Universidad Continental

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de Ingeniería Electrónica

Tesis

Diseño de un sistema antirrobo mediante huella dactilar para optimizar la seguridad de los vehículos M1 en Huancayo

Hector Manuel Maravi Aylas
Hector Fabricio Segura Sanchez

Para optar el Título Profesional
de Ingeniero Electrónico

Huancayo, 2024

Universidad Continental

INFORME DE CONFORMIDAD DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

A	:	Decano de la Facultad de Ingeniería
DE	:	Eulogio Alberto Pari Aguilar Asesor de trabajo de investigación
ASUNTO	:	Remito resultado de evaluación de originalidad de trabajo de investigación
FECHA	:	8 de Octubre de 2024

Con sumo agrado me dirijo a vuestro despacho para informar que, en mi condición de asesor del trabajo de investigación:

Título:
Diseño de un sistema antirrobo mediante huella dactilar para optimizar la seguridad de los vehículos M1 en Huancayo

Autor:
Hector Manuel Maravi Aylas – EAP. Ingeniería Electrónica
Hector Fabricio Segura Sanchez – EAP. Ingeniería Electrónica

Se procedió con la carga del documento a la plataforma "Turnitin" y se realizó la verificación completa de las coincidencias resaltadas por el software dando por resultado 18 % de similitud sin encontrarse hallazgos relacionados a plagio. Se utilizaron los siguientes filtros:

- Filtro de exclusión de bibliografía — SI [X] NO [ ]
- Filtro de exclusión de grupos de palabras menores — SI [X] NO [ ]
  N° de palabras excluidas **(10)**:
- Exclusión de fuente por trabajo anterior del mismo estudiante — SI [ ] NO [X]

En consecuencia, se determina que el trabajo de investigación constituye un documento original al presentar similitud de otros autores (citas) por debajo del porcentaje establecido por la Universidad Continental.

Recae toda responsabilidad del contenido del trabajo de investigación sobre el autor y asesor, en concordancia a los principios expresados en el Reglamento del Registro Nacional de Trabajos conducentes a Grados y Títulos – RENATI y en la normativa de la Universidad Continental.

Atentamente,

AGRADECIMIENTO

Agradecer a todas las personas en general que hicieron posible el progreso de mi formación personal y profesional a lo largo de todo este tiempo, cada uno de ellos tuvo un aporte muy importante en cada paso dado.

Asimismo, a la Universidad Continental por la formación integra que me brindó. A cada uno de mis docentes que de igual manera me brindaron los conocimientos necesarios. Llegando así gracias al apoyo de cada uno de las personas e institución mencionada.

Agradecido con cada uno de ellos y con la sociedad en general, en reciprocidad brindo este proyecto de investigación en beneficio del progreso y desarrollo de nueva tecnología, así como mejora de la seguridad de vida.

DEDICATORIA

Dedico esta tesis, en primer lugar, a mi abuelita Teodosia en agradecimiento a su soporte ilimitado en cada momento de mi vida, así como a mis padres, hermano y tías que fueron de gran apoyo en mi desarrollo personal y académico. A cada persona que fue parte de este proceso: docentes, compañeros de estudio y amigos que, con su apoyo, ideas, consejos; se pudo realizar esta tesis. Totalmente agradecido con cada uno de ellos.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Al analizar la actualidad que vive la ciudadanía de la provincia de Huancayo, se observa una cifra porcentual alta en inseguridad ciudadana teniendo así una tasa significativa en el de hurto de carros, debido a que el 3.7 % de ciudadanos sufrió este robo y el 1.5 % de las personas fue víctima de intento de robo de su carro.

Identificando la problemática que se vive en la provincia de Huancayo obtenidos en cifras porcentuales, se procede al diseño de un dispositivo de activación del sensor de par de la dirección del vehículo mediante huella dactilar optimizando así la seguridad del vehículo ante un posible robo, este dispositivo lleva consigo un sensor biométrico lector de huella dactilar donde se podrá almacenar las huellas dactilares de los dueños del vehículo, activando así el sensor de par de la dirección del vehículo, en caso contrario, si no está identificado la huella dentro del dispositivo este bloqueará el sensor de par de la dirección del vehículo impidiendo así el giro del volante, evitando así el robo de vehículos y dando tranquilidad a los usuarios.

Se tiene en consideración el procedimiento de ejecución en los distintos campos como la simulación respectiva del sistema donde analizamos el funcionamiento de los distintos componentes electrónicos, de igual forma se utilizó el análisis del diseño factorial 2^3, teniendo una mejor perspectiva de la utilización y la optimización de maximizar el comportamiento del dispositivo de activación del sensor de par.

Finaliza la tesis de investigación con resultados que se esperan obtener, logrando un sistema de seguridad efectiva con la activación del sensor de par de la dirección del vehículo mediante señales generadas a partir del uso de huellas dactilares y proporcionando una mejor calidad de seguridad en los vehículos M1 en la provincia de Huancayo

Palabras claves: sensor de par, huella dactilar, sensor biométrico, componentes electrónicos, diseño factorial, vehículos M1.

ABSTRACT

It begins with the analysis of the current situation experienced by the citizens of the Province of Huancayo, reaching a high percentage figure in citizen insecurity, thus having a significant rate in car theft, because 3.7% of citizens suffered this theft and 1.5% of people were victims of attempted theft of their car.

Identifying the problems experienced in the Province of Huancayo obtained in percentage figures, we proceed to the design of a device for activating the torque sensor of the vehicle's steering using a fingerprint, thus optimizing the security of the vehicle against possible theft, this device It carries with it a biometric fingerprint reader sensor where the fingerprints of the vehicle owners can be stored, thus activating the vehicle's steering torque sensor. Otherwise, if the fingerprint is not identified inside the device, it will block the fingerprint sensor. torque of the vehicle's steering, thus preventing the steering wheel from turning, thus preventing vehicle theft and giving users peace of mind.

The execution procedure is taken into consideration in the different fields such as the respective simulation of the system where we analyze the operation of the different electronic components, in the same way we make use of the analysis of the 2^3 factorial design, having a better perspective of the use and Optimizing to maximize the behavior of the torque sensor activation device.

The research thesis ends with the results expected to be obtained, achieving an effective security system with the activation of the vehicle steering torque sensor through signals generated from the use of fingerprints and providing a better quality of security in vehicles. M1 in the Province of Huancayo.

Key words: torque sensor, fingerprint, biometric sensor, electronic components, factorial design, M1 vehicles.

INTRODUCCIÓN

La constante innovación de tecnología en seguridad de vehículos conlleva a que la mayoría de personas obtengan dispositivos que resguarden la propiedad privada, es así como se realiza el diseño de un dispositivo de activación del sensor de par de la dirección del vehículo mediante huella dactilar optimizando así la seguridad del vehículo ante un posible robo, reduciendo así el gran porcentaje de vehículos hurtados en la provincia de Huancayo, asimismo mejorando los sistemas de seguridad ya vulnerados por el amigo de lo ajeno, que con el desarrollo de tecnología también han desarrollado equipos capaces de vulnerar dichos sistemas de seguridad. La presente tesis está compuesta en 5 capítulos.

Capítulo I: presenta el planteamiento y formulación del problema, la misma forma el problema general y problemas específicos, también se considera los objetivos de respuesta a cada problema planteado, justificación e importancia, los alcances de la investigación, limitaciones, descripción y operacionalización de variables del mismo modo están incluidos dentro del capítulo I.

Capítulo II: se consideran los antecedentes del problema, que incluye la revisión de tesis y artículos científicos que ayudan en el desarrollo del trabajo de investigación, de la misma forma se considera la base teórica y definición de términos básicos.

Capítulo III: se identifica la necesidad del problema y los requerimientos, así como la solución al problema, también se considera la prueba de solución (diseño de control, diseño de software y diseño electrónico) y la simulación del dispositivo en el programa Proteus.

Capítulo IV: una vez obtenido pruebas mediante la simulación, dentro del presente capitulo se realiza el análisis exhaustivo de resultados.

Capítulo V: se muestra el costo de inversión del trabajo de investigación.

Para seguir generando innovación tecnológica y haciendo frente a la delincuencia generada en la provincia de Huancayo se presenta esta tesis de aplicación tecnológica, con la que se pretende generar alternativas a los ya vulnerados sistemas de seguridad de los vehículos.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1. Fundamentación del problema

Internacionalmente, se han desarrollado sistemas de seguridad para prevenir la vulnerabilidad de los vehículos en caso de robos, pero con el pasar de los años se ha desarrollado diferentes dispositivos y modos de eludir dichos sistemas de seguridad. Actualmente, los sistemas antirrobo de vehículos se encuentran muy desfasados, además que las personas malintencionadas han encontrado distintas formas de evadirlas. Lamentablemente, la tecnología no se ha visto librada de los delincuentes y cada día es más la imaginación que se facilita para lograr un acto delictivo perfecto y sin marcas. El procedimiento favorito de los delincuentes es el actuar sin dejar evidencia de los hechos. Fácil, rápido y sin disputas es el acto delictivo perfecto para los delincuentes. Siguiendo dichos antecedentes, los delincuentes han desarrollado un dispositivo capaz de captar las señales que emiten las llaves con chip que activan el acceso de seguridad a los vehículos. "Encontrarse en un rango accesible de dos a tres metros es lo que se necesita el malhechor para acceder al control de su vehículo, dicho dispositivo tiene la similitud a una laptop que fácilmente y sin que se pueda notar capta la señal del chip y es almacenada en una memoria y sin importar donde se ubique su auto el malhechor accederá al mando del vehículo tal cual como si fuera suyo" (1).

"Perú es el segundo país con los números más altos de actos delictivos superado solo por Venezuela en Latinoamérica. Resultados presentados al INEI del semestre actual (Mar – Agos 2018) mostrado por el INEI, en el Perú una de las principales ciudades con un alto porcentaje de actos delictivos es la provincia de Huancayo, uno de los actos delictivos con un porcentaje alto es el robo de vehículos, ya que el 3.7% de la población ha sido víctima de algún incidente de este tipo, mientras que el 1.5% de la población de Huancayo son víctimas de intento de robo de vehículos" (2).

"Actualmente, según análisis de las entidades encargadas del tránsito y transporte de la provincia de Huancayo, se obtuvo un balance del parque automotor, detallando que se cuenta con 11 mil 636 vehículos M1 formales de servicio público, más los vehículos particulares e unidades no formales, contamos con aproximadamente 70 mil vehículos en circulación en la provincia de Huancayo" (3); dada estas cifras es por lo que los delincuentes encuentran en Huancayo un lugar con mayores posibilidades de realizar sus malas acciones.

1.2. Planteamiento y formulación del problema

1.2.1. Problema general

- ¿Cómo diseñar un sistema antirrobo mediante huella dactilar para optimizar la seguridad en vehículos M1 en Huancayo?

1.2.2. Problemas específicos

- ¿Cuál es el funcionamiento del sensor Biométrico en la implementación del sistema antirrobo mediante huella dactilar del vehículo?

- ¿En qué forma el sistema antirrobo del vehículo mediante huella dactilar optimiza la seguridad vehicular M1 en Huancayo?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

- Diseñar un sistema antirrobo del vehículo mediante huella dactilar para optimizar la seguridad en vehículos M1 en Huancayo.

1.3.2. Objetivos específicos

- Analizar el funcionamiento del sensor biométrico en la implementación del sistema antirrobo mediante huella dactilar del vehículo.

- Determinar en qué forma el sistema antirrobo del vehículo mediante huella dactilar optimiza la seguridad vehicular M1 en Huancayo.

1.4. Justificación e importancia

1.4.1. Justificación tecnológica

"Seguridad electrónica es uso de mejoras en la protección de la propiedad al impedir el acceso de personas no autorizadas" (4). El dispositivo por diseñar de activación del sensor de

par de la dirección del vehículo mediante huella dactilar optimizando la seguridad vehicular se ha desarrollado teniendo en cuenta lo avances tecnológicos en la ingeniería electrónica ya que el sistema de digitalización dactilar es uno de los más seguros.

1.4.2. Justificación teórica

Este dispositivo se ha desarrollado teniendo en cuenta que la vulnerabilidad de los sistemas y dispositivos de seguridad son violentados frecuentemente por la poca consistencia de lo mismo, destacando teóricamente que el sistema de digitalización dactilar es uno de los más seguros por no encontrarse una similitud en los seres humano, lo que justifica que la medida de seguridad a implementarse busca dar al conductor la seguridad de obtener un sistema muy eficaz, el que permitirá a los propietarios de los vehículos poder transitar con más libertad, despreocupación y confianza. “La biometría es un procedimiento de reconocimiento de individuos establecido en las descripciones físicas y/o fisiológicas, cada vez más útil para tecnologías relacionados con la seguridad” (5).

1.4.3. Justificación social

Los índices de vulnerabilidad de los vehículos se ha incrementado de manera que no existe medidas de seguridad efectivas en el ámbito de protección del vehículo, visto esta problemática y habiéndome desarrollado durante estos años académicos en la EAP Ingeniería Electrónica, me conlleva a desarrollar este dispositivo, destacando que esta implementación es dirigida a los vehículos, devolviéndole a la sociedad la confianza de poder parquear o estacionar su vehículo mientras realiza sus actividades cotidianas, de este modo se reducirá en gran cantidad el porcentaje de apropiación ilícita de vehículos, ya que el dispositivo a imponerse tendrá la efectividad esperada.

1.4.4. Justificación metodológica

La metodología fundamental para la evolución de desarrollo para proyectos en la ingeniería electrónica es tener variedad de ideas y tecnologías para la ejecución de mejoras tecnológicas en el ámbito de la instrumentación electrónica, así como su objetivo principal es satisfacer las necesidades y desarrollo de nueva tecnología, es así como la implementación de un dispositivo de activación del sensor de par de la dirección del vehículo mediante huella dactilar genera nuevos campos de desarrollo tecnológico en la ingeniería electrónica, con un alto porcentaje de nivel de seguridad y protección de vehículos en la provincia de Huancayo.

1.5. Delimitación del proyecto

1.5.1. Limitaciones económicas

La realización del proyecto de investigación trae consigo la accesibilidad de poder contar con los componentes electrónicos a costos económicos, por lo mismo la accesibilidad de costo para la población.

1.5.2. Limitaciones bibliográficas

Se asumió limitaciones al momento de recopilar bibliografía acerca de investigaciones referentes al uso de tecnología biométrica en seguridad vehicular.

1.5.3. Limitaciones de diseño

Una de las principales limitaciones que más afecto el desarrollo del proyecto en el proceso de diseño y simulación, fue el de no contar con el sensor biométrico dentro de libreras de programas de simulación y/o diseño.

1.6. Hipótesis

1.6.1. Hipótesis general

- El diseño del sistema antirrobo mediante huella dactilar optimiza la seguridad de los vehículos M1 en Huancayo.

1.6.2. Hipótesis específicas

- El funcionamiento del sensor biométrico se activa en la implementación del sistema antirrobo mediante huella dactilar del vehículo.

- El sistema antirrobo del vehículo funciona correctamente mediante huella dactilar optimizando la seguridad vehicular M1 en Huancayo.

1.7. Variables y operacionalización de variables

Tabla 1. ***Operacionalización de variables***

Título:	Diseño de un sistema antirrobo mediante huella dactilar para optimizar la seguridad de los vehículos M1 en Huancayo	
Problema	¿Cómo diseñar un sistema antirrobo mediante huella dactilar para optimizar la seguridad en vehículos M1 en Huancayo?	
Variables	Independiente	Dependiente
	Diseño de un sistema antirrobo mediante huella dactilar	Optimización de la seguridad de los vehículos M1 en Huancayo
Definición conceptual	Uso de un sensor biométrico de lectura de huella dactilar para activar el sensor de par del vehículo con rasgos físicos únicos de	Mejorar la seguridad vehicular ya vulnerada, en sus diferentes tipos de seguridad ya sea llaves, chips alarmas,
Definición operacional	Variable que detectan rasgos físicos accionando así elementos fundamentales de movimiento	Variable que detectan la optimización de la seguridad de vehículos en el parque automotor

Tabla 2. ***Descripción de variable independiente***

Variable independiente	Diseño de un sistema antirrobo mediante huella dactilar			
Dimensiones o subvariables	Indicador	Unidad	Tipo de variable	Instrumento
Sensor biométrico	Tiempo de adquisición	Milisegundos	Numérica Continua	Temporizador del Sensor
Flujo de corriente	Distribución de corriente	Amperios	Numérica Continua	Amperímetro
Flujo de voltaje	Distribución de voltaje	Voltaje	Numérica Continua	Voltímetro

Tabla 3. ***Descripción de variable dependiente***

Variable depen	Optimización de la seguridad de los vehículos M1 en Huancayo			
Dimensiones o subvariables	Indicador	Unidad	Tipo de variable	Instrumento
Tiempo de respuesta	Tiempo de accionamiento	Milisegundos	Numeral continua	Timer On/Off
Accionamiento del sistema	Señal de salida	Frecuencia	Numeral continua	Osciloscopio

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Artículos científicos

Ciertamente que los métodos utilizados como llaves, chips o claves en seguridad se encuentran vulnerados, por consiguiente, el uso de biometría como reconocimiento inequívoco de personas basados en rasgos físicos beneficia considerablemente en desarrollo proyectos de seguridad, en consecuencia, León, en el año 2011 presenta el artículo científico titulado: "Avances en técnicas biométricas y sus aplicaciones en seguridad" (6) dado a conocer los beneficios de la implementación de técnicas biométricas en la seguridad de la sociedad.

El reconocimiento de rasgos físicos genera altos índices de seguridad, siendo eficiente y eficaz dentro del campo a desarrollarse, por lo que, Cortés, Medina y Muriel en el 2010 presentan el artículo científico titulado: "Sistemas de seguridad basados en biometría" (7). Teniendo como objetivo principal de exponer las distintas descripciones al momento de implementar dispositivos de seguridad basados en descripción biométrica.

En el 2009, Pro, Gonzales, Contreras y Yáñez presentan el artículo científico titulado: "Tecnología biométrica aplicada a la seguridad en organizaciones" (8) teniendo como propósito principal la aplicación de la biometría en campos donde la seguridad se hacen cada vez más vulnerables, ocasionando pérdidas económicas y afectando la integridad de las personas.

2.1.2. Tesis

El sistema de seguridad que se ha estado diseñando hace un tiempo por la fuerte necesidad de los conductores de cuidar su integridad física o su vehículo; en varios países la mayoría de los establecimientos públicos o privados cuentan con diferentes sistemas de seguridad, como sistemas de circuitos cerrados de video – cámara y sistema de alarma (sensor, alarma, etc.), Pero, estos sistemas han sido vulnerados no cumpliendo así con la eficiencia a desarrollarse en el ámbito de seguridad. Por lo que en los últimos años se está empleando con gran eficiencia el uso de sistemas de huella dactilar o sensores biométricos teniendo consigo mayor seguridad en el tema de acceso a la propiedad privada.

Es necesario encontrar un método de autenticación seguro y que no cause confusión, debido a este problema nacieron los sistemas biométricos, que le dan gran importancia y valor a la confidencialidad, integridad y disponibilidad de la información, bajo esta premisa, en el año 2017; Giraldo y Gómez, en la Ciudad de Bogotá, desarrollaron el proyecto de tesis titulado: "Estado del arte de la seguridad en sistemas biométricos" (9).

La ciudad Arica, Soto, 2014 presenta la investigación titulada: "Diseño de un sistema de seguridad en base a control, monitoreo, y visualización de acceso mediante huella dactilar a la Clínica San José de Arica" (10), en este documento destaca el empleo del sistema de seguridad mediante huella dactilar realiza el acceso de personas al recinto.

En el año 2009, Lizano, Palacios, Vargas y Leyton, presentaron un trabajo de investigación titulado: "Estudio y diseño de sistema de vigilancia y monitoreo de video a tiempo real, sobre una red IP, para un terminal de despacho y bombeo de combustible de gerencia regional sur PETROCOMERCIAL" (11) que tiene el objetivo es sentar las bases para el funcionamiento de sistemas de vigilancia en redes IP como alternativa a los servicios tradicionales de seguridad y detección de intrusos.

En la actualidad se encuentran en marcha una gran cantidad de proyectos, estudios e investigaciones diversas sobre el uso de sistemas de seguridad, que contribuyen significativamente al beneficio de la sociedad.

2.2. Bases teóricas

2.2.1. Sistema antirrobo del vehículo

Conforme se iba desarrollando la fabricación de los autos, los sistemas de seguridad de los vehículos iban evolucionando ya que se sentía el gran incremento de la delincuencia en general. Es por lo que, los autos de marca Toyota y modelo Yaris contaban con un sistema de seguridad,

que consistía en pestillos mecánicos que eran accionados con la llave del mismo vehículo. Con este sistema se pensaba hacer del Toyota Yaris un auto seguro por el hecho de que las llaves eran únicas para cada auto; es decir, que los pestillos no se accionaban siempre y cuando introdujeran la llave fabricada con ranuras únicas. Además "estos sistemas también ofrecen al conductor espejos retrovisores que eran accionados mecánicamente, mediante un pin que se utilizaba como la especie de una palanca y regulaba al espejo acorde el conductor prefería" (13). Esto contaba como parte del sistema de seguridad, además que ofrecía mayor comodidad al conductor.

2.2.2. Biometría

La palabra biométrico se deriva de las palabras bios (vida) y metric (medición), por lo que se refiere a que todos los dispositivos biométricos se basan en una tecnología de seguridad que mide e identifica algunas características físicas únicas e intransferibles que serán diferentes... de los seres vivos...

Tabla 4. ***Comparativa de sistema biométrico***

comparación de tecnología biométrica					
Tipo.	Universalidad.	Precisión.	Facilidad de uso	Aceptación de los usuarios.	Estabilidad a largo plazo.
Análisis de firma dinámica.	Bajo.	Bajo.	Alto.	Muy Alto.	Medio.
Imagen facial.	Bajo.	Bajo.	Medio.	Medio.	Medio.
Huella digital.	Alto.	Alto.	Alto.	Alto.	Alto.
Geometría de la mano.	Medio.	Medio.	Alto.	Alto.	Medio.
Reconocimiento del iris.	Alto.	Muy Alto.	Alto.	Medio.	Alto.
Teclado.	Bajo.	Bajo.	Alto.	Desconocido.	Desconocido.
Huella de la palma.	Medio/Alto.	Medio/Alto.	Alto.	Desconocido.	Desconocido.
Escaneo de retina.	Muy Alto.	Alto.	Bajo.	Bajo.	Alto.
Contacto de piel.	Alto.	Desconocido.	Desconocido.	Desconocido.	Desconocido.
Verificación de voz.	Bajo.	Bajo.	Alto.	Alto.	Medio.
Biométrica vascular.	Medio/Alto.	Medio.	Medio/Alto.	Alto.	Alto.
ADN.	Alto.	Alto.	Bajo.	Alto.	Muy Alto.
Forma del oído.	Alto.	Desconocido.	Medio.	Desconocido.	Desconocido.
Forma de caminar.	Medio.	Desconocido.	Alto.	Desconocido.	Bajo.

Tomada de "Manual de Aplicación de Tecnologías Biométricas", EEUU 2008.

En este proyecto se analizaron las ventajas y desventajas de cada sistema existente, y se determinó que el uso de huellas dactilares era la mejor solución por su alta seguridad y familiaridad con el uso de este dispositivo.

La identificación mediante huellas dactilares es una de las aplicaciones más representativas de la tecnología biométrica. Una huella digital consta de una serie de surcos, cuyos extremos o puntas se denominan detalles diminutos, cada uno de los cuales tiene una ubicación característica y única que puede medirse. Comparando esta distribución se puede obtener la identidad de la persona que intenta acceder a un sistema universal mensurable. Comparando esta distribución se puede obtener la identidad de la persona que intenta acceder al sistema universal, como se muestra en la figura que describe estos puntos de digitalización de huellas dactilares.

Figura 1. Punto minucia de huellas dactilar

2.2.2.1. Huella dactilar

La idea de huella dactilar puede hacer referencia a dos situaciones diferentes, aunque cabe destacar que en ambos casos están relacionadas con la seguridad y la identificación personal. En un caso, las huellas dactilares se refieren a las huellas dactilares de una persona, que se utilizan para identificarla de forma única. "En este caso, las huellas dactilares son uno de los principales medios utilizados para identificar a las personas a nivel nacional porque las huellas dactilares de cada persona son diferentes, incluso; aunque sean gemelos" (14). Gracias a esto, Cada persona tendrá una huella dactilar única e irrepetible, por lo que se aprovecha este aspecto para identificar eficazmente a cada persona. De esta manera, se tomarán las huellas dactilares de cada niño y se almacenarán para su uso futuro. Las huellas dactilares han ayudado a resolver muchos delitos y ahora se utilizan en sistemas de identificación biométrica.

2.2.2.2. Digitalización de huella dactilar

El primer paso en un sistema biométrico es registrar una descripción física y/o de comportamiento. Dependiendo del tipo de sistema biométrico, se procesan mediante algoritmos numéricos. Estos algoritmos pueden estar basados en detalles, basados en modelos o híbridos. En nuestro diseño, utilizamos este último algoritmo porque es más confiable, integra la precisión de los algoritmos basados en detalles y la velocidad comparativa de los algoritmos basados en muestras, y complementa la información almacenada en la base de datos. Luego, al acceder, el sistema comparará el algoritmo numérico leído con el algoritmo contenido en la base de datos creada previamente. Si hay una discrepancia, el sistema denegará el acceso; de lo contrario, permitirá el acceso. La tecnología actual tiene diferentes tasas de error que van del 60% al 99,9%, dependiendo de la calidad y precisión del lector.

La eficacia de una medición biométrica suele estar determinada por la tasa mínima de aceptación falsa (FAR), que es el porcentaje de huellas dactilares que no están en la base de datos que se aceptan como válidas, y la tasa de rechazo falso (tasa de falsas coincidencias o FNMR). , también conocida como tasa de falso rechazo, FRR), es posibilidad de que la persona real no sea identificado, debido a esto, se le niegue el acceso.

Durante la autenticación (o verificación), las descripciones biométricas se comparan únicamente con la descripción de la plantilla almacenada, proceso también conocido "uno a uno" (1:1); Lo más probable es que este proceso implique conocer la identidad de la persona que se está autenticando, por lo que esta persona ha presentado algún tipo de credenciales que serán verificadas o no verificadas después de aprender el proceso de autenticación biométrica.

Durante el proceso de reconocimiento, las descripciones biométricas se comparan con las descripción de un conjunto de plantillas almacenadas, proceso también conocido uno a N (1:N); Este proceso supone que, sin conocer la supuesta identidad de la persona, se obtiene una nueva muestra de los datos biométricos del usuario y se compara uno a uno con las muestras que ya están en el registro. El resultado de este proceso es la identidad del individuo y es un valor de verdadero o falso en el proceso de autenticación.

2.2.2.3. Sensor huella dactilar

El sensor de huella dactilar o biométrico ha sido desarrollado en el campo de la ingeniería electrónica con la capacidad de guardar, reconocer y leer huellas dactilares, este sensor dactilar también conocido como sensor biométrico escanea datos de cualquier dedo de una persona. En su mayoría el ser humano escanea el dedo pulgar, todos los sensores biométricos tienen un

componente sensible al tacto que al poner el dedo registrado sobre el cristal se encenderán leds del sensor dactilar. El sensor es energizado con una Nota de 3.3 a 5 voltios de corriente directa y una tensión negativa y además cuenta con dos salidas que son recepción y transmisión que por medio de estos dos cables trasmite datos hacia un módulo de control que en este caso es un arduino. Este sensor tiene la capacidad de registrar hasta 162 huellas dactilares. Los sensores dactilares pueden cumplir la función de trabajar como switch o interruptores para abrir o cerrar un circuito, siendo utilizado como medidas de seguridad para grandes bóvedas o pequeñas cajas fuertes. El sensor dactilar hoy en día es el más usado si se trata de seguridad esto es por seguridad que brinda ante cualquier circunstancia. Este sistema se utiliza para controlar el ingreso y la salida de los empleados en una empresa, en los cajeros automáticos, en los bancos y acceso a zonas restringidas etc. "Este sistema es el que brinda más seguridad y más efectivo, de 1 000 casos solo uno da como resultado error y su grado de aceptación al momento que una persona se registra es de 99 % comparadas con distintos sistemas de seguridad que se encuentra en el mercado" (14).

2.2.2.4. Estándar de tecnología biométrica

A nivel internacional, el único órgano coordinador de la normalización biométrica corresponde al Subcomité 17 (SC17) del Comité Técnico Conjunto sobre Tecnología de la Información (ISO/IEC JTC1), la Organización de Normas Internacionales de Química (ISO) y la Comisión Electrotécnica Internacional (CEI).

Las normas más relevantes son:

- Estándar ANSI / INCITS 358-2002

El estándar fue creado por ANSI en 2002 y se llama BioAPI 1.1. (Interfaz de programación de aplicaciones biométricas) es una interfaz de comunicación diseñada para utilizar equipos existentes con procedimientos de prueba para garantizar la interoperabilidad de productos y sistemas y verificar el cumplimiento del estándar BioAPI con otros estándares biométricos.

- CBEFF o NISTIR 6529

Estándares CBEFF (Formato Común de Intercambio Biométrico): Este conjunto de estándares ha sido desarrollado por varias organizaciones internacionales de estandarización, como el Comité Técnico de Biometría M1 del Comité Internacional de Estándares de Tecnología de la Información (INCITS) y el Comité Técnico Conjunto 1 (JTC) ISO/IEC. 1) SC 37 – El Subcomité de Biometría define las estructuras de datos básicos, conjuntos de elementos y valores que respaldan el intercambio directo de datos biométricos en un Repositorio de datos biométricos (BIR) diseñado para revelar el formato y la identidad de los datos biométricos. BIR

Otros atributos sin revelar el uso de los datos biométricos en sí manteniendo la confidencialidad de los datos biométricos.

La versión original de este estándar CBEFF se publicó como NISTIR 6529. Grupo de interfaz TeleTrusT.

- NISTIR 6529-A o ANSI INCITS 398-2005

El NISTIR 6529-A se lanzó el 5 de abril de 2004 y es una versión mejorada del NISTIR 6529 con compatibilidad y rendimiento mejorados. INCITS ha sido adoptado como estándar nacional estadounidense y publicado como ANSI INCITS 398-2005.

- ANSI 378

Creado por ANSI en 2004, define un estándar para la presentación e intercambio de información de huellas dactilares utilizando detalles finos. El propósito de esta norma es permitir que los sistemas biométricos de huellas dactilares utilicen información biométrica de otros sistemas para realizar procesos de autenticación e identificación.

- Estándares Internacionales

El 2003, empezó un proyecto para desarrollar una versión mundial de CBEFF y piezas de la norma se han publicado en las normas ISO/IEC. Las diversas partes de las Normas Internacionales que se han publicado incluyen:

- ✓ Parte 1: ISO/IEC 19785-1 cubre especificación de elementos de datos publicada en mayo de 2006 revisó el formato estándar ISO/IEC 197974-2 para el intercambio de datos.
- ✓ Parte 2: Procedimientos operativos de inscripción biométrica, publicados en mayo de 2006, revisados para incluir la inscripción adicional requerida por ISO/IEC 197974-2.
- ✓ Parte 3: En diciembre de 2007 se publicó una especificación de formato de muestra con cambios para reflejar los nuevos elementos de datos agregados por el CBEFF en la Parte 1.

2.2.2.5. Funcionalidad del sistema biométrico con huella dactilar

Todos los sistemas biométricos tienen una base operativa muy similar, ver Figura 2, que muestra las diferentes etapas de operación de estos sistemas e identifica cuatro procesos principales: recopilación de datos, almacenamiento de datos, procesamiento de señales y toma de decisiones.

Esto se describe en detalle a continuación en relación con el sistema biométrico basado en huellas dactilares que sustenta este proyecto.

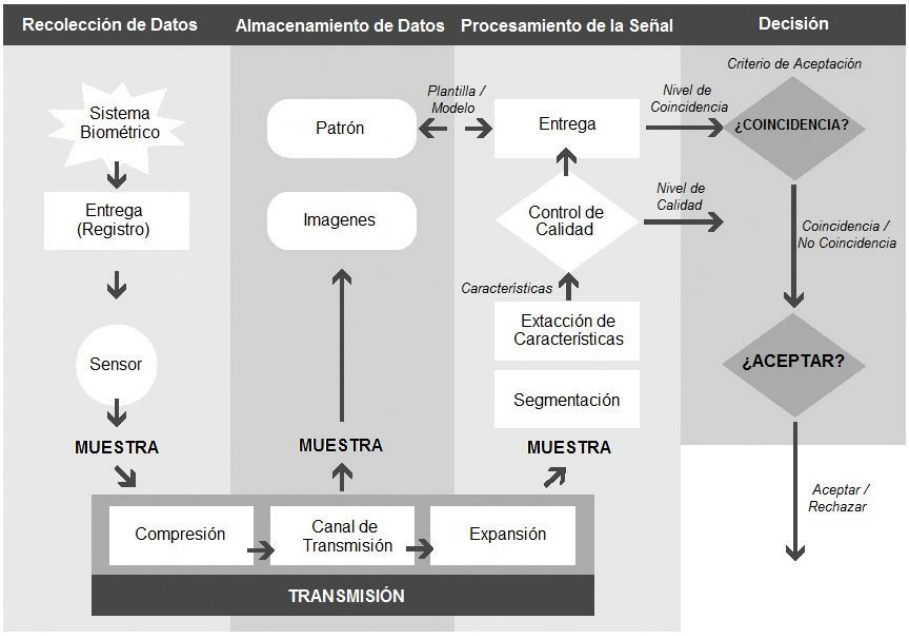


Figura 2. Estructura de funcionalidad del sistema biométrico
Tomada de Biometría básica, Manual de Aplicación de Tecnologías Biométricas, Estados Unidos 2008.

1. **Recopilación de datos:** este primer paso se configurará el parte biométrico utilizado, en este caso mediante huellas dactilares.

Para ello, el usuario coloca su dedo sobre el sensor de manera que el punto de luz se dirija hacia el material óptico o prisma que refleja la imagen de regreso al dispositivo de captura de imágenes, como se muestra en la Figura 1.3. en la imagen. Esta información se comprime y almacena. La transmisión depende de si el sensor accede a un nuevo usuario o prueba muestras utilizando información almacenada.

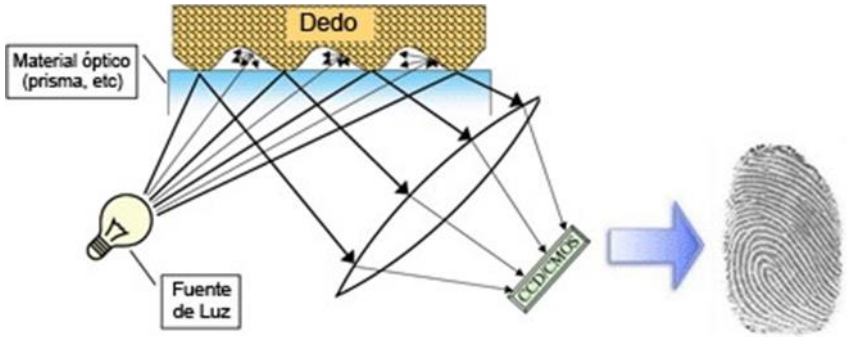


Figura 3. Captura de huellas digitales

2. **Acumulación de datos:** En este proceso, el sensor debe configurarse en modo de almacenamiento y luego la imagen capturada se captura y se transforma en datos matemáticos utilizando los puntos de referencia, ya que tienen su propia descripción, como

tipo de punto, ubicación y orientación, con la ayuda de un algoritmo. En un modelo matemático llamado modelo. Esta plantilla se almacena en la memoria del dispositivo o en un dispositivo externo, creando una base de datos con la que se compararán las huellas dactilares del usuario para una verificación adecuada, como se muestra en la Figura 4.

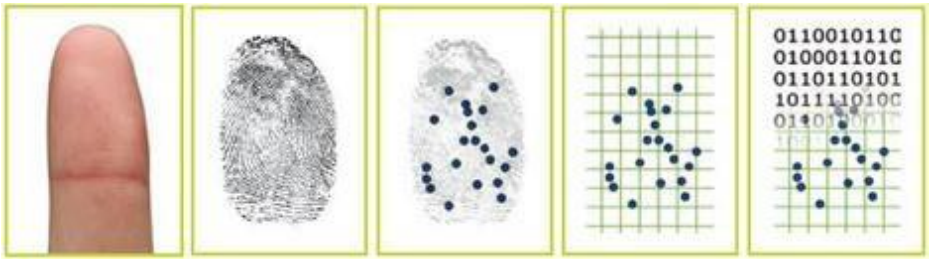


Figura 4. Toma de información para la digitalización

3. **Análisis de la señal:** En esta etapa, el sensor debe estar en modo de verificación de perfil, donde el perfil se segmenta y los descriptores clave se extraen de las huellas dactilares. Estas descripciones se verifican mediante control de calidad de muestras. Si no se encuentra la mejor calidad, se rechaza y no se realiza ninguna validación. Si la muestra es de buena calidad entrará en la fase de decisión.

2.2.3. Elección de partes para el sistema de seguridad

Para comprender los componentes necesarios para que el sistema funcione correctamente, es necesario conocer el diagrama del circuito funcional de la alarma.

- **Esquema de preparación del carro**

Se podrá ver los circuitos que se emplean para encender el coche encendiendo la bomba de combustible eléctrica. Este circuito se puede utilizar en motores con carburador, sistemas de inyección de combustible, así como en automóviles con inyección de combustible diésel.

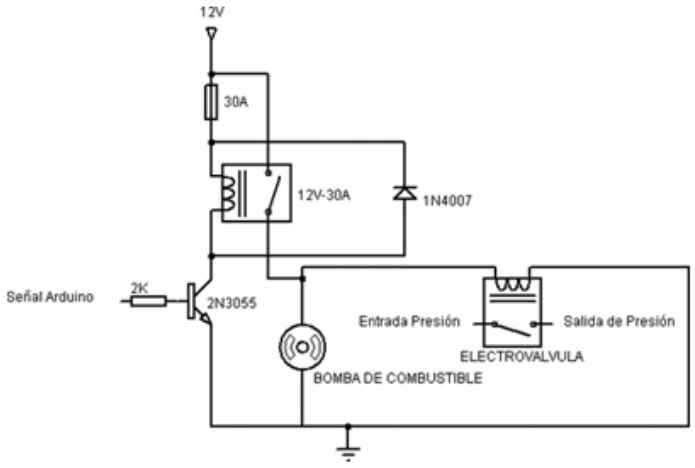


Figura 5. Esquema acondicionamiento de bomba de combustible eléctrica

Si su motor está equipado con bomba de combustible mecánica, la bobina encendida puede perder potencia.

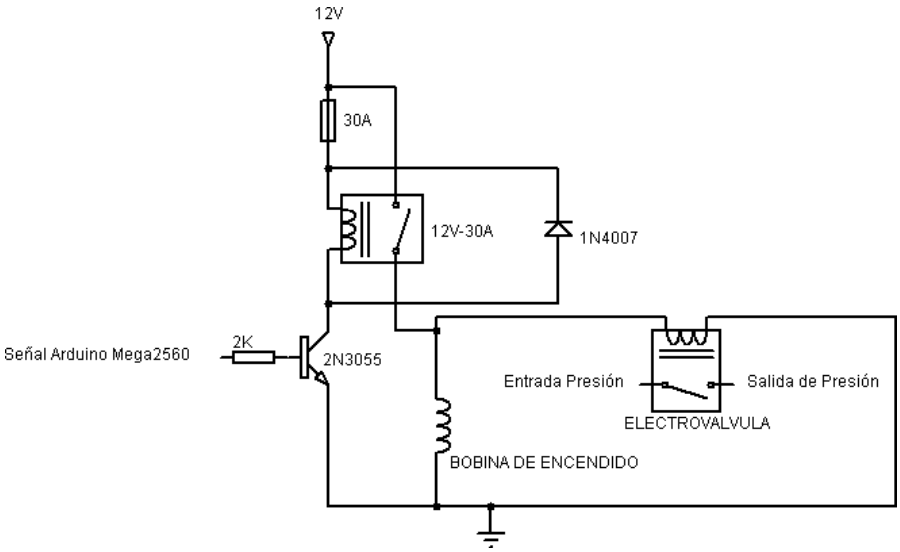


Figura 6. Diagrama de conexión de la "bobina de encendido"

- **Esquema de fase de hurto del carro**

Este paso utiliza 2 reguladores de voltaje (7805) conectados al cable negativo de alimentación de la batería y al cable del interruptor de encendido. Convierten el voltaje de 12 V a 5 V recibir señales en los módulos Arduino para la siguiente conexión con el propietario del automóvil.

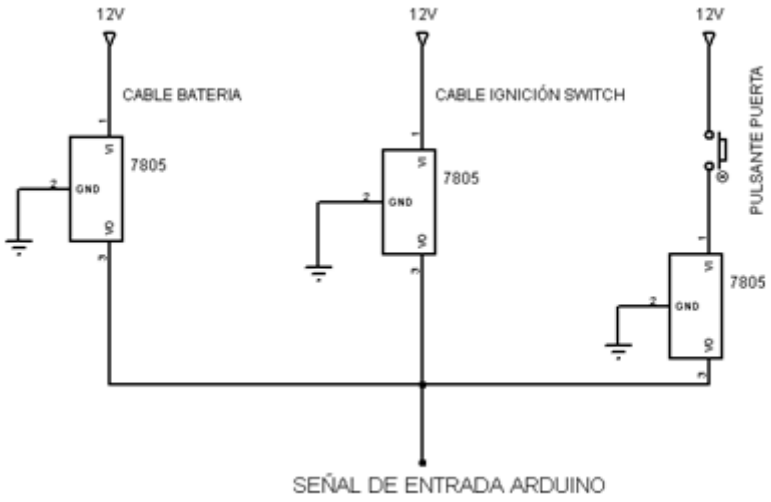


Figura 7. Esquema de fase de hurto del carro

- **Diagrama fase de hurto del carro**

El funcionamiento de este circuito es muy sencillo, al presionar uno de los 3 interruptores ubicados en las áreas críticas del auto, enviarán una señal al Arduino y bloquearán el acceso total al vehículo.

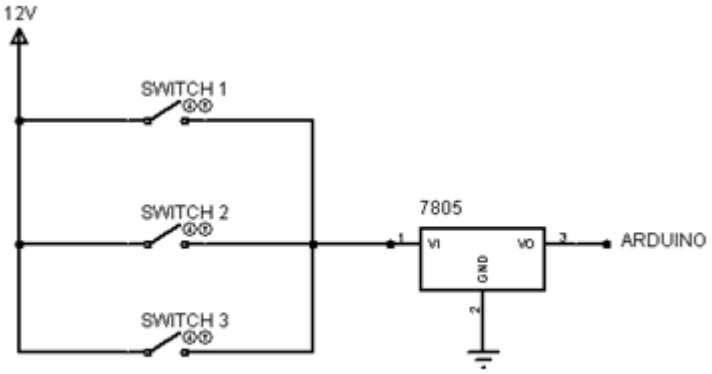


Figura 8. Diagrama circuito eléctrico hurto de carro

Una vez decidido el método de diseño, se procede a la selección de los elementos principales que aseguren el adecuado montaje y funcionalidad del circuito.

- **Circuito al 100%**

Mostramos el prototipo del sistema de seguridad.

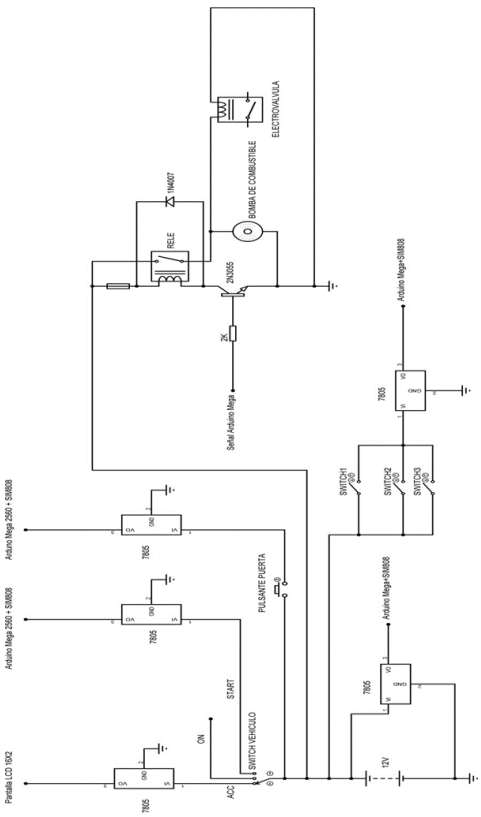


Figura 9. Esquema del circuito ala 100%.

2.2.3.1. Arduino UNO

Arduino es uno de los sistemas más complejos en ingeniería porque está basado en ATMega328P y está diseñado para hacer que la programación de microcontroladores sea simple e intuitiva. La comunicación entre el ordenador y el Arduino es a través del puerto USB, y en ocasiones basta con conectarlo como impresora.

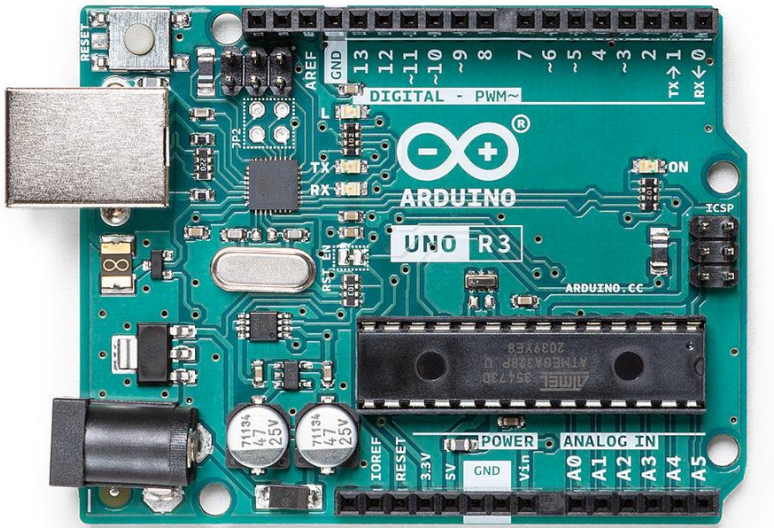


Figura 10. Arduino UNO
Tomada de Electronics

Tabla 5. ***Ficha técnica Arduino UNO***

Descripción Arduino UNO	
Microcontrolador.	ATmega328P
Voltaje Operativo.	5V
Voltaje de Entrada.	7-12V
Límite de Voltaje de Entrada.	6-20V
Pines digitales de entrada y salida.	14
Pines de E/S digitales PWM.	6
Pines analógicos de entrada.	6
Frecuencia de reloj.	16MHz
Longitud.	68.6mm
Ancho.	53,4mm
Peso.	25 gr

Tomada de Electronics

a) Ventajas

- Se puede integrar un sistema altamente programable.
- Tiene 14 puertos digital, 6 puertos PMW y 6 puertos analógico.
- Tiene memoria 32 KB y voltaje de 5V DC.
- Fácil adaptabilidad y alta flexibilidad ya que la programación en la que trabaja es de código abierto y este Arduino funciona para distintos proyectos.
- El bajo costo que tiene la placa Arduino y sus demás componentes.

b) Pines Arduino

Arduino UNO nos facilita la funcionalidad necesaria para poder acceder a los pines digitales de una manera sencilla. Estas funciones son pinMode, digitalWrite y digitalRead.

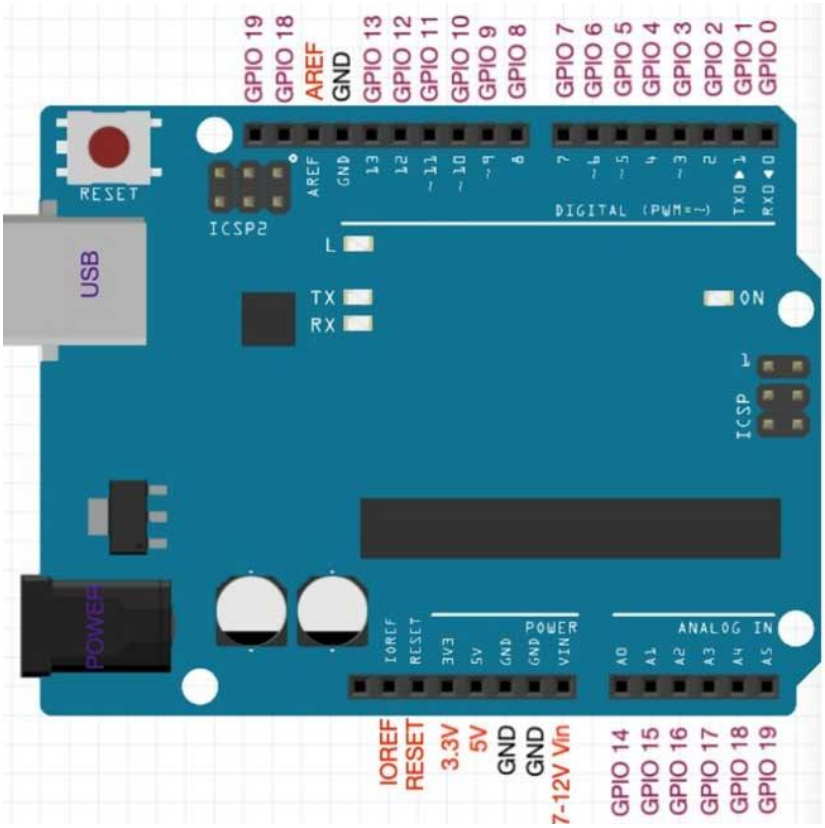


Figura 11. Diagrama Pines Arduino UNO
Tomada de Electronics

2.2.3.2. Relé automotriz 12V-30A

La comunicación de líneas de media a alta potencia a través de circuitos electrónicos de baja potencia se logra mediante relés, los cuales son componentes electromagnéticos cuya principal ventaja y motivo de su uso frecuente en electrónica es que las líneas eléctricas quedan

completamente aisladas de la fuente de energía. Dicho esto, podemos destacar que podemos crear circuitos electrónicos con la ayuda de relés (temporizador, fotocélula, etc.).

El relé utilizado consta de 4 polos 12 V - 30 A, la tensión y la corriente se han seleccionado en función de batería y los parámetros de función del coche. (Idrowo, 2017).

Figura 12. Relé Automotriz 12V -30A.
Tomada de Electronics

a) Descripción relé automotriz

Tabla 6. ***Descripción Relé Automotriz***

Descripción relé automotriz.	
Numero terminales.	04
Voltaje alimentación.	12V
Amperaje operación.	30A
Longitud.	53.1mm
Ancho.	27.8mm
Alto.	16.8mm

Tomada de M Y B Electronico S.A.

2.2.3.3. Display LCD 12X6

Uno de los métodos más económicos y sencillos es una pantalla LCD, que dota a nuestro proyecto de una pantalla que nos permite ver resultados importantes en el sistema automatizado. Tienen diferentes especificaciones ya que se fabrican en diferentes tamaños como LCD 16X2 (2 líneas y 16 caracteres), 20x4, 20x2 y 40x2. Dedicadas a pantallas LCD monocromáticas, hay un máximo de 80 caracteres alfanuméricos. Tienen retroiluminación azul o verde y un pin que permite cambiar el contraste de la pantalla LCD mediante un potenciómetro Arduino.

Figura 13. Display LCD 16 x 2.
Tomada de Física con Arduino.

a) Descripción display LCD 16x2

Tabla 7. ***Descripción display LCD***

Descripción display LCD 16 x 2	
Voltaje alimentación	5V
Backlight.	Azul
Tamaño carácter.	5.23 x 3 mm
Nro. carácter por línea	16x2
Color carácter.	Blanco.

Tomada de Física Arduino

b) Ventaja display L.C.D. 16 x 2.

- Dispositivos utilizan una cantidad mínima de energía o corriente, son fáciles de programar y, por lo general, los carga el fabricante.
- Consisten en lámparas fluorescentes y consiguen un alto contraste de color.
- Son delgadas.

c) Pin display LCD 16x2

Figura 14. Diagrama de pin display L.C.D. 16 x 2
Tomada de Microcontrollerslab, 2020

2.2.3.4. Lector huella dactilar AS608

Es un sensor biométrico que permite un sistema de procesamiento de imágenes digitales mediante un procesador de señal, incluyendo la comparación de la imagen procesada con una base de datos. Este dispositivo utiliza protocolo serial por lo que puede usarse con cualquier microcontrolador o placa de desarrollo. Se pueden almacenar hasta 162 huellas dactilares en la memoria del dispositivo.

Figura 15. Sensor de huella digital AS608.
Tomada de Unit Electronics.

a) Descripción AS608

Tabla 8. ***Descripción módulo AS608.***

Descripción sensor AS608.	
Voltaje de alimentación	3.6 a 6 V.
Corriente funcionamiento.	120mA
Tiempo entrada imagenescaneada.	<1seg
Temperatura trabajo.	-20°C a 50°C

Tomada de Unit Electrónicos

b) Pines módulo AS608

El módulo dispone de un total de 8 contactos, 02 alimentación y 06 entrada y salida de datos. Proporcionado al proyecto para que almacene y reconozca la huella digital necesitamos conectar los 4 pines que están:

- V+: alimentación 5v
- G N D: tierra
- T X: transmite dato
- R X: recibe dato

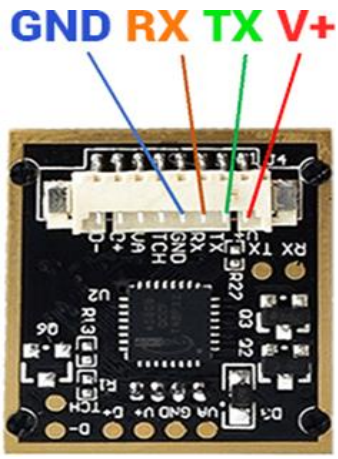


Figura 16. Pin sensor huella AS608
Tomada de Shojaei, 2021

2.2.3.5. Diodo 1N4007

Usado mayoritariamente en circuitos rectificadores de fuentes de alimentación y supresor de picos para relés, soporta un voltaje inverso de hasta 700V y su corriente máxima es de 30Amp.

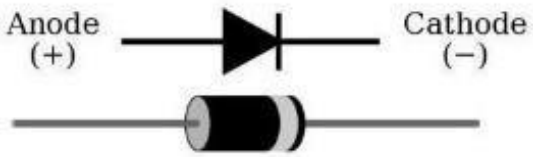


Figura 17. Diodo - 1N4007.
Tomada de Issac, 2020.

2.2.3.6. Transistor - 2N3055.

Debido al pequeño espacio entre el voltaje colector-emisor, se utiliza en circuitos de media tensión, el resultado también es 70hFE, el voltaje máximo entre el colector y el emisor es 60V y la corriente limite del colector es 15Amp.

a) Descripción transistor - 2N3055.

Tabla 9. ***Descripción transistor - 2N3055.***

Descripción transistor - 2N3055.	
Tipo	NPN
Voltaje colector emisor máx.	60V
Voltaje base-emisor máx.	7V
Corriente base	7 Amp
Temperatura operación	-65°C a 200°C
Potencia disipada	115W

Tomada de Issac, 2020

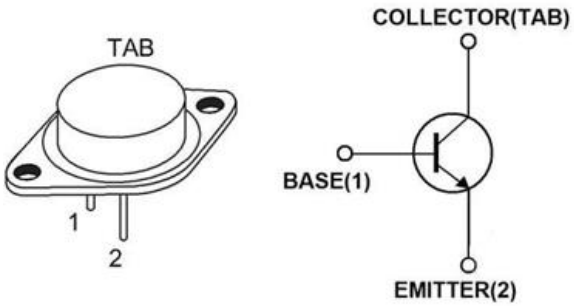


Figura 18. Transistor NPN 2N3055
Tomada de Issac, 2020

2.2.4. Elementos para bloquear en un carro

Hay varias formas diferentes de bloquear un carro mediante métodos de control mecánicos, eléctricos y electrónicos. Las herramientas más populares que se utilizan actualmente para bloquear vehículos son:

2.2.4.1. Sensor de par de dirección del vehículo

Cuando se gira el volante, el sensor del volante detecta su posición y velocidad. Esta información se envía al módulo de control de la dirección asistida junto con la entrada del sensor de par de dirección montado en el eje de dirección. También se tienen en cuenta otras entradas, como la velocidad del vehículo y las entradas del control de tracción o de los sistemas de control de estabilidad, para determinar cuánta asistencia de dirección se requiere. Luego, el módulo de control ordena al motor que gire una cierta cantidad, y los sensores del motor proporcionan retroalimentación al módulo de control para que el módulo de control pueda monitorear la condición del motor (12).

2.2.4.2. Columna dirección.

Sistema mecánico realiza la trabajo de bloquear el volante girándolo en solo un sentido. Para desbloquear, se debe mover la manija mientras se inserta la llave y girarla hacia el interruptor.

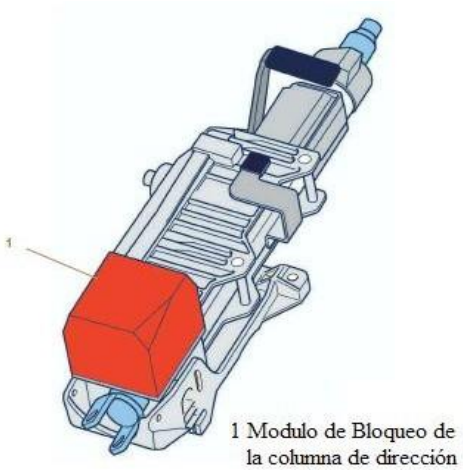


Figura 19. El Bloqueo de columna de dirección
Tomada de Nissan Motor CO. LTD, Manuales eléctricos de servicio, Japón 2010

- **Función**

  Posición reposo.

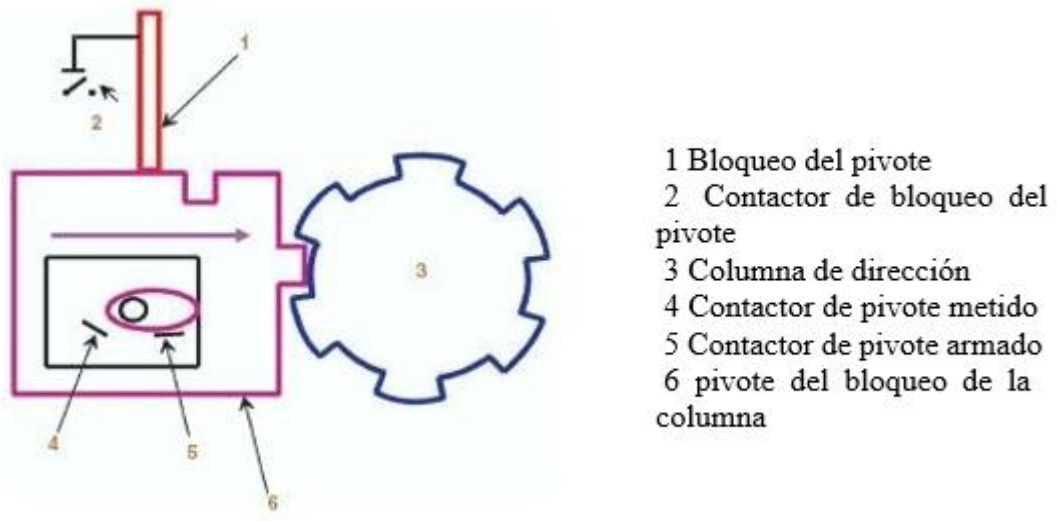
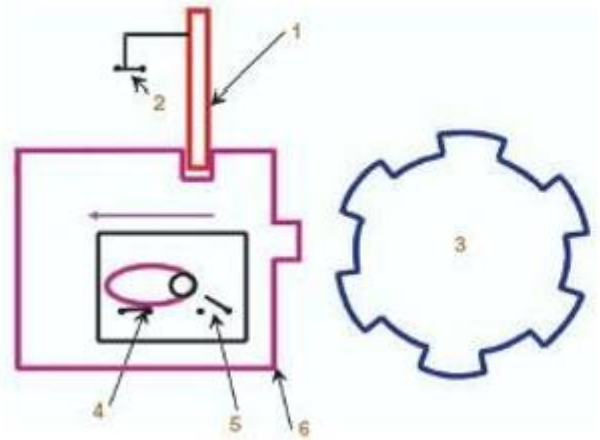


Figura 20. Columna dirección bloqueado
Tomada de Nissan Motor CO. LTD, Manuales eléctricos de servicio, Japón 2010

El pasador de pivote (6) bloquea la columna de dirección (3) cuando el sistema está parado y la función inmovilizadora del vehículo está activa. El interruptor giratorio de stand-by (5) se cierra e informa al ordenador de control que el sistema está en reposo (columna bloqueada).

- Columna desbloqueada



1 Bloqueo del pivote
2 Contactor de bloqueo del pivote
3 Columna de dirección
4 Contactor de pivote metido
5 Contactor de pivote armado
6 pivote del bloqueo de la columna

Figura 21. Columna dirección desbloqueado
Tomada de Nissan Motor CO. LTD, Manuales eléctricos de servicio, Japón 2010

La computadora de control de la carrocería envía un comando de desbloqueo al módulo de bloqueo de la columna de dirección. Este comando se refiere al código de salida que se envía cuando el sistema inmovilizador está desactivado. Cuando el módulo de bloqueo reconozca el código, liberará la columna de dirección según las instrucciones.

El interruptor giratorio (4) está cerrado, indicando que el sistema está desbloqueado, el husillo (1) está cerrado y el interruptor giratorio (2) está cerrado.

2.2.4.3. Bloqueo al encendido

Un dispositivo inmovilizador denominado inmovilizador consta de varios elementos electrónicos que se comunican entre sí para evaluar si la llave introducida en el cilindro de encendido es la llave de identificación de ese vehículo.

Para realizar la tarea de impedir el arranque del motor, el sistema inmovilizador cuenta con varios componentes: un transmisor, un amplificador, un decodificador y una computadora de inyección, como se ve en la imagen.

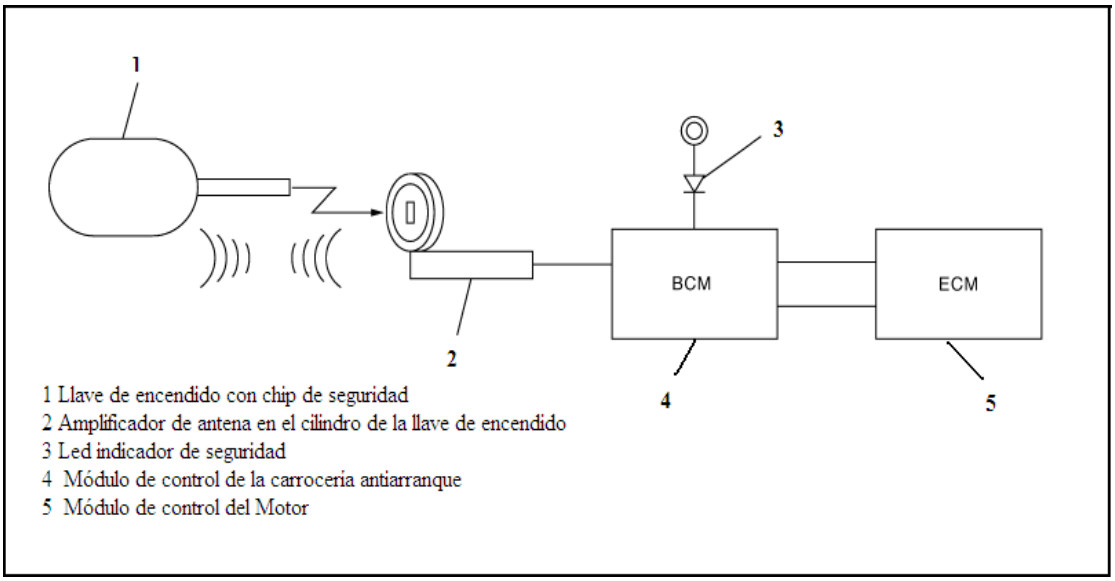


Figura 22. Sistema de antiarranque
Tomada de Nissan Motor CO. LTD, Manuales eléctricos de servicio, Japón 2010

El sistema funciona cuando el interruptor de encendido (1) envía una señal a través de un chip codificado a la antena (2) en el cilindro maestro. Esta señal es amplificada por la antena y enviada a la computadora del motor (4) para ser analizada. Después del desmontaje, esta señal es verificada por el módulo y, si es necesario, se envía un comando al módulo de control del motor (5) para activar el encendido y activar el relé de la bomba de combustible y el relé de control de inyección para activar la llama. Este sistema de coche dispone de una luz de seguridad (3) que indica el estado del sistema, activo o inactivo. Cada clave utilizada en este sistema debe estar registrada. Esto significa que el BCM y el ECM deben aprender la clave antes de arrancar el vehículo. Cada uno tiene un número diferente de claves para aprender. Diseñador y configuración de sistemas.

2.2.4.4. Bloqueo alimentación combustible

El sistema funciona cuando el interruptor de encendido (1) envía una señal a través de un chip codificado a la antena (2) en el cilindro maestro. Esta señal es amplificada por la antena y enviada a la computadora del motor (4) para su análisis. Una vez retirado, el módulo verifica esta señal y si es correcta, el sistema de su vehículo tiene una luz (3) que indica el estado del sistema, activo o inactivo. Todas las claves utilizadas en este sistema deben estar registradas. Esto significa que el BCM y el ECM deben aprender la clave antes de que se pueda arrancar el vehículo. La cantidad de claves a aprender varía según el diseño y la configuración del sistema.

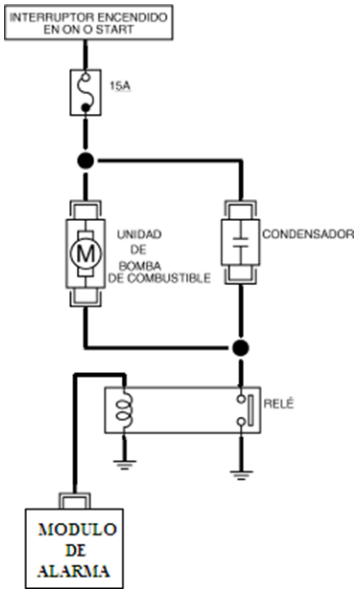


Figura 23. Corte bomba de combustible.
Tomada de Nissan Motor CO. LTD, Manuales eléctricos de servicio, Japón 2010

2.2.4.5. Bloqueo arranque

Es el método de bloqueo más utilizado en los sistemas de alarma de automóviles en la actualidad porque tiene esquemas de cableado fáciles de instalar y difíciles de desactivar, presentando así un alto grado de seguridad. Estas ventajas han hecho que este sistema sea el que se utilizará para el desarrollo del proyecto. Su instalación se realiza cortando el suministro de 12 V tras el encendido, lo que evita la activación de elementos eléctricos como el motor. tablero, etc Los mismos que se pondrán en servicio únicamente cuando exista autorización del módulo de alarma.

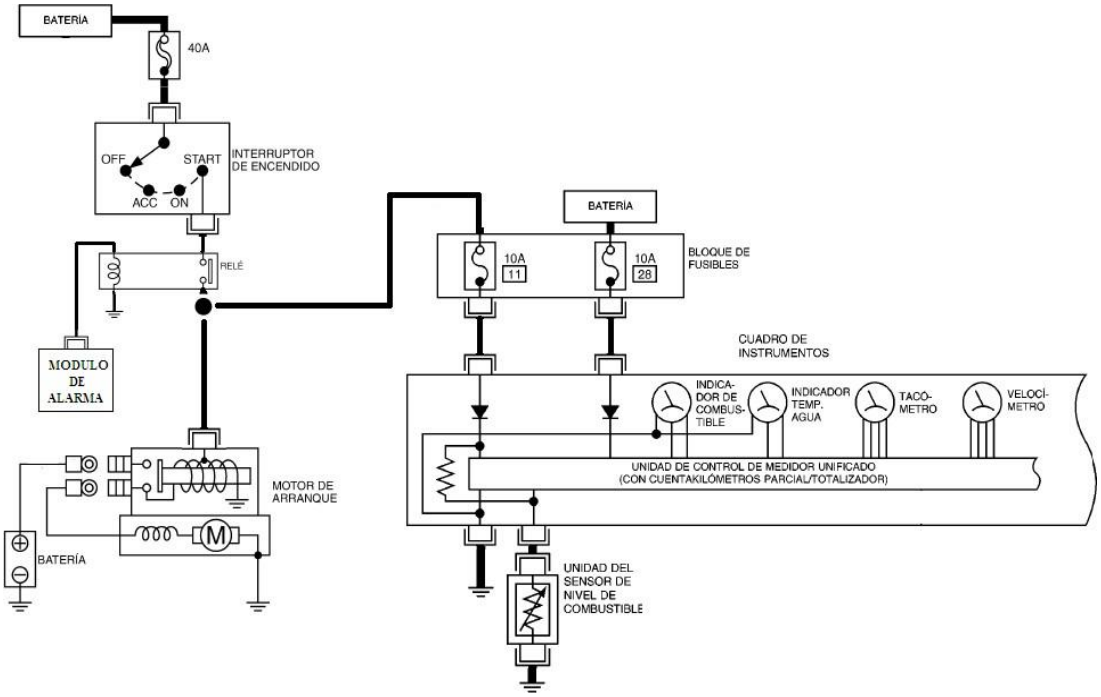


Figura 24. Bloqueo arranque además del cuadro de instrumento
Tomada de Nissan Motor CO. LTD, Manuales eléctricos de servicio, Japón 2010.

2.2.5. Arduino y su definición

"Arduino es una plataforma de prototipos electrónica de código abierto (open – source) basada en hardware y software flexibles y fáciles de usar. Está pensado e inspirado en artistas, diseñadores, y estudiantes de computación o robótica y para cualquier interesado en crear objetos o entornos interactivo, o simplemente por hobby. Arduino consta de una placa principal de componentes eléctricos, donde se encuentran conectados los controladores principales que gestionan los demás complementos y circuitos ensamblados en la misma. Además, requiere de un lenguaje de programación para poder ser utilizado y, como su nombre lo dice, programado y configurarlo a nuestra necesidad, por lo que se puede decir que Arduino es una herramienta "completa" en cuanto a las herramientas principales nos referimos, ya que sólo debemos instalar y configurar con el lenguaje de programación de esta placa los componentes eléctricos que queramos para realizar el proyecto que tenemos en mente, haciéndola una herramienta no sólo de creación, sino también de aprendizaje en el ámbito del diseño de sistemas electrónicos-automáticos y, además, fácil de utilizar. Arduino también simplifica el proceso de trabajo con microcontroladores, ya que está fabricada de tal manera que viene "preensamblada" y lista con los controladores necesarios para poder operar con ella una vez que la saquemos de su caja, ofreciendo una ventaja muy grande para profesores, estudiantes y aficionados interesados en el desarrollo de tecnologías. Las posibilidades de realizar proyectos basados en esta plataforma tienen como limite la imaginación de quien opera esta herramienta" (15).

2.2.6. Conclusiones

En este capítulo se analizó el aspecto general de los sistemas biométricos, se discutieron las ventajas y desventajas entre los diferentes sistemas existentes y cuál es la mejor alternativa de sistema biométrico para este proyecto, su funcionamiento y características, los microcontroladores y se determinaron los mejores dispositivos que soportan el proyecto, tales como formas de cerrar un vehículo.

CAPÍTULO III
METODOLOGÍA

3.1 Método y alcances de investigación

La metodologia de investigación es científico, basado en la recolección de datos para establecer modelos de comportamiento y verificar teorías mediante la verificación de hipótesis basadas en mediciones numéricas y análisis estadístico. Además, los presupuestos se establecen de antemano, antes de la recopilación y el análisis de datos. La recopilación de datos se basa en mediciones y análisis estadísticos.

3.1.1 Tipo de investigación

Por los objetivos de esta investigación, es cuantitativa, de diseño experimental puro, abductiva (resultado, regla, caso), transversal, correlativa, causal. Se trata de un estudio descriptivo del segundo nivel de profundidad de conocimiento en el que el problema es establecido y conocido por el investigador. Por lo tanto, la investigación se utiliza para responder preguntas específicas, como cómo optimizar la seguridad de los vehículos M1 en Huancayo.

3.1.2 Nivel investigación

El nivel es descriptivo y explicativo, consiste en la comprensión de situaciones a través de una descripción precisa del diseño de un sistema antirrobo mediante huella dactilar y optimización de la seguridad de los vehículos M1 en Huancayo. Su finalidad no se limita a la recopilación de datos, sino a predecir e identificar las relaciones que existen entre dos o más variables. Los investigadores no son simples tabuladores, sino que recopilan datos basados en una hipótesis o teoría, presentan y resumen cuidadosamente la información y luego analizan cuidadosamente los resultados para extraer generalizaciones significativas que contribuyan al conocimiento.

3.2 Diseño de investigación

El diseño de la investigación es analítico, descriptivo y explicativo ya que nuestro enfoque de investigación es cualitativo, el análisis de nuestro estudio se realizará de forma natural, describiendo las variables de investigación ya establecidas que el investigador utiliza para informar y controlando las variables de estudio. Su propósito es establecer límites controlados a las observaciones sobre la seguridad de los vehículos M1 ya optimizados, es decir, como se organizarán o formarán los diferentes resultados de la investigación, se podrán determinar los parámetros que influyen en el diseño. sistema antirrobo de huellas dactilares.

3.3 Población y muestra

3.3.1 Población

La población está formada por todos los vehículos de la ciudad de Huancayo.

3.3.2 Tamaño muestral

Viene a ser los vehículos M1 de Huancayo, que no cuentan con un sistema antirrobo mediante huella dactilar, Aquí es donde se realizó toda la investigación y se extrajeron todos los datos necesarios para esta investigación.

3.4 Técnica de recolección de dato.

- Inspección del lugar de trabajo donde se realizará la presente tesis.
- Recopilación de mapeo en el área de trabajo.
- Selección del área donde se realizará el diseño
- Monitoreo y conteo de los ciclos.
- Aplicación del nuevo diseño.
- Tomar fotografía en el lugar de trabajo.

3.5 Técnicas y análisis de datos

- Laptop.
- Software AutoCad.
- Hojas de cálculo Excel.

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1 Identificación de necesidad del problema e identificación de requerimientos

Teniendo por objetivo principal la optimización de los sistemas de seguridad en vehículos M1 y el desarrollo de nueva tecnología en la provincia de Huancayo, así como la disminución de un gran porcentaje de hechos delictivos en contra de los vehículos de los ciudadanos, se desarrolla el trabajo de investigación con componentes electrónicos de fácil accesibilidad, costos bajos y que tenga la eficiencia requerida para el buen desempeño del dispositivo de activación del sensor de par de la dirección del vehículo mediante huella dactilar en el campo a desarrollarse.

4.2 Propuesta solución al problema o necesidad

Los trabajos están definidos en dar solución al planteamiento de un problema, por lo general una necesidad de la población. Se reúnen una variedad de metodologías, ideas y tecnologías para su implementación, pero el objetivo principal es satisfacer todas sus necesidades y aspectos. Teniendo en consideración algunas restricciones para la ejecución del prototipo, así como considerando puntos necesarios se desarrolla la simulación del dispositivo de activación del sensor de par de la dirección del vehículo mediante huella dactilar, obteniendo el funcionamiento requerido y datos importantes para su pronta ejecución.

El proceso de elaboración del dispositivo está comprendido en tres procesos fundamentales para su eficiente funcionamiento.

4.2.1 Sensor biométrico

El funcionamiento del dispositivo comienza a partir de la lectura del sensor biométrico de la huella dactilar de la persona que desea accionar o tomar el control del vehículo donde se encontrara instalado el dispositivo.

4.2.2 Comparación de patrones biométricos

El dispositivo cuenta con el almacenamiento de patrones biométricos de las personas que tienen permitido el accionar del sensor de par de la dirección del vehículo, compara los patrones biométricos almacenados con los patrones de las personas que deseen el accionamiento de este.

4.2.3 Activación del sensor de par

La activación del sensor de par permite tener el control de la dirección del vehículo, logrando así la movilidad de este, esto no sucederá si los patrones biométricos no coinciden con los almacenados.

4.3 Diseño del sistema de seguridad biométrico

Hoy en día se utilizan muchos sistemas biométricos según sea necesario, todos los cuales se utilizan para garantizar una mayor seguridad y confiabilidad para la identificación y verificación del usuario.

Para ello su primer objetivo es mejorar los sistemas de seguridad en el vehículo, se debe realizar un análisis para determinar los parámetros de diseño según el alcance definido.

4.3.1 Sensor huella digital

La biometría se basa en la verificación de la identidad de una persona a partir de una descripción única de su cuerpo o comportamiento y una valoración, en los sistemas biométricos se utilizan muchos métodos.

Los parámetros de cada sistema deben analizarse cuidadosamente para determinar un sistema en función de su confiabilidad, ventajas, desventajas y rendimiento. Entre los sistemas biométricos analizados, la huella dactilar es el que se ajusta a los parámetros de diseño considerados, lo que no sólo es útil, sino también cómodo de aplicar y logra rápidamente la autenticación.

4.3.1.1 Fiabilidad

Una de las formas más inteligentes de distinguir las huellas dactilares es utilizar un patrón que sigue las líneas y surcos y se puede clasificar según las tres características principales que se muestran en la imagen.

Figura 25. Patrones de las clasificaciones de huellas digitales
Tomada de Nissan Motor CO. LTD, Manuales eléctricos de servicio, Japón 2010

En algunos lugares, las líneas o ramas de las huella dactilar se cortan accidentalmente para formar piezas mecánicas, y estas dos piezas se combinan para formar aproximadamente el 80 % de los elementos individuales del dedo y crear un modelo único. Dado que los gemelos idénticos varían de persona a persona, la probabilidad de que se vuelva a enviar la huella dactilar se estima en 1 entre 64 millones, ya que los sistemas de huellas dactilares son muy fiables porque es el principal parámetro que considerar a la hora de elegir un sistema biométrico que no pueda manipularse. con. Sistemas en la frontera de este proyecto.

En el proceso de diseño del proyecto, analizar las ventajas y desventajas del sistema de huellas dactilares es fundamental, ya que es la mejor manera de determinar si el sistema elegido es adecuado para la descripción del diseño propuesto.

4.3.1.2 Ventaja

- Así como se puede adivinar su contraseña, su patrón de huellas dactilares no se puede adivinar.
- Es universal porque es poco probable que se pierda un dedo o ambas manos.
- Accesible con múltiples sensores de huellas dactilares.
- Alta aceptación por parte de los usuarios debido al uso prolongado de las huellas dactilares.
- Las huellas dactilares son muy duraderas porque es poco probable que desaparezcan con el tiempo.
- Funciona bien porque su algoritmo de huellas dactilares es eficiente y preciso y no ocupa mucho espacio para almacenar huellas dactilares.
- Precisión, seguridad y confiabilidad.
- Sistema ergonómico y fácil de usar

4.3.1.3 Desventaja

- Los cortes, la piel seca, el polvo o el contacto con sustancias pueden provocar una mala lectura de las huellas dactilares, por lo que se sugiere que el mismo empleador registre 02 o más huellas dactilares.
- El uso espacial de las huellas dactilares puede provocar delitos e invasión de la privacidad.

4.3.1.4 Prestaciones

Los sistemas de huellas dactilares se utilizan desde el siglo pasado y ahora se están desarrollando por su eficacia, ya que son una tecnología muy confiable que no se puede falsificar.

Los sistemas de huellas dactilares son una tecnología en evolución, por lo que el costo es relativamente bajo y es muy importante desarrollar y probar las tecnologías subyacentes a lograr los resultados en referente en autenticación y verificación de usuarios.

Por ser un sistema ergonómico, puede desarrollarse en diversos ambientes, razón por la cual fue elegido para dicho proyecto.

4.3.2 Descripción del sensor de huella digital utilizado

En base a este análisis y tras investigar las mejores opciones, se eligió el módulo FIM 5360 de la empresa coreana NITGEN, líder en el sector del reconocimiento de huellas dactilares.

FIM 5360 es un dispositivo de identificación de huellas dactilares con una descripción excelente y buenas ventajas, como alta calidad de identificación, bajo consumo de energía e interfaces de control serial UART para una fácil integración con una amplia gama de aplicaciones. Es un dispositivo robusto y compacto con un módulo de identificación de huellas dactilares que contiene un sensor óptico en su interior. Las descripciones clave se pueden ver en las tablas detalladas a continuación.

Tabla 10. ***Descripción principal del sensor FIM-5360***

descripción principal del sensor FIM-5360		
Ítem		FIM5360
Especificación	CPU	S3C2410 (ARM9 266Mhz)
memoria	DRAM	16MByte SDRAM
	Flash rom	8Mbyte
Dimensiones		43 x 60 [m]

Sensor		NITGEN-OPP06
Voltaje de Alimentación		5 / 3.3 [V]
Consumo Corriente	Normal	70 [mA]
	Máxima	220 [mA]
Temperatura operación		-20 ~ 60 [°C]
Humedad		~ 90 [% RH]
Canal de comunicación		RS232 level UART Speed: 9600 ~ 115200 [bps] (1 start bit, 8 data bit, no parity, 1 stop bit)
Almacenamiento máximo de usuarios		1000 Usuarios

Nota: NITGEN CO. LTD, Datasheet Nitgen Fim5360 1.02, Korea 2012

Tabla 11. ***Especificacion de operación***

Especificaciones de operación	
Ítem	FIM-5360
Velocidad captura	0.2s
Velocidad verificación	Menor a 1 [s]
Tiempo arranque	0.4 [s] para 100 usuarios 0.5 [s] para 1000 usuarios
Método de encriptación de datos	AES guardar datos AES comunicación DB

Nota: NITGEN CO. LTD, Datasheet Nitgen Fim5360 1.02, Korea 2012

Tabla 12. ***Descripción del sensor***

Descripción sensor	
OPP–06	
Nombre sensor	OOP - 6
Tipo detección.	Óptico
Área detección.	15.0mm x 18.5mm
Resolución imagen	500 DPI
Tamaño de imagen	260 x 300

Nota: NITGEN CO. LTD, Datasheet Nitgen Fim5360 1.02, Korea 2011

4.3.3 Generación circuito habilitación vehículo

4.3.3.1 Armado circuito

Se monta la placa de circuito en la placa de prueba de acuerdo con el diagrama de la imagen, mientras se ensambla la placa de circuito.

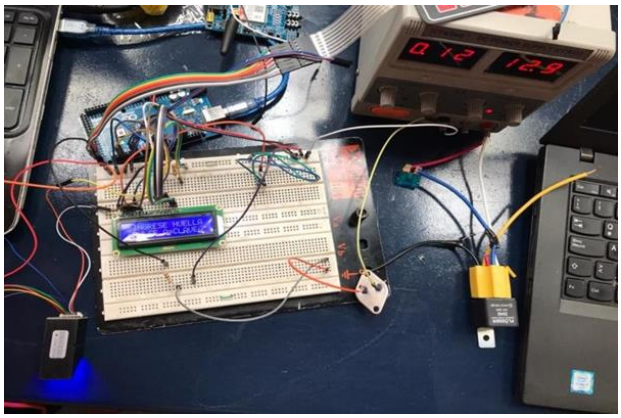


Figura 26. Armado circuito fase habilitación carro

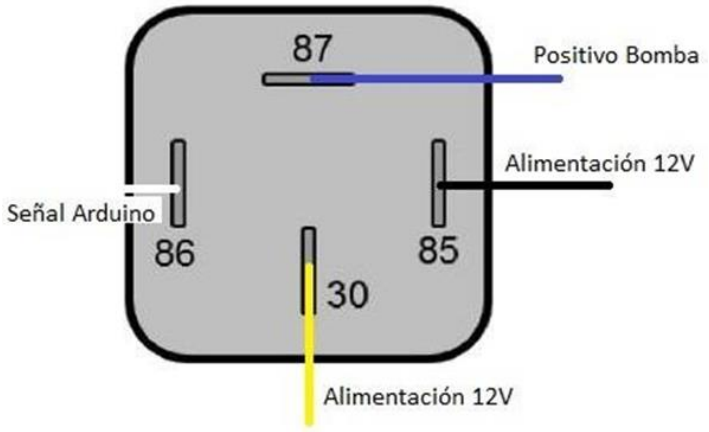


Figura 27. Esquemas terminales relé

Para comprobar el correcto funcionamiento del circuito, medimos el voltaje de salida del contacto 87 del relé, el cual debe ser de 12 V para activar la bomba eléctrica de combustible o la bobina de encendido.

4.3.3.2 Programación Arduino

El programa utilizado para controlar los elementos que pertenecen a cada circuito según sus fases es Arduino 1.8.13, ya que el lenguaje de programación de su código es sencillo y de muy fácil interpretación para los usuarios.

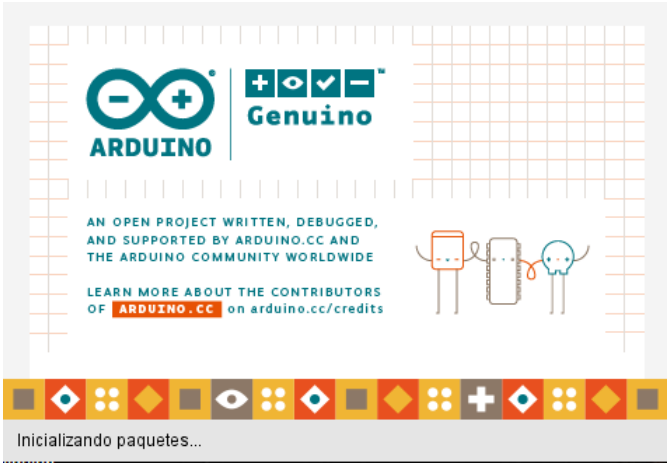


Figura 28. Pantalla inicio de programa Arduino

Para una correcta programación es necesario contar con las librerías de cada uno de los componentes a utilizar, para que al ejecutar los comandos sean reconocidos y puedan realizar cada una de sus funciones.

```
1  #include <Wire.h>
2  #include <LiquidCrystal_I2C.h>
3  LiquidCrystal_I2C lcd(0x27,20,4);
4  #include <Adafruit_Fingerprint.h>
5  #include <SoftwareSerial.h>
6  int getFingerprintIDez();
7  SoftwareSerial mySerial(2, 3);
8  Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
9  #include <Servo.h>
0  Servo miServo;
```

Figura 29. Librerías de los elementos de Arduino

4.3.3.3 Programación fase habilitación vehículo

En la etapa de activación del vehículo tenemos la pantalla LCD, el botón de pase, además del sensor de huellas dactilares AS608. Para que estos elementos funcionen bien juntos, debe inicializar la programación definiendo los puertos serie a utilizar.

```
12  int scan_pin = 11;      //Pin for the scan push button
13  int add_id_pin = 10;    //Pin for the add new ID push button
14  int close_door = 9;     //Pin to close the door button
15  int green_led = 8;      //Extra LEDs for open or close door labels
16  int red_led = 7;
17  ////////////////////////////////////////////////////////////////////////////
18  ////////////////////////////////////////////////////////////////////////////
19  int main_user_ID = 1;
20  int door_open_degrees = 180;
21  int door_close_degrees = 0;
22  ////////////////////////////////////////////////////////////////////////////
23  bool scanning = false;
24  int counter = 0;
25  int id_ad_counter = 0;
26  bool id_ad = false;
27  uint8_t num = 1;
28  bool id_selected = false;
29  uint8_t id;
30  bool first_read = false;
31  bool main_user = false;
32  bool add_new_id = false;
33  bool door_locked = true;
```

Figura 30. Iniciación de pantalla LCD y huella dactilar AS608

Se colocará los comandos en el programa para iniciar el sistema y que se muestre en la pantalla se un mensaje para añadir una huella dactilar o sensor desactivado, con el pulsador seleccionaremos la acción que deseamos realizar y se mostrará mediante leds indicadores.

```
void setup() {
  Serial.begin(57600);

  lcd.init();
  lcd.backlight();
  lcd.setCursor(0,0);
  lcd.print("   Press SCAN   ");
  lcd.setCursor(0,1);
  lcd.print("  S.Desactivado ");


  pinMode(scan_pin,INPUT);
  pinMode(add_id_pin,INPUT);
  pinMode(close_door,INPUT);
  digitalWrite(red_led,HIGH);
  digitalWrite(green_led,LOW);
  finger.begin(57600);
}
```

Figura 31. Configuración de comandos iniciales

El registro de las huella dactilar, se realizará desde el mismo sistema de desbloqueo, por ello se debe de tener una huella principal que será la del propietario del vehículo, con esta huella maestra se permitirá la validación de registro de otras huellas de otros usuarios de manera que

inscribirá un nuevo registro de usuario y los guardara para que se utilizará más tarde para activar la máquina.

```
/*This function will add new ID to the database*/
uint8_t getFingerprintEnroll() {

  int p = -1;
  if(!first_read)
  {
  lcd.setCursor(0,0);
  lcd.print("Add new as ID#  ");
  lcd.setCursor(14,0);
  lcd.print(id);
  lcd.setCursor(0,1);
  lcd.print("  Place finger  ");
  }

  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
    case FINGERPRINT_OK:
      lcd.setCursor(0,0);
      lcd.print("  Image taken!  ");
      lcd.setCursor(0,1);
      lcd.print("                ");
      delay(100);
      first_read = true;
      break;
```

```
  case FINGERPRINT_NOFINGER:
    lcd.setCursor(0,0);
    lcd.print("Add new as ID#  ");
    lcd.setCursor(14,0);
    lcd.print(id);
    lcd.setCursor(0,1);
    lcd.print("  Place finger  ");
    break;
  case FINGERPRINT_PACKETRECIEVEERR:
    lcd.setCursor(0,0);
    lcd.print("  Comunication  ");
    lcd.setCursor(0,1);
    lcd.print("     ERROR!     ");
    delay(1000);
    break;
  case FINGERPRINT_IMAGEFAIL:
    lcd.setCursor(0,0);
    lcd.print("     -Image     ");
    lcd.setCursor(0,1);
    lcd.print("     ERROR!     ");
    delay(1000);
    break;
  default:
    lcd.setCursor(0,0);
    lcd.print("    -Unknown    ");
    lcd.setCursor(0,1);
    lcd.print("     ERROR!     ");
    delay(1000);
    break;
  }
}
```

Figura 32. Registro huella dactilar en el sistema

Cuando se registran la huella de los usuarios que utilizan el carro, el programa identifica cada huella mientras se conduce.

El dedo índice debe colocarse sobre el sensor, pero se puede utilizar cualquier dedo a discreción del usuario. Esto activa el relé de control de la bomba de combustible eléctrica y permite que el motor funcione.

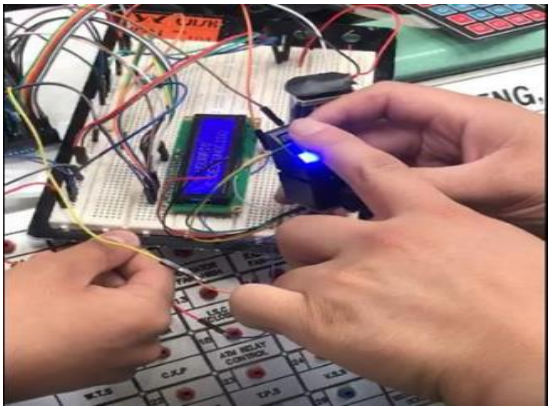


Figura 33. Proceso de registro huella dactilar

4.4 Pruebas de solución

Las pruebas realizadas a la simulación dan muestra del buen funcionamiento y la eficiencia del trabajo de investigación en el campo a desarrollarse, generado una gran expectativa para su pronto ensamblaje.

4.4.1 Activación del sensor de par

Se plantea el siguiente diseño de solución, teniendo en consideración la implementación de componentes electrónicos, así como la programación que son los principales requerimientos para el eficiente desarrollo del trabajo de investigación.

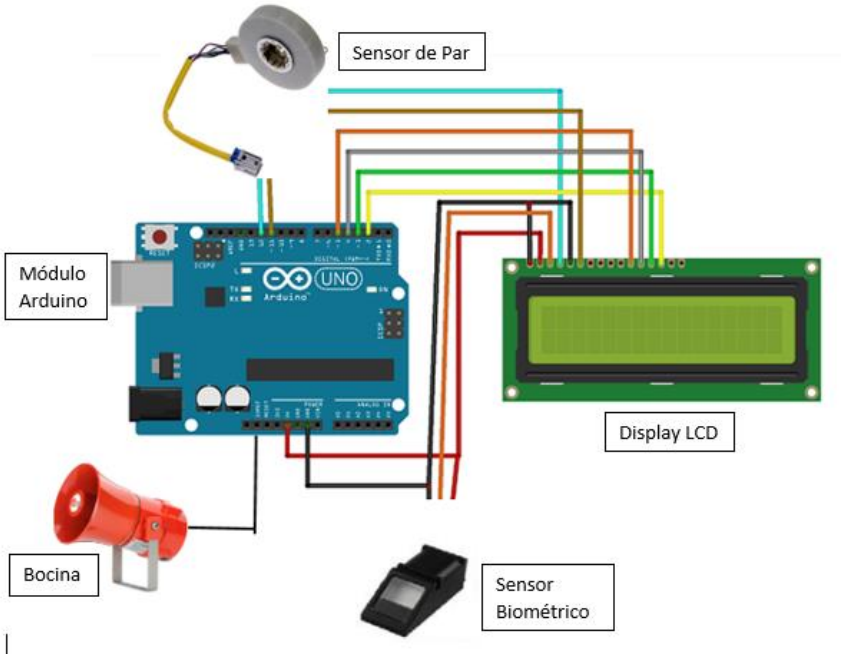


Figura 3435. Diseño de activación de sensor

4.4.2 Diseño de control de dispositivo

Es necesaria la fácil manipulación del sistema de control del dispositivo, por lo que se propuso un diseño fácil y accesible para las personas, que tenga los requerimientos necesarios para la modificación de parámetros en el sistema y que conserve su eficacia al momento del almacenamiento de huella dactilar.

Figura 36. Diseño de control del dispositivo

4.4.3 Diseño de software

Se definió el diseño del software considerando los componentes electrónicos a utilizar, así como la interface requerida para cada uno, la arquitectura diseñada en leguaje de programación cumple con los objetivos requeridos para el funcionamiento del dispositivo, también se consideran ciertas restricciones que favorecen al mejoramiento de este.

```
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x27,20,4);
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
int getFingerprintIDez();
SoftwareSerial mySerial(2, 3);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
#include <Servo.h>
Servo miServo;

int scan_pin = 11;      //Pin for the scan push button
int add_id_pin = 10;    //Pin for the add new ID push button
int close_door = 9;     //Pin to close the door button
int green_led = 8;      //Extra LEDs for open or close door labels
int red_led = 7;
////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////
int main_user_ID = 1;
int door_open_degrees = 180;
int door_close_degrees = 0;
```

```
bool scanning = false;
int counter = 0;
int id_ad_counter = 0;
bool id_ad = false;
uint8_t num = 1;
bool id_selected = false;
uint8_t id;
bool first_read = false;
bool main_user = false;
bool add_new_id = false;
bool door_locked = true;



void setup() {
  Serial.begin(57600);

  lcd.init();
  lcd.backlight();
  lcd.setCursor(0,0);
  lcd.print("   Press SCAN   ");
  lcd.setCursor(0,1);
  lcd.print("  S.Desactivado ");


  pinMode(scan_pin,INPUT);
  pinMode(add_id_pin,INPUT);
  pinMode(close_door,INPUT);
  digitalWrite(red_led,HIGH);
  digitalWrite(green_led,LOW);
```

```
  finger.begin(57600);
}

////////////////////////////////////////////////////

void loop() {

  if(digitalRead(close_door))
  {
    door_locked = true;
    digitalWrite(red_led,HIGH);
    digitalWrite(green_led,LOW);
    lcd.setCursor(0,0);
    lcd.print("  Apagando S.  ");
    lcd.setCursor(0,1);
    lcd.print("               ");
    delay(2000);
    lcd.setCursor(0,0);
    lcd.print("   Press SCAN   ");
    lcd.setCursor(0,1);
    lcd.print("  S.Desactivado ");
  }


////////////////////////////////Scan button pressed//
 if(digitalRead(scan_pin) && !id_ad)
 {
  scanning = true;
  lcd.setCursor(0,0);
  lcd.print("  Place finger  ");
  lcd.setCursor(0,1);
```

```
 lcd.print("SCANNING--------");
}

while(scanning && counter <= 60)
{
 getFingerprintID();
 delay(100);
 counter = counter + 1;
 if(counter == 10)
 {
   lcd.setCursor(0,0);
   lcd.print("  Place finger  ");
   lcd.setCursor(0,1);
   lcd.print("SCANNING  ------");
 }

 if(counter == 20)
 {
   lcd.setCursor(0,0);
   lcd.print("  Place finger  ");
   lcd.setCursor(0,1);
   lcd.print("SCANNING    ----");
 }

 if(counter == 40)
 {
   lcd.setCursor(0,0);
   lcd.print("  Place finger  ");
   lcd.setCursor(0,1);
   lcd.print("SCANNING      --");
 }
if(counter == 50)
{
  lcd.setCursor(0,0);
  lcd.print("  Place finger  ");
  lcd.setCursor(0,1);
  lcd.print("SCANNING        ");
}
if(counter == 59)
{
  lcd.setCursor(0,0);
  lcd.print("    Timeout!    ");
  lcd.setCursor(0,1);
  lcd.print("   Try again!   ");
  delay(2000);
  if(door_locked)
  {
    lcd.setCursor(0,0);
    lcd.print("   Press SCAN   ");
    lcd.setCursor(0,1);
    lcd.print("  S.Desactivado ");
  }
  else
  {
    lcd.setCursor(0,0);
    lcd.print("   Press SCAN   ");
    lcd.setCursor(0,1);
    lcd.print("    S.Activo    ");
  }
 }
}
scanning = false;
```

```
 counter = 0;
//////////////////////////////END WITH SCANNING PART


/////////////////////////////////////////Add new button pressed///
if(digitalRead(add_id_pin) && !id_ad)
 {

  add_new_id = true;

  lcd.setCursor(0,0);
  lcd.print(" Scan main user ");
  lcd.setCursor(0,1);
  lcd.print("  finger first! ");

  while (id_ad_counter < 40 && !main_user)
  {
    getFingerprintID();
    delay(100);
    id_ad_counter = id_ad_counter+1;
    if(!add_new_id)
    {
      id_ad_counter = 40;
    }
  }
  id_ad_counter = 0;
  add_new_id = false;

    if(main_user)
    {
          lcd.setCursor(0,0);
          lcd.print(" Add new ID# to ");
          lcd.setCursor(0,1);
          lcd.print("  the database  ");
          delay(1500);
          print_num(num);
          id_ad = true;

        }
        else
        {
          lcd.setCursor(0,0);
          lcd.print("ERROR! Only main");
          lcd.setCursor(0,1);
          lcd.print("user can add IDs");
          delay(1500);
          if(door_locked)
          {
            lcd.setCursor(0,0);
            lcd.print("   Press SCAN   ");
            lcd.setCursor(0,1);
            lcd.print("  S.Desactivado ");
          }
          else
          {
            lcd.setCursor(0,0);
            lcd.print("   Press SCAN   ");
            lcd.setCursor(0,1);
            lcd.print("    S.Activo    ");
          }
          id_ad = false;
```

```
 }
}

if(digitalRead(scan_pin) && id_ad)
{

 id=num;
 while (!  getFingerprintEnroll() );
 id_ad = false;
 lcd.clear();
 lcd.setCursor(0,0);
 lcd.print("  New ID saved  ");
 lcd.setCursor(4,1);
 lcd.print("as ID #");
 lcd.setCursor(11,1);
 lcd.print(id);
 delay(3000);
 if(door_locked)
   {
    lcd.setCursor(0,0);
    lcd.print("   Press SCAN   ");
    lcd.setCursor(0,1);
    lcd.print("  S.Desactivado ");
   }
   else
   {
    lcd.setCursor(0,0);
    lcd.print("   Press SCAN   ");
    lcd.setCursor(0,1);
    lcd.print("    S.Activo    ");
   }
  }
 add_new_id = false;
 main_user = false;
 id_ad = false;


}

if(digitalRead(add_id_pin) && id_ad)
{
 num = num + 1;
 if(num > 16)
 {
  num=1;
 }
 print_num(num);
}
}

//end of void
////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////


/*This function will print the ID numbers when adding new ID*/
void print_num(uint8_t)
{
 if (num == 1)
 {
  lcd.setCursor(0,0);
```

```
{
  if (num == 1)
  {
    lcd.setCursor(0,0);
    lcd.print("Select ID number");
    lcd.setCursor(0,1);
    lcd.print(">1  2   3   4   ");
    delay(500);
  }
  if (num == 2)
  {
    lcd.setCursor(0,0);
    lcd.print("Select ID number");
    lcd.setCursor(0,1);
    lcd.print(" 1 >2   3   4   ");
    delay(500);
  }
  if (num == 3)
  {
    lcd.setCursor(0,0);
    lcd.print("Select ID number");
    lcd.setCursor(0,1);
    lcd.print(" 1  2  >3   4   ");
    delay(500);
  }
  if (num == 4)
  {
    lcd.setCursor(0,0);
    lcd.print("Select ID number");
    lcd.setCursor(0,1);
    lcd.print(" 1  2   3  >4   ");
    delay(500);
}
if (num == 5)
{
  lcd.setCursor(0,0);
  lcd.print("Select ID number");
  lcd.setCursor(0,1);
  lcd.print(">5  6   7   8   ");
  delay(500);
}
if (num == 6)
{
  lcd.setCursor(0,0);
  lcd.print("Select ID number");
  lcd.setCursor(0,1);
  lcd.print(" 5 >6   7   8   ");
  delay(500);
}
if (num == 7)
{
  lcd.setCursor(0,0);
  lcd.print("Select ID number");
  lcd.setCursor(0,1);
  lcd.print(" 5  6  >7   8   ");
  delay(500);
}
if (num == 8)
{
  lcd.setCursor(0,0);
  lcd.print("Select ID number");
```

```
  lcd.print(" 5  6   7  >8   ");
  delay(500);
}
if (num == 9)
{
  lcd.setCursor(0,0);
  lcd.print("Select ID number");
  lcd.setCursor(0,1);
  lcd.print(">9  10  11  12  ");
  delay(500);
}
if (num == 10)
{
  lcd.setCursor(0,0);
  lcd.print("Select ID number");
  lcd.setCursor(0,1);
  lcd.print(" 9 >10  11  12  ");
  delay(500);
}
if (num == 11)
{
  lcd.setCursor(0,0);
  lcd.print("Select ID number");
  lcd.setCursor(0,1);
  lcd.print(" 9  10 >11  12  ");
  delay(500);
}
if (num == 12)
{
  lcd.setCursor(0,0);
  lcd.print("Select ID number");
  lcd.setCursor(0,1);
  lcd.print(" 9  10  11 >12  ");
  delay(500);
}
if (num == 13)
{
  lcd.setCursor(0,0);
  lcd.print("Select ID number");
  lcd.setCursor(0,1);
  lcd.print(">13  14  15  16 ");
  delay(500);
}
if (num == 14)
{
  lcd.setCursor(0,0);
  lcd.print("Select ID number");
  lcd.setCursor(0,1);
  lcd.print(" 13 >14  15  16 ");
  delay(500);
}
if (num == 15)
{
  lcd.setCursor(0,0);
  lcd.print("Select ID number");
  lcd.setCursor(0,1);
  lcd.print(" 13  14 >15  16 ");
  delay(500);
}
if (num == 16)
{
  lcd.setCursor(0,0);
```

```
    delay(500);
  }
  if (num == 16)
  {
    lcd.setCursor(0,0);
    lcd.print("Select ID number");
    lcd.setCursor(0,1);
    lcd.print(" 13  14  15 >16 ");
    delay(500);
  }
}

/*This function will read the fingerprint placed on the sensor*/
uint8_t getFingerprintID()
{
  uint8_t p = finger.getImage();
  switch (p)
  {
    case FINGERPRINT_OK:
    break;
    case FINGERPRINT_NOFINGER: return p;
    case FINGERPRINT_PACKETRECIEVEERR: return p;
    case FINGERPRINT_IMAGEFAIL: return p;
    default: return p;
  }
// OK success!

  p = finger.image2Tz();
  switch (p)
  {
    case FINGERPRINT_OK: break;
    case FINGERPRINT_IMAGEMESS: return p;
    case FINGERPRINT_PACKETRECIEVEERR: return p;
    case FINGERPRINT_FEATUREFAIL: return p;
    case FINGERPRINT_INVALIDIMAGE: return p;
    default: return p;
  }
// OK converted!

  p = finger.fingerFastSearch();

  if (p == FINGERPRINT_OK)
  {
    scanning = false;
    counter = 0;
    if(add_new_id)
    {
      if(finger.fingerID == main_user_ID)
      {
        main_user = true;
        id_ad = false;
      }
      else
      {
        add_new_id = false;
        main_user = false;
        id_ad = false;
      }
    }
```

```
else
{
miServo.write(door_open_degrees); //degrees so door is open
digitalWrite(red_led,LOW);       //Red LED turned OFF
digitalWrite(green_led,HIGH);    //Green LED turned ON, shows door OPEN

lcd.clear();
lcd.setCursor(0,0);
lcd.print("   User match   ");

lcd.setCursor(0,1);
lcd.print(" ID: #");

lcd.setCursor(6,1);
lcd.print(finger.fingerID);

lcd.setCursor(9,1);
lcd.print("%: ");

lcd.setCursor(12,1);
lcd.print(finger.confidence);

door_locked = false;
delay(4000);
lcd.setCursor(0,0);
lcd.print("   Press SCAN   ");
lcd.setCursor(0,1);
lcd.print("    S.Activo    ");
delay(50);
}
```

```
}//end finger OK

else if(p == FINGERPRINT_NOTFOUND)
{
  scanning = false;
  id_ad = false;
  counter = 0;
  lcd.setCursor(0,0);
  lcd.print("    No match    ");
  lcd.setCursor(0,1);
  lcd.print("   Try again!   ");
  add_new_id = false;
  main_user = false;

  delay(2000);
  if(door_locked)
    {
      lcd.setCursor(0,0);
      lcd.print("   Press SCAN   ");
      lcd.setCursor(0,1);
      lcd.print("  S.Desactivado ");
    }
    else
    {
      lcd.setCursor(0,0);
      lcd.print("   Press SCAN   ");
      lcd.setCursor(0,1);
      lcd.print("    S.Activo    ");
    }
  delay(2);
```

```
}//end finger error
}// 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!
return finger.fingerID;
}
```

```
/*This function will add new ID to the database*/
uint8_t getFingerprintEnroll() {

 int p = -1;
 if(!first_read)
 {
 lcd.setCursor(0,0);
 lcd.print("Add new as ID#  ");
 lcd.setCursor(14,0);
 lcd.print(id);
 lcd.setCursor(0,1);
 lcd.print("  Place finger  ");
 }

 while (p != FINGERPRINT_OK) {
   p = finger.getImage();
   switch (p) {
   case FINGERPRINT_OK:
     lcd.setCursor(0,0);
     lcd.print("  Image taken!  ");
     lcd.setCursor(0,1);
     lcd.print("                ");
     delay(100);
     first_read = true;
     break;
   case FINGERPRINT_NOFINGER:
     lcd.setCursor(0,0);
     lcd.print("Add new as ID#  ");
     lcd.setCursor(14,0);
     lcd.print(id);
     lcd.setCursor(0,1);
     lcd.print("  Place finger  ");
     break;
   case FINGERPRINT_PACKETRECIEVEERR:
     lcd.setCursor(0,0);
     lcd.print("  Comunication  ");
     lcd.setCursor(0,1);
     lcd.print("     ERROR!     ");
     delay(1000);
     break;
   case FINGERPRINT_IMAGEFAIL:
     lcd.setCursor(0,0);
     lcd.print("     -Image     ");
     lcd.setCursor(0,1);
     lcd.print("     ERROR!     ");
     delay(1000);
     break;
   default:
     lcd.setCursor(0,0);
     lcd.print("    -Unknown    ");
     lcd.setCursor(0,1);
     lcd.print("     ERROR!     ");
     delay(1000);
     break;
   }
 }

 // OK success!

 p = finger.image2Tz(1);
 switch (p) {
   case FINGERPRINT_OK:
     lcd.setCursor(0,0);
     lcd.print("Image converted!");
     lcd.setCursor(0,1);
     lcd.print("                ");
     break;
   case FINGERPRINT_IMAGEMESS:
     lcd.setCursor(0,0);
     lcd.print("Image too messy!");
     lcd.setCursor(0,1);
     lcd.print("                ");
     delay(1000);
     return p;
   case FINGERPRINT_PACKETRECIEVEERR:
     lcd.setCursor(0,0);
     lcd.print("  Comunication  ");
     lcd.setCursor(0,1);
     lcd.print("     ERROR!     ");
     delay(1000);
     return p;
```

```
    case FINGERPRINT_FEATUREFAIL:
      lcd.setCursor(0,0);
      lcd.print(" No fingerprint ");
      lcd.setCursor(0,1);
      lcd.print("features found  ");
      delay(1000);
      return p;
    case FINGERPRINT_INVALIDIMAGE:
      lcd.setCursor(0,0);
      lcd.print(" No fingerprint ");
      lcd.setCursor(0,1);
      lcd.print("features found  ");
      delay(1000);
      return p;
    default:
      lcd.setCursor(0,0);
      lcd.print("    -Unknown    ");
      lcd.setCursor(0,1);
      lcd.print("     ERROR!     ");
      delay(1000);
      return p;
    }

  lcd.setCursor(0,0);
  lcd.print(" Remove finger! ");
  lcd.setCursor(0,1);
  lcd.print("                ");
  delay(2000);
  p = 0;
  while (p != FINGERPRINT_NOFINGER) {
    p = finger.getImage();
  }
  lcd.setCursor(0,1);
  lcd.print("ID# ");
  lcd.setCursor(4,1);
  lcd.print(id);
  p = -1;
  lcd.setCursor(0,0);
  lcd.print("Place again the ");
  lcd.setCursor(0,1);
  lcd.print("same finger     ");
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
    case FINGERPRINT_OK:
      lcd.setCursor(0,0);
      lcd.print("  Image taken!  ");
      lcd.setCursor(0,1);
      lcd.print("                ");
      break;
    case FINGERPRINT_NOFINGER:
      lcd.setCursor(0,0);
      lcd.print("Place again the ");
      lcd.setCursor(0,1);
      lcd.print("same finger     ");
      break;
    case FINGERPRINT_PACKETRECIEVEERR:
      lcd.setCursor(0,0);
      lcd.print("  Comunication  ");
      lcd.setCursor(0,1);
      lcd.print("     ERROR!     ");
      delay(1000);
      break;
    case FINGERPRINT_IMAGEFAIL:
      lcd.setCursor(0,0);
      lcd.print("     -Image     ");
      lcd.setCursor(0,1);
      lcd.print("     ERROR!     ");
      delay(1000);
      break;
    default:
      lcd.setCursor(0,0);
      lcd.print("    -Unknown    ");
      lcd.setCursor(0,1);
      lcd.print("     ERROR!     ");
      delay(1000);
      break;
    }
  }

  // OK success!
```

```
  p = finger.image2Tz(2);
  switch (p) {
    case FINGERPRINT_OK:
      lcd.setCursor(0,0);
      lcd.print("Image converted!");
      lcd.setCursor(0,1);
      lcd.print("                ");
      break;
    case FINGERPRINT_IMAGEMESS:
      lcd.setCursor(0,0);
      lcd.print("Image too messy!");
      lcd.setCursor(0,1);
      lcd.print("                ");
      delay(1000);
      return p;
    case FINGERPRINT_PACKETRECIEVEERR:
      lcd.setCursor(0,0);
      lcd.print("  Comunication  ");
      lcd.setCursor(0,1);
      lcd.print("     ERROR!     ");
      delay(1000);
      return p;
    case FINGERPRINT_FEATUREFAIL:
      lcd.setCursor(0,0);
      lcd.print(" No fingerprint ");
      lcd.setCursor(0,1);
      lcd.print("features found  ");
      delay(1000);
      return p;
    case FINGERPRINT_INVALIDIMAGE:
      lcd.setCursor(0,0);
      lcd.print("  Comunication  ");
      lcd.setCursor(0,1);
      lcd.print("     ERROR!     ");
      delay(1000);
      return p;
    default:
      lcd.setCursor(0,0);
      lcd.print("    -Unknown    ");
      lcd.setCursor(0,1);
      lcd.print("     ERROR!     ");
      delay(1000);
      return p;
  }

  // OK converted!
lcd.setCursor(0,0);
lcd.print(" Creating model ");
lcd.setCursor(0,1);
lcd.print("for ID# ");
lcd.setCursor(8,1);
lcd.print(id);

  p = finger.createModel();
  if (p == FINGERPRINT_OK) {
    lcd.setCursor(0,0);
    lcd.print(" Print matched! ");
    lcd.setCursor(0,1);
    lcd.print("                ");
    delay(1000);
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    lcd.setCursor(0,0);
```

```
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
  lcd.setCursor(0,0);
  lcd.print("  Comunication  ");
  lcd.setCursor(0,1);
  lcd.print("     ERROR!     ");
  delay(1000);
  return p;
} else if (p == FINGERPRINT_ENROLLMISMATCH) {
  lcd.setCursor(0,0);
  lcd.print("Fingerprint did ");
  lcd.setCursor(0,1);
  lcd.print("not match       ");
  delay(1000);
  return p;
} else {
  lcd.setCursor(0,0);
  lcd.print("    -Unknown    ");
  lcd.setCursor(0,1);
  lcd.print("     ERROR!     ");
  delay(1000);
  return p;
}

lcd.setCursor(0,1);
lcd.print("ID# ");
lcd.setCursor(4,1);
lcd.print(id);
p = finger.storeModel(id);
if (p == FINGERPRINT_OK) {
  lcd.setCursor(0,0);
  lcd.print("     Stored     ");
   lcd.setCursor(0,1);
   lcd.print("                ");

   delay(1000);
   first_read = false;
   id_ad = false;

 } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
   lcd.setCursor(0,0);
   lcd.print("  Comunication  ");
   lcd.setCursor(0,1);
   lcd.print("     ERROR!     ");
   delay(1000);
   return p;
 } else if (p == FINGERPRINT_BADLOCATION) {
   lcd.setCursor(0,0);
   lcd.print("Could not store ");
   lcd.setCursor(0,1);
   lcd.print("in that location");
   delay(1000);
   return p;
 } else if (p == FINGERPRINT_FLASHERR) {
   lcd.setCursor(0,0);
   lcd.print("Error writing to");
   lcd.setCursor(0,1);
   lcd.print("flash           ");
   delay(1000);
   return p;
 } else {

   lcd.setCursor(0,0);
   lcd.print("    -Unknown    ");
   lcd.setCursor(0,1);
   lcd.print("     ERROR!     ");
   delay(1000);
   return p;
  }
}
```

Figura 37. Programación

4.5 Simulación

Teniendo en consideración la propuesta de diseño electrónico, de software, de control y la funcionalidad componentes electrónicos que forman parte del desarrollo del dispositivo, se realizó la simulación correspondiente en el programa Proteus como se muestra en la figura N°8, el cual muestra en mejor panorama la funcionalidad del dispositivo, asimismo la simulación ayuda a la manipulación de los componentes para mejorar y maximizar el funcionamiento del dispositivo evitando errores.

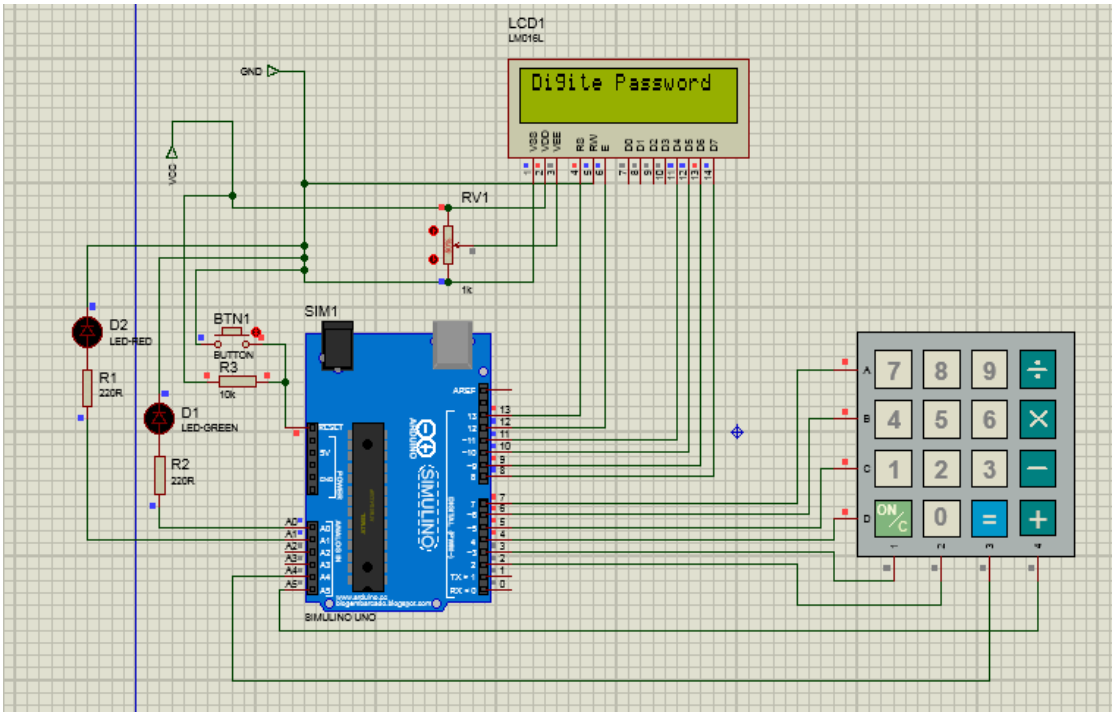


Figura 38. **Simulación**

4.5.1 Pruebas experimentales

Obtenido la implementación de la simulación, se procedió a las pruebas experimentales de funcionalidad, asimismo la corrección de errores y mejoras del dispositivo. Teniendo el funcionamiento óptimo se ejecuta el uso de dispositivo para los fines que fue desarrollado, como se muestra en la figura N°9 la activación del sensor de par (LED-GREEN) se encuentra en un estado encendido, ya que la lectura de la huella dactilar almacena en la memoria del sensor biométrico coinciden y de igual manera el display LCD confirma con un mensaje “Correcto” la aceptación de la lectura de la huella dactilar**.**

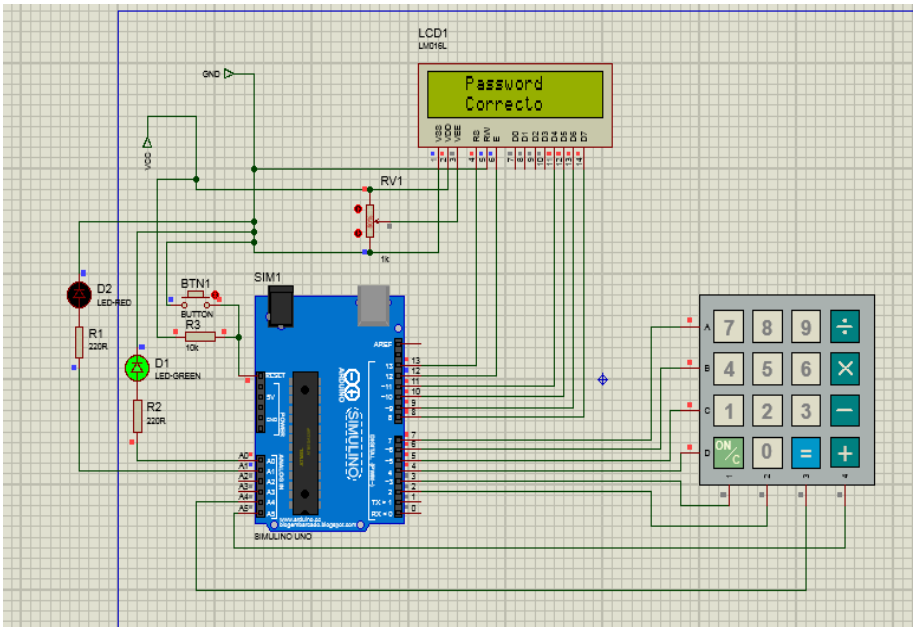


Figura 39. Simulación - aceptación

De igual forma, se procede a la lectura de una huella dactilar distinta a la almacenada en el sensor biométrico para analizar el funcionamiento del dispositivo, el dispositivo tiene un margen de error de tres intentos del cual, como se puede observar en la figura N°10, si el tercer intento no activa el sensor de par (LED-GREEN), dicha salida es direccionada a un sistema de alerta (LED-RED) y de igual manera el display LCD muestra un mensaje “Alerta Policía Intrusos” rechazando la lectura de la huella dactilar.

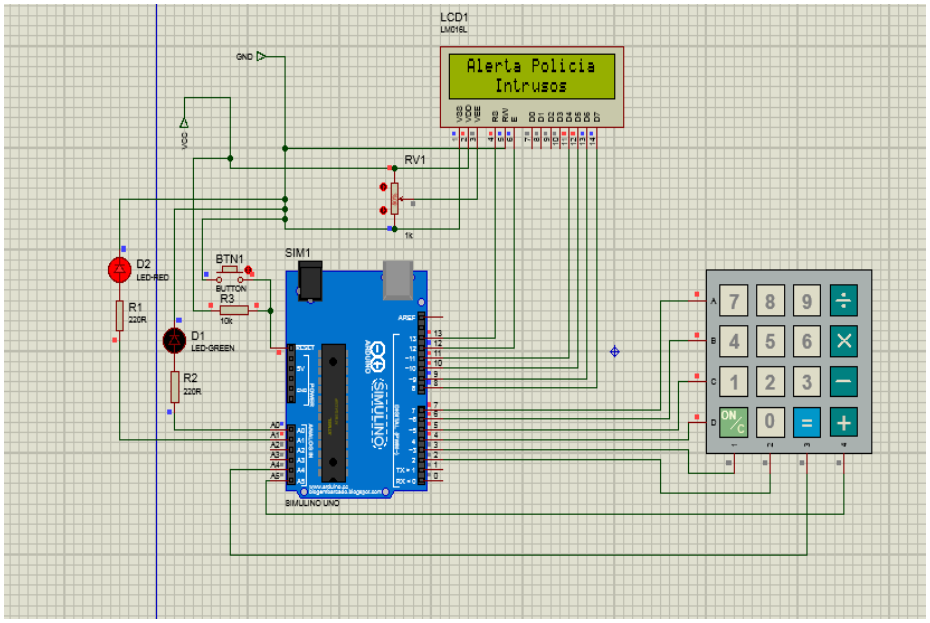


Figura 40. Simulación - rechazo

4.5.2 Pruebas estadísticas

4.5.2.1 Instrumento para análisis experimental

El instrumento a utilizar para nuestro análisis experimental de datos recopilados de nuestras pruebas de simulación es la prueba de diseño factorial $\mathbf{2^3}$, el cual nos da una mejor percepción de la aplicación de los factores utilizados dentro del trabajo de investigación, teniendo en consideración un nivel alto y un nivel bajo para cada factor, también se manipulo dos replicas por cada combinación de tratamiento, de esta forma se busca el mejor resultado óptimo de salida para los fines necesarios del dispositivo a desarrollar.

Tabla 13. ***Diseño factorial 2^3***

LETRA	FACTOR	BAJO (-1)	ALTO (1)
A	Voltaje	3.6v	6v
B	Corriente	65 mA	120 mA
C	Tiempo de Adquisición	800 ms	1000 ms

Tabla 14. Matriz factorial

N°	Combinación de tratamiento	Niveles de tratamiento			Niveles de Respuesta	
		A	B	C	Replica 01	Replica 02
1	[1]	-1	-1	-1	3.35	3.4
2	a	1	-1	-1	5.79	5.75
3	b	-1	1	-1	3.3	3.39
4	ab	1	1	-1	5.8	5.85
5	c	-1	-1	1	3.49	3.55
6	ac	1	-1	1	5.89	5.8
7	bc	-1	1	1	3.39	3.4
8	abc	1	1	1	5.9	5.97

4.5.2.2 Análisis del diseño factorial 2^3

Se realizó el análisis del diseño factorial $\mathbf{2^3}$ con el programa Minitab, llevando a estudio las dos réplicas obtenidas en la matriz factorial de las diferentes combinaciones de tratamiento de los tes factores, buscando la combinación que máxime el uso eficiente del dispositivo a desarrollar. El análisis más importante es saber si los datos son materia de estudio, los valores dados en la tabla N°6 según el valor P con respecto a la significancia $\alpha = 0{,}05$, da a conocer que todas las combinaciones de tratamiento al ser menor que $\alpha = 0{,}05$ son significativos para materia de estudio, entonces podemos afirmar que A(voltaje), C (tiempo de adquisición) y AB (voltaje y corriente); son materia de estudio por lo cual no se puede descartar ni un facto.

Tabla 15. ***Evaluacion varianza***

Nota	GL	SC Ajust.	MC Ajust.	Valor F	Valor p
Modelo	7	23.7807	3.3972	1731.08	0.000
Lineal	3	23.7530	7.9177	4034.48	0.000
A	1	23.7169	23.7169	12085.04	0.000
B	1	0.0000	0.0000	0.01	0.913
C	1	0.0361	0.0361	18.39	0.003
Interaccion de 2 términos	3	0.0234	0.0078	3.98	0.053
A*B	1	0.0225	0.0225	11.46	0.010
A*C	1	0.0000	0.0000	0.01	0.913
B*C	1	0.0009	0.0009	0.46	0.517
Interacciones de 3 términos	1	0.0042	0.0042	2.15	0.180
A*B*C	1	0.0042	0.0042	2.15	0.180
Error	8	0.0157	0.0020		
Total	15	23.7964			

El resumen de modelo mostrado en la tabla N°18 da el valor de la S (varianza de estudio) del que podemos interpretar la variabilidad de datos respecto a la media, con un valor de 0.0443 podemos afirmar que mejor será descrita la respuesta del modelo, de igual forma R-cuadrado ($\mathbf{R^2}$) según su aproximación del 99.93 % al 100 % , tenemos un calidad de modelo aceptable para los resultados. El R-cuadrado (ajustado) de igual forma respecto al 100 %, el 98.57 % según tamaño de la muestra nos da una mejor perspectiva de elegir el modelo correcto, por último, tenemos un 99.74 % de predicción aceptable, según los porcentajes analizados los resultados a obtener serán óptimos y notables.

Tabla 16. ***Resumen modelo***

S.	R-cuad.	R-cuad. (ajustado)	R-cuad. (pred)
0.0443001	99.93%	99.88%	99.74%

La ecuación de regresión en unidades no codificadas proyectada en la tabla N°19 permite una predicción a la respuesta a los factores significativos.

Tabla 17. ***Ecuación regresión unidades no codificadas***

Resultados	= 4.6263 + 1.2175 A - 0.0012 B + 0.0475 C + 0.0375 A*B - 0.0012 A*C - 0.0075 B*C + 0.0163 A*B*C

El Pareto de efectos estandarizados mostrados en la figura N°49, da un mejor entender de qué combinaciones son significativos como muestra de estudio, esto se obtiene a partir de la referencia que se muestra 2.3, todas las combinaciones que sobrepasen la referencia son muestra de estudio.

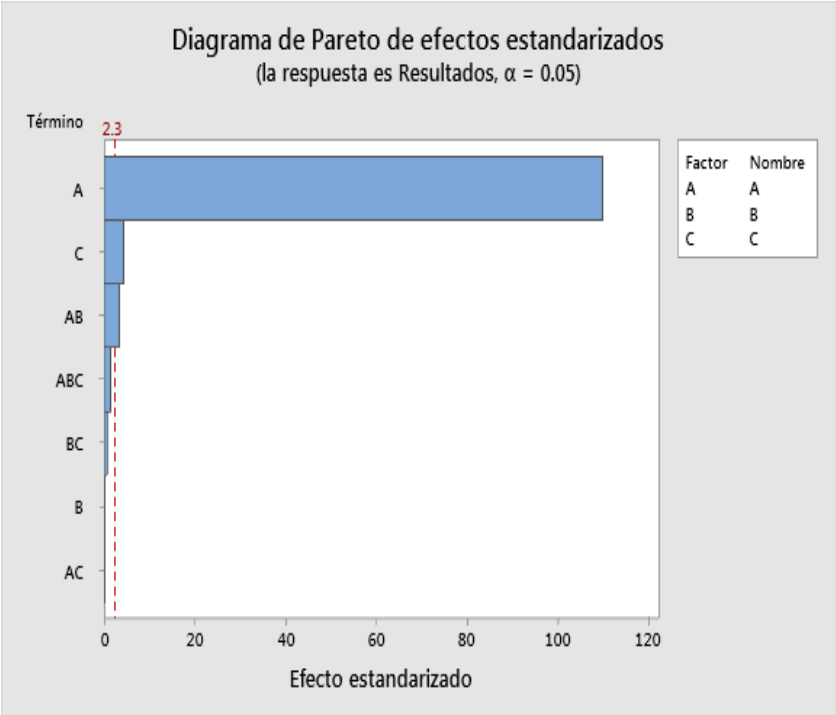


Figura 41. Diagrama de Pareto de efectos estandarizados

La figura N°50 muestra el comportamiento de los residuos manejados. En la gráfica de probabilidad normal, podemos ver que las líneas son rectas, por lo que se puede ver que la gráfica de residuos vs. los puntos de calibración se coloca aleatoriamente a cada lado de la base 0, por lo que los residuos se distribuyen aleatoriamente y siempre son variables. El histograma muestra la simetría de los residuos y, finalmente, el gráfico muestra los residuos en el orden de recopilación de datos.

Figura 42. Gráfica de residuos para resultados

La interpretación de la gráfica de efectos principales para resultados observados en la figura N°13 se enfoca principalmente en el factor A en comparación a B y C, este se puede interpretar que A es mucho más significativo dentro del estudio a comparación de los otros factores, ya que existe una magnitud mayor de efecto en el cambio de nivel baja a alto.

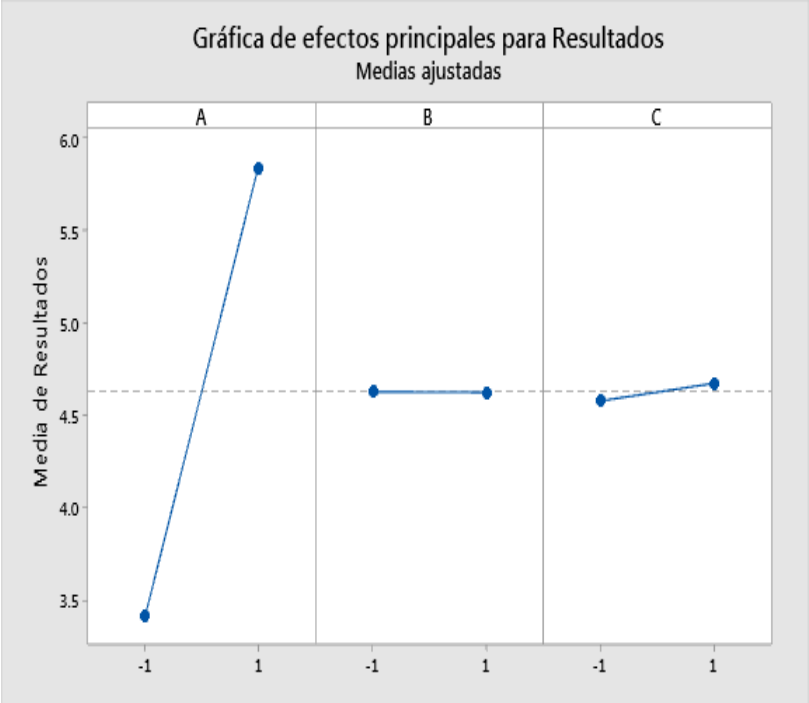


Figura 43. Gráfica de efectos principales para resultados

La interacción de los factores en sus niveles altos y bajos que se expresan en la gráfica de interacción para resultados proyectado en la figura N°14, se explica el funcionar y los cambios de respuesta que obtenemos durante la simulación, por lo que podemos describir que la interacción AB y AC tiene una variación significativa respecto a la manipulación de estos en nivel bajo a un nivel alto.

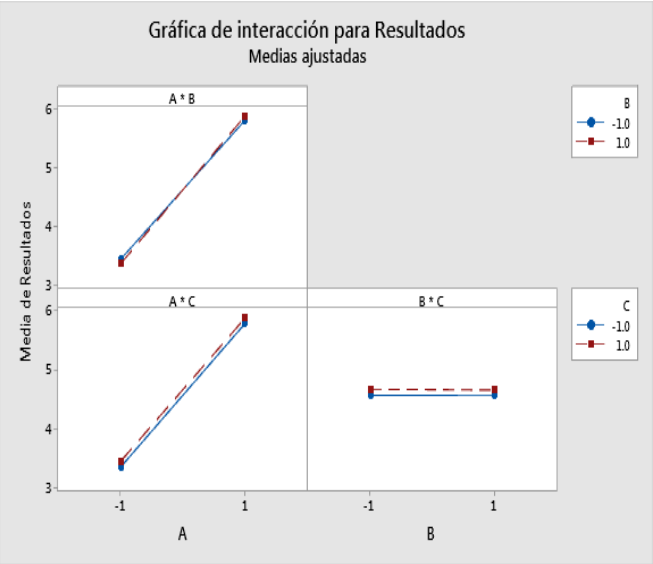


Figura 44. Gráfica de interacción para resultados

Las siguiente grafica de cubos de resultados proyectado en la figura N°15 muestra los valores resultantes de la combinación de A, B y C en sus distintos niveles altos y bajos, del cual se puede observar para el presente estudio que se desea mejorar y maximizar el funcionamiento del dispositivo a desarrollar que la mejor combinación de utilización es factor A en nivel alto (1), factor B en nivel alto (1) y factor C en nivel alto (1), obteniendo un valor 5.935 comparativamente alto con respecto al análisis de las combinaciones realizadas.

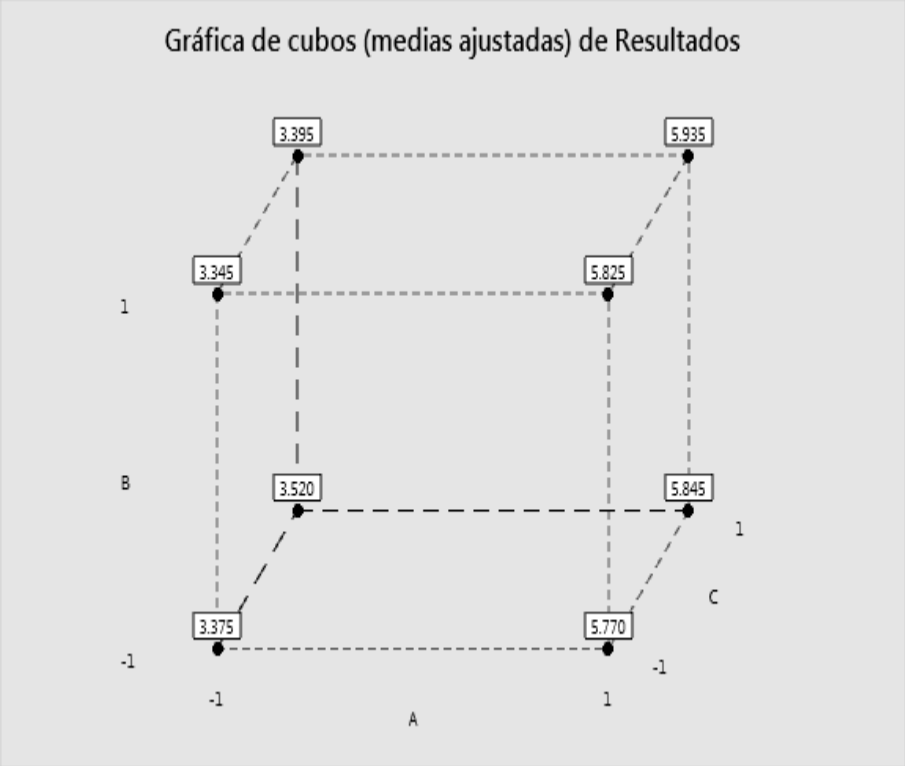


Figura 45. Gráfica de cubos de resultados

4.6 Elección de la mejor solución

El análisis realizado a los 16 niveles de respuesta de las combinaciones de tratamiento de los factores en el programa Minitab, da una solución de maximización de funcionalidad del dispositivo como se muestra en la tabla N°9 con un resultado de 5.935, el cual se obtiene con la combinación de tratamiento de los factores, cada uno en sus niveles altos: factor A en nivel alto (1), factor B en nivel alto (1) y factor C en nivel alto (1).El resultado obtenido es la mejor solución para que nuestro dispositivo sea eficiente y eficaz en su perfeccionamiento.

Tabla 18. ***Solucion***

Solución	A	B	C	Resultados Ajuste	Deseabilidad compuesta
1	1	1	1	5.935	0.986891

La predicción de respuesta múltiple expuesto en la tabla N°10, ratifica que la mejor combinación de tratamiento de los factores que se requiere para maximizar el funcionamiento del dispositivo es la utilización de los tres factores en sus niveles altos respectivamente, de igual forma se destaca en la tabla N°10 el IC intervalo de confianza al 95 % en una margen de 5.8628 a 6.0072, donde localizaremos nuestro resultado de 5.9350. Los valores de la réplica u observaciones se encuentran dentro del intervalo IP de 95% (5,8099; 6,0601).

Tabla 19. ***Predicción respuesta múltiple***

Variable	Valor configuración
A	1
B	1
C	1

Respuesta	Ajuste	EE ajuste	IC 95%	IP 95%
Resultados	5.9350	0.0313	(5.8628, 6.0072)	(5.8099, 6.0601)

4.6.1 Especificaciones técnicas de la solución

Los resultados obtenidos en el análisis del diseño factorial 2^3 proporciona una perspectiva con mayor consistencia en la manipulación de la combinación de tratamiento de los factores, se logra el objetivo previsto de maximizar la funcionalidad del dispositivo a desarrollar, para obtener dichos resultados se manipuló tres factores: voltaje, corriente y tiempo de adquisición, los cuales, como se puede observar en el diagrama de Pareto, son necesarios para realizar y obtener estos resultados. Para el correcto funcionamiento del dispositivo y sus componentes electrónicos que lo conforman se tiene en consideración el factor A (voltaje) en su nivel bajo a 3v y su nivel alto a 6v, el que cómo se observa en la figura N°16 que es el factor que más significancia tiene en la manipulación de combinación de tratamiento de los factores, según la variación del factor A es que se define la salida o resultado con una mínima afectación de los factores B y C. El factor B (corriente) se maneja en su nivel bajo a 65 mA y su nivel alto a 120 mA, de igual manera el análisis del factor B es considerado para el total funcionamiento del dispositivo y sus componentes electrónicos, ya que cada uno independientemente funciona dentro de ese rango. El factor C (tiempo de adquisición) es estudiado únicamente al sensor biométrico en sus niveles de tiempo de lectura, nivel bajo a 800 ms y nivel alto a 1000 ms. Los factores B y C como se muestran en la figura N°16 no son tan significantes dentro del análisis, ya que la variación que generan a la salida o resultados son mínimos, mas no se puede rechazar dichos factores ya que son necesarios en la combinación de tratamiento de los factores. Finalmente, se puede afirmar que si el funcionamiento del factor voltaje a 6 voltios, factor corriente a 120 mA y el tiempo de adquisición del sensor biométrico a 1000 ms se obtiene los resultados requeridos de maximización de funcionamiento del dispositivo a realizar, se tiene un voltaje óptimo para el funcionamiento de los componentes electrónicos, de igual forma un adecuado flujo de corriente por el dispositivo y por último el funcionamiento correcto del sensor biométrico en la lectura de huella dactilar evitando problemas a causas de bajo voltaje, corriente o demoras en la lectura.

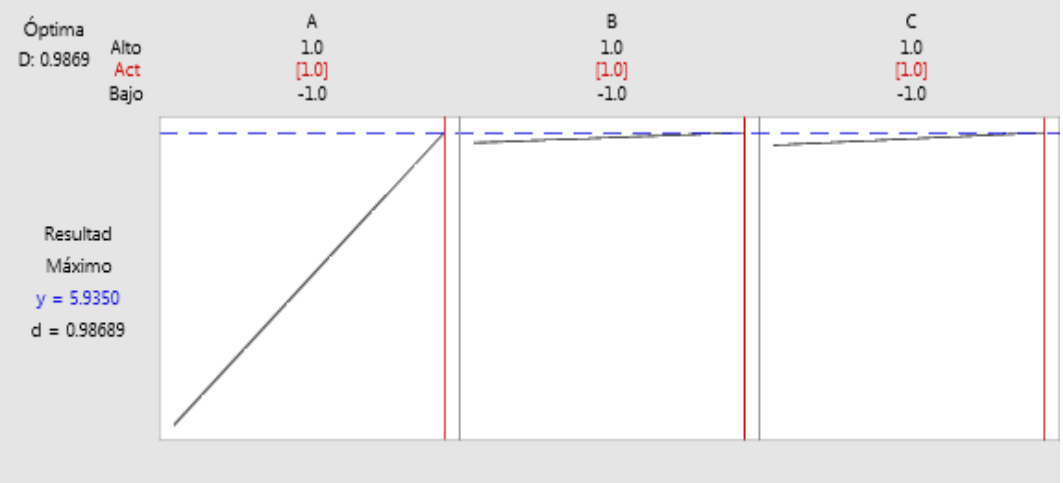


Figura 46. Resultado máximo

4.7 Resultados

El resultado general de la fabricación del dispositivo de seguridad está basado en ser una herramienta que impida vulnerar el accionamiento de la unidad vehicular impidiendo su movilización o traslado por personas extrañas que no registren su descripción dactilar dentro del dispositivo, bloqueando así el sensor de par de activación de la dirección del volante del vehículo sin poder tener ningún direccionamiento. Con este dispositivo se espera llegar a masificar la seguridad por cuanto no debe tener costos excesivos, considerando el parque automotor de esta ciudad y el promedio del poder adquisitivo del usuario, sin restarle el máximo índice de efectividad por este aspecto económico, por consiguiente, el dispositivo de seguridad debe de alcanzar los máximos niveles para lo que está elaborado, de esta manera las pruebas realizadas al diseño factorial 2^3 de manipulación de la combinación de tratamiento de los factores, dan soporte a la realización del dispositivo, los porcentajes y números dados en la prueba estadística realizada nos dan la certeza de un resultado óptimo sin margen a error.

Estos estudios están basados en la vulnerabilidad de los sistemas de seguridad antirrobo de los vehículos, de manera que, la realización del dispositivo debe cumplir con todas las deficiencias e incorreciones de los sistemas antiguos. La simulación da muestra del funcionamiento del sistema, el sensor biométrico hace una lectura de la huella dactilar comparándola con dicha huella recopilada con la base de datos, si se cumple la comparación el sensor de par es activado, existe un margen de error de tres intentos, por lo que si en un tercer intento las comparaciones de huellas no coinciden el voltaje de salida es direccionado a una bocina de alerta. Se puede afirmar que el funcionar del dispositivo de activación del sensor de par como se observa en las pruebas de simulación cumple con las perspectivas de un óptimo sistema de seguridad,

Al aplicar el uso de huella o biometría dactilares, se genera un nivel de seguridad alto, por consecuente que la huella dactilar es un rasgo físico único de cada persona, no pudiéndose falsificar fácilmente. Así, se logra conseguir la activación del sensor de par de la dirección del volante del vehículo únicamente por el propietario y/o personas que hayan almacenado la identificación de huella dactilar en el dispositivo.

4.8 Análisis de resultados

Considerando el planteamiento de los objetivos específicos propuestos en el trabajo de investigación, se estudió el comportamiento de diferentes componentes electrónicos que asumieran un funcionar eficiente para el desarrollo del dispositivo a ejecutar, como base principal del dispositivo se necesitó un microcontrolador programable capaz de ejecutar las órdenes de funcionamiento que deseamos para nuestro dispositivo, como podemos observar en la figura N°55 el módulo Arduino es el dispositivo programable que se utilizó, ya que la disposición del mismo es mucho más accesible, de igual forma la manipulación, reprogramación, corrección de fallas y seguridad es mayor en comparación a otros dispositivos programables. La programación del módulo Arduino es libre y propia del dispositivo, por lo que la gestión de la programación es mucho más sencilla, corrigiendo errores y mejorando su funcionamiento de manera instantánea, de esta manera se realizó la programación obteniendo resultados óptimos del funcionamiento de los principales componentes electrónicos, como el comportamiento del sensor biométrico, del cual podemos afirmar que es un componente idóneo y necesario, que brinda la óptima seguridad que se requiere para el dispositivo. Desarrollado los objetivos específicos, generamos el planteamiento del objetivo general de diseñar el dispositivo de activación del sensor de par de la dirección del vehículo mediante huella dactilar.

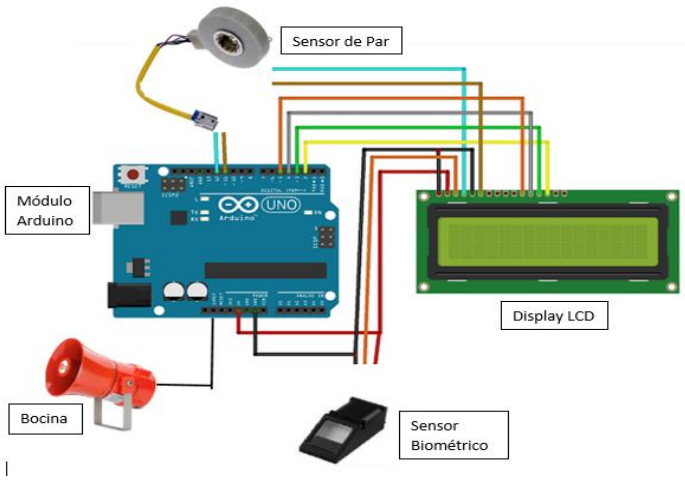


Figura 47. Diseño propuesto

Teniendo el diseño y simulación del dispositivo de activación del sensor de par de la dirección del vehículo mediante la huellas dactilares como se define en la figura N°56, se analizan los resultados del funcionamiento, la programación realizada cumple con su funcionalidad, el sensor de par (LED-GREEN) se encuentra inactivo al igual que el sistema de alerta (LED-RED), en el display LCD se muestra el mensaje "Lectura de huella", eso indica que el dispositivo se encuentra en funcionamiento mas no realiza ninguna otra acción debido a que aún no se hace uso del sensor biométrico.

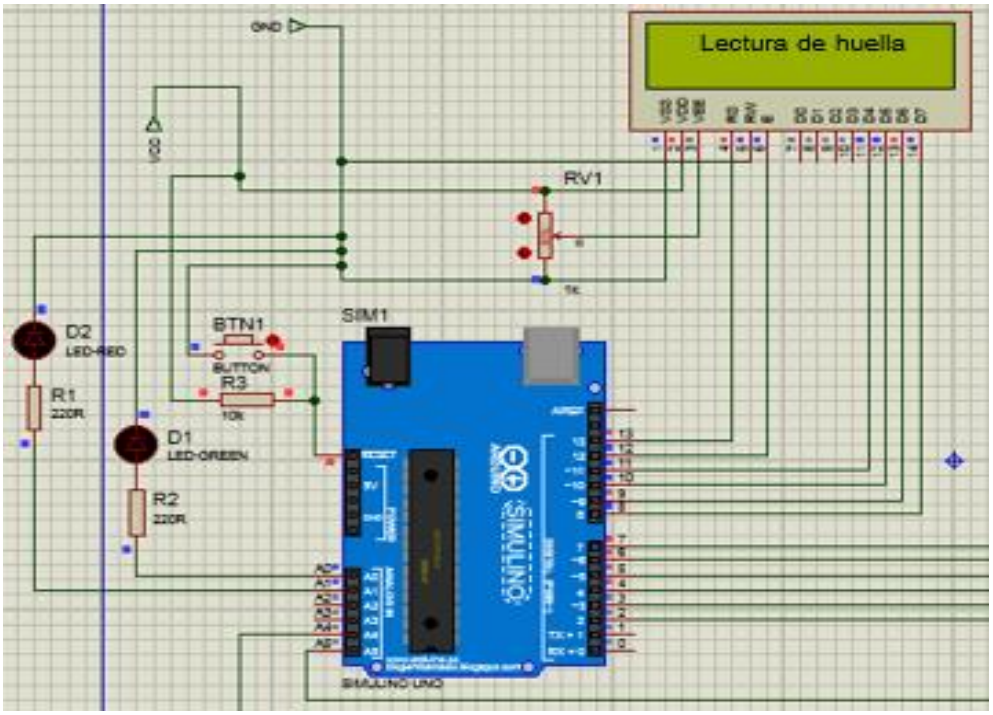


Figura 48. **Circuito del dispositivo**

El principal objetivo del desarrollo del dispositivo es tener una óptima seguridad, que no pueda ser vulnerado. Por lo que el uso del sensor biométrico efectuará estas necesidades perdidas en los sistemas de seguridad antiguos o desfasados. Como se observa en la figura N°57 se hace uso del sensor biométrico, este hace una lectura de la huellas dactilares y la compara con la huella ya almacenadas en la memoria interna o base de datos del dispositivo, realizada la comparación si las huellas dactilares son semejantes el dispositivo tiene una salida en voltaje la cual es direccionada al sensor de par (LED-GREEN) el cual es activado y entra en funcionamiento. Así mismo se muestra un mensaje "Correcto" en el display LCD de confirmación de compatibilidad de la lectura de huella dactilar.

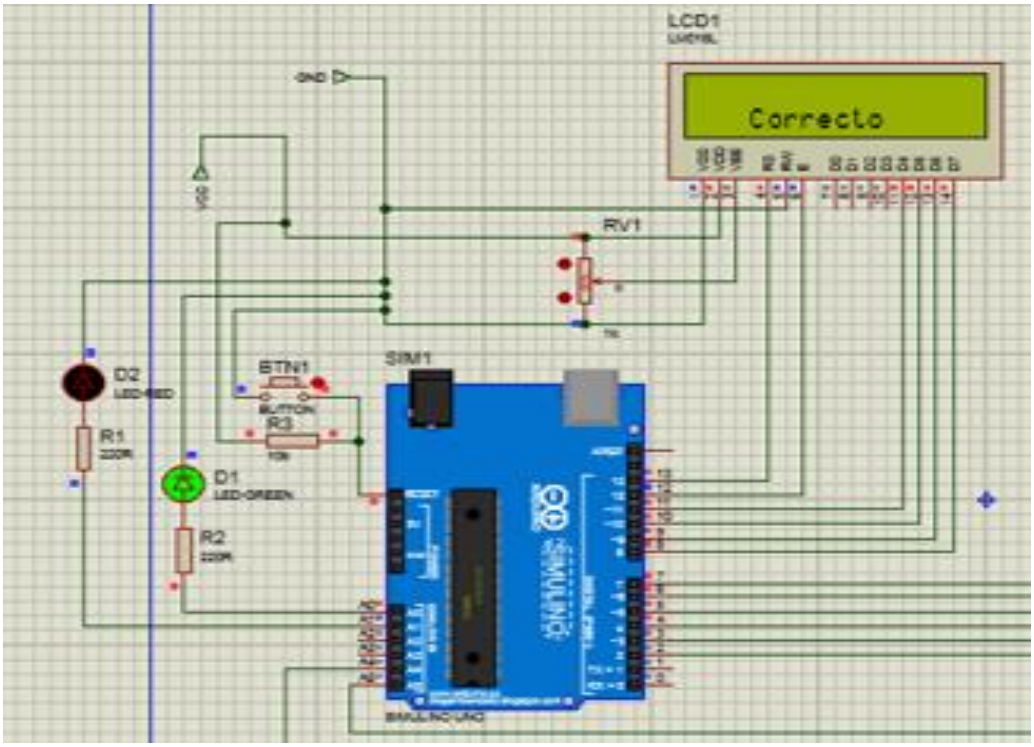


Figura 49. Sensor de par activado

La programación efectuada en el dispositivo permite tener un margen de error de tres intentos de lectura de huella dactilar en comparación de la huella acumulada en la memoria interna o base de dato, la figura N°58 muestra cual es el funcionamiento del dispositivo en caso de que se haya realizado los tres intentos. Si al tercer intento, el dispositivo no encuentra semejanza de las huellas comparadas, direcciona la señal de salida en voltaje a un sistema de alarma “LED-RED” el cual servirá de alerta ante cualquier intruso que quiera accionar el sensor de par de la dirección del vehículo, asimismo se muestra un mensaje “Alerta Policía Intrusos” confirmando el no accionar de sensor de par.

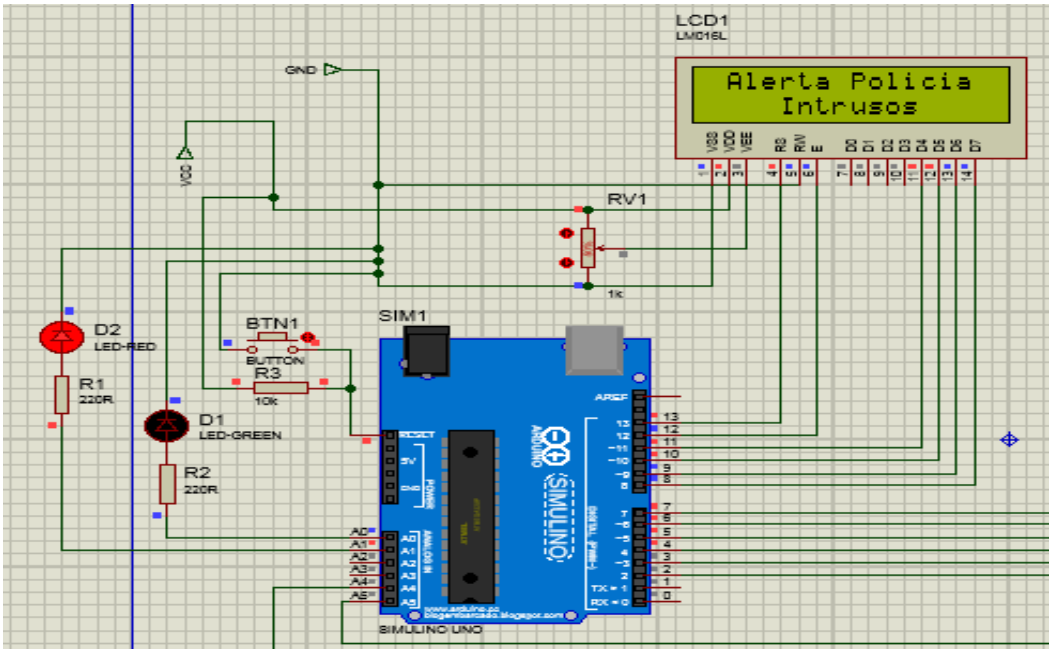


Figura 50. **Sistema de seguridad activado**

Según el análisis de los resultados, se puede confirmar que el dispositivo desarrollado cumple con todas las necesidades y objetivos planteados dentro del trabajo de investigación, con un máximo nivel de uso de los componentes analizados mediante el diseño factorial 2^3, la funcionalidad del dispositivo será eficaz y eficiente en el campo a ser utilizado.

4.8.1 Comparación de resultados con los resultados de los antecedentes

Constantemente se desarrollan sistemas de seguridad, como necesidad fundamental de la persona, debido a la gran cantidad de delincuencia que muchas veces afecta la propiedad y la salud. En el año 2017, Giraldo y Gómez desarrollan el proyecto de tesis titulado: "Estado del arte de la seguridad en sistemas biométricos", en el que demuestran que los rasgos biométricos, al ser únicos en cada ser humano, se usan para reconocer y autenticar con la evaluación de patrones y/o descripción físicas, comparando registros de los datos previamente almacenados. Del mismo modo, los estudios realizado en esta tesis indican que el rasgo biométrico de reconocimiento de huella dactilar obtiene una valoración mayor a diferencia de otros rasgos biométrico es por ello el uso de huella dactilar es usada en el desarrollo del dispositivo de activación del sensor de par de la dirección del vehículo mediante huella dactilar.

La aplicación de los rasgos biométricos como seguridad abarca un gran campo de aplicación, por consiguiente, en la ciudad de Arica, Víctor, en el 2014, presenta la tesis titulada: «Diseño de un sistema de seguridad en base a control, monitoreo, y visualización de acceso mediante huella dactilar a la Clínica San José de Arica», que se enfoca en el acceso y registro de personas a la Clínica San José de Arica mediante huella dactilar, el funcionar de este sistema incluye un

registro de patrones e información de datos, no cuenta con ninguna sistema de alerta o bloqueo de acceso, más solo en el control de ingreso y salida de las personas, a diferencia del dispositivo de activación del sensor de par de la dirección del vehículo mediante huella dactilar, compara la lectura de huella dactilar con la almacenada, si no coinciden se activa el sistema de alerta y bloquea en acceso a la volante del vehículo.

En la Universidad Pontificia Universidad Católica del Perú; Palacios, Vargas y Leyton, presentaron la tesis titulada: "Diseño e implementación de un sensor biométrico de seguridad para viviendas", a partir del cual se propuso mejoras que ayuden a la eficiencia del dispositivo de activación del sensor de par de la dirección del vehículo mediante huella dactilar, uno de ellos el uso del módulo Arduino en comparación con el microcontrolador, ya que se tenía un mejor manejo y fácil corrección de fallas de la programación, también en consideración el análisis factorial, permite tener una mejor respuesta de utilización de los componentes electrónicos, con el adecuado uso de voltaje, corriente y tiempo de adquisición.

4.9 Análisis de mercado y económico

4.9.1 Costo de inversión

La inversión efectuada comprende los recursos humanos, referido a la cantidad de personas que presentan o brindan sus servicios y conocimientos para la realización y ejecución del proyecto. Los recursos materiales, son los elementos y componentes para ver nuestro proyecto en escrituras, de igual manera la tabla N 11 se muestra los servicios necesarios a utilizar y el costo de utilización, obteniendo un costo de inversión total de S/ 7810.00.

Tabla 20. ***Costo de inversión***

Denominación	Cantidad	Precio unitario s/.	Precio total s/.
Recursos humanos			
Responsable del proyecto	1	2000.00	2000.00
Asesoramiento	1	1000.00	1000.00
Colaborador(es)	2	250.00	500.00
Recursos materiales			
Computadora	1	1200.00	1200.00
Impresora	1	750.00	750.00
Libros y separatas	3	50.00	150.00
Útiles de oficina		300.00	300.00
Otros		100.00	100.00
Servicios			

Internet		1200.00	1200.00
Fotocopias		150.00	150.00
Digitación		100.00	100.00
Recolección de información		150.00	150.00
Anillado (juego)	3	10.00	30.00
Encuadernación (juego)	3	10.00	30.00
Pasajes		100.00	100.00
Otros		50.00	50.00
C. TOTAL S/			7810

4.9.2 Evaluación económica

Obtenido el costo total de inversión del trabajo de investigación, se realiza la evaluación económica, necesaria para poder observar la proyección económica de los próximos 10 años, asimismo el comportamiento económico que tendrá nuestro dispositivo, si será viable económicamente, si se obtendrá ganancias o si se tendrá perdidas en su ejecución.

Tabla 21. ***Costo de inversión***

PROYECTO ALTERNATIVO N° 1	PERIODO "0"	Año 1	Año 2	Año 3	Año 4	Año 5	Año 6	Año 7	Año 8	Año 9	Año 10
I. COSTOS DE INVERSIÓN	7,810.00										
I.1 COSTOS DE INVERSION INICIAL	7,810.00	-	-	-	-	-	-	-	-	-	-
		-	-	-	-	-	-	-	-	-	-
Recursos Humanos	3,500.00										
Recursos Materiales	2,500.00										
Servicio	1,810.00										
I.2. COSTOS DE OPERACIÓN Y MANTENIMIENTO		3,120	3,120	3,120	3,120	3,120	3,120	3,120	3,120	3,120	3,120
1.2.1 COSTOS OPERATIVOS		3,120	3,120	3,120	3,120	3,120	3,120	3,120	3,120	3,120	3,120
Personal (30)		360	360	360	360	360	360	360	360	360	360
servicio (electricidad, internet, etc)		600	600	600	600	600	600	600	600	600	600
materiales y equipos (180)		2,160	2,160	2,160	2,160	2,160	2,160	2,160	2,160	2,160	2,160
II. Ingresos		5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400
2.1. COSTOS DE OPERACIÓN Y MANTENIMIENTO		5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400
2.1.1. Costos de operación y mantenimiento		5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400	5,400
Ventas x unidad (350)		4,200	4,200	4,200	4,200	4,200	4,200	4,200	4,200	4,200	4,200
Servicios (100)		1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200	1,200
III. COSTOS INCREMENTALES (I - II)	7,810.00	(2,280)	(2,280)	(2,280)	(2,280)	(2,280)	(2,280)	(2,280)	(2,280)	(2,280)	(2,280)

Los indicadores económicos mostrados en la tabla N°13 s dan a conocer si el proyecto es viable o no económicamente, según la proyección futuras la tasa interna de retorno(TIR) resulta un 23 %, por lo tanto, se afirma que el dispositivo a realizar retribuye lo invertido, con un tiempo aproximado de tres años como muestra la tabla N°13, el valor actual neto (VAN) igual a S/ 8,232.44 y la relación beneficio costo igual a 2.18 son datos que sustentan la viabilidad del proyecto.

Tabla 22. ***Indicadores económicos***

Tasa de Descuento Empleada	12%
TIR	29%
VAN	8,232.44
Tiempo de Recupero de la Inversión (años)	3.43
BENEFICIO/COSTO	2.18

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

1. La naturaleza del dispositivo de seguridad está basado en ser una herramienta que impida vulnerar el accionamiento de la unidad vehicular impidiendo su movilización o traslado por personas extrañas que no registren sus descripciones dactilares dentro del dispositivo, bloqueando así el sensor de par de activación de la dirección del volante del vehículo sin poder tener ningún direccionamiento, es consecuencia de otros casos basados en la vulnerabilidad de los sistemas de seguridad antirrobo de los vehículos, de manera que, la realización del dispositivo debe cumplir con todas las deficiencias e incorreciones de los sistemas antiguos.

2. Al aplicar el uso de huella o biometría dactilar generamos un nivel alto de seguridad, dado que, la huella dactilar es un rasgo físico único de cada persona, no pudiéndose falsificar fácilmente, tiene como finalidad evitar la suplantación de la persona, logrando así conseguir la activación del sensor de par de la dirección del volante del vehículo únicamente por el propietario y/o personas que hayan almacenado la identificación de huella dactilar en el dispositivo.

3. Se desarrolló y generó la programación para el mejor funcionamiento del módulo Arduino; es libre y propia del dispositivo, por lo que la manipulación de la programación es mucho más sencilla, corrigiendo errores y mejorando su funcionamiento de manera instantánea, de esta forma se realizó la programación obteniendo resultados óptimos del funcionamiento de los principales componentes electrónicos, optimizando de manera eficaz el comportamiento

del sensor biométrico, del cual podemos afirmar que es un componente idóneo y necesario, que brinda la óptima seguridad que se requiere para el dispositivo.

4. En ese sentido, con este dispositivo alcanzaremos masificar la seguridad del parque automotor en la ciudad de Huancayo, por cuanto los costos de desarrollo no deben ser excesivos, considerando el promedio del poder adquisitivo del usuario, sin restarle el máximo índice de efectividad por este aspecto económico, por consiguiente, el dispositivo de seguridad debe de alcanzar los máximos niveles para lo que está elaborado, de esta manera las pruebas realizadas y manipulación de la combinación de tratamiento de los factores, dan soporte a la realización del dispositivo, los porcentajes y números dados en la prueba estadística realizada otorgan la certeza de un resultado óptimo sin margen a error.

5. Todos estos elementos apuntados están basados en ser una herramienta que impida vulnerar el accionamiento de la unidad vehicular impidiendo su movilización o traslado por personas extrañas que no registren sus descripciones dactilares dentro del dispositivo, permiten afirmar que no se trata de un dispositivo más de las demás existentes, sino que se trata de un óptimo sistema de seguridad.

5.2. Recomendaciones

1. Teniendo en consideración que el uso de huella o biometría dactilar genera un nivel alto de seguridad, este sistema de seguridad debería de aplicarse a todo tipo de vehículos; implementándose, este dispositivo como un sistema integrado para las puertas, capot e incluso en el sistema de alimentación de combustible de los vehículos , asimismo en vehículos menores (motos, bicicletas y otros). Este dispositivo de seguridad debe masificarse para la implementación en las viviendas y en otros bienes patrimoniales que requieran de este sistema de seguridad biométrica.

2. Un proyecto económico que se puede ampliar y crear una industria de última generación que ofrezca precios bajos a los usuarios que quieran mejorar la seguridad de su vehículo.

3. Probado en varios vehículos de distintas marcas y modelos para garantizar un rendimiento constante en todos los casos.

4. Se decidió con base en los objetivos de El desarrollo de este proyecto que este sistema ofrece un alto nivel de seguridad para los vehículos ya que los usuarios pueden instalarlo como una seguridad adicional a la existente, sin importar el tipo de vehículo, esta es una de las

descripciones más importantes que hacen mucho. Prototipo versátil, fiable y sobre todo seguro.

5. Las alarmas de automóviles conectadas y los sistemas de huellas dactilares también pueden monitorear el estado del automóvil desde una perspectiva de seguridad.

REFERENCIAS BIBLIOGRÁFICAS

1. INEI. Estadística de Seguridad Ciudadana. Junio- Diciembre de 2018. [En línea] INEI, 2018 [Fecha de consulta: 23 de febrero del 2024] Disponible en: https://www.inei.gob.pe/media/MenuRecursivo/boletines/04-informe-tecnico-n04_estadisticas-seguridad-ciudadana-ene-jun2018.pdf
2. CASTILLO, German. Parque Automotor en Huancayo. Revista Correo, junio de 2018, págs. 1-2.
3. SIVYTEC SAS. Equipos de Seguridad Electrónica. [En línea] 2018 [Fecha de consulta: 23 de febrero del 2024] Disponible en: https://www.vitec.com.co/
4. DEL POZO, Carlos. Memoria de investigación 2012. [En línea]Universidad de las Palmas [Fecha de consulta: 23 de febrero del 2024] Disponible en: https://sudocument.ulpgc.es/files/original/92c8af328e16d8e09519a05a68bdbec264da2661.pdf
5. CASABÓN, Julián. Desarrollo de proyectos en la ingeniería electrónica, un método fundamental para la evolución de la ciencia aplicada. [En línea] Colombia, Universidad de Nariño, 2014. [Fecha de consulta: 18 de marzo del 2024] Disponible en: file:///C:/Users/User/Downloads/biteca,+997-1297-1-PB.pdf
6. LEON, Susan. Avances en técnicas biométricas y sus aplicaciones en seguridad. [En línea] Universidad de Carabobo, Valencia, 2011. [Fecha de consulta: 23 de febrero del 2024] Disponible en: https://alfa-redi.org/sites/default/files/articles/files/leon.pdf
7. CORTÉS, Jimy, MEDINA, Francisco y MURIEL, José. Sistemas de Seguridad basados en biometría . *Scientia Et Technica.* 2010, diciembre, XVII (46), pp. 98-102
8. PRO, Luzmila, GONZALES, Juan, CONTRERAS, Walter y YAÑEZ, Carlos. Tecnologías biométricas aplicadas a la seguridad en las organizaciones. *Revista de Ingeniería de Sistemas e Informática.* 2009, julio - diciembre, 6 (2), 55 - 66.
9. GIRALDO, Andrea y GOMEZ, Diana. Estado del arte de la seguridad en sistemas biométricos. Monografía (Título de Especialista en Seguridad Informática). Bogotá: Universidad Abierta y a Distancia -UNAD, 2017, 94 pp.
10. SOTO, Víctor. Diseño de un sistema de seguridad en base a control, monitoreo y visualización de acceso mediante huella dactilar a la Clínica San José de Arica. Tesis (Título de Ingeniero Eléctrico). Tarapacá: Universidad de Tarapacá, 2014.
11. LIZANO, Washington, PALACIOS, Kleber, VARGAS, Miguel y LEYTON, Edgar. Estudio y diseño de un sistema de vigilancia y monitoreo de video en tiempo real, sobre una red IP, para un terminal de despacho y bombeo de combustible de la gerencia regional

sur de PETROCOMERCIAL. [En línea]Lima, 2009. [Fecha de consulta: 23 de febrero del 2024] Disponible en: https://dspace.espol.edu.ec/bitstream/123456789/665/1/1171.pdf

12. MOTOROK. Dirección electro asistida, ¿qué es y cómo funciona este sistema? [En línea] 20 de Febrero de 2020. [Fecha de consulta: 7 de mayo del 2024] Disponible en: https://www.motorok.com/noticias/en-que-consiste-direccion-electroasistida/.
13. TOYOTA. Sistema Antirobo Vehiculos Toyota. Tokio: Toyota, 2010.
14. MAYA, Adriana. Sistema biométrico de reconocimiento de huella dactilar en control de acceso de entrada y salida. [En línea]Bogotá, 2013 [Fecha de consulta: 7 de mayo del 2024] Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/11168/MayaVargasAdriana2013.pdf?sequence=1&isAllowed=y
15. ARDUINODHTICS. Arfuinmo. Tecnología para todos [En línea] 2019. Fecha de consulta: 7 de mayo del 2024] Disponible en: https://arduinodhtics.weebly.com/iquestqueacute-es.html

ANEXOS

Anexo 1

Matriz de consistencia

"Diseño de un sistema antirrobo mediante huella dactilar para optimizar la seguridad de los vehículos M1 en Huancayo"

Problemas	Objetivos	Hipótesis	Variables	Metodología de investigación
¿Cómo diseñar un sistema antirrobo mediante huella dactilar para optimizar la seguridad en vehículos M1 en Huancayo?	Diseñar un sistema antirrobo del vehículo mediante huella dactilar para optimizar la seguridad en vehículos M1 en Huancayo.	El diseño del sistema antirrobo mediante huella dactilar optimiza la seguridad de los vehículos M1 en Huancayo.	**Independiente** Diseño de un sistema antirrobo mediante huella dactilar.	**Método** Científico **Tipo** Cuantitativo **Nivel**
¿Cuál es el funcionamiento del sensor biométrico en la implementación del sistema antirrobo mediante huella dactilar del vehículo?	Analizar el funcionamiento del sensor Biométrico en la implementación del sistema antirrobo mediante huella dactilar del vehículo.	El funcionamiento del sensor Biométrico se activa en la implementación del sistema antirrobo mediante huella dactilar del vehículo.		descriptivo y explicativo **Diseño** Analítico **Población** Está constituida por todos los vehículos de la ciudad de Huancayo.
¿En qué forma el sistema antirrobo del vehículo mediante huella dactilar optimiza la seguridad vehicular M1 en Huancayo?	Determinar en qué forma el sistema antirrobo del vehículo mediante huella dactilar optimiza la seguridad vehicular M1 en Huancayo.	El sistema antirrobo del vehículo funciona correctamente mediante huella dactilar optimizando la seguridad vehicular M1 en Huancayo.	**Dependiente** Optimización de la seguridad de los vehículos M1 en Huancayo.	**Muestra** La muestra viene a ser los vehículos M1 de Huancayo, que no cuentan con un sistema antirrobo.

Anexo 2

Comandos de programación e intercomunicación del lector de huella digital

Code	System Information	Value Range	Default Value	
0x02	SI_USING_LOG	True/False	False	
0x17	SI_IDENTIFY_TIMEOUT	255 or 10~250	30	100ms tick
0x18	SI_RELAY_TIME	0 or 1~100	10	100ms ticks
0x19	SI_CAPTURE_TIMEOUT	More than 10	50	100ms ticks
0x20	SI_IMAGE_BRIGHTNESS	0~100	45	100 - brightest
0x21	SI_IMAGE_GAIN	1,2,4,8	2	
0x22	SI_IMAGE_CONTRAST	0~100	20	
0x28	SI_ADAPTIVE_CAPTURE	True/False	False	
0x30	SI_VERIFY_SECURITY_LEVEL	1~9	5	
0x31	SI_IDENTIFY_SECURITY_LEVEL	6~9	8	
0x32	SI_REGISTER_QUALITY	30~100	40	
0x33	SI_VERIFY_QUALITY	10~100	30	
0x49	SI_CHANNEL1_BAUDRATE	0 – 115200 1 – 57600 2 – 38400 3 – 19200 4 – 9600	4	
0x4A	SI_CURR_CHANNEL_BAUDRATE			
0x50	SI_MAX_USER			
0x51	SI_FP_FULL_ROTATION	True/False	False	
0x52	SI_LENGTH_OF_USER_ID	4~15	10	
0x53	SI_NUM_OF_ADAPTIVA_CAP	1~10	5	
0x54	SI_MAX_TEMPLATE			Read Only

Anexo 3

GLOSARIO DE TÉRMINOS BÁSICOS

Biometría

En la actualidad, la huella digital es la solución biométrica más expandida y conocida por un gran público, pero no es la única. De esta forma, la biometría es el análisis morfológico de los caracteres únicos de una persona, el cual puede efectuarse con huellas digitales, el iris, las venas y además, la morfología de la mano. La lectura de la biometría puede ser recopilada y guardada en una memoria interna con la que cuenta la mayoría de los sensores biométricos, posteriormente este se usa en comparación con la lectura actual de biometría.

Identificación biométrica

La biometría se encuentra en la medida de las Descripciónmorfológicas únicas de un individuo. En sólo unos años, esta tecnología de punta se convirtió en el medio más confiable de identificación de una persona. Llegó a sustituir o reforzar los dispositivos de memoria o tarjetas de acceso, las cuales podían presentar fallas en materia de seguridad. La identificación biométrica abarca muchos campos que se encuentra ligado con los rasgos físicos de la persona, para el presente trabajo de investigación se tiene en consideran el uso de identificación biométrica que vendría a ser el de identificación mediante huella dactilar.

Falsa aceptación

La tasa de falsa aceptación, o TFA, es la medida de la probabilidad de que el sistema de seguridad biométrico acepte incorrectamente un intento de acceso por parte de un usuario no autorizado. La TFA de un sistema generalmente se establece como la relación del número de aceptaciones falsas dividido por el número de intentos de identificación" (18); por ejemplo, alguien podría clonar una credencial de identificación, o adueñarse de los números confidenciales de una persona para hacer una transacción en perjuicio de su legítimo dueño y hasta falsificar su firma.

Falso rechazo

Consiste en no aceptar a alguien que SI es ya que su identificación no se pudo realizar debido a múltiples motivos, como por ejemplo: que la imagen de la huella capturada por el dispositivo lector esté muy dañada, o a que tenga una capa de suciedad, o que el lector no tenga la calidad suficiente para tomar correctamente la lectura y, en el peor de los casos, que la huella dactilar de la persona haya sufrido algún tipo de deformación ya sea por cortes o quemaduras.

Metodología de desarrollo

Reglas y procedimientos que nos guían en el desarrollo de un proyecto.

Modelo de datos

Estructura en la cual se representa o se plasma una realidad de la manera más convenientemente posible, teniendo en cuenta que este modelo plasma objetivos a trazar.

Base de datos

Base de datos es la representación de la realidad (entiéndase como organización) en forma de datos; los que están entrelazados de la manera más coherente posible, almacenados con una redundancia calculada y estructurados de tal manera que facilite su explotación, y que se pueda satisfacer las necesidades de información de los diferentes usuarios.

Sistema de información

Sistema manual o automatizado que comprende personas, máquinas y/o métodos organizados para recolectar, procesar, transmitir y diseminar datos que representen la información del usuario.