CENTRO UNIVERSITARIO TECNOLÓGICO

CEUTEC

FACULTAD DE INGENIERÍA Y ARQUITECTURA

PROYECTO DE GRADUACIÓN O PRÁCTICA PROFESIONAL

DISEÑO Y MONTAJE DE UNA CERRADURA ELECTRÓNICA CON SENSOR DE HUELLA AS608

SUSTENTADO POR

VICTORIA ALEJANDRA MARTÍNEZ ELVIR, 318111114

PREVIA INVESTIDURA AL TITULO DE LICENCIATURA EN NOMBRE DE LA CARRERA INGENIERÍA EN ELECTRÓNICA

TEGUCIGALPA M. D. C HONDURAS, C.A.

ENERO, 2023

DEDICATORIA

El presente proyecto de graduación es un fruto de mi esfuerzo y perseverancia. La dedico principalmente a mis padres que me han apoyado incondicionalmente a lo largo de mi carrera universitaria, así como también a mis familiares que me motivan a ser una mejor persona.

Victoria Alejandra Martínez Elvir

AGRADECIMIENTOS

Agradezco a mis padres por siempre brindarme su apoyo en todo momento de mi vida, a mis hermanos que me alientan para salir adelante y me motivan para continuar formándome como profesional, a mis compañeros por apoyarme desde los inicios de mi carrera y fueron una pieza clave para lograr culminar este proyecto. También agradezco a mi novio por siempre estar para mí apoyándome en los momentos más difíciles, motivarme cada día para seguir y poder terminar mi carrera.

Victoria Alejandra Martínez Elvir

RESUMEN EJECUTIVO

Para esta investigación se realizó un diseño y montaje de una cerradura electrónica con sensor de huella para su futura implementación en el entorno industrial o residencial. Se está trabajando con el sensor de huella AS608 que funciona captando una imagen de las huellas dactilares de las personas para luego compararlas con cada una de las huellas que existen en su base de datos y poder permitir o denegar el paso. El uso de la biometría en conjunto con la tecnología hace que se desarrollen grandes proyectos como este para agilizar los procesos. Para la comunicación del sensor de huella junto con los demás elementos del proyecto se utilizó un Arduino IDE (software de programación lógica) en el cual se da instrucciones para el correcto funcionamiento del circuito. Con el Arduino y el sensor de huella se logró enrolar una cantidad de huellas para realizar las pruebas necesarias al circuito y corroborar que tenga un funcionamiento adecuado. El periodo de pruebas consta de dos diferentes métodos al que se sometió la cerradura, uno donde se enrola una sola huella digital para probar los aciertos del sensor, y otra prueba donde se enrolaron 10 huellas digitales diferentes y se hizo 5 intentos con las huellas de manera al azar para ver el comportamiento del sensor ante una mayor cantidad de huellas y poder sacar un porcentaje en relación a la cantidad de fallos de este. También para esta investigación se realizó una comparación de costos del prototipo con otras cerraduras de diferentes marcas donde se tomó en cuenta que este proyecto es solo un prototipo y para saber su valor final es necesario agregar una carcasa que protejan el circuito junto con todos sus elementos, así como también cambiarle el microcontrolador a uno de tamaño más pequeño y el picaporte por uno magnético como usualmente se usan en las cerraduras que existen en el mercado. Este proyecto está abierto para futuras investigaciones donde se le puede agregar más elementos que sean necesarios para el control del acceso de los individuos como ser un módulo wifi u otro tipo componente de rasgo biométrico para realizar sistemas híbridos.

Palabras clave: biometría, sensor de huella, microcontrolador, aciertos, cantidad de fallos.

ABSTRACT

For this research, a design and assembly of an electronic lock with fingerprint sensor for its future implementation in the industrial or residential environment was carried out. It will be working with the AS608 fingerprint sensor that works by capturing an image of the fingerprints of people and then compare them with each of the fingerprints that exist in its database and to allow or deny the entry. The use of biometrics together with technology makes great projects like this one to streamline processes. For the communication of the fingerprint sensor along with the other elements of the project an Arduino IDE (logic programming software) was used in which instructions are given for the correct operation of the circuit. With the Arduino and the fingerprint sensor it was possible to enroll a number of fingerprints to perform the necessary tests to the circuit and verify that it has a proper functioning. The testing period consists of two different methods to which the lock was subjected, one where a single fingerprint is enrolled to test the sensor hits, and another test where 10 different fingerprints were enrolled and 20 attempts were made with the fingerprints randomly to see the behavior of the sensor to a greater number of prints and to get a percentage in relation to the number of failures of this. Also for this research a cost comparison of the prototype with other locks of different brands was made where it was taken into account that this project is only a prototype and to know its final value it is necessary to add a case to protect the circuit along with all its elements, as well as changing the microcontroller to a smaller size and the latch for a magnetic one as usually used in the locks that exist in the market. This project is open for future research where we can add more elements that are necessary to control the access of individuals such as a wifi module or other type of biometric feature component to make hybrid systems.

Keywords: biometrics, fingerprint sensor, microcontroller, successes, number of failures.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

Arduino IDE: software de desarrollo para realizar la lógica programable a circuitos que requieran de su uso.

Biometría: ciencia que estudia las características distintivas del cuerpo humano para el reconocimiento de las personas.

BJT (Transistor de Unión Bipolar): es un dispositivo electrónico de estado sólido consistente en dos uniones PN muy cercanas entre sí, que permite aumentar la corriente y disminuir el voltaje, además de controlar el paso de la corriente a través de sus terminales.

C++: lenguaje de programación que permite la manipulación de objetos.

FTIR (Infrarrojo Transformado de Fourier): es una técnica de análisis espectroscópica que utiliza una parte del espectro electromagnético. (FOSS, s.f.)

Identificación: es la aplicación de la biometría con el uso de diferentes herramientas tecnológicas para determinar factores distintivos en las personas y reconocerlas.

Picaporte: es un componente utilizado para permitir o denegar el paso en un sitio, también es conocido como cerrojo.

Rasgos biométricos: son diferentes características que tiene el ser humano con patrones distintivos que se pueden utilizar para la identificación de personas.

Sensor de huella: es un dispositivo electrónico que es utilizado para identificar huellas dactilares por medio de diferentes procesos dependiendo del tipo de sensor.

UPS (Uninterruptible Power Supply): también llamado Sistema de Alimentación Ininterrumpida (SAI), es un sistema que provee energía eléctrica de respaldo temporal a equipos de aplicación crítica ante eventos de falla en el suministro eléctrico principal.

Verificación: proceso donde se comprueba la autenticidad de una cosa, en este caso de las huellas digitales que correspondan a la persona que está ingresando al lugar.

VingCard: “es una resistente cerradura (RFID) especialmente desarrollada para actualizar instalaciones con cerradura de llave metálica a la plataforma de hardware de cerraduras (RFID) más reciente lo que permite que no sea necesario de perforar la puerta” (Arboleda, s.f.).

I. INTRODUCCIÓN

En el presente informe se habla sobre la importancia del uso de las cerraduras electrónicas, su funcionamiento, la eficiencia y su rentabilidad en la industria. Se sabe que en gran parte de las industrias son muy utilizadas para el ingreso a oficinas, salas de trabajo, espacios que requieran de mucha seguridad, etc. Actualmente los sistemas que utilizan los rasgos biométricos se están utilizando mucho por lo que se debe estar en constante aprendizaje sobre ellos para poderles dar una buena aplicación como lo es en este proyecto. Se hará un prototipo físico de la cerradura electrónica para comprobar que el sensor de huella capta solo las huellas establecidas en la programación correspondiente en el microcontrolador y verificar la seguridad que este tiene. Es de gran importancia hablar de la evolución de las cerraduras electrónicas, cómo cambian con respecto al tiempo y los diferentes tipos que existen, así como su aplicación.

También es importante mencionar el tema de rentabilidad, costos de producción, presupuesto con respecto a los materiales utilizados del producto final ya que es un aspecto que se considera mucho al momento de su implementación.

II. PLANTEAMIENTO DEL PROBLEMA

2.1 Antecedentes

La cerradura es un elemento que funciona para abrir o cerrar diferentes elementos como ser una puerta, un gabinete, un portón, una caja fuerte, entre otros, con la ayuda de una llave, un movimiento mecánico, un software, una huella o una secuencia de dígitos.

Este invento se creó hace muchos años, aproximadamente 4000 años atrás en China, donde este invento consistía en distintas piezas que se accionaban haciendo un movimiento giratorio hacia un lado mediante una llave de madera, no muy diferente al que hoy en día conocemos. Fueron empleadas en Egipto y Babilonia donde construyeron diferentes tipos de cerradura incrementando las cuñas de madera o el material del que estaba fabricado, los romanos utilizaron el bronce con sus primeras cerraduras y las hacían de un tamaño más pequeño. Tiempo después los mismos romanos desarrollaron pernos, abrazaderas y llaves metálicas para construir una cerradura metálica y de ahí la invención de las cerraduras mecánicas que se ven en las casas actualmente que se abren con la ayuda de una llave. (Ingeniería.es, 2021)

Con el tiempo se fueron creando diferentes tipos de cerraduras hasta llegar a las cerraduras electrónicas que funcionan a partir de diferentes componentes electrónicos. En la actualidad se tienen cerraduras accionadas por sensores de huella, entrada de dígitos, con módulos de bluetooth para abrirlas con el celular, reconocimiento de iris y, las más comunes, las cerraduras mecánicas.

El sensor de huella es un elemento electrónico que tiene como función leer los patrones característicos de las huellas dactilares, es decir los patrones formados en los dedos para reconocer una persona. El uso de las huellas dactilares data de hace años, sin embargo, en 1901 se comienzan a utilizar para la identificación criminal en Inglaterra. Las primeras invenciones con lectores de huellas digitales son los celulares Toshiba en el 2007 con la función de desbloquear el celular de la misma manera que un lector de huella puede dar paso a la apertura de una cerradura. (Español, 2015)

2.2 Definición del problema

Todas las empresas necesitan de sistemas de cerraduras para restringir el acceso al interior de esta. En la actualidad existen muchos de estos sistemas y de varios tipos, estos existen hace muchos años, pero con el tiempo se van mejorando para trabajar de forma eficiente y siempre buscando la facilidad a las personas y brindando seguridad. En este caso el proyecto está orientado a desarrollar el diseño de un circuito que utilice la tecnología del sensor de huella para abrir una cerradura magnética y dar paso a las personas. La intención de la creación de este circuito es crear un sistema seguro, eficiente y de bajo costo

Se utiliza un sensor de huella porque según el estudio médico “Las huellas dactilares como herramienta esencial para la investigación criminal” (Rodas & Arreaga, 2018), se dice que las huellas digitales son únicas para cada persona por lo que muy difícilmente alguien podrá tener acceso a el área bloqueada. Junto con otros elementos el sensor de huella actuará para bloquear o permitir el paso de las personas a un área restringida, lo cual protege lo que hay dentro como información, objetos de valor e incluso el personal de la empresa.

El sensor de huella va a ser capaz de comparar la huella ingresada con las diferentes huellas que tiene enroladas para identificar a la persona y junto con los demás componentes permitir o denegar el acceso a la persona.

2.3 Preguntas de investigación

- ¿Cuál es el porcentaje de validaciones para una huella en específico?
- ¿Cuál es el rango de tolerancia para una huella en específico?
- ¿Cuál es el costo de fabricación de una cerradura electrónica con sensor de huella?
- ¿Cómo podemos hacer funcionar la cerradura electrónica cuando no hay flujo de energía?

2.4 Hipótesis

- H_1

La cerradura electrónica con sensor de huella propuesta en este informe es la más económica del mercado.

- H_2

La cerradura electrónica con sensor de huella presentada es funcional y logra mantener segura la entrada de personal.

- H_3

El porcentaje de aceptación de huellas en respuesta al sensor de huella es mayor a 90%.

Tabla 2.1 *Operacionalización de las Variables*

Variable	Definición Conceptual	Definición Operacional
Costo	El costo o coste es el gasto económico que representa la fabricación de un producto o la prestación de un servicio. (Definición.de, s.f.)	Precio final del prototipo donde se incluye cada uno de los componentes necesarios para llevar a cabo el proyecto.
Funcionamiento de sensor de huella	Lente óptico que se encarga de hacer la renderización de la imagen, cálculo, hallazgo de características y emparejamiento de una plantilla con una existente en la memoria. (Parra & Elías, 2018)	Con el lector del sensor de huella se compara la huella ingresada junto con las demás huellas enroladas en el programa.
Porcentaje de aceptación	Indicador que mide el porcentaje de tus alertas aceptadas del total de alertas en un determinado periodo de tiempo. (Beat, s.f.)	Porcentaje de aceptación de las huellas dactilares en el sensor de huella

En esta tabla se muestran las diferentes variables encontradas en las hipótesis con las que se trabajará en la investigación

2.5 Justificación

El presente proyecto se elabora con el fin de evaluar el porcentaje de aceptación de una cerradura electrónica que utiliza la tecnología del sensor de huella como elemento principal para su correcto funcionamiento.

Cada vez la biometría está siendo más utilizada para la identificación de personas. Existen diversos tipos que utilizan la biometría ya que utiliza características diferentes de las personas para realizar determinadas acciones y, a su vez, darle diferentes aplicaciones a los sistemas que contengan esta tecnología. Se sabe que la huella digital es un patrón único en cada persona, por lo que el diseño y montaje de este tipo de cerraduras es útil para controlar la entrada de personal a un sitio en específico ya que se considera a este elemento como un elemento de alta seguridad. Se busca que las características de esta cerradura sean funcional, eficiente y económica para que cumpla con los objetivos del proyecto.

III. OBJETIVOS

3.1 Objetivo General

Diseñar el circuito de una cerradura electrónica que incorpore el sensor de huella como elemento principal.

3.2 Objetivos Específicos

1. Construir un pequeño prototipo de la cerradura donde se pondrá a prueba su funcionamiento para analizar las características que tiene el proyecto.
2. Verificar su correcto funcionamiento en base al porcentaje de aceptación entre las huellas.
3. Demostrar que la cerradura electrónica con sensor de huella es un sistema eficiente y capaz de reconocer diferentes huellas para dar ingreso al individuo.

IV. MARCO TEÓRICO

4.1 La biometría

La biometría es una ciencia que analiza los patrones de las partes del cuerpo humano para lograr distinguir o identificar a cada ser humano. Es una herramienta muy utilizada en la criminología para identificar a los criminales. La biometría analiza diferentes rasgos que pueden ser utilizados en la actualidad para investigaciones médicas, desarrollo de aparatos eléctricos y electrónicos, investigaciones forenses, controlar accesos, etc. Entre algunos rasgos biométricos más conocidos se tiene la cara, la mano, el iris, la retina, la firma, la voz y las huellas dactilares. En la actualidad la biometría se está utilizando mucho por lo que es necesario conocer un poco sobre ella y cada una de las características que tienen los rasgos para identificar a un individuo. (Serratosa, 2015)

Los rasgos biométricos son patrones únicos en cada persona por lo cual no se pueden compartir, copiar o extraviar, pueden ser similares entre parientes, pero nunca serán exactamente iguales. Estos rasgos son los que identifican a cada individuo como un ser diferente y nos ayudan a reconocer a las personas entre tantos individuos que existen en el mundo.

Al combinar la tecnología con la biometría se pueden obtener resultados extraordinarios para el reconocimiento de personas y que se le puede dar aplicaciones muy efectivas para usos policiales, criminalística, en la industria para el control de acceso e inclusive para desarrollar nuevos dispositivos de reconocimiento con la ayuda de los rasgos biométricos.

4.1.1 Sistemas Biométricos

En la biometría existen dos tipos de sistemas para la identificación de personas, el sistema de identificación y el sistema de verificación. Los sistemas de identificación utilizan los rasgos biométricos para reconocer a una persona, en este sistema no se requiere de ningún tipo de identificación por parte del individuo para reconocerlo, existe un tipo de escaneo a la persona donde se analizan los rasgos biométricos y se comparan con otros existentes en una base de datos. Por otra parte, el sistema de verificación es para cerciorarse de la identificación de la persona, en este sistema el individuo proporciona una identificación y por medio de los rasgos

biométricos se asegura que si sea la misma persona que está en la identificación. A este sistema de verificación también se le puede llamas sistema de autentificación. (Serratosa, 2015)

Un sistema biométrico debe ser capaz de:

1. Obtener los datos biométricos necesarios para su reconocimiento.
2. Sacar la muestra de los datos dependiendo del tipo de rasgo que se tiene (Iris, retina, voz, huella digital, firma, mano, cara, etc.).
3. Hacer una comparación de la muestra con la base de datos que se tiene guardada.
4. Verificar que los datos correspondan entre la muestra y la base de datos.
5. Dar un resultado o hacer una función dependiendo del sistema que tengamos (Permitir un acceso, aceptación de datos, realizar una transacción, etc.).

4.1.2 Ventajas y desventajas de la biometría

La biometría tiene muchas ventajas de las cuales se les puede sacar provecho al momento de desarrollar nuevos sistemas en la industria, en este caso para el desarrollo de una cerradura electrónica que utiliza el rasgo biométrico de la huella dactilar para permitir o restringir el acceso a los individuos, pero al igual que todas las cosas también posee desventajas que las debemos tener presentes al momento de utilizar los sistemas que utilizan la biometría.

Tabla 4.1 *Ventajas y desventajas de la biometría.* ***(Navalpotro, 2014)***

Ventajas	Desventajas
Es segura debido a que no existe ningún tipo de contraseña que pueda ser copiada, olvidada, falsificada, o que necesite ser cambiada después de cierto tiempo.	Al ser un sistema digital se puede ver las bases de datos por lo que podrían ser hackeadas por otros usuarios.

Es cómoda ya que no se necesita tener a mano ningún objeto como llave, clave, tarjeta, etc., solo se necesita al ser humano para poder utilizarla.	Se puede ver violada la privacidad de las personas en algunos de los rasgos como ser el reconocimiento facial.
Es económica ya que no se necesita estar comprando cierta cantidad de llaves o tarjetas para cada uno de los empleados.	En ciertos rasgos el coste puede ser muy elevado dependiendo de los componentes y la tecnología que se utilice.
Tiene muchas aplicaciones y se puede combinar con diferentes sistemas.	Es posible que ocurran fallos al momento de la identificación y no se reconozca la persona.

En esta tabla se ven reflejadas las ventajas y desventajas que se encuentran en la biometría.

4.1.3 Los rasgos biométricos

4.1.3.1 La cara

También llamado reconocimiento facial, es uno de los rasgos biométricos más conocido debido a que es la parte del cuerpo que más se aprecia, con la cara podemos reconocer la edad y el género de la persona. También con las métricas faciales podemos reconocer las personas por la posición de los ojos, boca, nariz y orejas. Otro aspecto muy llamativo de las características de la cara son los gestos, las expresiones faciales y la sonrisa. Estos son los aspectos que se toman en cuenta al momento de hacer el reconocimiento de una persona con la cara. Algunos de los dispositivos que contienen la tecnología del reconocimiento de cara son los teléfonos con el Face ID, Face Station, las cámaras de seguridad que incluyen el reconocimiento facial, entre otros. (Suprema, s.f.)

Figura 4.1 *Dispositivo Face Station para reconocimiento facial.* ***(TECNOSeguro, s.f.)***

4.1.3.2 La mano

El primer dispositivo de reconocimiento con la mano fue creado en los años 70. Estados Unidos patentó el uso de este dispositivo para los bancos en 1985 y en 1996 fue utilizado en los Juegos Olímpicos para controlar el acceso de las personas. (Sites, s.f.)

La mano es otro rasgo biométrico con el que podemos reconocer a una persona por el tamaño, el grosor y largo de los dedos, la simetría de la mano y los dedos, y los patrones encontrados en la mano que son muy parecidos a las huellas dactilares solo que estas se encuentran en la palma de las manos. En la palma de las manos encontramos líneas en diferentes direcciones y un poco más marcadas por lo que hace más fácil el reconocimiento del individuo. Otro dato acerca de la biometría de las manos son las venas que pueden ser localizadas por medio de sensores o escáneres infrarrojos. (Serratosa, 2015)

Una desventaja que se encuentra en los sensores de reconocimiento de la mano es que son dispositivos más grandes debido a que la mano es un rasgo biométrico grande y ocupa más espacio por lo que este llega a ser un poco más costoso que uno de tamaño más pequeño.

Figura 4.2 *Dispositivo SCHLAGE para reconocimiento de la geometría de la mano.* ***(Amazon, s.f.)***

4.1.3.3 El iris

En el ojo se encuentra un órgano llamado iris, este se encuentra detrás de la córnea, este órgano es el que determina el color de ojos de cada persona y en el centro de este se encuentra la pupila. El iris es un rasgo biométrico distintivo en cada persona ya que es único al igual que las huellas dactilares. La toma para el reconocimiento del iris se hace mediante un mecanismo de escáner que ubica el iris, toma una foto, lo divide en bloque, lo codifica y lo analiza para hacer el proceso de reconocimiento. (Cruz & Athó, 2006)

Algunas de las ventajas que encontramos en este rasgo es que no se necesita ningún tipo de contacto para realizar el reconocimiento, se puede hacer el reconocimiento del iris aun cuando el individuo tiene objetos puestos como sombrero o lentes y se puede hacer el reconocimiento en la noche por medio del sensor infrarrojo que viene incorporado en los sistemas. Una desventaja que tiene este rasgo es que requiere una cámara especial para la lectura del iris y se necesita un acercamiento bastante próximo entre el ojo del individuo y el dispositivo.
(Serratosa, 2015)

Figura 4.3 *Dispositivo ANVIZ para el reconocimiento de iris.* ***(Kimaldi, s.f.)***

4.1.3.4 La retina

La retina son el conjunto de venas que se encuentran en el ojo. Si observamos bien nuestro ojo podemos ver que existe una especie de patrón y este al igual que el iris es diferente para cada persona, pero a diferencia del iris este si puede cambiar con el tiempo debido a alguna enfermedad que le dé a la persona. También para el escaneo de la retina se necesita luz para que haya mejor visibilidad de las venas del ojo o de la retina. El

reconocimiento de la retina posee ventajas muy parecidas a la del iris sin embargo como se menciona antes esta puede cambiar por lo que surge una desventaja para este reconocimiento y además de eso se puede decir que el reconocimiento de retina es invasivo debido a que a luz entra al ojo y puede ocasionar alguna especie de molestia en el individuo. (Faces, 2021)

Figura 4.4 *Dispositivo EyeLock para reconocimiento de retina.*

4.1.3.5 La firma

Este rasgo biométrico fue y es muy utilizado para documentos legales, transacciones, cartas, etc. Se sabe que existen personas que falsifican las firmas, pero eso solo ocurre ante la perspectiva del ojo ya que la forma de escribir de cada individuo es diferente y más la forma en la que escribe su nombre, sin embargo, este rasgo puede cambiar en diferentes ocasiones debido a las emociones y estado de ánimo de la persona. El reconocimiento de la firma tiene dos enfoques diferentes, uno llamado estático donde se analiza la firma en papel o escaneada solo mediante una toma o una perspectiva ocular y existe el enfoque dinámico que es en la que se analiza la firma en un dispositivo electrónico ya sea una tablet, celular, con lápiz electrónico, etc., en este enfoque se analiza la posición del lápiz, el ángulo y la presión. (Raúl & Judith, 2021)

Figura 4.5 *Módulo Evolis de reconocimiento de firma.* ***(LEDESMA, 2022)***

4.1.3.6 La voz

La voz es otro rasgo biométrico con el que podemos reconocer a una persona, ya sea por el timbre de su voz, u otro aspecto de esta. La voz también es un rasgo que puede presentar cambios debido a la salud de la persona ya que se sabe que existen enfermedades como ser la gripe o la amigdalitis, que tienen este efecto, incluso por emociones fuertes la voz puede cambiar por lo que el reconocimiento de voz es un rasgo no muy efectivo. También existen personas que son muy buenas haciendo imitaciones por lo que se debe tener cuidado al implementar un sistema por reconocimiento de voz, sin embargo, tiene la ventaja de que no se necesita de ningún objeto ni de tocar nada para poder hacer el proceso de reconocimiento. (Serratosa, 2015)

Figura 4.6 *Módulo de reconocimiento de voz.* ***(HETPRO, 2021)***

4.1.3.7 Las huellas dactilares

Su origen viene de la palabra dactiloscopia que es una ciencia que estudia las huellas dactilares y sus formas de reconocerlas, el término proviene del griego daktilo que significa dedo y skopein que significa examinar. Como hemos mencionado antes, las huellas dactilares son un rasgo biométrico muy utilizado y es catalogado como el mecanismo más seguro debido a que las huellas digitales son patrones encontrados en la yema de los dedos y estos son diferentes en cada dedo y en cada persona por lo que tiene un 99% de aceptación. Este rasgo es muy aceptado debido a que la huella dactilar no cambia, desde que nacemos hasta que morimos tenemos la misma huella y no hay nada que pueda alterar a esta. (Rojas & Suárez, 2018)

Figura 4.7 *Dispositivo HID para reconocimiento de huella.* ***(SIASA, 2011)***

Tabla 4.2 Escala de las características de los rasgos biométricos. (Serratosa, 2015)

Rasgo Biométrico	Característica						
	Universalidad	**Particularidad**	**Permanencia**	**Medible**	**Rendimiento**	**Aceptabilidad**	**No Falsificable**
Cara	Alta	Baja	Media	Alta	Baja	Alta	Alta
Mano	Media	Media	Media	Alta	Media	Media	Media
Iris	Alta	Alta	Alta	Media	Alta	Baja	Alta
Retina	Alta	Alta	Media	Baja	Alta	Baja	Alta
Firma	Baja	Baja	Baja	Alta	Baja	Alta	Baja
Voz	Media	Baja	Baja	Media	Baja	Alta	Baja
Huellas Dactilares	Media	Alta	Alta	Baja	Alta	Media	Media

En esta tabla se analizan los rasgos biométricos y el nivel de cada una de las características que posee.

4.2 La Huella Digital

La huella digital es uno de los métodos de identificación biométrica más antiguo, en sus inicios se sacaba su impresión por medio de arcilla u otro material donde se pudiese ver reflejada esta, hoy en día podemos ver que la huella digital se está usando en muchos dispositivos nuevos para el acceso, ya sea en teléfonos, lugares restringidos, para controlar el acceso de las personas, debido a que es una tecnología innovadora, de un precio bastante razonable y muy fácil de utilizar. Los sensores con los que se captan las huellas han evolucionado con respecto al tiempo y los sensores que existen hoy en día capturan la huella dactilar en alta resolución lo cual permite apreciar la huella mejor para hacer un reconocimiento efectivo. La desventaja del reconocimiento por medio de huella dactilar es que se necesita un acercamiento entre la persona y el dispositivo ya que el dedo debe tocar la superficie del sensor. (Chavarrea & Chiluisa, 2013)

4.2.1 Formas de la Huella Digital

La huella dactilar está conformada por un núcleo que es la parte central de la huella, las crestas que son protuberancias que tienen diferentes formas, las llamaremos líneas de la huella y las bifurcaciones y terminaciones de las crestas que son uniones o puntos de cierre ubicados en las líneas de la huella digital.

La huella dactilar posee muchas formas que son muy importantes para el reconocimiento de esta, entre ellas tenemos:

- Secante: Unión de dos líneas ubicadas en la huella en forma cruzada con un punto en común.
- Punto: pequeño fragmento circular de la huella digital.
- Desviada: Dos líneas de la huella que no se tocan, están ubicadas de forma paralela.
- Continua: Línea de la huella que no se corta ni toca ningún otro fragmento de huella.
- Transversal: Líneas que se atraviesan una por sobre la otra sin necesidad de un punto en común.

- Ensamble: Unión de dos líneas de la huella, pero en su inicio o su final se convierten en una sola línea.
- Vuelta: Línea de la huella con giro en U para cambiar la dirección de esta.
- Fragmento: Línea pequeña de la huella.
- Abrupta: Línea de la huella que se encuentra entre dos fragmentos
- Bifurcada: Línea de la huella que en cierto punto se divide en dos líneas de manera paralela.
- Unión: Es la combinación de dos o más líneas en la huella.
- Ojal: Unión de dos líneas de la huella en forma circular.
- Microforma: Es cualquier característica de las anteriores, pero poco visual, es decir, poco marcada.

4.2.2 Identificación por Huella Digital

Existen dos grupos con los cuales podemos identificar a un individuo por medio de las huellas dactilares, general y específica. Estos grupos se caracterizan por la forma en que los patrones de la huella digital están formados para poder tener una mejor vista y hacer más fácil el proceso de identificación.

a. Identificación general: es la que se enfoca en observar y analizar la huella completa siguiendo los patrones formados por las líneas de la huella, estas deben estar agrupadas en una sola forma. Hay 4 posibles agrupaciones de huellas para su identificación y estas son:

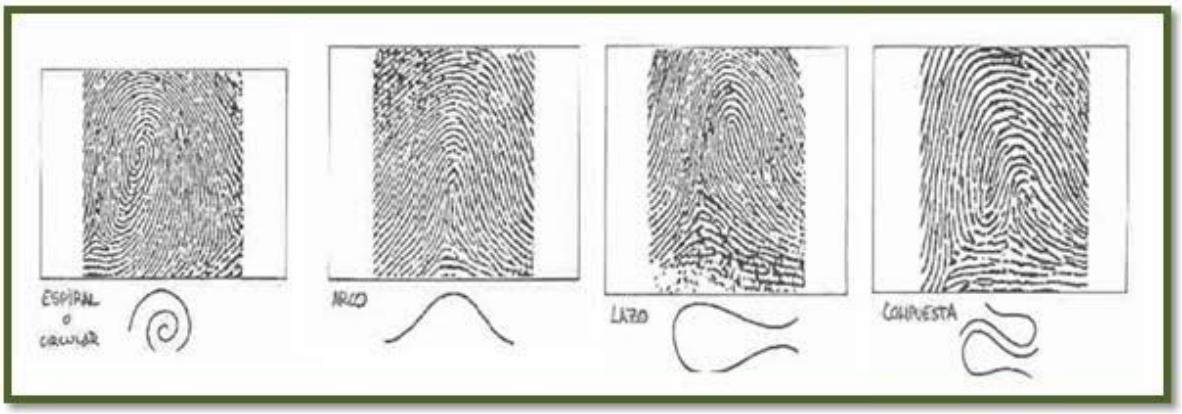


Figura 4.8 *Identificación general de la huella digital.*

b. Identificación específica: esta se enfoca en observar y analizar la huella digital de manera más cercana viendo cada uno de los fragmentos de línea que se encuentran en ella. De esta manera facilitar la identificación por medio de puntos en la huella muy distintivos.

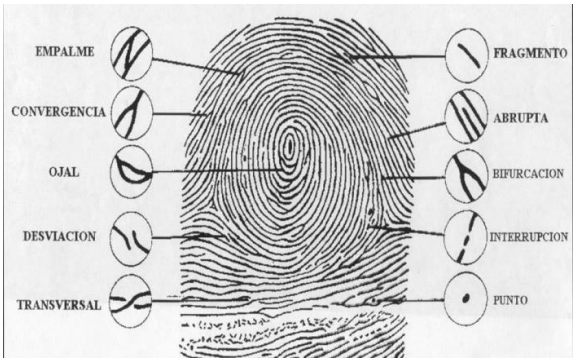


Figura 4.9 *Identificación específica de la huella digital.* ***(Forenses, 2017)***

4.2.3 Características de la huella digital

1. Todos los seres humanos las tienen con la singularidad de que son diferentes en cada individuo.
2. No cambian con respecto al tiempo a menos que se sufra de un accidente.
3. Se regeneran.
4. Son perennes, es decir, permaneces toda la vida desde que nacemos hasta que morimos.
5. Se pueden clasificar según su forma general.

4.2.4 Aplicaciones del uso de la huella digital

Una huella digital puede tener una gran cantidad de aplicaciones que el usuario le puede dar, sin embargo, se debe pensar en cómo se puede aplicar los sistemas con reconocimiento de huella digital. A continuación, se enlistan algunas aplicaciones que se le da a las huellas digitales:

1. Acceso a empresas en toda la industria (empresas, farmacias, bancos, universidades, escuelas, laboratorios, tiendas comerciales, etc.).
2. Transacciones bancarias.
3. Giros electrónicos.

4. Desbloqueo de equipo y funciones (dispositivos móviles y sus aplicaciones).
5. Aplicaciones residenciales.
6. Protección de equipo y objetos valiosos.
7. Identificación de víctimas de catástrofes.

Estos son algunos ejemplos de cómo podemos utilizar la huella digital hoy en día tomando en cuenta que son sistemas diferentes y para cada uno su uso es diferente. Está claro que estos sistemas necesitan de la huella digital para su funcionamiento por lo que se debe enrolar cada una de las huellas de las personas que pueden tener acceso a los sistemas antes mencionados.

4.2.5 Ventajas y desventajas de la huella digital

En este espacio se hablará sobre las ventajas y desventajas que tiene el uso de las huellas digitales en la industria según las aplicaciones y cómo estas nos facilitan al momento de utilizar los sistemas que contienen reconocimiento de huellas digitales.

Tabla 4.2 Ventajas y desventajas de la huella digital.

Ventajas	Desventajas
Lectura rápida de los datos biométricos.	La huella puede ser copiada si se tiene un proceso muy minucioso para evitar dañar la huella.
Aceptación del 99% por parte de las personas que ya han utilizado un sistema con reconocimiento de huella digitas. (Rojas & Suárez, 2018)	Inexactitud en el sistema debido a la suciedad que existe en el lente,
Fácil instalación y uso.	El uso de un sistema como este puede parecer que se quiere controlar a las personas.
Única para cada individuo y no cambia con el tiempo.	Si la huella no se enrola bien puede presentar fallos en el reconocimiento.

En la tabla anterior se enumeran las ventajas y desventajas que posee la huella digital.

Son muchas las ventajas que se pueden mencionar acerca del uso de las huellas dactilares y estas solo son una pequeña parte de ellas. Recordando un poco la huella digital data desde hace muchos años atrás y aún sigue siendo utilizada por lo que una de las más grandes ventajas es que es innovadora y se puede decir que en un futuro tendrá muchas aplicaciones más.

4.4 Seguridad en sistemas de cerraduras

La seguridad es un tema que se remonta desde los inicios del ser humano ya que antes las personas trataban de mantenerse a salvo de los animales, el clima y cualquier otra actividad que podía ocurrir en el mundo. Estos se protegían con diferentes materiales encontrados a su alrededor y desde ese entonces viene lo que es la seguridad, mantenerse a salvo uno mismo y sus pertenencias. Debido a estos eventos aparece lo que es la cerradura que se crea para evitar el robo de objetos o personas, saqueos a lugares y ataques. Tiempo atrás la cerradura que se podía utilizar eran pasadores de palos de madera, piedra y con el tiempo fueron evolucionando para hacerlos de metal hasta llegar a los que utilizamos hoy en día.

La seguridad es un elemento primordial en una empresa porque protege las personas que trabajan dentro de ella, toda la información que se maneja sobre clientes, proveedores, cuentas bancarias, etc. y todo el equipo que está dentro de la misma. Hoy en día las empresas buscan contar con una buena cerradura, que sea confiable y eficiente por lo que combinarlas con los sistemas biométricos es muy atractivo, cuenta con llaves diferentes para cada individuo debido a que son rasgos biométricos y son confiables debido a su gran funcionamiento.

4.3 La Cerradura

La cerradura es un elemento indispensable en todos los comercios, empresas, escuelas, universidades, etc. ya que ellas restringen o permiten el acceso a las personas. Las cerraduras han evolucionado con el tiempo y hoy en día existen muchos tipos de ellas y con nuevas tecnologías para hacer de ellas un sistema seguro, funcional y eficiente.

4.3.1 Tipos de Cerradura

En este apartado se enlistarán los diferentes tipos de cerradura que existen, cada una de ellas tiene una función diferente y depende de cada persona escoger la más adecuada para su

negocio. Las cerraduras se pueden dividir en dos grupos de los cuales este proyecto utiliza el principio de una para el funcionamiento de esta.

a. La cerradura tradicional: en estas cerraduras podemos encontrar sistemas que no necesitan de ningún tipo de electricidad para poder permitir o restringir el paso a una persona, sin embargo, necesitan de una llave o movimiento giratorio para poder abrirlas. Típicamente están formadas por piezas de metal, tornillos y pasadores que son los que permiten o no el paso. Una ventaja que tienen este tipo de cerraduras es que son de fácil instalación y fácil uso que incluso hasta un niño puede usarlas si tiene la llave necesaria para abrir esta, ahora bien, una desventaja que se puede encontrar en este tipo de cerraduras es que se necesita una llave para cada uno de los individuos que pueden tener acceso a los lugares donde se encuentran las cerraduras. Entre este tipo de cerradura podemos encontrar cerraduras de embutir, cerraduras de sobreponer y cerradura de Borjas que funcionan con el mismo principio de la llave solo se diferencian en la forma del pasador y como este está ensamblado en la puerta.

Figura 4.10 *Cerraduras tradicionales de tipo embutir, sobreponer y de borjas.* ***(Bricovel, 2021)***

b. Cerradura Digital: hoy en día este tipo de cerraduras son muy utilizadas en hoteles, parqueos, universidades, laboratorios, entre otros. Estas cerraduras necesitan de energía para poder funcionar y no necesitan una llave de metal para poder abrirlas, estas cerraduras utilizan tarjetas, sistemas biométricos, patrones o código de números como llave.

Figura 4.11 *Cerradura digital electrónica y electromagnética.*

Las cerraduras digitales son un invento del ingeniero y político Tor Sornes quien inició inventando la VingCard para las empresas hoteleras donde se utilizaba un código para poder entrar a la habitación.

Las cerraduras digitales son la innovación debido a su combinación con sistemas biométricos donde solo se utiliza el cuerpo humano como llave para ellas y es una ventaja debido a que los rasgos biométricos son diferentes en todos los individuos y muy difícilmente estas podrán ser falsificados. Dentro de las cerraduras digitales tenemos las cerraduras electrónicas y las cerraduras electromagnéticas.

Las cerraduras electrónicas están diseñadas para que cuando no haya energía, estas se mantengan cerradas y esté asegurado lo que hay dentro del espacio restringido, a esto se le llama ***Fail Secure*** que traducido significa ***al fallar estar seguro***, en cambio las cerraduras electromagnéticas funcionan cuando hay energía eléctrica creando así un campo electromagnético para mantener los imanes ionizados y esta permanezca cerrada, pero, en el caso de no haber energía, estas se abren por seguridad de los usuarios por si se presenta una emergencia dentro de las instalaciones y a este modo se le llama ***Fail Safe*** que se traduce como ***al fallar estar a salvo***. Es decisión de cada persona cuál de las dos cerraduras le conviene más tomando en cuenta los modos con los que estas trabajan, pero es recomendable integrar un sistema de emergencia con baterías o UPS para que la cerradura funcione de manera normal. (Avilés, 2022)

En este proyecto se utiliza la cerradura digital porque cumple con las características necesarias para el correcto funcionamiento de la cerradura, específicamente se utiliza la cerradura electromagnética para que al estar energizado el circuito este permanezca cerrado y en el caso de no haber energía, este se abre para salvaguardar la vida de las personas que se encuentren dentro del sitio donde está ubicada la cerradura.

Se combina la cerradura electromagnética junto con un sensor de huella que es capaz de medir los datos biométricos de la huella digital para permitir o denegar el acceso a un individuo, todo esto junto con la lógica de programación implementada en el microcontrolador que dará las instrucciones a todos los elementos que forman parte del proyecto.

4.3.2 Ventajas y desventajas de las cerraduras electrónicas y electromagnéticas

En este segmento se hará mención de las ventajas que presentan este tipo de cerraduras, así como también las desventajas debido a que es de suma importancia conocer ambas para poder escoger la cerradura que más se acerque a nuestras necesidades.

Tabla 4.3 Ventajas y desventajas de las cerraduras electrónicas y electromagnéticas.

(Cerrajero, 2020)

Ventajas	Desventajas
Mecanismo seguro y confiable	En caso de fallo de energía se generan inconvenientes.
Fácil instalación y uso.	Algunos modelos no cuentan con baterías de respaldo para un corte de energía.
Son de modelos duraderos, no invasivos y existen muchas opciones para elegir.	Pueden abrirse ante un corte de energía.

En esta tabla se muestran las ventajas y desventajas de las cerraduras electrónicas y electromagnéticas.

4.5 Componentes para utilizar en el proyecto

4.5.1 Sensor de huella

Es un elemento que combina la tecnología con el uso de los datos biométricos de la huella digital para identificar a las personas y realizar una acción como ser dar o denegar el acceso a un individuo. El sensor de huella es el elemento más utilizado en las cerraduras electrónicas ya que tiene una gran aceptación por parte de las personas y ha demostrado que es muy efectivo para reconocer a las personas en la base de datos de cada empresa. (Chavarrea & Chiluisa, 2013)

Como lo mencionamos antes, las huellas digitales tienen patrones de líneas por lo que el sensor de huella en dos pasos puede hacer la autenticación de esta, primero se tiene la inscripción, en este paso el individuo debe enrolar la huella digital del dedo que estará utilizando para tener acceso, en este proceso se requiere de varias tomas de la huella en diferentes posiciones para tener una amplia vista de la huella digital. Luego está el paso de verificación que es cuando se empieza a probar si la huella tomada funciona y da el acceso a las personas enroladas y ya poder seguir captando las huellas, escaneándolas y con los rasgos característicos de esta hacer el reconocimiento. (Ayudaley, 2020)

4.5.1.1 Tipos de sensores de huella digital

Existen 5 tipos de sensores de huella digital que se caracterizan por hacer el escaneo o la lectura de forma diferente.

4.4.1.1.1 Sensores ópticos

Es uno de los sensores más comunes para utilizar con la huella digital y consta de un escáner con luces para poder captar la imagen de huella digital clara con gran visibilidad de sus crestas para facilitar el reconocimiento. Tienen la ventaja de que son de bajo costo, sin embargo, se debe estar limpiando el lente debido a que se puede acumular rastros de otras huellas digitales y hacer que impida un buen reconocimiento.

Este sensor utiliza la tecnología FTIR que es donde se obtiene la huella mediante una luz reflejada a través de un prisma invertido para obtener la misma huella digital sin alteraciones. (Navalpotro, 2014)

Para este proyecto se utilizará el sensor óptico AS608 que tiene un procesador de alta velocidad y una memoria con capacidad de hasta 162 huellas. (Ada, s.f.)

Figura 4.12 *Sensor de huella AS608 óptico.* ***(tecHNologia, s.f.)***

4.4.1.1.2 Sensores Capacitivos

Al igual que los sensores ópticos, captan la huella digital con sus crestas, pero en lugar de hacerlo con luz estos lo hacen con corriente eléctrica. Los patrones de las crestas están conduciendo la energía eléctrica y entre las crestas pasa el aire por lo que de esta manera se obtiene la imagen de la huella digital. Este sensor está conformado por uno o varios condensadores de silicio cubiertos por cedas, las celdas incluyen dos placas conductoras con una capa aislante. Tiene la ventaja de que es necesario tener una huella digital real debido a que necesita los espacios de aire entre las crestas y las mismas crestas para conducir la energía y tener la captura de la huella digital. (Chavarrea & Chiluisa, 2013)

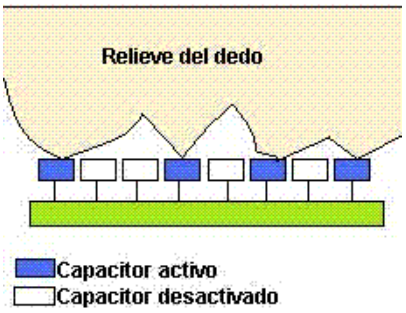


Figura 4.13 *Funcionamiento de un sensor de huella capacitivo.* ***(Moderna, s.f.)***

4.4.1.1.3 Sensor Ultrasónico

Estos sensores son los más nuevos para el escaneo de las huellas digitales, funcionan mediante un sonido ultrasónico de alta frecuencia y requiere de un transmisor y receptor

ultrasónico. “El proceso implica el uso de un pulso ultrasónico, que se envía a través del transmisor ultrasónico hacia el dedo que descansa sobre el escáner. Tan pronto como este pulso golpea el dedo, se transmite una parte, mientras que otra parte se refleja.

Este pulso reflejado es luego recogido por un receptor ultrasónico que, dependiendo de la intensidad del pulso, captura una representación en 3D de la huella digital”. (Ayudaley, 2020)

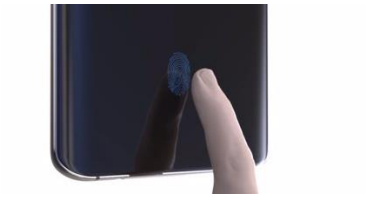


Figura 4.14 *Teléfono Qualcomm con sensor de huella ultrasónico.* ***(Español, 2015)***

4.4.1.1.4 Sensor Térmico

En este sensor se hace la toma de la huella digital mediante la temperatura de las crestas y el aire que hay entre ellas. Son más utilizados en zonas donde hay cambios ambientales, donde se presenta humedad, temperaturas muy altas y donde hay contaminación por agua u otros componentes ya que este sensor tiene una función donde se limpia el solo para quitar resto de otras huellas que hayan quedado. Una desventaja que presenta este tipo de sensores es que consume un poco más de energía que cualquier otro sensor debido al calentamiento que produce. (Chavarrea & Chiluisa, 2013)

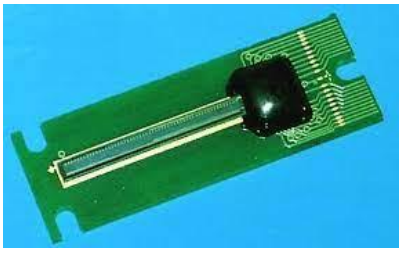


Figura 4.15 *Sensor de huella digital térmico Atmel.*

4.4.1.1.5 Sensor Mecánico

Se trata de un sensor construido por varios transductores de presión lo cual hacen que se cierren o abran cuando se ejerza una fuerza sobre ellos. Al ser crestas hay una mayor presión sobre los transductores lo cual hacen que la figura de la huella digital se vaya formando mediante ellos y

cuando se encuentra el aire entre las crestas los transductores permanecen cerrados indicando que ahí existe un espacio. (Chavarrea & Chiluisa, 2013)

Figura 4.16 *Sensor de huella mecánico.*

Estos son todos los tipos de sensores de huella digital que existen y ahora se hablará sobre el microcontrolador que se va a utilizar en este proyecto para enviar instrucciones a cada uno de los componentes necesarios.

4.5.2 Arduino

Arduino es una placa de desarrollo con un microcontrolador programable que puede ser utilizado para diseñar y montar circuitos junto con otros elementos para que funcionen en la vida real. En el Arduino se conectan todos los componentes necesarios para el circuito creando una comunicación entre ellos y siendo este el que manda las instrucciones para realizar una función.

"El microcontrolador es el chip principal que nos permite programar la placa para que ejecute comandos y pueda tomar decisiones basadas en las lecturas proporcionadas por varias entradas (pines). El chip puede variar según el tipo de Arduino con el que estamos trabajando, pero generalmente encontraremos controladores Atmel, como ATmega8, ATmega168, ATmega328, ATmega1280 o ATmega2560. Las diferencias entre ellos son sutiles, pero importantes a la hora de encarar ciertos proyectos; por ejemplo, integran distinta cantidad de memoria" (Peña, 2020)

Arduino también es un hardware libre, lo que quiere decir que es una placa con un circuito impreso con diferentes elementos incluyendo el microcontrolador y con una serie de pines donde se conectan sensores y actuadores. Algunas de las características son que su software es

libre, gratis y es multiplataforma, la mayoría de los sistemas operativos pueden instalar su programa y haciendo mención sobre esto, su lenguaje de programación es C++. Es muy fácil de usar y el Arduino puede ser utilizado varias veces ya que es reprogramable. (Moreno & Córcoles, 2018)

Figura 4.17 *Arduino Leonardo.* ***(Moreno & Córcoles, 2018)***

4.5.3 Picaporte

Para el proyecto se necesita un elemento de seguridad que abra y cierre la puerta, para ello se escogió un picaporte de bajo consumo eléctrico, fácil de instalar y que cumpla con su función de abrir y cerrar la puerta cuando el sensor de huella le envíe la señal. Este tipo de picaportes son estables, de material de acero inoxidable y se puede aplicar a puertas, gavetas, archivos, cajones, entre otras. (Tecnopura, s.f.)

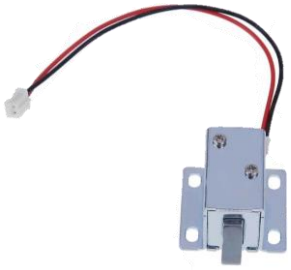


Figura 4.18 *Picaporte Solenoide de 12V.* ***(Tecnopura, s.f.)***

4.5.4 Mosfet IRF520

Se utiliza este componente para activar al picaporte antes mencionado. Un IRF520 es utilizado para manejar cargas altas o niveles de potencia significativos. Los transistores de tipo

Mosfet presentan mejores características que los BJT en aplicaciones de Encendido/Apagado de cargas de alto amperaje. Para activar el mosfet se debe de enviar 5 Voltios al Gate del Mosfet, esto permitirá que la corriente fluya a través de la carga y esta se active. (Mechatronics, s.f.)

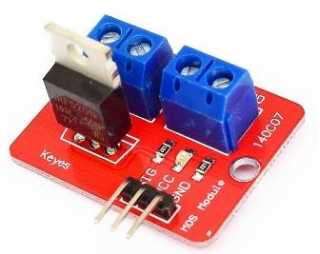


Figura 4.19 *Mosfet IRF520.* ***(Mechatronics, s.f.)***

4.6 Costo de Fabricación

En este segmento se hará una lista del costo de cada uno de los materiales que son necesarios para el montaje de la cerradura. Se hizo la cotización de todos los componentes en la empresa de dispositivos electrónicos C&D TecHNologia ubicada en Tegucigalpa, Honduras. Se detalla la cantidad de cada elemento utilizado y el valor en lempiras de cada uno para tener un precio exacto al final de la investigación.

Tabla 4.5 Presupuesto del prototipo.

Componente	Cantidad	Precio Unitario
Sensor de huella AS608	1	L. 750
Arduino UNO R3	1	L. 480
Mosfet IRF520	1	L. 90
Picaporte Solenoide 12 V	1	L. 211
Pulsador	1	L. 6.4
Jumpers (Kit de 40)	1	L. 122
Protoboard	1	L. 176
Buzzer	1	L. 56
Pantalla LCD 16x2	1	L. 250
Total		**L. 2,141.4**

En esta tabla se muestra la cantidad y el precio de los elementos utilizados para el montaje del circuito y tener un prototipo final.

Un aspecto por considerar para saber el precio final del proyecto es que el Arduino no va incluido en el prototipo y se debe cambiar por un circuito integrado programable que ocupa menor espacio para el montaje de la cerradura. Así como también la placa de pruebas solo es necesaria para las pruebas, pero ya en un montaje final no se agrega solo se cambia por una baquelita donde se pueden soldar todos los componentes.

Tabla 4.6 Costo final de prototipo.

Componente	Cantidad	Precio Unitario
Sensor de huella AS608	1	L. 750
PIC 18F2550	1	L. 235
Relé de 1 canal 5v	1	L. 117
Picaporte Solenoide 12 V	1	L. 211
Pulsador	1	L. 6.4
Baquelita	1	L. 50
Buzzer	1	L. 56
Pantalla LCD 16x2	1	L. 250
Total		**L. 1,675.4**

En la tabla anterior se detalla el precio final del prototipo con los elementos que son necesarios para tener un prototipo completo y que pueda ser montado en una carcasa para su introducción al mercado.

Este costo es sin tomar en cuenta la carcasa que protege al circuito y la mano de obra por el montaje de este.

4.7 Circuito

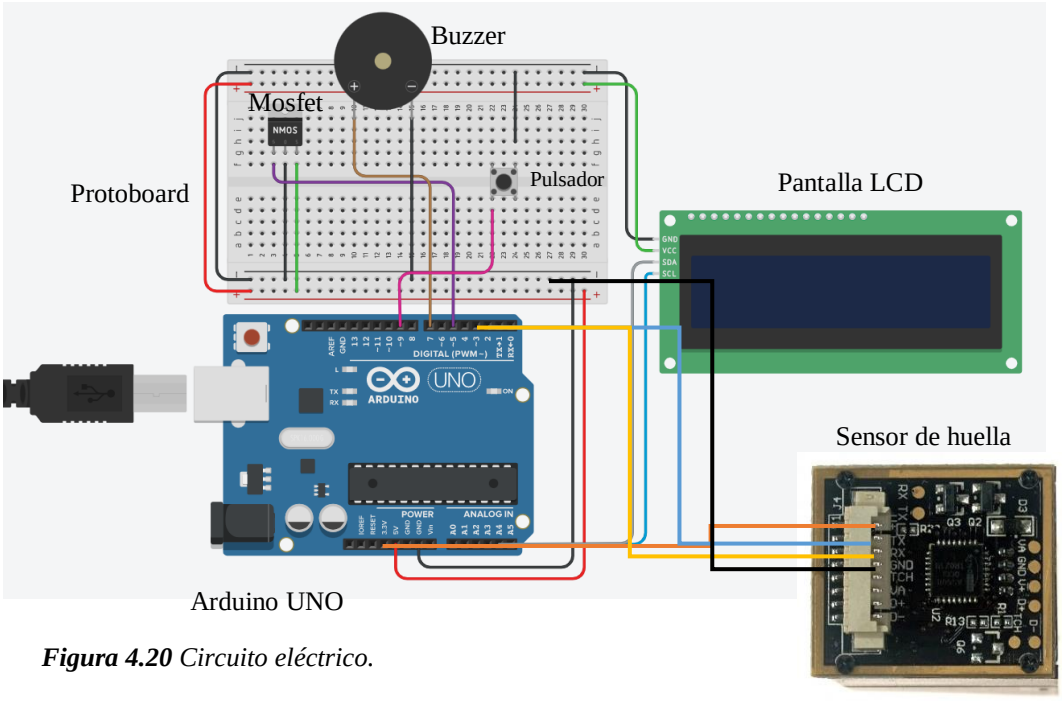


Figura 4.20 *Circuito eléctrico.*

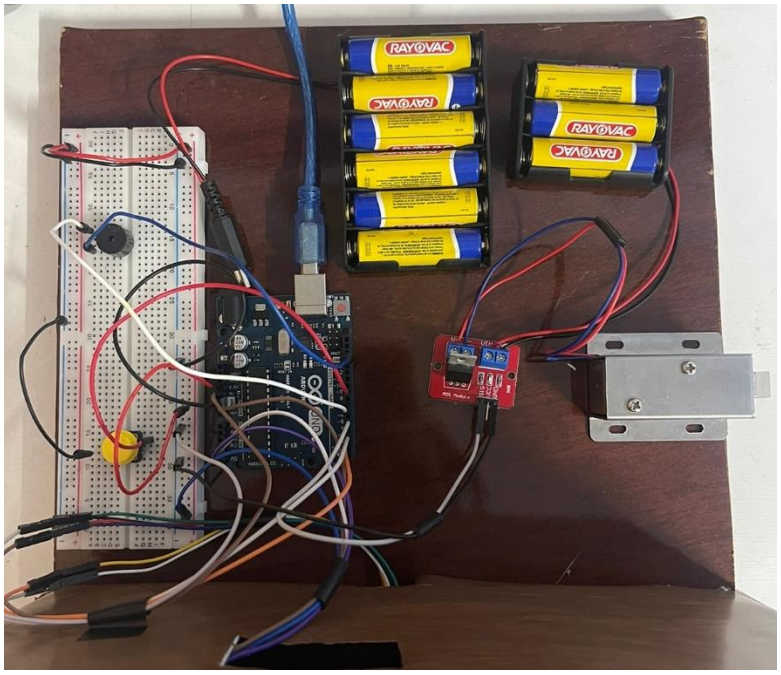


Figura 4.21 *Circuito eléctrico montado.*

Las figuras anteriores nos muestran el circuito del diseño de la cerradura para su montaje, así como también las conexiones específicas de cada elemento para permitir una buena comunicación entre ellos.

El funcionamiento de la cerradura se basa en un microcontrolador que conecta todos los elementos para que trabajen en conjunto donde el sensor de huella capta las huellas digitales, las compara y luego envía una señal a través del Arduino al buzzer para que este suene 1 vez sí permite el acceso o 2 veces si lo niega, también esa señal va hasta la pantalla LCD donde se ve reflejado en palabras el acceso o no a la entrada, y por último la señal también llega hasta el picaporte para que realice la acción de abrirse o cerrarse dependiendo de la respuesta que se tenga del sensor. Para la salida solo es necesario pulsar el botón de salida y automáticamente la cerradura se abre.

Prototipo

Figura 4.22 *Prototipo Apagado.*

Figura 4.23 *Prototipo Encendido.*

4.7 Proceso de enrolamiento de huellas

La cerradura electrónica con sensor de huella debe enrolar todas las huellas que van a tener acceso por lo que primero hay un proceso de enrolamiento, Con el programa de Arduino y la librería del sensor de huella enrolar las huellas dactilares es muy fácil. Primero debemos cargar el programa y en las opciones de ejemplo en la librería del sensor aparece una opción llamada enroll traducida al español como enrolar. Se debe subir ese programa al Arduino y el programa va dando instrucciones de como enrolar la huella, se comienza enumerando la huella y luego se toma la captura de esta.

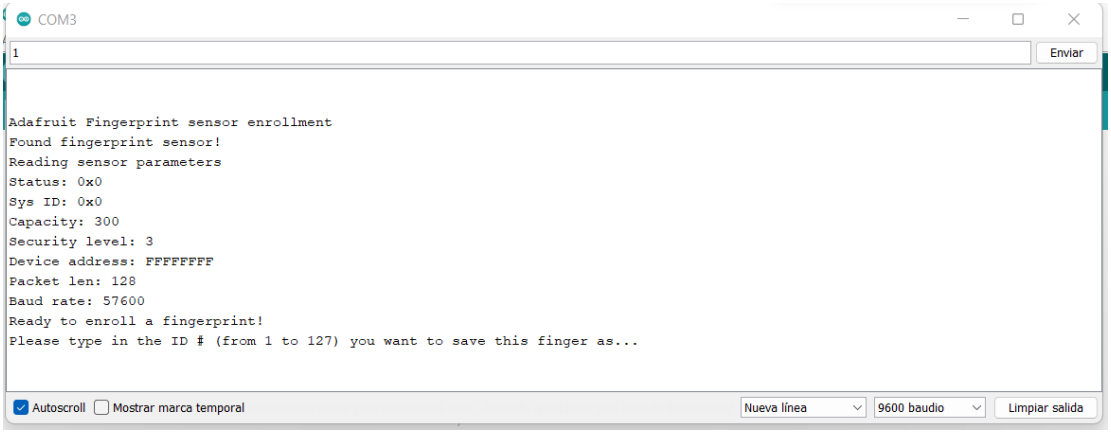


Figura 4.24 *enrolando huella para prueba 1.*

Figura 4.25 *enrolando huella 1 y 2 para prueba 2.*

Figura 4.26 *enrolando huella 3 para prueba 2.*

Figura 4.27 *enrolando huella 4 para prueba 2.*

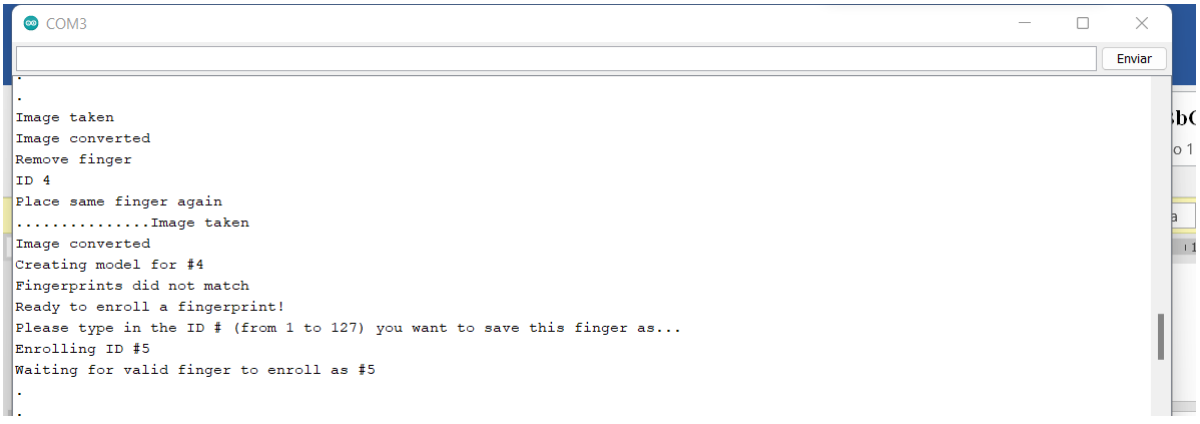


Figura 4.30 *enrolando huella 5 para prueba 2.*

Figura 4.31 *enrolando huella 6 para prueba 2.*

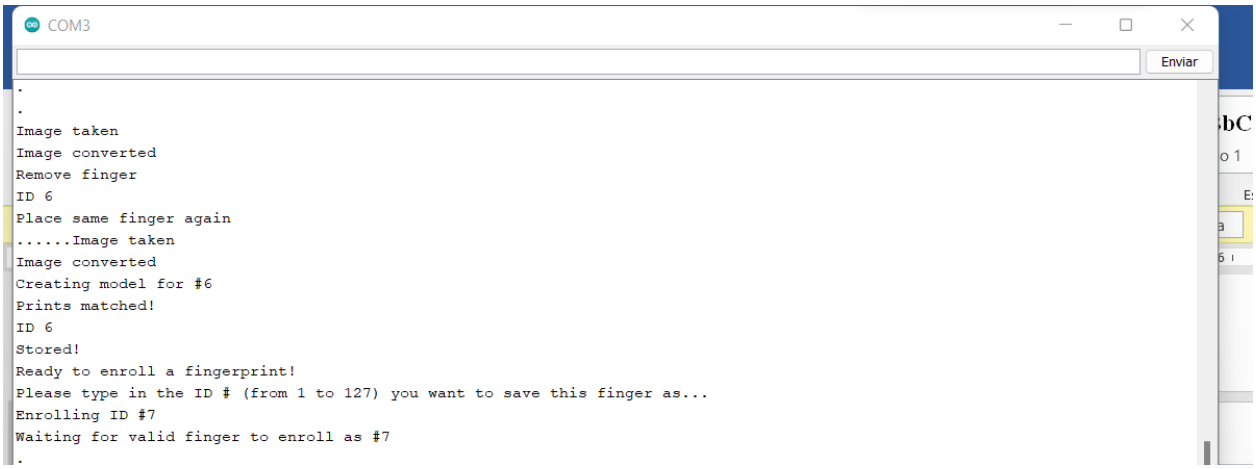


Figura 4.32 *enrolando huella 7 para prueba 2.*

Figura 4.33 *enrolando huella 8 para prueba 2.*

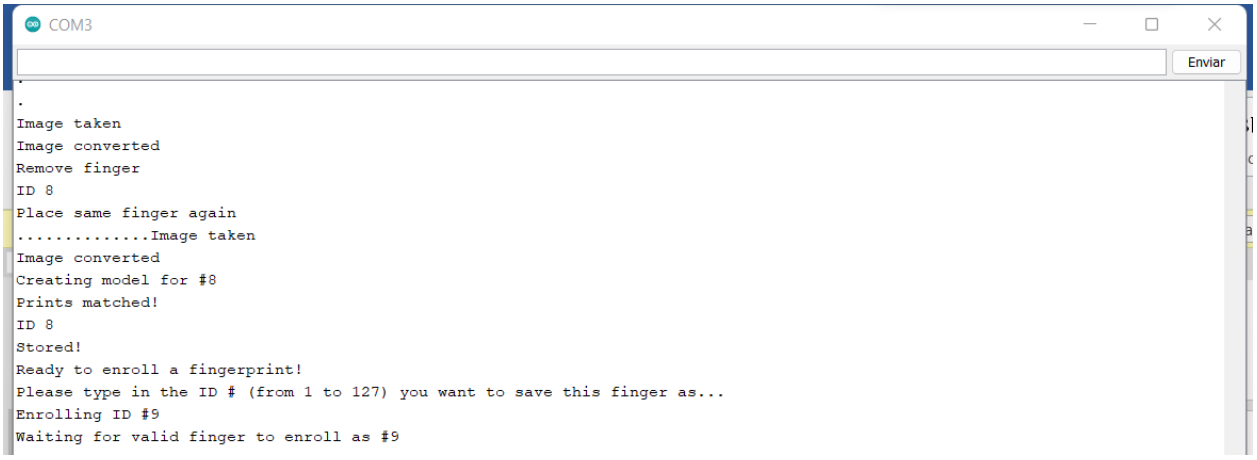


Figura 4.34 *enrolando huella 9 para prueba 2.*

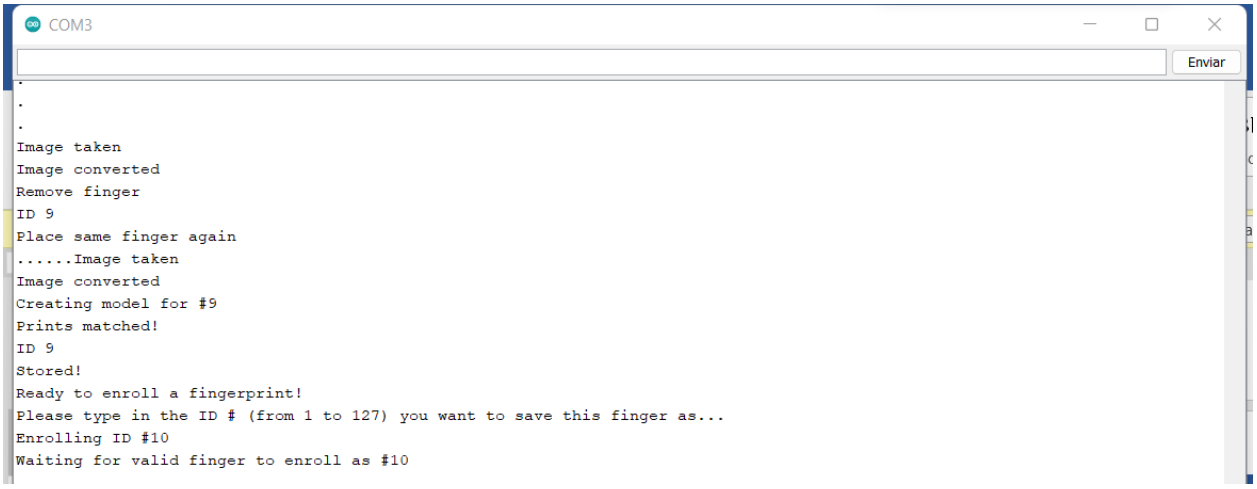


Figura 4.35 *enrolando huella 10 para prueba 2.*

V. Metodología / Proceso

5.1 Enfoque y Métodos

El enfoque de esta investigación es de tipo experimental ya que es un proyecto en el cual se hará el prototipo de una cerradura electrónica con sensor de huella mediante el microcontrolador Arduino y su lógica programable para poderlo llevar a cabo. Específicamente será del tipo cuantitativo debido a que se tiene el precio de cada elemento para tener un costo de fabricación total y así poder comparar los precios con otras cerraduras que existen en el mercado. También los resultados se verán reflejados mediante pruebas con diferentes huellas dactilares para corroborar el funcionamiento de la cerradura.

Con el diseño y montaje de la cerradura, podrá ser capaz de ser implementado en hogares, empresas, escuelas, universidades y en muchos otros lugares donde sea necesario controlar el acceso de las personas.

5.2 Población y Muestra

En este caso debido a que es un proyecto con un prototipo físico, se tiene que la población y muestra es un conjunto de datos recopilados a lo largo del tiempo de pruebas al mismo para tener un control sobre los fallos y aciertos que este tuvo durante ese periodo de tiempo.

Se le realizaron 2 tipos de pruebas al prototipo, una en base a la cantidad de aciertos obtenidos con la misma huella y otra donde se enrolaron 10 huellas dactilares diferentes para ver la cantidad de fallos al haber ya un número más grande de huellas dactilares.

5.3 Unidad de Análisis y Respuesta

Se realizó el prototipo donde se ve reflejado el circuito con sus respectivas conexiones entre los elementos e incluyendo un buzzer indicador de la apertura de la puerta (suena 1 vez) y para una huella no identificada (suena 2 veces). También en la pantalla LCD se puede ver cuando hay una autorización para entrar o se niega el paso. (Ver figura 5.3.1 y 5.3.2). Como se indica en las figuras antes mencionadas se muestra el buen funcionamiento de la cerradura para tener un control de acceso de las personas en un lugar específico.

Con el costo final del prototipo se logró hacer una comparación entre distintas cerraduras con sensor de huella que se encuentran en el mercado y de esta manera verificar si el prototipo tiene un menor costo.

5.4 Técnicas e Instrumentos Aplicados

Los instrumentos que se utilizaron para el desarrollo del prototipo de este proyecto son todos aquellos componentes que forman parte del circuito de este además de las herramientas necesarias para el ensamble del prototipo y para hacer ajustes en él.

5.4.1 Técnica aplicada al diseño de circuitos

Las técnicas aplicadas para este proyecto son todas las aprendidas durante la carrera como ser el montaje de circuito, la lógica para el desarrollo de estos, la lógica al momento de desarrollar un código para el Arduino, identificar errores y darle soluciones, todo esto para poder explicar el desarrollo de la cerradura que se acciona mediante las huellas dactilares.

5.4.2 Técnica aplicada al procesamiento de datos

Otra técnica aplicada al proyecto son las pruebas que se hicieron al mismo para verificar su correcto funcionamiento. La primera técnica fue medir los intentos acertados en el sensor de huella con una sola huella. Luego se realizó otra prueba donde se enrolaron 10 huellas digitales diferentes para poder demostrar que la cerradura acepta una mayor cantidad de huellas y tiene la habilidad de reconocer cada huella diferente. Después de pasar estas dos pruebas, la cerradura es capaz de ser implementada en la industria ya que se ha demostrado que funciona bien.

5.5 Fuentes de Información

Fuentes Primarias

La biometría para la identificación de las personas

https://sistemamid.com.ar/panel/uploads/biblioteca/2015-03-22_12-05-01117594.pdf

Páginas 5-30.

La huella dactilar como mecanismo de identificación biométrica para la no portabilidad de documentos de identidad.

https://revistas.udistrital.edu.co/index.php/tia/article/view/12761/14691
Páginas 1-4.

Construcción e implementación de un circuito electrónico mediante un sensor de huellas dactilares para el control de ingreso y salida del personal autorizado al cuarto de equipos de computación ubicado en el instituto de estudios del petróleo quito.
https://bibdigital.epn.edu.ec/bitstream/15000/6359/1/CD-4882.pdf
Páginas 14-36

Software Arduino

Fuentes Secundarias

Estudio y análisis comparativo de las actuales técnicas biométricas.
https://oa.upm.es/32372/1/tesis_master_mario_navalpotro_molina.pdf
Páginas 21-37, 71-217.

Análisis y diseño de un sistema que permita el control de acceso al personal administrativo ubicado en la matriz de la universidad técnica de babahoyo, utilizando tecnología rfid.
http://dspace.utb.edu.ec/bitstream/handle/49000/11695/E-UTB-FAFI-SIST.INF-000002.pdf?sequence=1&isAllowed=y
Páginas 14-16.

Arduino: Curso Práctico.
https://books.google.es/books?hl=es&lr=&id=yo6fDwAAQBAJ&oi=fnd&pg=PA183&dq=Arduino:+Curso+Pr%C3%A1ctico.+RA-MA&ots=iMhph5R_Wa&sig=FybDMo65fPNRGh33-q8awMdX8WE#v=onepage&q&f=false
Páginas 21-32.

Fuentes Terciarias

Diseño de un sistema de acceso por reconocimiento de huella dactilar mediante la plataforma Arduino
https://repositorio.utp.edu.co/server/api/core/bitstreams/cb65c3f1-f3d9-44b3-bf97-a0240f29dc5f/content
Páginas 6-22.

Las huellas dactilares como herramienta esencial para la investigación criminal
https://roderic.uv.es/bitstream/handle/10550/65470/6273008.pdf?sequence=1&isAllowed=y
Páginas 1-11.

VI. Resultados y Análisis

Con los siguientes resultados se responde a la primera hipótesis acerca del costo de la cerradura en comparación con otras que ya existen en el mercado.

Tabla 6.1 Comparación de costos cerraduras.

Cerraduras	**Cerradura Electrónica con Sensor de Huella (Prototipo)**	**Kwikset Halo Touch**	**eufy Security Smart Lock Touch & Wi-Fi**	**Candado de huellas dactilares BIRX.**
Costo	**L. 2.141.4**	**L. 5997.60**	**L. 4627.68**	**L. 1431.56**

La tabla anterior muestra los precios de las diferentes cerraduras analizadas para la comparación de costos con el prototipo que se está haciendo en esta investigación.

En la tabla anterior se muestran 3 cerraduras diferentes en el mercado para comparar su precio con el prototipo fabricado para esta investigación. Los precios varían y esto se debe a los componentes que se utilizan en cada una de ellas, todas tienen la misma funcionalidad, pero en cuanto a tamaño, componentes y características varían un poco y por eso es razonable que tengan un costo diferente. En la cerradura Kwikset y Eufy su precio es más elevado debido a que poseen la capacidad de conectarse a internet y se comprende que tiene más elementos y otras funcionalidades, para el candado de huellas dactilares BIRX su precio es menor debido a que es un candado que se abre con la huella digital, también por su tamaño su precio es menor. Por lo tanto, podemos decir que el precio de las cerraduras varía según sus funcionalidades, sus elementos y las características que cada uno posee y en este caso el prototipo para la cerradura electrónica con sensor de huella es el de menor valor.

Para responder a la segunda y tercera hipótesis se necesitó del circuito y su montaje y en base a las pruebas se obtuvieron los siguientes resultados.

En la primera prueba se tomó como referencia solamente una huella digital donde se realizaron 100 intentos para verificar el comportamiento de la cerradura en base a un porcentaje de aciertos.

Tabla 6.2 Resultados de prueba 1.

Prueba 1										
# de intentos	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	A	A	A	A	A	A	A	A	A	A
2	A	A	A	A	A	A	A	A	A	A
3	A	A	A	A	A	A	A	A	A	A
4	A	A	A	A	A	A	A	A	A	A
5	A	A	A	A	A	A	A	A	A	A
6	A	A	A	A	A	A	A	A	A	A
7	A	A	A	A	A	A	A	A	A	A
8	A	A	A	A	A	A	A	A	A	A
9	A	A	A	A	A	A	A	A	A	A
10	A	A	A	A	A	A	A	A	A	A
% intentos Acertados										**100%**

Esta tabla muestra los resultados obtenidos en cada uno de los intentos realizados para la primera prueba a la cerradura.

Para la segunda prueba realizada a la cerradura se utilizaron 10 huellas digitales diferentes y se hicieron 100 intentos en total para calcular el porcentaje de fallos que se puede obtener al haber un mayor número de huellas enroladas en el sistema.

Figura 6.1 *Pantalla principal de la cerradura en funcionamiento.*

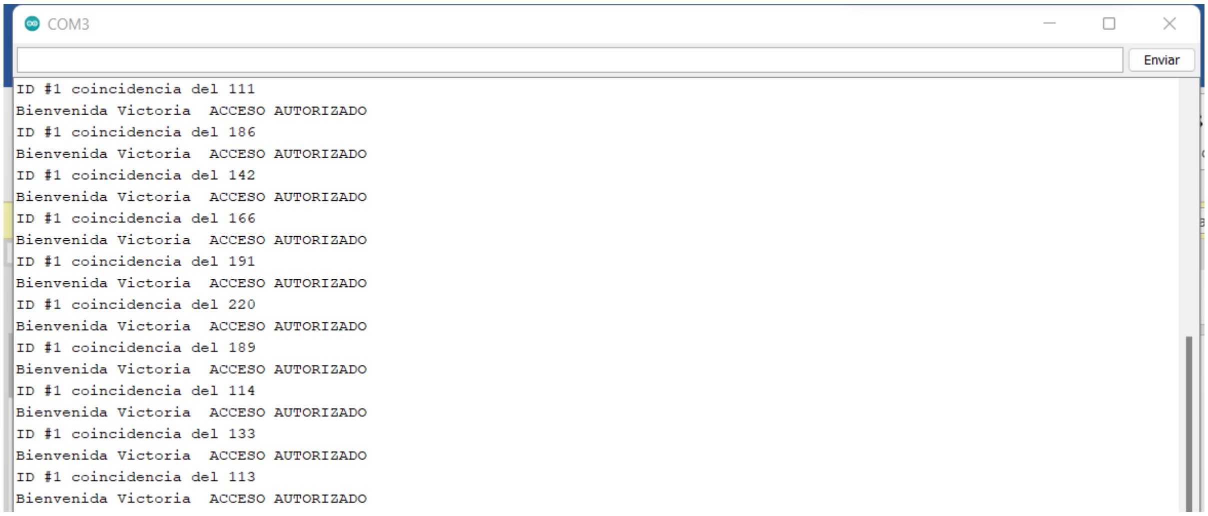


Figura 6.2 *Intentos de prueba 1.*

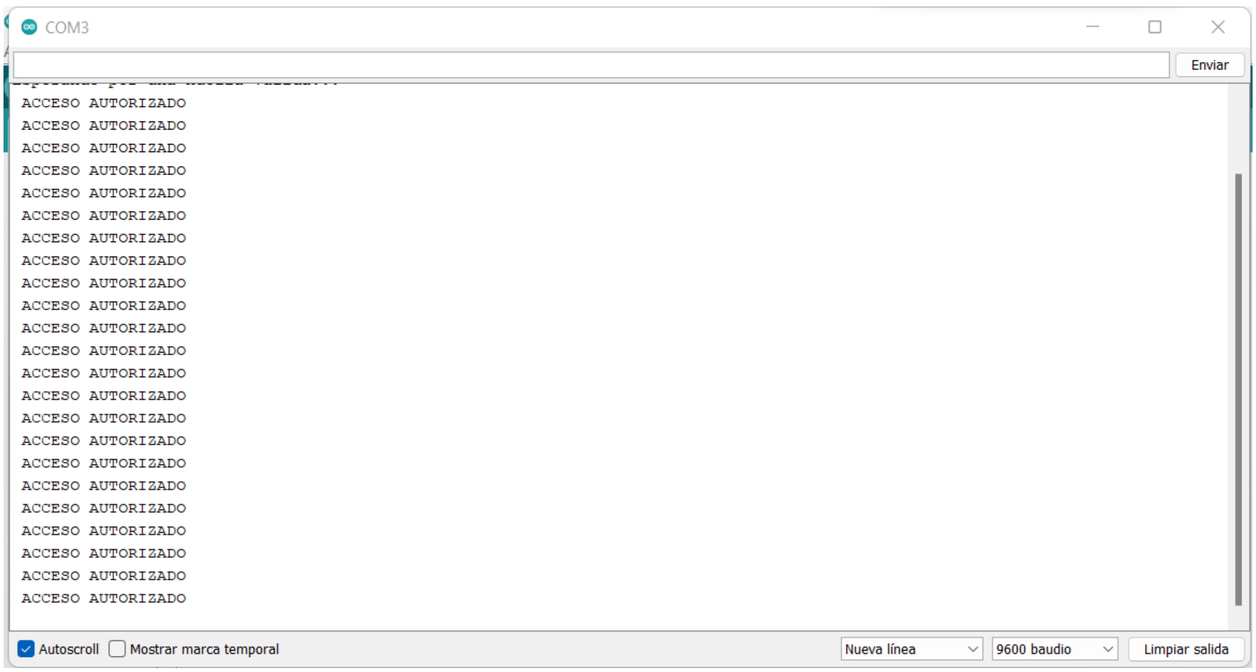


Figura 6.3 *Intentos de prueba 1.*

Estos fueron algunos de los intentos realizados al sensor de huella con una sola huella para verificar su funcionamiento.

Tabla 6.3 Resultados de prueba 2.

Prueba 1										
	Huella									
# de intentos	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	A	D	A	A	A	A	A	A	A	A
2	A	A	A	A	A	A	A	A	A	A
3	A	A	A	A	A	D	A	A	A	A
4	A	A	A	A	A	A	A	A	A	D
5	A	A	D	A	A	A	A	A	A	A
6	A	A	A	A	A	A	A	A	A	A
7	A	A	A	A	A	A	A	A	D	A
8	A	A	A	A	A	A	A	A	A	A
9	A	A	A	A	A	A	A	A	A	A
10	D	A	A	A	A	A	A	A	A	A
% intentos Acertados										94%
% intentos Fallidos										6%

En esta tabla podemos observar el análisis de los intentos con 10 huellas diferentes para sacar un número de aciertos y fallos obtenidos en la segunda prueba a la cerradura.

Como se puede observar en las tablas 6.2 y 6.3 que indican los resultados de las pruebas realizadas a la cerradura se puede inferir que la cerradura es un sistema funcional con un 100% de intentos acertados para la primera prueba y un 6% de intentos fallidos en la segunda prueba que nos indican el porcentaje de aceptación para este sistema, debido a que sobrepasa el 90% de intentos acertados el sistema se acepta.

Figura 6.4 *Pantalla principal de la cerradura en funcionamiento.*

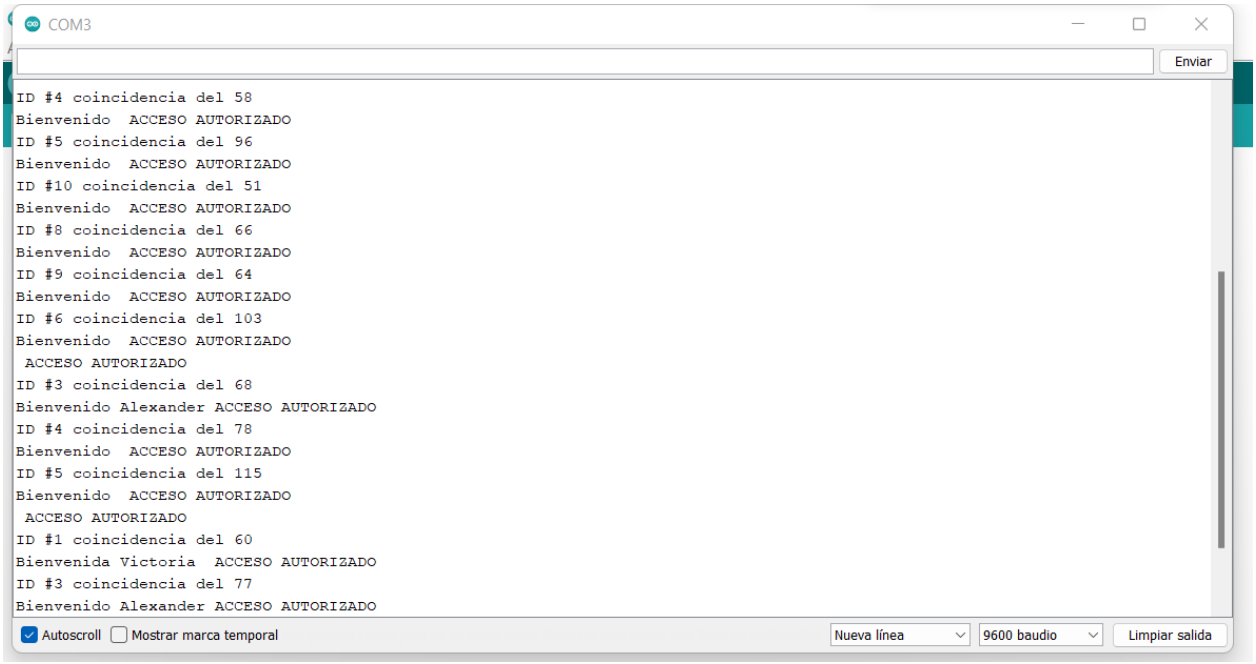


Figura 6.5 *Intentos de prueba 2.*

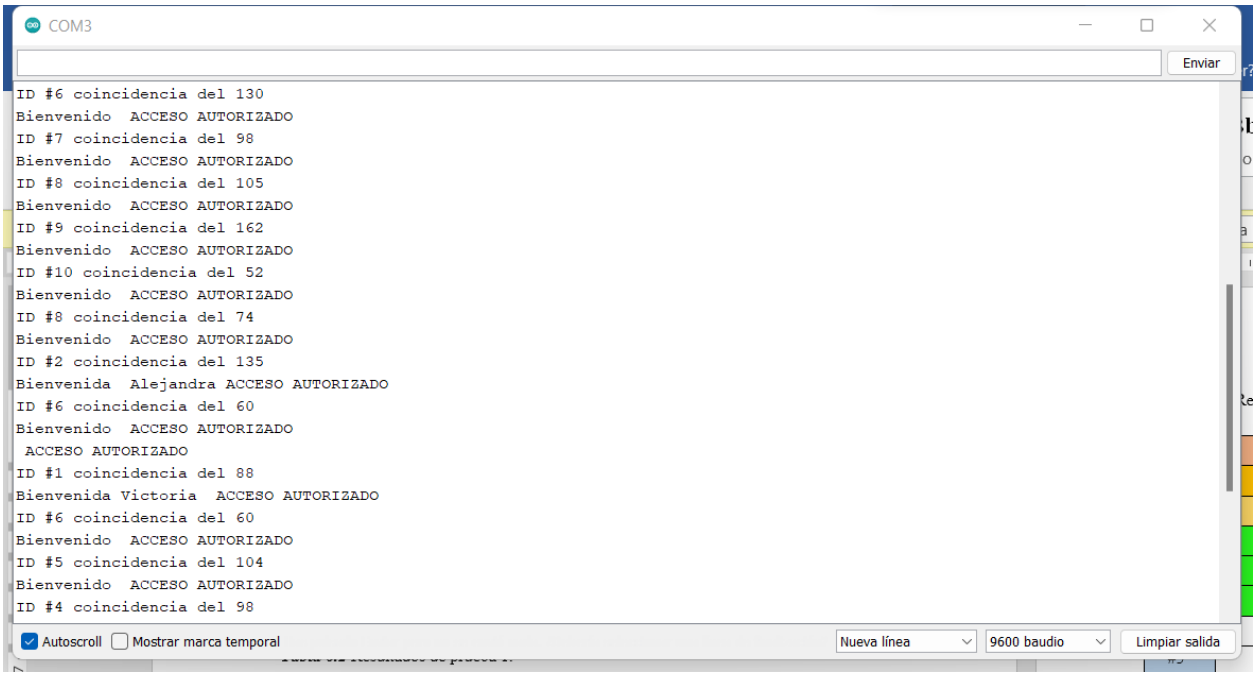


Figura 6.6 *Intentos de prueba 2.*

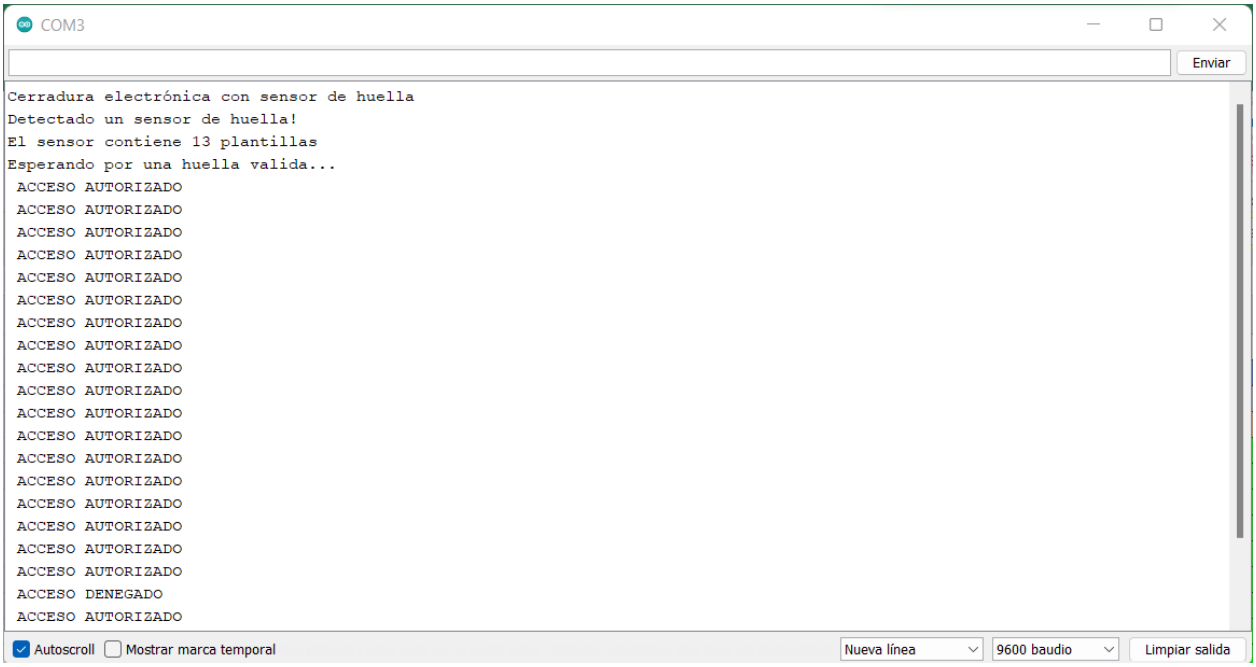


Figura 6.7 *Intentos de prueba 2.*

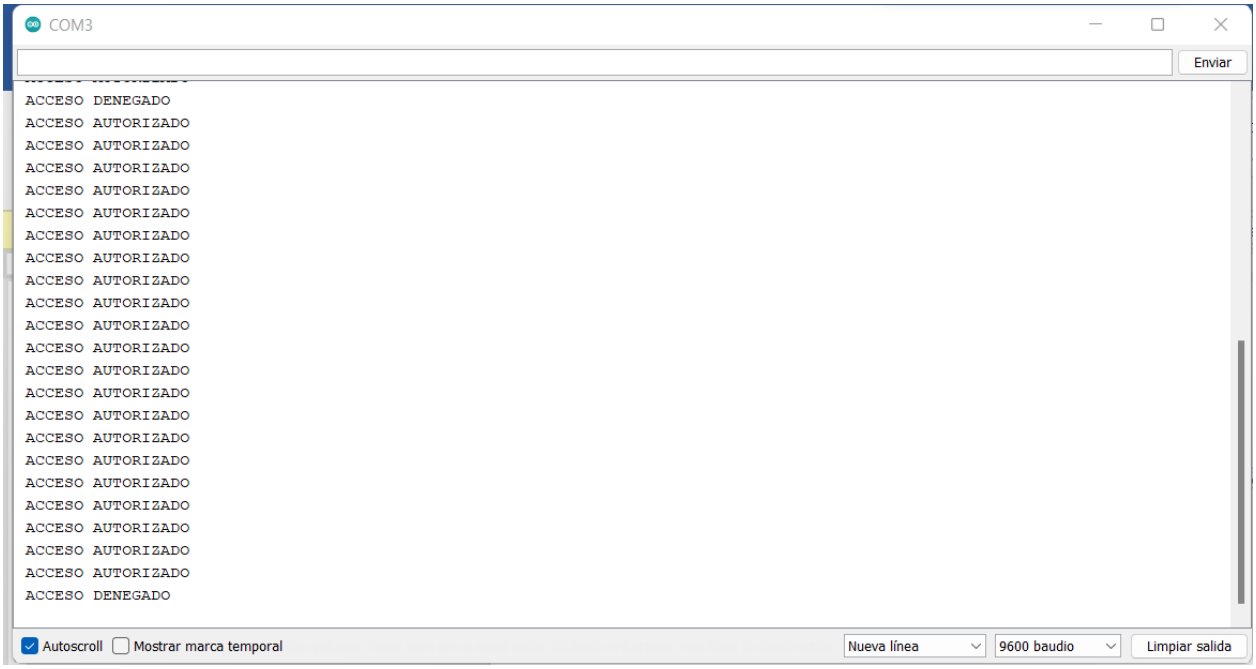


Figura 6.8 *Intentos de prueba 2.*

VII. Conclusiones

Con el circuito ya montado y luego de someterlo a las pruebas indicadas para esta investigación se puede decir que se logró con éxito el diseño de una cerradura electrónica con sensor de huella que logra cumplir con su función de dar acceso a los individuos que se encuentran en su base de datos. Este montaje se puede implementar en diferentes espacios donde sea necesario tomando en cuenta que solo cuenta con un espacio para 162 huellas.

El circuito es funcional y se logró comprobar por medio de dos pruebas a la cerradura donde dan constancia de que la cerradura puede captar diferentes huellas digitales y compararlas con la base de datos del sistema para dar o negar el acceso a un individuo. Por medio de los resultados obtenidos durante el periodo de prueba de la cerradura se acepta esta cerradura para darle una implementación en el mercado ya que tiene un 94% de aceptación.

Se hizo la comparación de costos en relación a diferentes cerraduras con sensor de huella y se observó que esta cerradura tiene un costo bajo en relación a la mayoría de las cerraduras, pero se debe tomar en cuenta que los precios varían de acuerdo a la marca, los componentes, el tamaño, el material de la carcasa y si tienen otras funciones como una aplicación para abrirla con la huella desde el teléfono, etc. Comparando la cerradura con las diferentes que se encuentran en el mercado podemos tener una mejor visión para darle un mayor efecto a la cerradura propuesta, se le puede agregar otros tipos de sistemas con rasgos biométricos para realizar un sistema híbrido, también un gran aporte para esta cerradura sería un módulo para tener un sistema con base de datos donde se pueda registrar la hora y fecha en la que un individuo ingresó a la empresa.

VIII. Recomendaciones

1. Reemplazar el Arduino por un microcontrolador programable PIC16F628A para disminuir el costo de la cerradura y también para que a este no se le pueda ser modificada su lógica y afectar el funcionamiento del mismo. El PIC utiliza el mismo lenguaje de programación que un Arduino por lo que la transición de Arduino a pic solo necesitaría un cambio de programa para poder utilizar el pic en el proyecto, los componentes son compatibles con el pic por lo que el sistema seguiría trabajando de la misma manera.

2. Incluir un sistema de respaldo para cuando no haya flujo de energía, lo que significa incluir una batería de 12 volts para que el sistema funcione al faltar la energía. También, si se cuenta con un UPS perfectamente podría suplir el voltaje necesario para que la cerradura funcione cuando el suministro eléctrico es interrumpido.

3. Incluir un módulo Wifi para desarrollar una aplicación donde se pueda abrir con el uso del teléfono celular, también para tener una base de datos externa y tener un mayor control en el acceso del personal.

4. Realizar una carcasa para tener una mejor presentación de la cerradura y evitar que los componentes se dañen y estén expuestos a diferentes sustancias que pueden arruinarlos.

5. Reemplazar el picaporte por una cerradura magnética.

6. Reemplazar el mosfet IRF520 por un relé.

IX. Bibliografía

1. 101, S. (s.f.). *Seguridad 101*. Obtenido de https://seguridad101.com/cerraduras-de-huella-digital-son-seguras-con-3-ejemplos/#:~:text=Las%20cerraduras%20de%20huella%20digital%20cuentan%20con%20un%20sensor%20capacitivo,el%20mecanismo%20de%20la%20cerradura.
2. Ada, L. (s.f.). *Adafruit*. Obtenido de https://cdn-learn.adafruit.com/downloads/pdf/adafruit-optical-fingerprint-sensor.pdf
3. Amazon. (s.f.). Obtenido de https://www.amazon.com/99590-002-Cerradura-inteligente-tradicional-concentrador/dp/B08DZ2QHC9/ref=sr_1_1_sspa?__mk_es_US=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=1V6ZHY9QO7XIM&keywords=Kwikset+Halo+Touch&qid=1670560068&sprefix=kwikset+halo+touch%2Caps%2C115&s
4. Amazon. (s.f.). Obtenido de https://www.amazon.com/-/es/dactilares-inteligente-electr%C3%B3nico-certificado-resistente/dp/B0967V8WWX/ref=sr_1_5?__mk_es_US=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=D2GP6ITL23E1&keywords=eufy+Security+Smart+Lock+Touch+%26+Wi-Fi&qid=1670560204&sprefix=eufy+
5. Amazon. (s.f.). Obtenido de https://www.amazon.com/-/es/dactilares-inteligente-Bluetooth-biom%C3%A9trico-casillero/dp/B0BKRFZ4R4/ref=sr_1_158?__mk_es_US=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=1Z4G2I6TJLXWW&keywords=fingerprint%2Bsensor%2Block&qid=1670560752&sprefix=cerradura%2Bcon%2Bs

6. Amazon. (s.f.). Obtenido de https://www.amazon.com/-/es/biom%C3%A9tricos-empleado-handpunch-Ethernet-Ingersoll/dp/B005HJUQM6
7. Arboleda, G. (s.f.). *Grupo Arboleda*. Obtenido de https://www.grupoarboleda.com/soluciones-para-hoteles/cerraduras-electronicas/vingcard-flex/
8. Avilés, C. (2022). *ANÁLISIS Y DISEÑO DE UN SISTEMA QUE PERMITA EL CONTROL DE ACCESO AL PERSONAL ADMINISTRATIVO UBICADO EN LA MATRIZ DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO, UTILIZANDO TECNOLOGÍA RFID.* Babahoyo: Universidad Técnica de Babahoyo.
9. Ayudaley. (18 de Mayo de 2020). *Ayudaley*. Obtenido de https://ayudaleyprotecciondatos.es/2020/05/18/sensor-huellas-dactilares/
10. Beat, T. (s.f.). Obtenido de https://thebeat.co/pe/terminos/tasa_de_aceptacion/#:~:text=La%20tasa%20de%20aceptaci%C3%B3n%20es,tu%20tasa%20de%20aceptaci%C3%B3n%20disminuye.
11. Bricovel. (24 de Diciembre de 2021). *Bricovel*. Obtenido de https://bricovel.com/blog/tipos-de-cerradura/
12. Cerrajero, M. (31 de Marzo de 2020). *Manual Cerrajero*. Obtenido de https://manualcerrajero.com/cerraduras-electricas-y-magneticas-ventajas-y-desventajas/
13. Chavarrea, G., & Chiluisa, A. (2013). *CONSTRUCCIÓN E IMPLEMENTACIÓN DE UN CIRCUITO ELECTRÓNICO MEDIANTE UN SENSOR DE HUELLAS DACTILARES PARA EL CONTROL DE INGRESO Y SALIDA DEL PERSONAL AUTORIZADO AL CUARTO DE EQUIPOS DE COMPUTACIÓN UBICADO EN EL*

INSTITUTO DE ESTUDIOS DEL PETRÓLEO QUITO. Quito : Escuela Politécnica Nacional.

14. Cruz, L., & Athó, F. (2006). *Reconocimiento de Iris.* Trujillo: Universidad Nacional de Trujillo.
15. Definición.de. (s.f.). Obtenido de https://definicion.de/entrada/
16. Definición.de. (s.f.). Obtenido de https://definicion.de/costo/
17. Dictionary, T. F. (s.f.). Obtenido de https://es.thefreedictionary.com/similitud
18. Español, E. (17 de Octubre de 2015). *El Español*. Obtenido de https://www.elespanol.com/elandroidelibre/moviles-android/accesorios/20151017/sensor-huellas-pasado-presente-futuro/72242817_0.html
19. Faces, R. (8 de Marzo de 2021). *Rec Faces*. Obtenido de https://recfaces.com/es/articles/escaner-de-iris#7
20. Forenses, C. d. (9 de Agosto de 2017). Obtenido de https://colegiodeperitosforenses.webnode.mx/l/el-publico-deberia-votar-sobre-el-acuerdo-final-del-brexit/
21. FOSS. (s.f.). Obtenido de https://www.fossanalytics.com/es-ar/news-articles/technologies/a-short-intro-to-ftir-analysis#:~:text=Infrarrojo%20Transformado%20de%20Fourier%20(FTIR,se%20le%20conoce%20como%20tal.
22. HETPRO. (2021). *HETPRO*. Obtenido de https://hetpro-store.com/TUTORIALES/modulo-de-reconocimiento-de-voz/
23. Ingeniería.es. (14 de Agosto de 2021). Obtenido de https://www.ingenieria.es/historia-y-evolucion-de-las-cerraduras/

24. Kimaldi. (s.f.). *Kimaldi*. Obtenido de https://www.kimaldi.com/productos/sistemas_biometricos/anviz/terminal_de_reconocimiento_de_iris_anviz_ultramatch/

25. LEDESMA, C. I. (2022). *Centros Informáticos LEDESMA*. Obtenido de https://informaticaledesma.com/es/tpv-s-lectores-banda-chip/4763-modulo-reconocimiento-de-firma-evolis-sig100-2518021914063.html

26. Mechatronics, N. (s.f.). *Naylamp Mechatronics* . Obtenido de https://naylampmechatronics.com/drivers/239-driver-mosfet-irf520-6a.html

27. Moderna, I. (s.f.). *Informática Moderna*. Obtenido de https://www.informaticamoderna.com/Lect_huella.htm

28. Moreno, A., & Córcoles, S. (2018). *Arduino: Curso Práctico.* RA-MA.

29. Navalpotro, M. (2014). *Estudio y Análisis Comparativo de las Actuales Técnicas Biométricas.* Madrid: Universidad Politécnica de Madrid.

30. Parra, S., & Elías, J. (2018). *Diseño de un sistema de acceso por reconocimiento de huella dactilar mediante la plataforma Arduino.* Pereira: Universidad Pedagógica de Pereira.

31. Peña, C. (2020). *Introducción a Arduino* .

32. Raúl, S., & Judith, J. (2021). *Dialnet.* Obtenido de https://dialnet.unirioja.es/servlet/dctes?codigo=301228

33. Robotics, I. (17 de Febrero de 2021). Obtenido de https://inlocrobotics.com/es/lector-de-huella-digital/

34. Rodas, A., & Arreaga, Q. (Marzo de 2018). *Universidad de Valencia.* Obtenido de https://roderic.uv.es/bitstream/handle/10550/65470/6273008.pdf?sequence=1&isAllowed=y

35. Rojas, A., & Suárez, J. (2018). La huella dactilar como mecanismo de identificación biométrica para la no portabilidad de documentos de identidad. *Tecnología, Investigación y Academia*, 39-45.

36. Serratosa, F. (2015). *La biometría para la identificación de las personas.* Catalunya: Universidad Oberta de Catalunya. Obtenido de https://sistemamid.com.ar/panel/uploads/biblioteca/2015-03-22_12-05-01117594.pdf

37. SIASA. (2011). *SIASA*. Obtenido de https://www.siasa.com/producto.php?prod=0100041

38. Sites, G. (s.f.). Obtenido de https://sites.google.com/site/sistemasbiometricoseliseoperez/home/reconocimiento-dela-geometria-de-la-mano

39. STMicroelectronics. (s.f.). *All Datasheet*. Obtenido de https://pdf1.alldatasheet.com/datasheet-pdf/view/22389/STMICROELECTRONICS/IRF520.html

40. Suprema. (s.f.). Obtenido de https://www.supremainc.com/es/solutions/facial-recognition-system.asp#:~:text=El%20dispositivo%20de%20reconocimiento%20facial,adem%C3%A1s%20de%20ofrecer%20varias%20posibilidades.

41. tecHNologia, C. (s.f.). *CYD tecHNologia*. Obtenido de https://cdtechnologia.net/sensores/465-modulo-lector-de-huellas-digital-as606.html

42. Tecnopura. (s.f.). *Tecnopura*. Obtenido de https://www.tecnopura.com/producto/mini-cerradura-electromagnetica-12v-tipo-solenoide/

43. TECNOSeguro. (s.f.). *TECNOSeguro*. Obtenido de https://www.tecnoseguro.com/productos/control-de-acceso/suprema-terminal-reconocimiento-facial-facestation-2

44. ti-America. (s.f.). *ti-America*. Obtenido de https://www.ti-america.com/respaldo-de-energia-ups/#:~:text=%C2%BFQu%C3%A9%20es%20un%20sistema%20UPS,en%20el%20suministro%20el%C3%A9ctrico%20principal.

45. Wikipedia. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Transistor_de_uni%C3%B3n_bipolar

X. Anexos

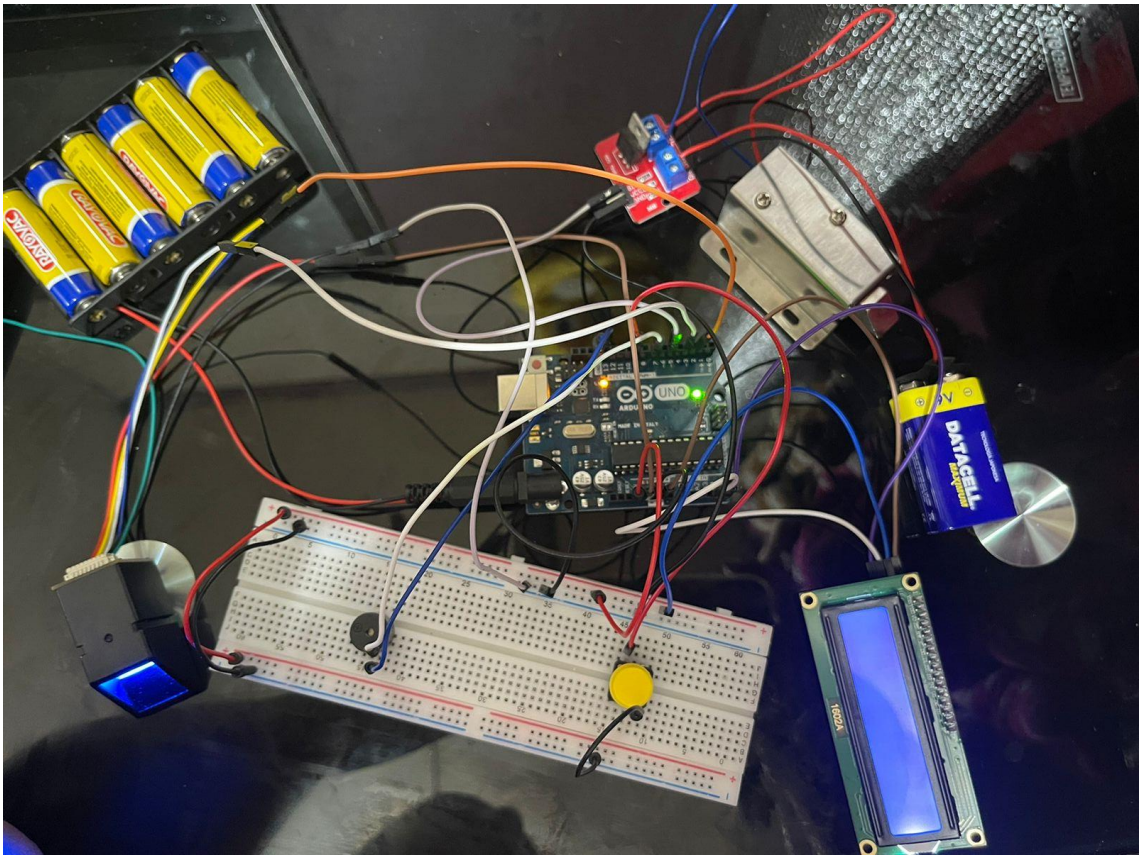


Figura 10.1 *Montaje del circuito.*

Technical Specification

EAGLE files: arduino-duemilanove-uno-design.zip Schematic: arduino-uno-schematic.pdf

Summary

Microcontroller	ATmega328
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Input Voltage (limits)	6-20V
Digital I/O Pins	14 (of which 6 provide PWM output)
Analog Input Pins	6
DC Current per I/O Pin	40 mA
DC Current for 3.3V Pin	50 mA
Flash Memory	32 KB of which 0.5 KB used by bootloader
SRAM	2 KB
EEPROM	1 KB
Clock Speed	16 MHz

the board

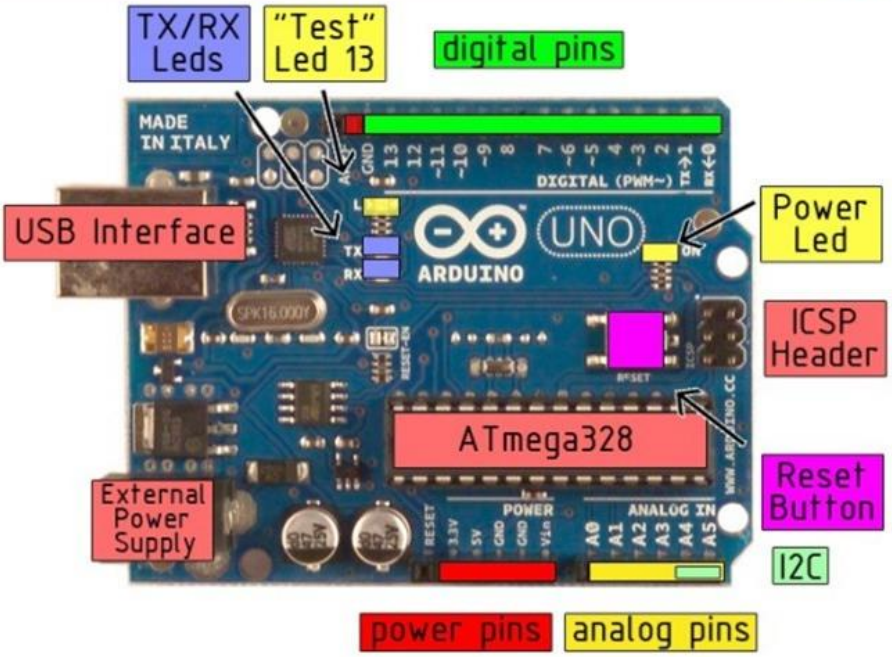


Figura 10.2 *Hoja técnica Arduino UNO.*

Secure your project with biometrics - this all-in-one optical fingerprint sensor will make adding fingerprint detection and verification super simple. These modules are typically used in safes - there's a high powered DSP chip that does the image rendering, calculation, feature-finding and searching. Connect to any microcontroller or system with TTL serial, and send packets of data to take photos, detect prints, hash and search. You can also enroll new fingers directly - up to 162 finger prints can be stored in the onboard FLASH memory.

We like this particular sensor because not only is it easy to use, it also comes with fairly straight-forward Windows software that makes testing the module simple - you can even enroll using the software and see an image of the fingerprint on your computer screen. But, of course, we wouldn't leave you a datasheet and a "good luck!" - we wrote a full Arduino library so that you can get running in under 10 minutes. The library can enroll and search so its perfect for any project (). We've also written a detailed tutorial on wiring and use (). This is by far the best fingerprint sensor you can get.

- Supply voltage: 3.6 - 6.0VDC
- Operating current: 120mA max
- Peak current: 150mA max
- Fingerprint imaging time: <1.0 seconds
- Window area: 14mm x 18mm
- Signature file: 256 bytes
- Template file: 512 bytes

- Storage capacity: 162 templates
- Safety ratings (1-5 low to high safety)
- False Acceptance Rate: <0.001% (Security level 3)
- False Reject Rate: <1.0% (Security level 3)
- Interface: TTL Serial
- Baud rate: 9600, 19200, 28800, 38400, 57600 (default is 57600)
- Working temperature rating: -20C to +50C
- Working humidy: 40%-85% RH
- Full Dimensions: 56 x 20 x 21.5mm
- Exposed Dimensions (when placed in box): 21mm x 21mm x 21mm triangular
- Weight: 20 grams

Figura 10.3 *Hoja técnica Sensor AS608.*

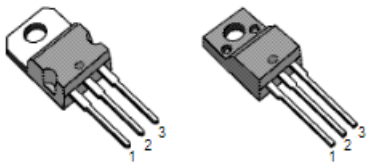
SGS-THOMSON MICROELECTRONICS

IRF520
IRF520FI

N - CHANNEL ENHANCEMENT MODE POWER MOS TRANSISTORS

TYPE	V_{DSS}	$R_{DS(on)}$	I_D
IRF520	100 V	< 0.27 Ω	10 A
IRF520FI	100 V	< 0.27 Ω	7 A

- TYPICAL $R_{DS(on)}$ = 0.23 Ω
- AVALANCHE RUGGED TECHNOLOGY
- 100% AVALANCHE TESTED
- REPETITIVE AVALANCHE DATA AT 100°C
- LOW GATE CHARGE
- HIGH CURRENT CAPABILITY
- 175°C OPERATING TEMPERATURE

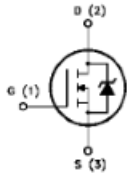


TO-220 ISOWATT220

APPLICATIONS

- HIGH CURRENT, HIGH SPEED SWITCHING
- SOLENOID AND RELAY DRIVERS
- REGULATORS
- DC-DC & DC-AC CONVERTERS
- MOTOR CONTROL, AUDIO AMPLIFIERS
- AUTOMOTIVE ENVIRONMENT (INJECTION, ABS, AIR-BAG, LAMPDRIVERS, Etc.)

INTERNAL SCHEMATIC DIAGRAM



ABSOLUTE MAXIMUM RATINGS

Symbol	Parameter	Value		Unit
		IRF520	IRF520FI	
V_{DS}	Drain-source Voltage (V_{GS} = 0)	100		V
V_{DGR}	Drain- gate Voltage (R_{GS} = 20 kΩ)	100		V
V_{GS}	Gate-source Voltage	± 20		V
I_D	Drain Current (cont.) at T_c = 25 °C	10	7	A
I_D	Drain Current (cont.) at T_c = 100 °C	7	5	A
I_{DM}(•)	Drain Current (pulsed)	40	40	A
P_{tot}	Total Dissipation at T_c = 25 °C	70	35	W
	Derating Factor	0.47	0.23	W/°C
V_{ISO}	Insulation Withstand Voltage (DC)	□	2000	V
T_{stg}	Storage Temperature	-65 to 175		°C
T_j	Max. Operating Junction Temperature	175		°C

(•) Pulse width limited by safe operating area

Figura 10.4 *Hoja técnica MOSFET IRF520.*

Figura 10.5 *Cerradura Kwikset Halo Touch.* ***(Amazon, s.f.)***

Figura 10.6 *Cerradura eufy Security Smart Lock Touch & Wi-Fi.* ***(Amazon, s.f.)***

Figura 10.7 *Candado de huellas dactilares BIRX.* ***(Amazon, s.f.)***

Tabla 10.1 Cronología de Trabajo.

Cronología de Trabajo										
Actividades Realizadas	**Semanas**									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Búsqueda de material de lectura										
Elaboración de primer avance										
Marco teórico										
Elaboración de segundo avance										
Adquisición de elementos										
Montaje de proyecto										
Pruebas del proyecto										
Elaboración del tercer avance										
Entrega Final										

En esta tabla se puede observar el tiempo en semanas de las actividades realizadas para concluir con la investigación.