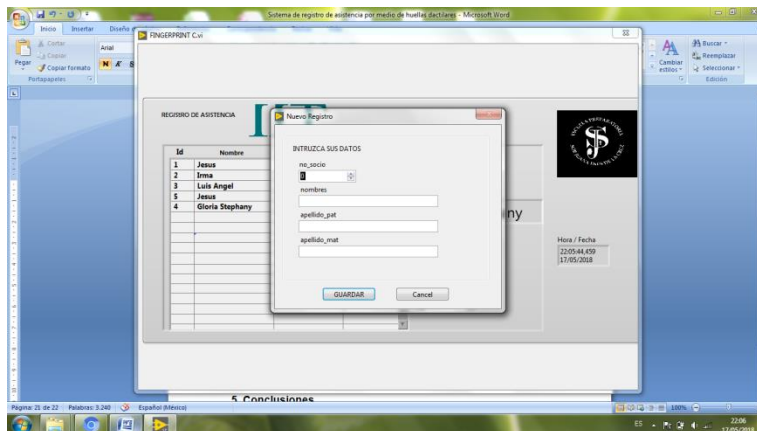
**Figura 17. Mensaje de asistencia y de bienvenida**

En la figura 18 se muestra la asistencia de los usuarios que fueron previamente registrados en la base de datos y en el programa de Arduino otorgando una bienvenida.



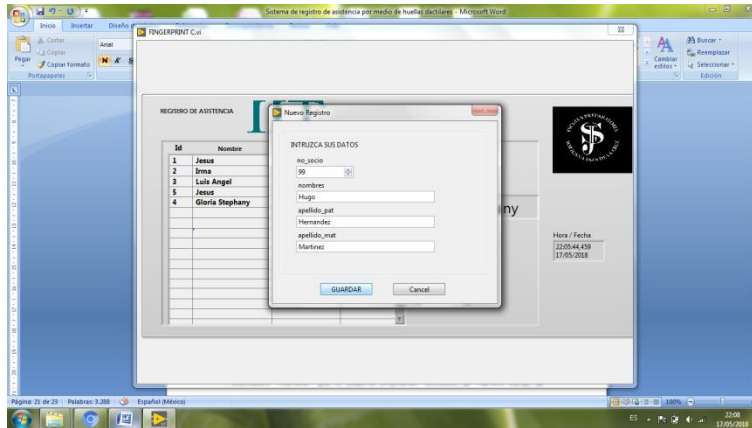
**Figura 18. Usuarios previamente registrados**

En la figura 19 se muestra la opción de registrar en la base de datos, puesto que si está registrado el id en el programa de Arduino, pero no en la base de datos, por consiguiente, se debe realizar un registro y dar de alta al usuario.



**Figura 19. Opción de registrar en la base de datos**

En la figura 20 ventana se hace el llenado correspondiente de los datos personales de la persona para después dar en "GUARDAR" al hacer eso el sistema automáticamente guardara la información en la base de datos.



**Figura 20. Datos personales de la persona**

En la ventana mostrada en la figura 21 observamos que después de dar de alta y registra al usuario tendremos que ingresar una vez más la huella para finalizar el registro del nuevo usuario, en la venta se muestra que una vez que se realizó el procedimiento antes mencionado se manda un mensaje de dando la bienvenida al nuevo usuario llamado “Hugo”.



**Figura 21. Un caso particular**

En la figura 22 se muestra que los usuarios registrados anteriormente fueron almacenados en la base de datos correctamente.

no_socio	nombres	apellido_pat	apellido_mat
1	Jesús	Ramos	Rivera
2	Irma	Rivera	Lozano
3	Luis Angel	Gonzalez	Rivera
4	Gloria Stepha	Quiñonez	Nieto
5	Josue	Salazar	Rivera
9	pedro	omar	alvarez
20	Irma	Rivera	Lozano
99	Hugo	Hernandez	Martinez
132	Hugo	Hernandez	Martinez
(Nuevo)			

Figura 22. Base de datos con información del ejemplo

## 7. Programación de LabVIEW

La programación de la computadora que trabaja como estación de control se realizó en LabVIEW, un lenguaje de programación visual. En la figura 23 se muestra el código completo del programa en LabVIEW.

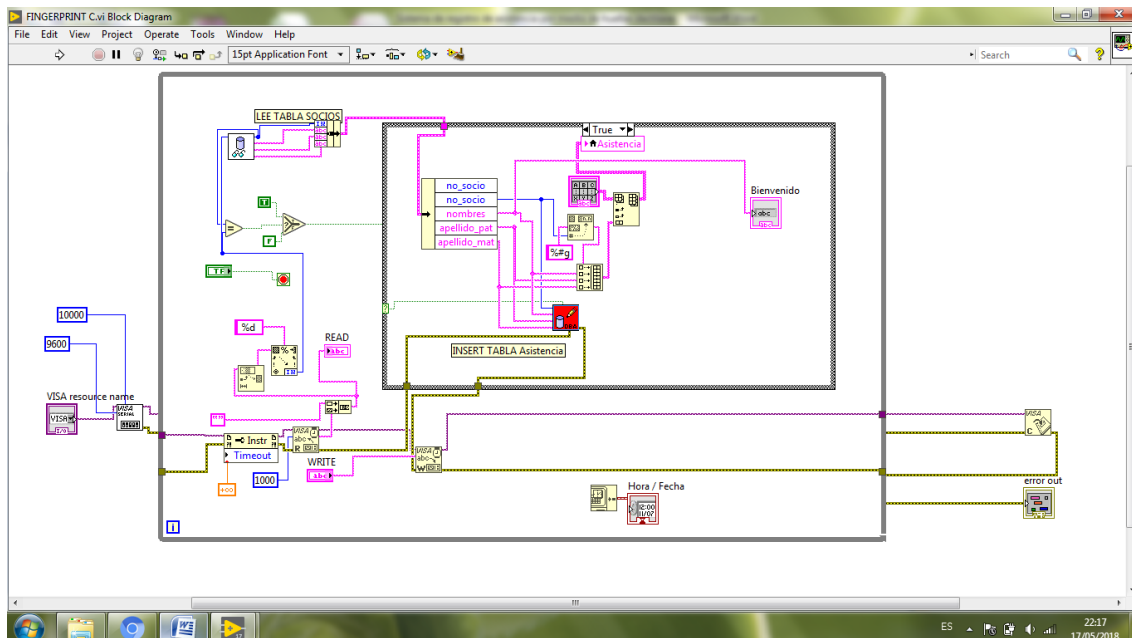


Figura 23. Código completo del programa en LabVIEW



## 8. Conclusiones

En este trabajo se presentó una forma funcional basando en la recopilación de huellas dactilares y bases de datos dentro de un ambiente laboral. los resultados muestran que el sistema propuesto funciona de manera eficaz de manera que cumple con los requerimientos de la organización al tener una interfaz sencilla y amigable a la hora de interactuar con el sistema, al ver los resultados después de ser registrado.

Las funciones que puede tener este sistema pueden ser para la industria y escuelas, ya que el desarrollo de este implica en la creación únicamente de nuevas tablas con información exclusiva para lo que será utilizado.

## 9. Referencias

- [1] Hong, L., Wan, Y., & Jain, A. (1998). Fingerprint image enhancement: Algorithm and performance evaluation. *IEEE transactions on pattern analysis and machine intelligence*, 20(8), 777-789.
- [2] Gaensslen, R. E., Ramotowski, R., & Lee, H. C. (2001). *Advances in fingerprint technology*. CRC press.
- [3] Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). Filterbank-based fingerprint matching. *IEEE transactions on Image Processing*, 9(5), 846-859.
- [4] Hong, L. (1998). *Automatic personal identification using fingerprints*. Michigan State University.
- [5] COLE, Simon A. More than zero: Accounting for error in latent fingerprint identification. *J. Crim. I. & Criminology*, 2004, vol. 95, p. 985.
- [6] Bonder, R., & Fisher Jr, A. J. (2000). *U.S. Patent No. 6,078,265*. Washington, DC: U.S. Patent and Trademark Office.
- [7] DEXTER, L. Meadows II; POURATIAN, Allen J. *Automated fingerprint identification system*. U.S. Patent No 5,869,822, 9 Feb. 1999.

**[8]** Igaki, S., Shinzaki, T., Yamagishi, F., Ikeda, H., & Yahagi, H. (1992). *U.S. Patent No. 5,109,428*. Washington, DC: U.S. Patent and Trademark Office.

**[9]** Baum, T. J., Gresshoff, P. M., Lewis, S. A., & Dean, R. A. (1994). Characterization and phylogenetic analysis of four root-knot nematode species using DNA amplification fingerprinting and automated polyacrylamide gel electrophoresis. *MOLECULAR PLANT MICROBE INTERACTIONS*, 7, 39-39.

**[10]** Sánchez Ávila, C. (2012). Aplicaciones de la biometría en seguridad.