UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE INGENIERÍA AUTOMOTRIZ

DESARROLLO DE UN SISTEMA DE SEGURIDAD PARA CONTROLAR EL ENCENDIDO DE UN VEHÍCULO SUBCATEGORÍA L3, BASADO EN UN MÉTODO DE AUTENTICACIÓN POR RECONOCIMIENTO FACIAL

Trabajo de titulación previo a la obtención del
Título de Ingeniero Automotriz

AUTORES: ANDRÉS DAVID GUALLASAMIN CHASI
BRAYAN FERNANDO GUALLICHICO GUALLICHICO

TUTOR: JHONNY JAVIER BARRERA JARAMILLO

Quito - Ecuador

2024

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Andrés David Guallasamin Chasi con documento de identificación N° 1719904433 y Brayan Fernando Guallichico Guallichico con documento de identificación N° 0850472804 manifiestos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 15 de febrero del año 2024

Atentamente,

Andrés David Guallasamin Chasi
1719904433

Brayan Fernando Guallichico Guallichico
0850472804

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, Andrés David Guallasamin Chasi con documento de identificación No. 1719904433 y Brayan Fernando Guallichico Guallichico con documento de identificación No. 0850472804 expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Proyecto Técnico: "Desarrollo de un sistema de seguridad para controlar el encendido de un vehículo subcategoría L3, basado en un método de autenticación por reconocimiento facial", el cual ha sido desarrollado para optar por el título de Ingenieros Automotrices, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana

Quito, 15 de febrero del 2024

Atentamente,

Andrés David Guallasamin Chasi
1719904433

Brayan Fernando Guallichico Guallichico
0850472804

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Jhonny Javier Barrera Jaramillo con documento de identificación N° 1400378475, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: DESARROLLO DE UN SISTEMA DE SEGURIDAD PARA CONTROLAR EL ENCENDIDO DE UN VEHÍCULO SUBCATEGORÍA L3, BASADO EN UN MÉTODO DE AUTENTICACIÓN POR RECONOCIMIENTO FACIAL, realizado por Andrés David Guallasamin Chasi con documento de identificación No. 1719904433 y Brayan Fernando Guallichico Guallichico con documento de identificación No. 0850472804, obteniendo como resultado final el trabajo de titulación bajo la opción: Proyecto Técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 15 de febrero del 2024

Atentamente,

Ing. Jhonny Javier Barrera Jaramillo, MsC
1400378475

DEDICATORIA

Dedico el presente proyecto principalmente a mis padres: Jaime y Cecilia, quienes han sido el pilar fundamental en este camino de formación profesional, por ser mi compañía en las noches de desvelo, en los momentos de frustración ser mi calma y, en los instantes de desesperación ser el consuelo y alivio. No puedo dejar de lado a mis hermanos: Fernando y Mónica, quienes son y serán mi ejemplo a seguir, que con sus virtudes y defectos han sido una inspiración más para no rendirme; gracias a mis cuñados, sobrinos y amigos.

Andrés D. Guallasamin C.

Dedico el presente proyecto a Dios por darme el privilegio de estudiar, a mis padres por todo su esfuerzo diario por darme todo lo que necesite para mis estudios y poner toda su confianza en mí para culminar la carrera universitaria.

Brayan F. Guallichico G.

AGRADECIMIENTO

Agradezco a Dios por haberme permitido alcanzar una meta más en mi vida. A mis padres por todo el esfuerzo que día con día realizaron para que no me falte nada en el trayecto de mi formación profesional. A mis hermanos y cuñados por sus consejos, por siempre tener la predisposición de escucharme y brindarme palabras de aliento cuando sentía que no podía más; a mis sobrinos, quienes cada que podían me recordaban lo importante que significo y reflejo en su vida. A mis queridos amigos "LOS CONFYS", como nos hacíamos llamar; quienes hicieron de esta travesía Universitaria un segundo hogar, un lugar dónde a pesar de las dificultades las risas no faltaron. Agradezco a mi compañero de Tesis, por el trabajo y la entrega que demostró en el proyecto; gracias también a nuestro tutor de Tesis, Ing. Jhonny Barrera; quién siempre estuvo presente en el desarrollo del proyecto, por brindarnos su apoyo y direccionamiento para alcanzar el objetivo del presente escrito. Un agradecimiento rotundo a una persona especial que la dejaré en anónimo porque "aquella" sabe lo especial e importante que significa en mi vida, gracias por el acompañamiento en toda esta travesía; por ser un apoyo más, un alivio, una solución y por todo el cariño y afecto que supo demostrar; manteniendo la frase "¿QUE EQUIPO SOMOS?; EL EQUIPO DINAMITA". Sin más, agradecido con todas las personas de todo mi entorno que no las nombro porque no acabaría, pero desde lo profundo de mi corazón "Gracias Infinitamente" porque cada uno de ustedes, forman parte de este logro.
"Una vida sin el amor de la familia, sin el acompañamiento de las amistades; es una muerte lenta, porque irse sin dejar huella es como nunca haber existido".

Andrés D. Guallasamin C.

Agradezco a Dios, primeramente, por la dicha que me dio de poder culminar mis estudios, después a mi madre Rocío Guallichico y a mi padre Darwin Cuji por el apoyo emocional y económico inmensurable a lo largo de mi formación profesional ya que sin ellos y sin Dios no sería nada de esto posible, a mi hermana por haber estado ahí cuando la necesitaba, también agradezco a todas las personas que han estado ahí conmigo a lo largo de esta travesía de mi carrera universitaria; amigos, abuelos, tíos, primos y enamorada que han sabido también brindarme su apoyo en todo este trayecto.
Agradezco también a mi compañero de tesis por el apoyo y dedicación en el trabajo de titulación, al tutor de Tesis Ing. Jonny Javier Barrera Jaramillo por su apoyo desde el principio hasta el final en el proyecto, por su valioso tiempo para las revisiones e incondicional ayuda.

Brayan F. Guallichico G.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El robo de vehículos subcategoría L3, constituye actualmente uno de los delitos que más ha crecido en los últimos años, debido principalmente a que sus sistemas de seguridad son incipientes y/o no siempre son efectivos lo que los convierte en vehículos muy vulnerables. Además de ser objetivos de robos, son utilizadas también como herramientas para realizar otros actos delincuenciales, gracias a las altas velocidades que pueden lograrse, a su facilidad de maniobrabilidad y a la rapidez con la que pueden abordarse o abandonarse estos vehículos.

Si bien, en la actualidad ya existen sistemas de seguridad antirrobo para motocicletas, se ha detectado que fácilmente son vulnerados por los delincuentes debido a su exposición y a su tipo de construcción que casi siempre es de tipo mecánica. Así tenemos los candados a los discos o las trabas del volante; los mismos que no presentan ningún desafío a los delincuentes. Esta situación, constituye entonces una realidad que requiere de la implementación de un sistema de seguridad antirrobo de alta innovación y que aproveche la tecnología; haciendo uso de técnicas de autenticación por reconocimiento facial para el reconocimiento del propietario u otras personas autorizadas. Para lograr esto, se utilizará un microcomputador Raspberry Pi, en el cual se entrenará una red neuronal programada y se alojará una base de datos creada mediante el lenguaje de programación “Python”. La red neuronal entrenada y programada, permitirá la validación del usuario, comparando el rostro detectado con la base de datos y así permitir el encendido del vehículo o denegar el mismo. En su diseño se considerarán diversos factores climáticos y de iluminación del entorno, lo cual permitirá demostrar la efectividad del sistema, y el comportamiento del mismo en las distintas condiciones, con la finalidad de lograr un resultado efectivo y enfatizar su efectividad de funcionamiento.

Si bien, los sistemas de seguridad presentan un grado de falencia, debido a que ninguno por más sofisticación que tenga es 100% efectivo, estando expuesto a ser vulnerado; pero la diferencia de la autenticación por reconocimiento facial, complica la suplantación de identidad, debido a que usa los rasgos biométricos y la geometría del rostro, propios de cada persona.

Palabras Claves: Autenticación, reconocimiento facial, seguridad, vehículos subcategoría L3, redes neuronales, infoentrenamiento, base de datos.

ABSTRACT

The theft of subcategory L3 vehicles is one of the crimes that has grown very considerably in recent years, mainly due to the fact that their security systems are incipient and/or are not always effective, which makes them very vulnerable vehicles. In addition to being targets for robberies, they are also used as tools to carry out other criminal acts, thanks to the high speeds that can be achieved, their ease of maneuverability and the speed with which these vehicles can be boarded or abandoned.

Although anti-theft security systems for motorcycles already exist, it has been detected that they are easily breached by criminals due to their exposure and their type of construction, which is almost always mechanical. Thus, we have the locks on the discs or the locks on the steering wheel; the same ones that present no challenge to criminals. This situation is a reality that requires the implementation of a highly innovative anti-theft security system that takes advantage of technology; making use of facial recognition authentication techniques for the recognition of the owner or other authorized persons. To achieve this, a Raspberry Pi microcomputer will be used, in which a programmed neural network will be trained and a database created using the "Python" programming language will be hosted. The trained and programmed neural network will allow the validation of the user, comparing the detected face with the database and thus allowing the vehicle to start or deny it. In its design, various climatic and lighting factors of the environment will be considered, which will allow to demonstrate the effectiveness of the system, and its behavior in the different conditions, in order to achieve an effective result and emphasize its effectiveness of operation.

The trained and programmed neural network will allow the validation of the user, comparing the detected face with the database and thus allowing the vehicle to start or deny it. In its design, various climatic and lighting factors of the environment will be considered, which will allow to demonstrate the effectiveness of the system, and its behavior in the different conditions, in order to achieve an effective result and emphasize its effectiveness of operation.

Keywords: Authentication, facial recognition, security, L3 subcategory vehicles, neural networks, info-training, database.

INTRODUCCIÓN

La autenticación por reconocimiento facial en la actualidad es considerada una de las técnicas de seguridad más confiable; gracias a su alto nivel de efectividad y amplio espectro de utilización.

Con el avance de la tecnología y la creación de ordenadores cada vez más eficientes y portátiles, se pueden usar algoritmos eficientes para la implementación de procesos de autenticación, conjuntamente con dispositivos de fácil configuración y a un costo bajo, ayudando a solucionar problemas de seguridad. El presente proyecto se concentra en el desarrollo de un sistema de seguridad basado en reconocimiento facial para controlar el encendido en un vehículo categoría L3 y está estructurado en cuatro capítulos, que se detallan a continuación.

En el Capítulo 1, se presenta un análisis situacional que aborda los antecedentes, las causas y las consecuencias relacionadas con la seguridad en vehículos de subcategoría L3. Se incluyen estadísticas, sistemas existentes y los desafíos en materia de seguridad. El Capítulo 2 se centra en el diseño del sistema de seguridad. Aquí se describen los criterios de diseño, se realiza un análisis y selección de alternativas, se efectúa una comparativa de las diferentes opciones, se seleccionan los componentes necesarios y se elaboran diagramas eléctricos utilizando el software PROTEUS. El Capítulo 3 detalla la implementación del sistema de seguridad en el vehículo. Se describen los pasos necesarios para incorporar el sistema en el automotor, lo que involucra la instalación de componentes y la configuración correspondiente. Finalmente, el Capítulo 4 documenta las pruebas y a la interpretación de los resultados obtenidos con la implementación del sistema. Se evalúa la efectividad de la autenticación por reconocimiento facial y se analizan los datos recopilados durante las pruebas.

En conjunto, estos capítulos proporcionan una visión completa del proyecto, desde la comprensión de la problemática de seguridad en vehículos de categoría L3 hasta la implementación y evaluación de una solución basada en la autenticación por reconocimiento facial.

PROBLEMA

En el país actualmente se ha observado una vulnerabilidad significativa en la seguridad de las motocicletas. Estos vehículos se han convertido en el blanco preferido de los delincuentes debido a su maniobrabilidad en el tráfico, su capacidad para alcanzar altas velocidades y la facilidad de abordar o abandonar el vehículo al cometer un acto delictivo. Esta situación ha llevado a la necesidad emergente de desarrollar sistemas de seguridad más efectivos que protejan estos automóviles.

En el debate actual sobre la reducción de los índices de robo de motocicletas, las autoridades han implementado reformas cada vez más estrictas con respecto al uso de estos vehículos. Una de estas reformas se centra en la circulación de las motocicletas con una sola persona, ya que se ha observado en numerosas ocasiones que para llevar a cabo el robo de una motocicleta se requiere la participación de dos individuos. Uno de ellos desciende de la motocicleta para violar los sistemas de seguridad y, posteriormente, ambos huyen con el vehículo sustraído.

Además, se ha identificado que existen múltiples sistemas de seguridad convencionales disponibles para motocicletas, como la traba de volante, las alarmas y los candados en los discos de freno, entre otros. No obstante, estos sistemas son ampliamente conocidos por los delincuentes y, por ende, resultan relativamente fáciles de corromper, lo que denota la necesidad de explorar nuevas tecnologías y enfoques de seguridad más avanzados.

En respuesta a estos desafíos, ha surgido la necesidad apremiante de implementar sistemas de seguridad innovadores que aprovechen los avances tecnológicos. Estos sistemas no convencionales se presentan como una solución potencial para combatir el robo de motocicletas y garantizar la protección de la inversión de los propietarios de estos vehículos.

Delimitación del problema.

En Ecuador, el robo de motocicletas ha experimentado un aumento alarmante en los últimos años, siendo Quito una las ciudades más afectadas, donde se registró un incremento del 8% en el año 2022 en comparación con el año 2021. Durante el transcurso del presente año, el incremento de

robos de motocicletas ha continuado creciendo de manera significativa en relación al año anterior (Primicias, 2022).

En este contexto, la presente investigación se enfoca en análisis de patrones e índices de robo de motocicletas en áreas urbanas de Ecuador, para determinar los factores y métodos específicos empleados por los delincuentes, así como en la evaluación de las políticas y estrategias gubernamentales vigentes destinadas a mitigar esta problemática.

El propósito final de esta investigación es la implementación de un mecanismo de seguridad basado en autenticación biométrica que contribuyan a reducir el robo de motocicletas y sus consiguientes repercusiones sociales.

Objetivo General.

Desarrollar un sistema de seguridad para controlar el encendido de un vehículo subcategoría L3, a partir de la autenticación por reconocimiento facial.

Objetivos Específicos.

- Analizar los principios de autenticidad y del reconocimiento facial, mediante la utilización de un software, aplicados en el campo automotriz como sistema de seguridad.
- Elaborar un sistema de seguridad por reconocimiento facial programando una tarjeta programable y configurando la base de datos para registrar los usuarios autenticados.
- Adaptar el sistema de seguridad al sistema de arranque de un vehículo subcategoría L3, para gestionar el encendido del motor a partir de la autenticación de los usuarios.
- Realizar pruebas de efectividad del sistema de seguridad, validando indicadores como: rasgos faciales de los usuarios ingresados; tomando en cuenta variables de iluminación propias de cada entorno; características que permitan determinar la funcionalidad del sistema

MARCO TEÓRICO

1.1 Autenticación

La autenticación es un método de seguridad que protege objetos o información personal. Según, (IBM, 2021) “la autenticación es la capacidad de demostrar que un usuario o una aplicación es realmente la persona o aplicación que asegura ser”. Entonces se puede relacionar la autenticidad con la exclusividad que cada persona tiene debido a la diferencia de sus rasgos biométricos.

La autenticación basada en biometría es caracterizada por hacer uso de los rasgos físicos o biológicos de cada persona; lo cual, permiten a los dispositivos u objetos que sean accesados de manera segura; para ello, se diseña una base de datos en la que se encuentran almacenadas las características propias de cada usuario. (Ihalainen, 2016).

1.2 Reconocimiento Facial

El sistema de reconocimiento facial permite confirmar la identidad de una persona, mediante la lectura de sus características faciales. Esta técnica en la actualidad se encuentra en: dispositivos móviles, acceso a residencias e incluso en la activación o desactivación de vehículos. Un sistema de autenticación usa una base de datos para el reconocimiento facial; pero no se trata únicamente del almacenamiento de fotos, sino que el sistema aprende constantemente identificando y reconociendo a una persona como propietario auténtico limitando así el acceso de otras personas; reduciendo el riesgo de suplantación de identidad mediante el uso de fotografías obtenidas de alguna otra fuente. (kaspersky, 2013).

1.2.1 Funcionamiento del reconocimiento facial

1.2.1.1 Reconocimiento facial

La cámara es la encargada de detectar la presencia del rostro de la persona que intenta acceder a un dispositivo para ponerlo en funcionamiento; para una mejor captura de reconocimiento, el usuario debe ubicar su rostro de forma frontal, no de perfil.

1.2.1.2 Análisis Facial.

Una vez que el usuario se coloca frente a la cámara; el software previamente entrenado hace captura de la imagen y luego de ello, analiza la geometría del rostro. Cumpliendo su objetivo el cual es identificar los puntos de referencia facial para distinguir el rostro. (kaspersky, 2013).

Los factores claves que son considerados en el proceso del análisis facial son:

- Distancia entre ojos.
- Profundidad de las cuencas de los ojos.
- Distancia desde la frente hasta el mentón.
- Forma de pómulos.
- Contorno de labios, orejas y mentón.

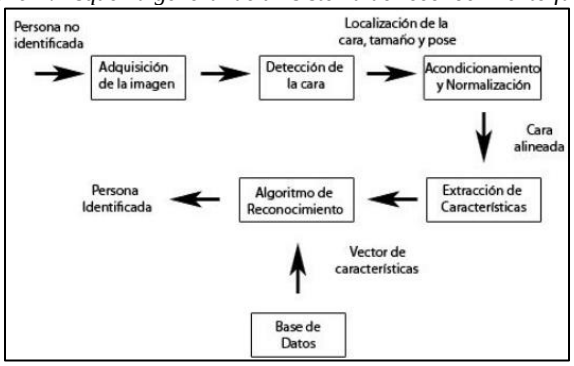
1.2.1.3 Conversión de la imagen en datos.

En esta fase; se realiza una conversión de información analógica (rostro) en una información digital (datos) que se basan en los rasgos faciales de la persona. Entonces el análisis del rostro de una persona se convierte en una fórmula matemática creando un código numérico llamado "impresión facial". (OneSpan, 2019).

1.2.1.4 Búsqueda de coincidencias.

La creación de una base de datos es indispensable en este sistema debido a que ahí se encontrará almacenada la información (fotos) del usuario permitido al acceso del dispositivo u objeto. Entonces, como proceso final, el software hace una comparación de la impresión facial actual con la información que está cargada en la base de datos; realizando un cálculo de coincidencia; permitiendo o negando el acceso del usuario. (RECFACES, 2021).

Figura 1. *Esquema general de un sistema de reconocimiento facial.*

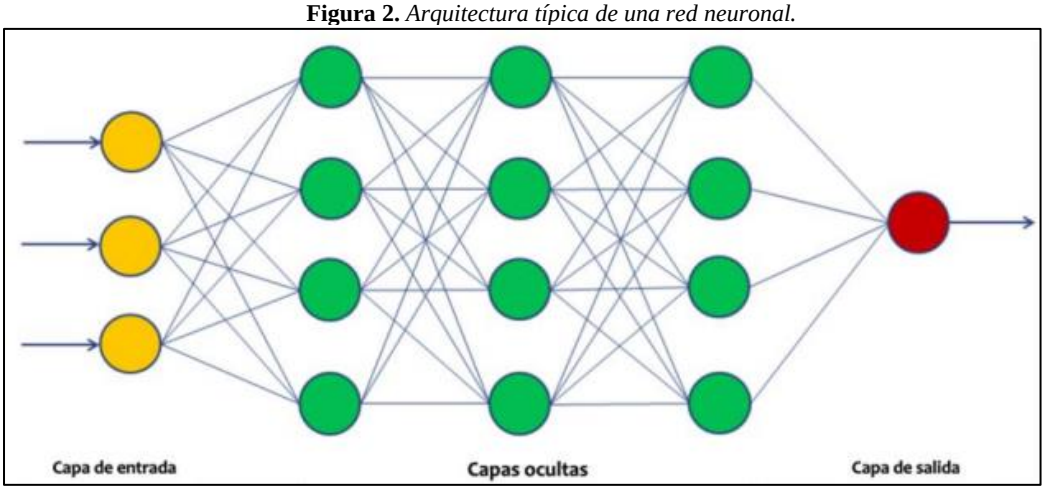


Fuente: *(Hernández, 2012)*

1.3 Redes Neuronales

El “Deep learning” es un método de aprendizaje automático que usa redes neuronales, con una capacidad de ingerir datos y extraer representaciones útiles sobre la base de ejemplos, es lo que la hace especial**.** La arquitectura de Redes Neuronales de Convolución (Convolutional Neural Network), es la más utilizada en la aplicación del reconocimiento facial. (Sánchez M. L., 2022)**.**

Figura 2. *Arquitectura típica de una red neuronal.*



Fuente: *(Sánchez M. L., 2022).*

1.3.1 Redes Neuronales de Convolución.

Está inspirada en las redes neuronales biológicas del cerebro humano. Están constituidas por elementos que se comportan de forma similar a la neurona biológica en sus funciones más comunes. Esta red neuronal aprende a través de la experiencia es decir generaliza los ejemplos previos a ejemplos nuevos y abstrae las características principales de una serie de datos almacenados en una base de información. (Olabe, 2016).

1.3.1.1 Características de las redes neuronales.

- Aprender: recopila la información previamente cargada en una base de datos; es decir tienen un conjunto de entradas; entonces se ajustan para producir salidas consistentes.
- Generalizar: con la base de datos cargada de información generalizan sus características dentro de un margen de error, creando respuestas correctas a distintas entradas que pueden presentar ciertas variaciones causadas por efectos de iluminación o posición.

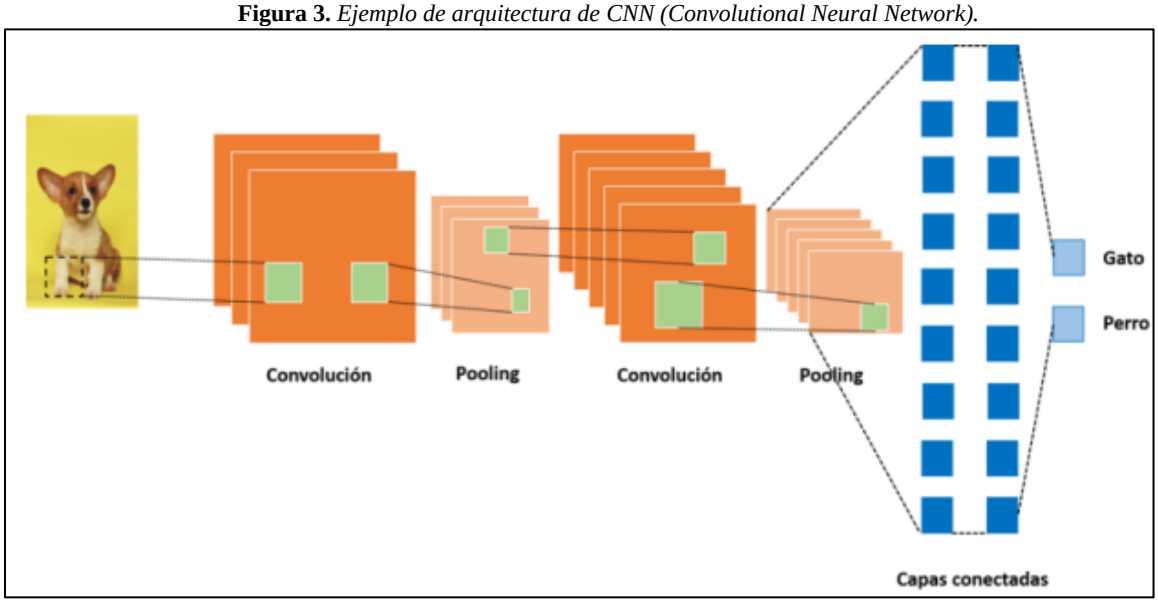
- Abstraer: diferenciar las entradas que no presenten aspectos comunes o relativos con la información cargada en una base de datos, negando así el acceso a la activación de un dispositivo.

1.3.1.2 Capas de las redes neuronales.

Las Redes Neuronales se componen de tres diferentes capas:

- Capa de convolución: Es la encargada de extraer las características de la imagen capturada por una cámara. Entonces, la convolución aprende las características de la imagen usando pequeños cuadrados de la imagen conservando la relación espacial entre pixeles. Emite un mapeo de características como una imagen de salida. (Sánchez M. L., 2022).
- Capa de agrupación: En esta fase de proceso; se encarga reducir las dimensiones erróneas de la imagen de entrada, reteniendo las características más importantes después de la convolución.
- Capa completamente conectada: En esta capa, las neuronas tienen una conexión completa con todas las actividades de las capas anteriores; es decir conecta neuronas de una capa con neuronas de otra capa. (Sánchez M. L., 2022).

Figura 3. *Ejemplo de arquitectura de CNN (Convolutional Neural Network).*



Fuente: *(Olabe, 2016)*

1.4 Algoritmos Optimizadores

Es un método utilizado para minimizar una función de error o maximizar la eficiencia de la misma. Los algoritmos son funciones matemáticas que dependen de los parámetros de aprendizaje del modelo; siendo parte de la ayuda de la red neuronal para que la misma entienda los posibles cambios que pueden existir. (Sánchez J. A., 2021).

1.4.1 Tipos de algoritmos optimizadores.

1.4.1.1 Gradient Descent (GD)

El algoritmo Gradiente Descendente es iterativo (es un proceso que se repite varias ocasiones, sin límite). Para ello requiere que el usuario introduzca dos parámetros para su funcionalidad. (Sotaquirá, 2018).

- Número de iteraciones: número de veces que se repetirá el proceso.
- Tasa de aprendizaje: también conocido como el parámetro alfa (es la cantidad mínima de repeticiones que requiere el algoritmo para encontrar el mínimo de una función).

1.4.1.2 Stochastic Gradient Descent (SGD)

También conocido como el Descenso de Gradiente Estocástico, el cual simplifica el cálculo considerando una sola muestra. A pesar de que supera las prestaciones del Gradiente Descendente (GD), la desventaja más notoria es que requiere de mucha memoria para cargar todo el conjunto de datos de "n" puntos. (InteractiveChaos, 2023).

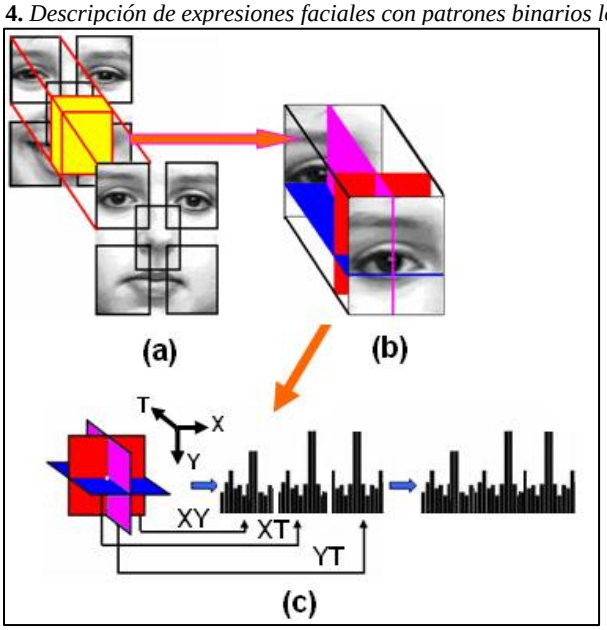
1.4.1.3 Adaptive Gradient Descent (AdaGrad)

Tiene como idea principal, tener una tasa de aprendizaje adaptativa; es decir que el entrenamiento de una red neuronal se adapte al medio cada que registre datos y realice la comparación entre los datos de entrada y los datos de salida. Esto se da, debido a que realiza actualizaciones más pequeñas para los parámetros asociados a las características que aparecen con frecuencia. (Sánchez J. A., 2021).

1.4.2 Algoritmo LBPH

El Patrón Binario Local (LBP), es un operador simple, pero con mucha eficiencia en la aplicación del reconocimiento facial, debido a que etiqueta los píxeles de una imagen mediante el umbral de la vecindad de cada píxel y considera el resultado como un número binario. (Prado, 2017).

Figura 4. *Descripción de expresiones faciales con patrones binarios locales.*



Fuente: *(Pietikainen, 2010)*.

El algoritmo LBPH, va de la mano con el reconocimiento facial; cumplen una tarea con gran similitud. El cual se divide en cinco pasos que se presentan a continuación:

1.4.2.1 Parámetros.

Son cuantificaciones, que cumple el LBPH.

- Radio: permite construir un patrón binario local circular; el cual se encarga de representar el radio alrededor del píxel central, que generalmente se establece en 1.
- Vecinos: es la cantidad de puntos de muestra que se encargan de construir el patrón local circular. El valor que normalmente se establece es de 8.
- Cuadrícula X: es el número de celdas que se encuentran dispuestas en forma horizontal. Si en la cuadrícula existen mayor cantidad de celdas mayor será la dimensionalidad del vector de características resultante; por eso se establece 8 celdas.

- Cuadrícula Y: es el número de celdas en la dirección vertical. Y al igual que la cuadrícula X; está establecida por 8 celdas.

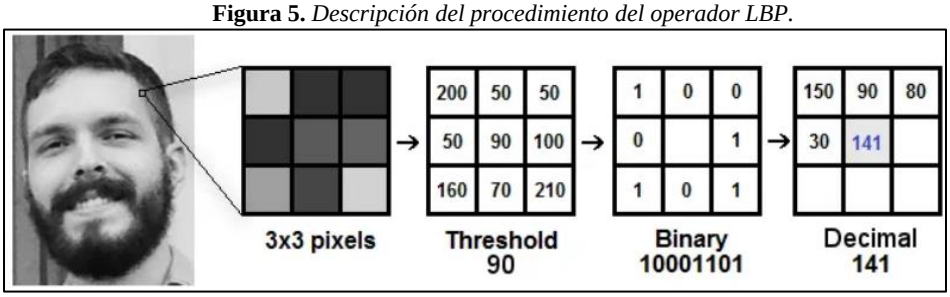
1.4.2.2 Entrenamiento del algoritmo.

El entrenamiento del algoritmo es la utilización de una base de datos la cual va a contener un conjunto de imágenes de las personas que se desea reconocer. Se establece una identificación que puede ser: un número o el nombre de la persona. Así el algoritmo reconocerá la imagen de entrada y brindará una salida.

1.4.2.3 Aplicación de la operación LBP

En esta fase, se produce el primer paso computacional del LBPH. Se crea una imagen intermedia que describe mejor la imagen original, resaltado las características faciales. (Saini, 2022).

Figura 5. *Descripción del procedimiento del operador LBP.*



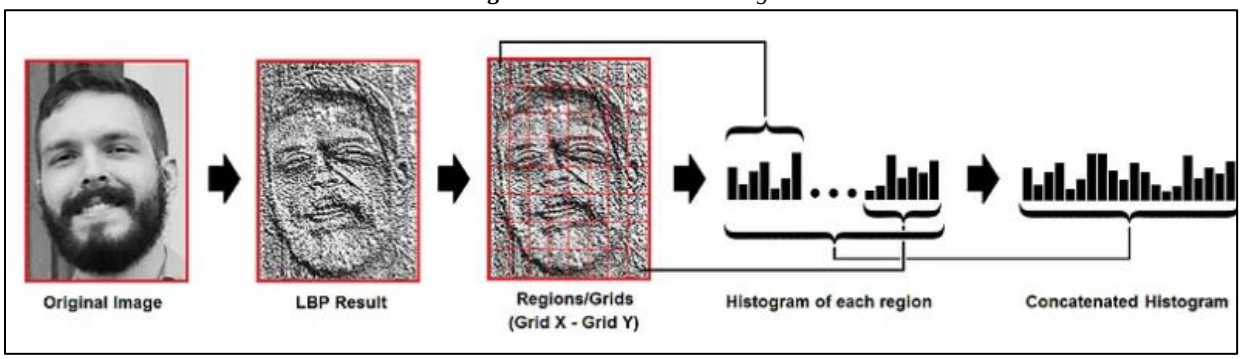
Fuente: *(Prado, 2017)*

Describiendo la figura 5; se explica gráficamente la función del algoritmo LBP; siendo que tenemos una imagen 3x3 píxeles. Entonces se establece un valor central el cual será el umbral; por lo tanto, se establece 1 para valores iguales o superiores al umbral y 0 para valores inferiores al umbral; y así la matriz contendrá solo valores binarios.

1.4.2.4 Extracción de los histogramas

En esta fase, utilizando la misma imagen; los parámetros (Cuadrícula X y Y), se puede dividir la imagen en múltiples cuadrículas que se aprecia a continuación.

Figura 6. *Extracción de Histogramas.*



Fuente: *(Prado, 2017)*

Entonces, con ayuda del ejemplo anterior; se asume que en la imagen de la figura 6 cada histograma tendrá solo 256 posiciones (0~255), las cuales representan las recurrencias de cada intensidad de píxel. Y así se obtiene el histograma final que representa las características de la imagen original. (Saini, 2022).

1.4.2.5 Reconocimiento

En este último paso, el algoritmo ya se encuentra entrenado entonces, se tendrá una imagen de entrada, y tendremos una respuesta de salida.

1.5 Hardware

1.5.1 Raspberry Pi 4

Es un microcomputador creado en el año 2006; con la finalidad de que cumpla las funciones de un ordenador con la facilidad de programarle para que realice las actividades que el usuario desee. Contiene puertos y entradas, lo cual permite conectar varios elementos adicionales como cámaras, pantallas, teclados. (Calvo, 2022). Es utilizada para aplicaciones de inteligencia artificial como reconocimiento facial, debido a las características que se presentan a continuación:

- Chip gráfico.
- Memoria RAM de hasta 8 GB.
- Procesador Gráfico VideoCoreIV.
- Conexión a red a través del puerto de Ethernet.
- Ranura para apertura de microSD.

1.5.2 Cámara - Arducam.

Es un módulo de cámara que se encuentra asociado con la Raspberry Pi 4; basada en el sensor de Sony IMX519 de 16 MP, para brindar una mejor resolución en la obtención de imágenes; y su coste no es tan elevado. (MCI Electronics, 2023).

1.5.3 Hosyond Pantalla táctil LCD; 3.5´´.

Se encarga de brindar información visual del software que está almacenado en la placa de la Raspberry; y se conecta directamente en el puerto GPIO.

1.5.3.1 Características

- Resolución 320 x 480.
- Control táctil resistivo.
- Compatible con sistemas Raspbian, Ubuntu, Kali Linux, etc.

1.5.4 Transformador de corriente.

Es un dispositivo eléctrico que se encarga de transferir energía eléctrica de un circuito a otro sin modificar su frecuencia. (Electrositio, 2023). Para la aplicación de una Raspberry, si se manejan voltajes mayores a 5 voltios, puede ocasionar el corto circuito de la placa; debido a que su voltaje máximo de trabajo es de 5 voltios.

1.5.4.1 Características

- Salida de 5.1 V / 3.0 A (DC).
- Protección contra cortocircuitos, sobre corrientes y sobrecalentamiento.
- Conector de salida USB-C.

1.6 Software

1.6.1 Raspbian

Es un sistema operativo basado en el sistema Linux Debian. Raspbian incluye gran variedad de funciones y paquetes de software que se pueden instalar con facilidad. Siendo un sistema operativo totalmente libre, y es compatible con cualquier versión de Raspberry Pi. (Moyens Staff, 2021).

1.6.2 Python

Es un lenguaje de programación que combina la simplicidad, potencia y versatilidad. En la actualidad es el más usado cuando se habla de aplicaciones con inteligencia artificial. Se encuentra enfocado en la legibilidad de su código y la extensa biblioteca estándar; facilitando la escritura y comprensión del código, adaptándose de manera clara y óptima a diferentes necesidades y escenarios. (Desarrolladores web, 2023).

1.6.3 OpenCV

Es una librería de código abierto que contiene en su paquete informático más de 2500 algoritmos totalmente optimizados, el cual permite el aprendizaje automático de máquinas o equipos. Aplicado en la inteligencia artificial por la facilidad de identificar objetos o rostros (reconocimiento facial), y esto es posible debido a que encuentra imágenes similares de una base de datos y permite el acceso o negación a la activación de un objeto, o sistema mediante un previo entrenamiento. (Rodríguez, 2021).

1.6.4 JavaScript

Es una plataforma informática de lenguaje de programación. La mayoría de productos y servicios digitales han sido diseñados en el lenguaje de Java. Es uno de los lenguajes que ha tenido y sigue teniendo participación en la base para desarrollar aplicaciones. (Saavedra, 2023).

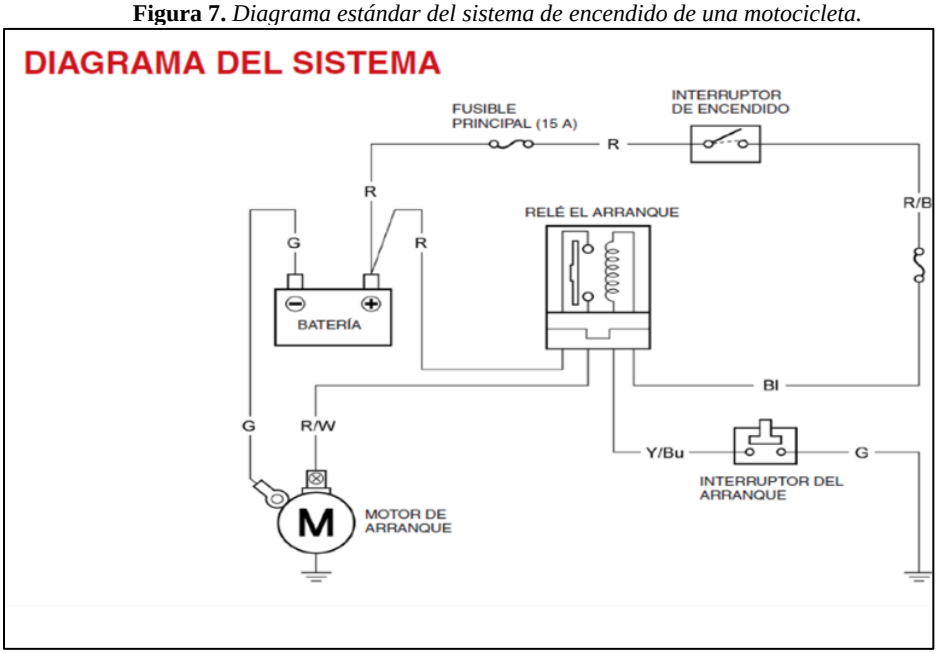
1.6.5 Gradle

Es una herramienta que permite la automatización de compilación de código abierto. Tiene una flexibilidad y rendimiento, que inclusive es mucho más sencillo que Java. Altamente personalizable y rápido al momento de ejecutar tareas, reutilizando las salidas de las ejecuciones anteriores; y solo procesar las entradas que presenten cambios o los datos guardados con anterioridad. (Muradas, 2020).

1.7 Sistema de encendido de una motocicleta

El sistema de encendido de un vehículo es el que permite dar el primer arranque para su funcionamiento. Es considerado como el sistema inicial para la puesta en marcha del vehículo, el cual tiene la función de producir una chispa dentro de los cilindros en el momento adecuado, para producir la combustión de la mezcla aire – combustible. (MotoGruaSaccsa, 2018).

Figura 7. *Diagrama estándar del sistema de encendido de una motocicleta.*



Fuente: (Chávez, 2023)

El sistema de encendido también puede ser considera como un sistema de seguridad, recalcando al hecho de que es el encargado de abrir o cerrar el circuito para la puesta en marcha del vehículo.

CAPÍTULO I
ANÁLISIS SITUACIONAL

1.1 Antecedentes.

En el Ecuador el índice de robos de motocicletas mantiene cifras muy considerables, debido a que son medios de transporte que facilitan a los delincuentes realizar acciones ilícitas con un escape más accesible que al uso de un vehículo L1. En enero 2020, se registró un total de 2.939 motos robadas, esta cantidad ha aumentado a enero 2021 con un total de 3.820 motos robadas. En el año actual el robo de motocicletas se ha incrementado considerablemente en relación a la última cifra evaluada, lo cual evidencia el alto riesgo al que se encuentran expuestos estos vehículos de subcategoría L3. El robo de motocicletas tiene una mayor concentración de robo en las noches, debido a que no hay un control o vigilancia suficiente como tal. (Fiscalía General Del Estado, FGE, 2021).

Debido a estas razones, el uso de un sistema de autenticación facial representa una importante alternativa para incorporar un mecanismo de seguridad basado en sistemas de infoentrenamiento, para permitir o no el encendido de una motocicleta, a partir del almacenamiento de la información del o los usuarios en una base de datos; de tal forma que el vehículo no arrancará si es abordado por personas desconocidas.

Actualmente, los sistemas de seguridad para vehículos livianos son considerados como una inversión, mas no como un gasto, y más cuando se trata de sistemas de autenticación por reconocimiento facial los cuales disminuyen el riesgo a que cualquier persona pueda hacer uso del vehículo de forma deliberada. (Lopez y otros, 2009).

1.2 Causas y Consecuencias de la inseguridad en vehículos subcategoría L3.

La realidad que vive el país (Ecuador) en el tema de la seguridad se encuentra violentado por la delincuencia que aumenta día a día. Para la ejecución de robos de motocicletas intervienen muchos factores tanto económicos como sociales. Según (FayalsMotos, 2022) “La economía, la poca rigurosidad de las leyes, y la corrupción en entidades gubernamentales; son las principales causas de la inseguridad.”

Entonces, teniendo en cuenta que el problema va más allá de un sistema social, la inseguridad en motocicletas es objeto del análisis del presente proyecto que tiene como fin el diseño de un prototipo de seguridad que genere complejidad a los delincuentes al momento de realizar el robo de una motocicleta.

1.2.1 Causas

- Sistemas de seguridad obsoletos, es decir que no generan ningún tipo de complejidad al delincuente al momento de ejecutar el robo de la motocicleta.
- Facilidad de maniobrabilidad al momento de realizar acciones ilícitas.
- Venta de partes a precios cómodos que llaman la atención de usuarios que desconocen la procedencia de la motocicleta.
- Reventa de motocicletas a precios elevados.
- Baja seguridad en calles y avenidas.

1.2.2 Consecuencias

- Aumento de actos delincuenciales en la sociedad.
- Reducción de la venta legítima y legal de motocicletas, debido a que los usuarios temen a ser atacados por la delincuencia.
- Personas que, por el desconocimiento de la procedencia de la motocicleta al momento de comprarla por medios electrónicos, son involucradas en actos ilícitos.

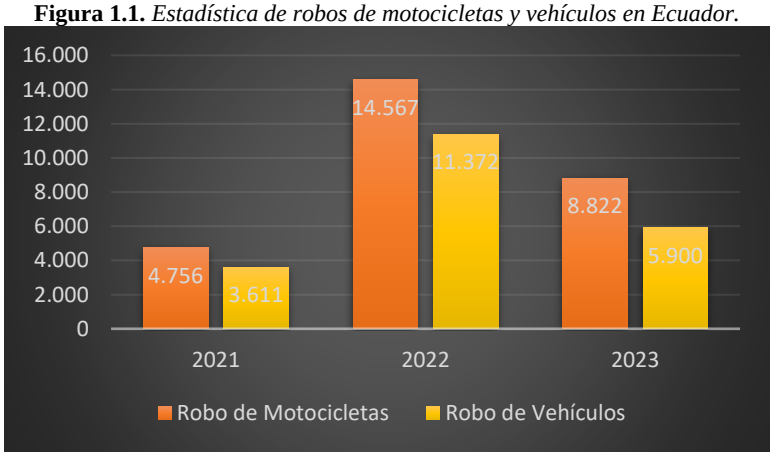
1.3 Estadísticas de Seguridad

La mayoría de robos de vehículos subcategoría L3, se producen en zonas periféricas. Esto se debe en gran parte a la falta de iluminación o poca afluencia de personas.

Según (Redacción Vistazo, 2023) “Con los datos de la FGE, entre enero y julio del presente año se registran 5.900 denuncias por robo de vehículos y 8.822 robos de motocicletas; presentando una disminución en cuanto al año 2022 que fue de 11.372 denuncias con respecto a vehículos y 14.567 con respecto a motocicletas”. Entonces, esto demuestra que el robo de motocicletas es mucho mayor al robo de vehículos debido a la inferencia de los factores ya mencionados anteriormente.

Según la figura 1.1, las estadísticas en cuanto al robo de motocicletas son mucho mayor a la de vehículos, siendo uno de los más grandes factores la vulnerabilidad de los sistemas antirrobo que mantienen las motocicletas en la actualidad. Sin dejar de lado, la demanda de uso para la ejecución acciones delincuenciales en el país.

Figura 1.1. *Estadística de robos de motocicletas y vehículos en Ecuador.*



Fuente: Autores.

1.4 Sistemas de seguridad actuales

En la actualidad los sistemas de seguridad antirrobo en vehículos subcategoría L3 no se encuentran altamente desarrollados a diferencia de los que se usan en los automóviles; a pesar que el robo de motocicletas va en aumento como se detalla en el ítem 1.3. Existen sistemas convencionales antirrobo más utilizados en Ecuador, que se detallan a continuación.

1.4.1 Candados

Los candados de seguridad permiten sujetar una parte de la moto a una superficie fija, ya sea una reja o un anclaje al piso, de manera que imposibilita el desplazamiento o movimiento del vehículo.

Figura 1.2. *Candados para inmovilizar la motocicleta.*

Fuente: *(ProSegur, 2022)*

1.4.2 Localización vehicular

Este sistema es uno de los más recomendados por la Policía Nacional, debido a que facilita el rastreo del vehículo al momento de haber sido robado. Según (ProSegur, 2022) “la localización vehicular es uno de los sistemas más eficaces en cuanto a la seguridad de la motocicleta”.
Es una derivación del conocido GPS, el cual, de acuerdo a las configuraciones del sistema, permitirá conocer de manera precisa la ubicación del vehículo.

1.4.3 Alarma con mando bidireccional

Las alarmas para motos se encargan de producir un sonido agudo el cual da una alerta que está siendo forzada a iniciar su encendido. Según (MOTOYCASCO, 2019) “Lo último en alarmas son los mandos que actúan de manera bidireccional. De acuerdo a los sensores que lleve la alarma se puede saber incluso el estado de la moto: en reposo, movida o aproximación de un desconocido”. Se considera también un sistema eficaz en cuanto a la seguridad de antirrobo de la motocicleta.

Figura 1.3. *Alarma con mando bidireccional.*

Fuente: *(MOTOYCASCO, 2019)*

1.5 Problemas de seguridad

- Facilidad de manipulación: Algunos sistemas de seguridad son relativamente fáciles de manipular por los delincuentes. Esto puede deberse a una mala instalación, a la falta de mantenimiento o a la falta de actualización de los sistemas de seguridad.
- Falta de disuasión: Algunos sistemas de seguridad no son lo suficientemente disuasivos para los delincuentes. Esto puede deberse a que son demasiado comunes, a que son fáciles de desactivar o a que no generan una alarma lo suficientemente potente.
- Coste elevado: Algunos sistemas de seguridad son muy caros, lo que puede dificultar su acceso para algunas personas.

CAPÍTULO II
DISEÑO DEL SISTEMA DE SEGURIDAD

En el presente capítulo, se documenta el diseño del prototipo del sistema de seguridad, el mismo que está basado en un proceso de autenticación por reconocimiento facial para el encendido de nuestro vehículo subcategoría L3. Se analizan las posibles alternativas que permitan cumplir con el objetivo, como también los sistemas de seguridad ya existentes tomándolos como referencia para reducir la vulnerabilidad del sistema propuesto, enfocados en alcanzar al menos una efectividad del 90%, debido a que ningún sistema de seguridad es 100% efectivo.

2.1 Criterios de diseño

2.1.1 Funcionalidad del sistema

El sistema de seguridad propuesto para vehículos de tipo L3 se fundamenta en la implementación de tecnología de reconocimiento facial con el propósito de autenticar y autorizar al conductor para el arranque de la motocicleta. A continuación, se detallan las funciones interactivas del sistema:

- Registro de rostros autorizados en la base de datos: Este sistema restringe la posibilidad de registrar rostros de personas autorizadas, ya sea del propietario o de aquellos designados para operar la motocicleta.
- Captura de rostro: Gracias a una cámara, se lleva a cabo la captura del rostro del individuo, lo cual es esencial para el funcionamiento del proceso de autenticación.
- Procesamiento de rostro: El sistema realiza el procesamiento del rostro capturado para extraer características faciales distintivas de la persona, preparándolo para la siguiente etapa del proceso.
- Comparación de rostros: Se efectúa una comparación entre el rostro capturado y aquel almacenado en la base de datos, calculando el grado de similitud como parte del proceso de autenticación.
- Autorización para el encendido: En caso de que el rostro presente un alto grado de similitud con el almacenado en la base de datos, se autoriza la activación del actuador para el contacto del vehículo, permitiendo posteriormente el encendido.

- Captura de rostros desconocidos: Si el sistema no identifica un grado de similitud en la comparación o si no reconoce el rostro capturado, se puede activar una alerta y dispositivos de advertencia, como el buzzer.

Este sistema de seguridad busca proporcionar un nivel adicional de protección para la operación de la motocicleta, limitando el acceso únicamente a personas autorizadas por el sistema.

2.1.2 Confiabilidad

Considerando que ningún sistema de reconocimiento facial es efectivo en su totalidad, para el presente proyecto se ha considerado un margen de error del 10% debido entre otros factores a confusiones en la comparación de la muestra que se obtenga de la cámara con la base de datos. No obstante, se prevé la funcionabilidad del sistema puede reducir hasta un 5% de error. Esto en cuanto al uso de la cámara, debido a que se pueden encontrar cámaras sofisticadas, las cuales permitan un reconocimiento facial minucioso en cuanto al análisis de la geometría del rostro, distancia entre ojos, profundidad de las cuencas de los ojos; pero en esta ocasión se utilizará una cámara genérica de 5 MP, la cual permite que el sistema realice su función sin ningún problema, y se mantenga el margen del 10% de error.

2.1.3 Usabilidad

El sistema puede ser adaptado a cualquier motocicleta siempre y cuando exista un espacio considerable para colocar el módulo que contiene los componentes que intervienen en el proceso de autenticación. El encendido del módulo se realiza por medio de un botón el cual arranca el programa de captura y verificación de las imágenes y decide si el vehículo puede o no dar arranque.

2.2 Análisis comparativo de las alternativas

Para el desarrollo del sistema se consideraron dos opciones en cuanto a la microcomputadora que se encargaría de realizar el reconocimiento facial; la tarjeta Raspberry Pi y la tarjeta Jetson Nano. A continuación, se detalla una comparación técnica entre estas dos alternativas:

Tabla 1. Comparación de Alternativas

	Raspberry Pi	**Tarjeta Jetson Nano**
Fácil Adquisición	SI (Se encuentra en el mercado nacional).	NO (Se debe importar de otro país).
Costos	$ 145	$ 400 dólares
Programación	Amigable	Compleja
Potencia de procesamiento	Procesador Broadcom BCM2711 de cuatro núcleos a 1.5 GHz.	Procesador ARM Cortex-A57 de cuatro núcleos a 1.43 GHz
Memoria RAM	Disponible con opciones de 2 GB, 4 GB y 8 GB de RAM.	Generalmente viene con 4 GB de RAM.
Puertos y conectividad	Incluye puertos USB, Ethernet, HDMI, y otros, lo que facilita la conexión de cámaras y otros dispositivos.	Incluye puertos USB, Ethernet y otras opciones de conectividad.
GPU	Video Core VI	Nvidia Maxwell con 128 núcleos CUDA

Fuente: Autores.

En cuanto a la capacidad de procesamiento ligeramente la Raspberry Pi es mejor que la Tarjeta Jetson Nano, cuentan con la misma cantidad de núcleos; pero la velocidad de procesamiento es distinta como se puede observar en la Tabla 1. El almacenamiento del microcomputador dependerá de la utilización y/o aplicación a la que esté direccionada, pero en este apartado si existe una diferencia de 4 GB entre los microcomputadores siendo que la Raspberry cuenta hasta con 8 GB de RAM y la tarjeta Jetson Nano solamente viene con 4 GB de RAM.

De acuerdo al enfoque del presente proyecto los dos dispositivos mencionados en la Tabla 1, son capaces de realizar las tareas de reconocimiento facial, siendo que es un prototipo de prueba con visiones futuras. Para aplicaciones de inteligencia artificial la tarjeta Jetson Nano brinda un rendimiento superior a la Raspberry Pi 4, debido a su GPU dedicada; pero al no ser el caso es un apartado irrelevante en el tema. Además, que la Raspberry Pi, tiene varias entradas y salidas para conectar distintos dispositivos al mismo tiempo.

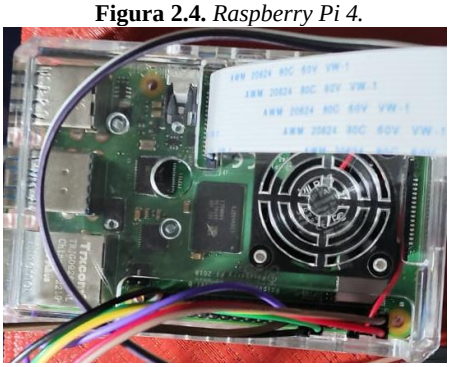
En tiempos de respuesta influye la utilización del software y la optimización del código, por lo tanto; depende de la utilización y/o aplicación que se le dé al dispositivo. Entonces, tomando en cuenta sus características y que los dos microcomputadores son capaces de realizar la actividad que se requiere en el prototipo del sistema de seguridad, se optó por desarrollarlo con la microcomputadora Raspberry Pi, debido a que se encuentra en el mercado nacional, el costo es relativamente más económico en cuanto a la tarjeta Jetson Nano, y el entrenamiento del sistema se puede realizar en un lenguaje de programación amigable como lo es “Python”.

2.3 Selección de los componentes para el sistema

- **Raspberry Pi 4**

Es un pequeño computador que corre un sistema operativo Linux capaz de permitirle a las personas de todas las edades explorar la computación y aprender a programar lenguajes como Scratch y Python.

Figura 2.4. *Raspberry Pi 4.*



Fuente: Autores.

- *Características:*
  - Procesador: Quad-core ARM Cortex-A72 @ 1.5 GHz
  - GPU: VideoCoreIV
  - Memoria RAM: 4 GB LPDDR4
  - Puertos: 2x micro HDMI, 2x USB 3.0, 2x USB 2.0, 1x puerto Ethernet, 1x conector de audio/vídeo compuesto
- *Aplicaciones:*
  - Aprendizaje electrónico
  - Automatización del hogar
  - Desarrollo de proyectos de hardware

- **Relé Electrónico JQC-3FF-S-Z**

El funcionamiento del relé JQC-3FF-S-Z se basa en un circuito de transistor que se activa cuando se aplica un voltaje al pin de entrada. Cuando el pin de entrada está bajo, el transistor está cortado y los contactos de salida están en su estado predeterminado.

Cuando el pin de entrada está alto, el transistor se enciende y los contactos de salida se cambian a su nuevo estado.

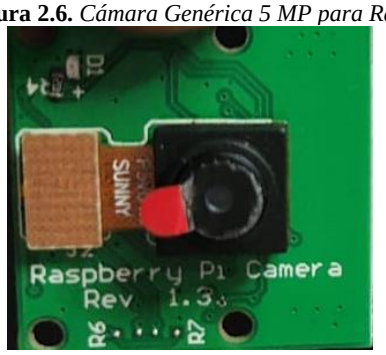
Figura 2.5. *Relé Electrónico JQC-3FF-S-Z.*

Fuente: Autores.

- **Cámara Genérica 5 MP**

Es un módulo de cámara de enfoque fijo que se conecta a la placa Raspberry Pi a través del conector GPIO. El módulo tiene un sensor CMOS de 5 megapíxeles que es capaz de capturar imágenes estáticas de hasta 2592 x 1944 píxeles y videos de hasta 1080p30.

Figura 2.6. *Cámara Genérica 5 MP para Raspberry.*



Fuente: Autores.

El funcionamiento de la cámara se basa en un circuito de captura de imagen que convierte la luz que ingresa a través del lente en una señal eléctrica. Esta señal eléctrica se procesa luego por un circuito de procesamiento de imagen que crea la imagen final.

- *Aplicaciones de la cámara:*
  - Captura de imágenes y videos
  - Reconocimiento facial
  - Detección de movimiento
  - Visión artificial

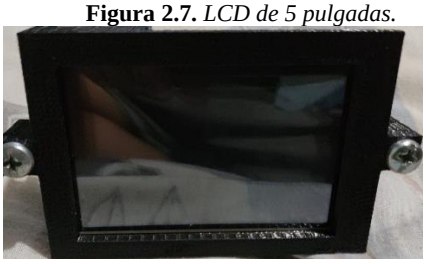
- *Características:*
    - Resolución: 5 megapíxeles (2592 x 1944 píxeles)
    - Formatos de imagen: JPEG, BMP, PNG
    - Formatos de video: H.264, MJPEG
    - Velocidad de fotogramas: hasta 1080p30
    - Ángulo de visión: 62 grados

- **LCD de 5”**

Es una pantalla táctil LCD de 5 pulgadas con una resolución de 800 x 480 píxeles. La pantalla se conecta a la Raspberry Pi 4 a través del conector DSI de la placa.

El funcionamiento de la pantalla LCD se basa en un circuito de controlador LCD que convierte las señales digitales de la Raspberry Pi 4 en señales analógicas que pueden ser interpretadas por el panel LCD.

Figura 2.7. *LCD de 5 pulgadas.*



Fuente: Autores.

- *Características:*
    - Resolución: 800 x 480 píxeles
    - Dimensiones: 108 x 64,8 mm
    - Ángulo de visión: 178 grados
    - Relación de contraste: 1000:1
    - Brillo: 350 nits
    - Tiempo de respuesta: 6 ms
    - Frecuencia de actualización: 60 Hz
- *Aplicaciones de uso:*
    - Interfaz gráfica de usuario (GUI)
    - Juegos.

- Visualización de datos
- Control de dispositivos

- **Buzzer**

La frecuencia del sonido producido por un buzzer electrónico depende de la frecuencia de la corriente eléctrica que se aplica a la bobina. La intensidad del sonido también depende de la corriente eléctrica.

Figura 2.8. *Buzzer.*

Fuente: *(Electrositio, 2023)*

➢ *Aplicaciones de uso:*

- Sistemas de seguridad.
- Dispositivos electrónicos.
- Instrumentos musicales.
- Alarmas.

2.3.1 Costos de los componentes seleccionados

A continuación, se proporciona un desglose completo de todos los elementos necesarios, junto con sus correspondientes precios, para la ejecución de este proyecto.

Tabla 2. *Costos de los componentes.*

Cantidad	Elemento	Descripción	Valor
1	Raspberry Pi 4	Kit básico.	$ 145.00
1	Relé	12V, 17 A.	$ 10.00
1	Buzzer	Transformador de energía eléctrica en sonido.	$ 5.00
1	Transformador	De 12V y 17A a 5V y 3A.	$ 20.00
1	Pantalla	LCD, HDMI de 3.5 pulgadas para Raspberry.	$ 35.00
1	Cámara	Para Raspberry Pi4 de 5MP	$ 7.50
TOTAL			**$ 222.50**

Fuente: Autores.

2.4 Diagramas eléctricos y electrónicos

2.4.1 Circuitos del sistema.

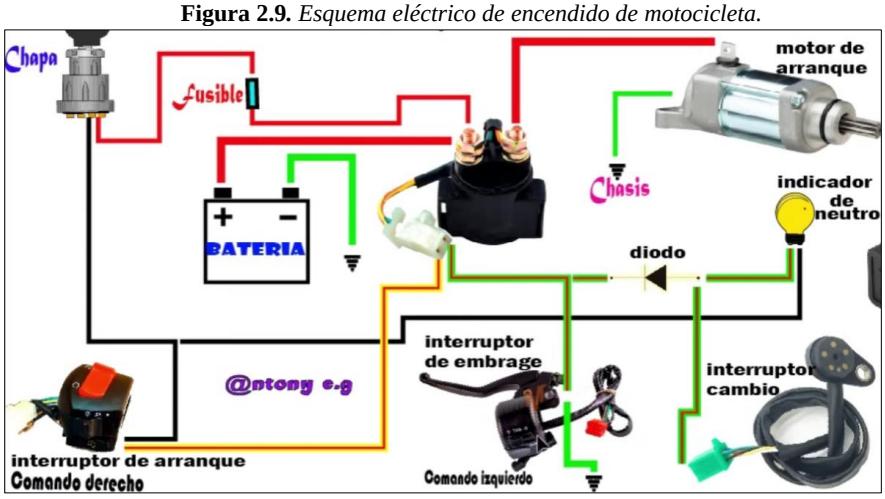
El sistema de encendido de una motocicleta se fundamenta en un motor eléctrico o motor de arranque, cuya potencia puede variar. Este componente es activado a través del interruptor de arranque, ubicado generalmente en el mando derecho de la motocicleta. De acuerdo a los estándares generales, el motor de arranque está equipado con un electroimán que se activa mediante corriente continua, proveniente exclusivamente de la batería.

Cuando se acciona el interruptor de encendido, el motor de arranque se energiza y pone en marcha el mecanismo de arranque. Este mecanismo transfiere la potencia al motor mediante ruedas dentadas internas, lo que provoca la rotación del cigüeñal. Este movimiento resulta crucial, ya que desencadena la generación de la chispa en el cilindro, logrando así el encendido del vehículo.

El sistema cuenta con las siguientes partes:

- Llave de encendido.
- batería.
- Selenoide
- Motor de arranque
- Comandos izquierdo y derecho
- Interruptor de cambios

Figura 2.9. *Esquema eléctrico de encendido de motocicleta.*



Fuente: Autores.

En lo que respecta al sistema que se requiere modificar, se integrará un relé entre la conexión entre la batería y la activación de la llave con el fin de suspender la línea de alimentación a todo el sistema eléctrico de la moto. Este relé se activa mediante una señal generada por la Raspberry al llevar a cabo la autenticación del rostro autorizado. Esta acción resulta en la activación del contacto en la motocicleta, lo que habilita la posibilidad de presionar el interruptor de arranque para encender la moto.

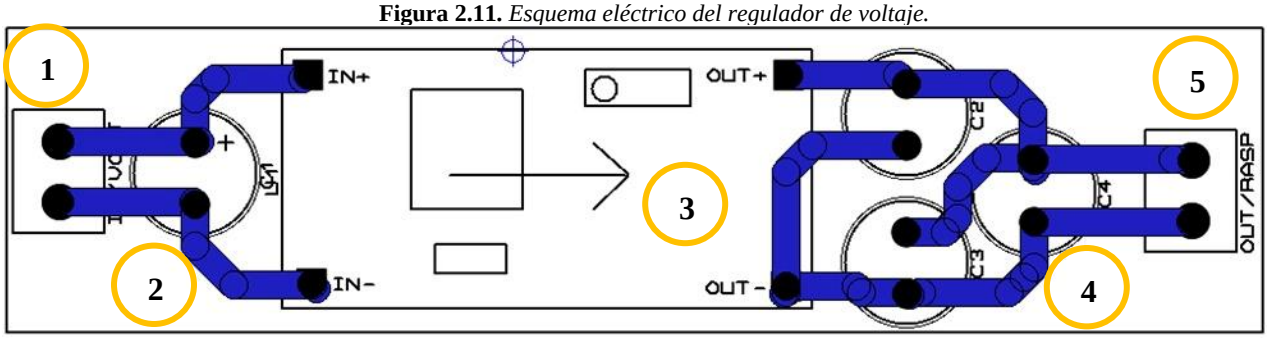
2.4.2 Circuito de alimentación de la Raspberry pi 4.

De acuerdo a las especificaciones técnicas del fabricante, la tarjeta Raspberry opera con un voltaje que no debe exceder los 5 voltios y una corriente de 2 amperios, por lo tanto, se optó por la instalación de un regulador de voltaje y corriente, que convierte la entrada de 12 voltios y 7 amperios a una salida de 5 voltios y 2 amperios. Esto permitirá asegurar el funcionamiento adecuado del dispositivo electrónico que se va a incorporar.

Figura 2.10. *Regulador de voltaje de 12V a 5V utilizado en el sistema.*

Fuente: Autores.

Figura 2.11. *Esquema eléctrico del regulador de voltaje.*



Fuente: Autores.

1. Entrada para los conectores.
2. Capacitor de entrada.
3. Reductor de corriente e intensidad
4. Capacitadores de almacenamiento de corriente.
5. Salida para los conectores.

Para la instalación y fijación del regulador, se diseñó una estructura de sujeción utilizando las impresoras 3D proporcionadas por la universidad. La ubicación del regulador se determinó junto a la batería de 12 voltios de la motocicleta. En este proceso, se conectaron dos cables a la entrada del regulador, los cuales fueron fijados al polo positivo y negativo de la batería. En el extremo de salida, se conectaron los cables al puerto destinado para la alimentación de la Raspberry, ya que este proporciona un voltaje no superior a 5 voltios, asegurando así el funcionamiento adecuado del dispositivo.

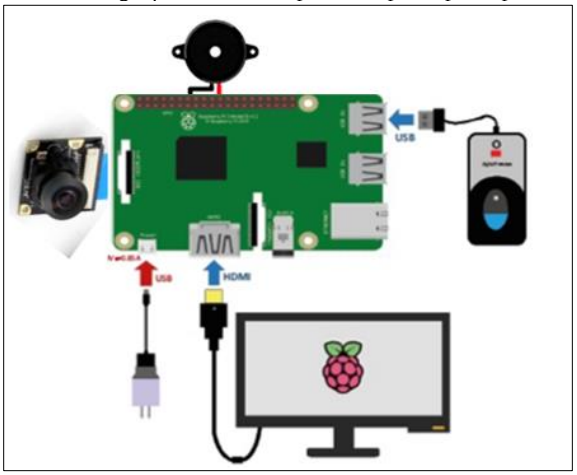
Figura 2.12. *Conexión del regulador del voltaje a la batería de la motocicleta.*

Fuente: Autores.

2.5 Estructura del sistema

En la representación gráfica proporcionada en la Figura 2.13, se observa una imagen de referencia que generaliza las conexiones efectuadas para la creación del sistema de seguridad. En dicha ilustración, se destacan elementos clave como la placa de Raspberry, el monitor utilizado para la visualización de la información capturada por la cámara, la entrada principal de alimentación, el puerto USB destinado para el control de la ejecución del programa mediante un mouse, el buzzer encargado de emitir alertas sonoras, y la propia cámara.

Figura 2.13. *Representación gráfica de los componentes principales para el desarrollo del sistema.*

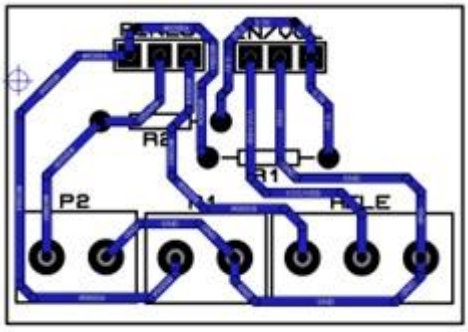


Fuente*:* Autores.

En la Figura 2.14, se presenta una placa de conexión que muestra de manera generalizada todas las conexiones. En dicha placa, se centralizan los pines destinados a la activación o desactivación, así como los puntos de conexión para GND y un voltaje constante de 5V que abastece a todos los dispositivos utilizados.

Esta disposición simplificada tiene como objetivo reducir la complejidad del cableado, al mismo tiempo que facilita el mantenimiento del orden y la compactación en el sistema.

Figura 2.14. *Esquema eléctrico de la placa de conexión.*

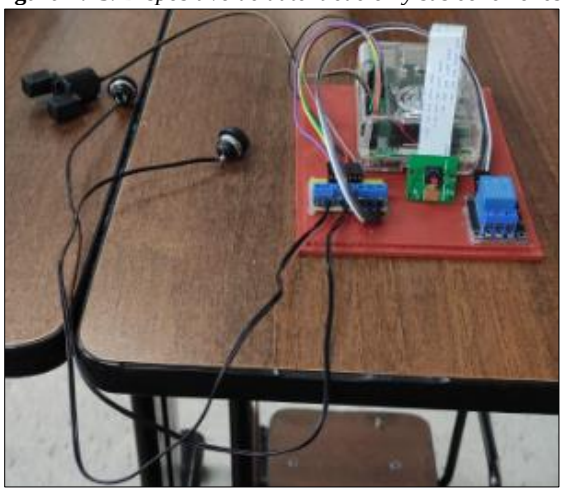


Fuente: Autores.

Entre la placa Raspberry y la placa de conexiones principales se establecieron las siguientes conexiones, tal como se ilustra en la Figura 2.15, y se detalla a continuación: El pin GPIO 18 de la Raspberry se conecta al pin 3 de la placa de conexiones, gestionando la activación o desactivación del relé. Por otro lado, el GPIO 22 está vinculado al polo positivo del buzzer, el cual se activa en ausencia de reconocimiento facial.

El botón de captura o detección facial activa la placa Raspberry a través del GPIO 17, mientras que el botón de reinicio del sistema se activa mediante el GPIO 27. Los GPIOS y pines principales fueron previamente descritos en la sección anterior. Las demás conexiones se dirigen, respectivamente, a la alimentación de 5V o GND de la placa madre. Por ejemplo, el otro cable del buzzer se conecta al pin 9, correspondiente a GND, para cerrar el circuito cuando la Raspberry emite un voltaje de activación, encendiendo el buzzer y generando el sonido de alerta.

Figura 2.15. *Dispositivo de autenticación y sus conexiones.*

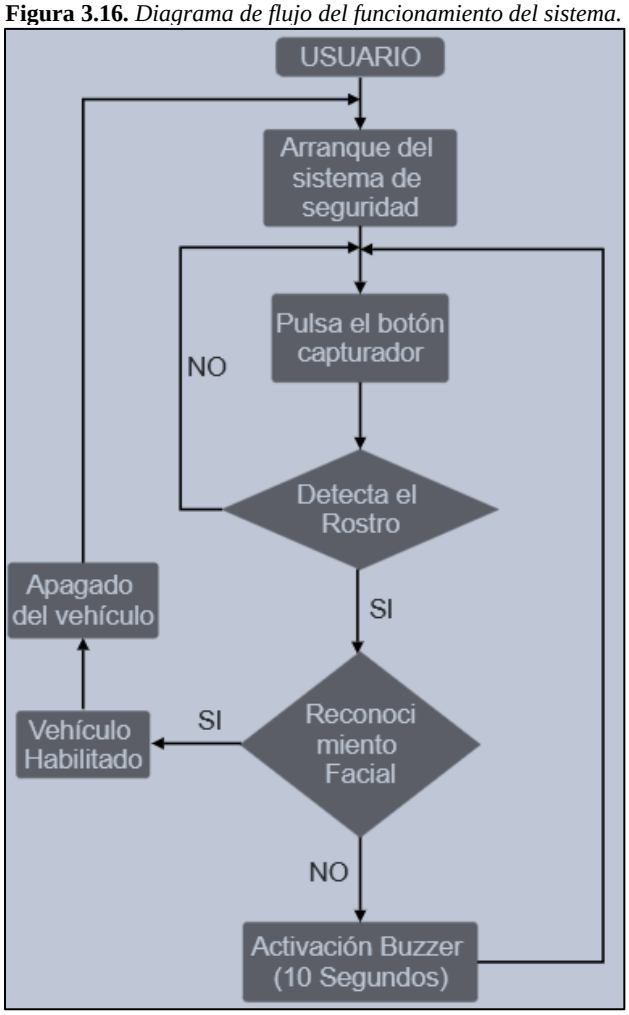


Fuente: Autores.

CAPÍTULO III
IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD

En el presente capítulo se describe el proceso de implementación del prototipo de seguridad por reconocimiento facial en un vehículo L3. Para la programación del módulo se usó el lenguaje Python y la biblioteca virtual face_recognition, la misma se encarga de realizar el proceso de reconocimiento facial, con un previo entrenamiento del sistema, para que la detección de rostros sea eficiente y precisa. Es importante destacar que aun cuando es un sistema altamente confiable, no es totalmente infalible debido a que los rasgos físicos de las personas en algunos casos son parecidos y eso tiende a afectar la efectividad del sistema, no obstante, se puede asegurar que esta alternativa es menos vulnerable a los convencionales ya existentes en el mercado.

Figura 3.16. *Diagrama de flujo del funcionamiento del sistema.*



Fuente: Autores.

3.1 Diseño del bloque de entrenamiento

Para iniciar un proceso de autenticación por reconocimiento facial se lleva a cabo el entrenamiento del dispositivo para asegurar una eficiencia óptima y minimizar el porcentaje de error en el reconocimiento facial.

En la Figura 3.17, se presenta la función encargada de detectar el rostro, donde el término "frame" representa el recuadro de salida diseñado para captar exclusivamente el rostro, subestimando otros elementos presentes en el entorno del sistema. Las variables "encodings_referencia" se utilizan para comparar los valores de referencia, mientras que "nombres" se emplea para acceder a las imágenes almacenadas en la carpeta, facilitando su posterior comparación.

Las librerías utilizadas en el bloque de entrenamiento de la red neuronal, que se encarga de realizar el proceso de reconocimiento facial se detallan a continuación:

- Import face_recognition: Esta librería contribuye al proceso de entrenamiento ya que ayuda analizar una imagen capturada identificando el rostro y comparándolo con los Data almacenados en el sistema. Si se encuentra una similitud alta entre la comparación permite la ejecución de acciones predefinidas como en este caso la activación de un relé.
- Import time: La utilidad de la librería en el proceso del entrenamiento radica en su capacidad de instruir al procesador para que aguarde un intervalo de tiempo para procesar la imagen antes de seguir a la siguiente instrucción de programación. Este proceso también se puede conocer como delay en términos de programación.

En la línea siguiente, se observa la variable "face_locations", la cual se destina a almacenar únicamente los rostros captados por la cámara mediante el comando "face_recognition". Este proceso contribuye al reconocimiento facial y permite enfocarse exclusivamente en las características faciales relevantes para el sistema.

Figura 3.17. *Código de entrenamiento del sistema.*

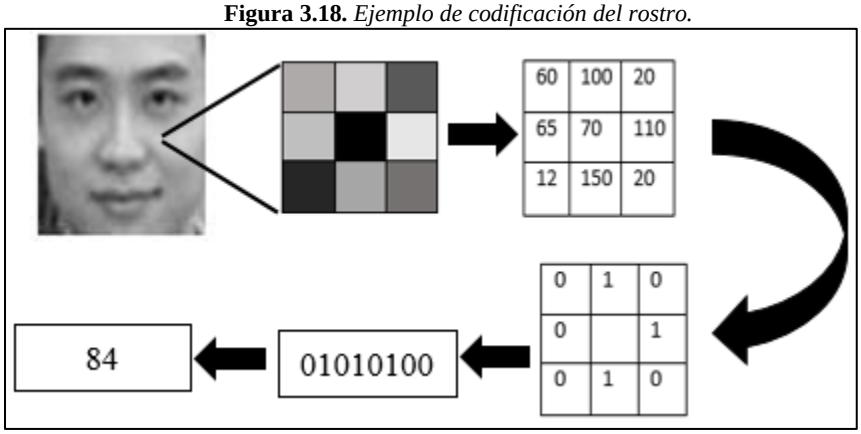
```
# Función para la detección facial
def detectar_persona(frame, encodings_referencia, nombres):
# Detectar rostros en el frame
face_locations = face_recognition.face_locations(frame)

# Si se detecta al menos un rostro
if face_locations:
# Codificar el rostro detectado
encoding_frame = face_recognition.face_encodings(frame, face_locations)[0]
```

Fuente: Autores.

Una red neuronal de convolución (CNN), relaciona la imagen con una matriz de números propias de la misma, entonces para ello; se utiliza la línea de código “enconding_frame”, visualizada en la figura 3.17.

El entrenamiento de una red neuronal consta de dos procesos: colección de datos y aprendizaje. Una vez que la cámara captura el rostro, la imagen es codificada en una matriz de números, donde cada número representa un color, es así que compara lo obtenido con la base de datos, y permite la activación del sistema, tomando en cuenta que no es una red neuronal que aprende automáticamente sino tiene una previa programación.

Figura 3.18. *Ejemplo de codificación del rostro.*



Fuente: *(ResearchGate, 2019)*

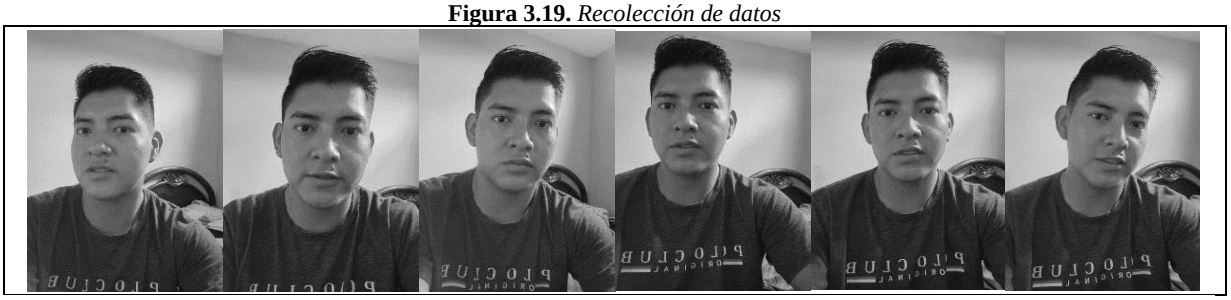
3.2 Diseño del bloque recolección de datos

En la primera etapa, se crea una base de datos en el sistema para almacenar los rostros de las personas autorizadas a encender la motocicleta. Es importante destacar que estas imágenes deben guardarse en formato jpg. y tener una resolución de 232x576 para que el sistema pueda procesarlas de manera efectiva. En este repositorio, se recopilan fotografías de los rostros de las personas permitidas, o de la persona específica según el caso, capturadas en diferentes momentos del día y con diversos gestos.

Este entrenamiento permite al sistema adaptarse a las variaciones en la iluminación, expresiones faciales y condiciones ambientales, facilitando la identificación de similitudes con los rostros capturados externamente. Dado que no siempre es posible capturar un rostro con los mismos gestos o bajo la misma claridad de luz, mientras mayor sean las tomas capturadas y guardadas en la base

de datos, se contribuirá a mejorar la capacidad del sistema para reconocer rostros de manera robusta y precisa.

Figura 3.19. *Recolección de datos*



Fuente: Autores.

3.3 Diseño del bloque de comparación de rostro

En la Figura 3.20, se presenta el bloque encargado de llevar a cabo la comparación de rostros. La secuencia comienza con la verificación de que el sistema haya identificado al menos un rostro. Luego, la variable que retiene la información del rostro se codifica en un formato comprensible para el microprocesador. Seguidamente, se inicia la comparación entre el rostro externo capturado y aquel almacenado en la base de datos, evaluando el grado de coincidencia entre ambas representaciones faciales.

El rostro externo, una vez capturado, se visualiza en la pantalla. Si es reconocido, el sistema emite una alerta que muestra el nombre del usuario identificado. En caso contrario, el sistema procesa la información como la presencia de un usuario desconocido. Este proceso de comparación y alerta contribuye a la función de reconocimiento facial del sistema de seguridad.

Figura 3.20. *Código de comparación de rostros.*

```
# Comparar con las imágenes de referencia
resultados = face_recognition.compare_faces(encodings_referencia,
encoding_frame, tolerance=0.5)

# Encontrar la coincidencia (si hay alguna)
nombre_encontrado = "No encontrado"
for i, resultado in enumerate(resultados):
if resultado:
nombre_encontrado = nombres[i]
break

# Mostrar el nombre en la ventana por 5 segundos
cv2.putText(frame, f'Nombre: {nombre_encontrado}', (50, 50),
cv2.FONT_HERSHEY_SIMPLEX, 1, (0, 255, 0), 2, cv2.LINE_AA)
cv2.imshow('Reconocimiento Facial', frame)
cv2.waitKey(5000) # Esperar 5 segundos
```

Fuente: Autores.

3.4 Diseño del bloque de procesamiento (Reconocimiento facial mediante la cámara).

En la Figura 3.21, se observa el código que inicia el proceso de captación de rostros por la cámara de la Raspberry. A continuación, se procede a la selección de la resolución de la cámara que será visualizada en la pantalla, permitiendo configurarla de acuerdo con las necesidades y el tamaño de la pantalla a utilizar.

Una vez capturadas las imágenes, se preparan según los parámetros de las imágenes de referencia almacenadas en la base de datos. Estas imágenes se utilizan posteriormente para llevar a cabo la comparación con los rostros capturados durante el proceso.

Figura 3.21. *Código de inicialización de la cámara, para la comparación de rostros.*

```
# Inicializar la cámara
cap = cv2.VideoCapture(0)

# Configurar la resolución de la cámara (ajustar según sea necesario)
cap.set(cv2.CAP_PROP_FRAME_WIDTH, 1280)
cap.set(cv2.CAP_PROP_FRAME_HEIGHT, 720)

# Lista de nombres y rutas de imágenes de referencia
nombres_referencia = ["Nando"] # Agrega más nombres según sea necesario
rutas_referencia = ["/home/pi/Desktop/codigos/img/nando.jpg"] # Rutas
correspondientes a las imágenes

# Cargar imágenes de referencia y sus nombres
encodings_referencia = []
nombres = []
for ruta in rutas_referencia:
imagen_referencia = face_recognition.load_image_file(ruta)
encoding_referencia = face_recognition.face_encodings(imagen_referencia)[0]
encodings_referencia.append(encoding_referencia)
nombres.append(ruta.split("/")[-1].split(".")[0]) # Extraer el nombre desde la
ruta

while True:
# Leer un frame de la cámara
ret, frame = cap.read()

# Verificar si el frame se leyó correctamente
if not ret:
print("Error al leer el frame.")
break

# Mostrar la vista de la cámara
cv2.imshow('Reconocimiento Facial', frame)
```

Fuente: Autores.

3.5. Autenticación por reconocimiento facial usando la red neuronal

El proceso de autenticación por reconocimiento facial es la parte central del sistema ya que comprende la ejecución del algoritmo para el procesamiento de las imágenes que lleva a cabo la red neuronal para realizar la comparación entre los rostros capturados y los almacenados. A continuación, se detallan las funciones principales de este proceso:

- **Red neuronal para el reconocimiento facial:** La red neuronal desempeña un papel crucial en el sistema de reconocimiento facial, y fue entrenada para aprender y reconocer las características y los patrones distintivos de un rostro al analizar numerosas imágenes almacenadas en la base de datos. Su objetivo es identificar las características únicas de los rostros autorizados.

  Preprocesamiento del rostro: Cuando el sistema captura un rostro, este pasa por un proceso de preprocesamiento para normalizar sus características. La red neuronal es esencial en este paso, asegurando que la información del rostro esté bien estructurada y lista para su análisis.

  Extracción de características: La red neuronal extrae automáticamente las características relevantes del rostro, como la disposición de los ojos, la forma de la nariz, la boca, entre otras. Estas características se transforman en datos numéricos comprensibles para el microprocesador, permitiendo su interpretación como un rostro.

  Comparación con la base de datos de rostros autorizados: La comparación implica calcular la similitud entre los datos numéricos extraídos y almacenados en la base de datos. Utilizando algoritmos específicos, se asigna una probabilidad de similitud que determina la autenticidad del rostro analizado.

En la Figura 3.22, se muestra el bloque de código que permite a la red neuronal la identificación y extracción de características únicas del rostro, además de la comparación con la base de datos para la toma de decisiones subsiguientes del sistema en el proceso de reconocimiento facial.

En el código se incluyeron comentarios de ayuda con la finalidad de brindar una mejor explicación del mismo, y pueda ser comprensible para innovaciones futuras.

Figura 3.22. *Bloque de Entrenamiento final del Sistema.*

```
import cv2
import face_recognition
import RPi.GPIO as GPIO
import time

# Desactivar las advertencias GPIO
GPIO.setwarnings(False)

# Configurar el modo de pines GPIO
GPIO.setmode(GPIO.BCM)

# Configurar los pines del pulsador y del relé
PIN_PULSADOR_DETECCION = 17
PIN_PULSADOR_APAGADO = 27
PIN_RELE = 23
PIN_BUZZER = 22 # Nuevo pin para el buzzer

# Configurar los pines de los pulsadores como entrada
GPIO.setup(PIN_PULSADOR_DETECCION, GPIO.IN, pull_up_down=GPIO.PUD_UP)
GPIO.setup(PIN_PULSADOR_APAGADO, GPIO.IN, pull_up_down=GPIO.PUD_UP)

# Configurar los pines del relé y del buzzer como salida
GPIO.setup(PIN_RELE, GPIO.OUT)
GPIO.setup(PIN_BUZZER, GPIO.OUT)

# Mantener el relé y el buzzer inicialmente apagados
GPIO.output(PIN_RELE, GPIO.LOW)
GPIO.output(PIN_BUZZER, GPIO.LOW)

# Función para la detección facial
def detectar_persona(frame, encodings_referencia, nombres):
# Detectar rostros en el frame
face_locations = face_recognition.face_locations(frame)

# Si se detecta al menos un rostro
if face_locations:
# Codificar el rostro detectado
encoding_frame = face_recognition.face_encodings(frame, face_locations)[0]

# Comparar con las imágenes de referencia
resultados = face_recognition.compare_faces(encodings_referencia,
encoding_frame, tolerance=0.5)

# Encontrar la coincidencia (si hay alguna)
nombre_encontrado = "No encontrado"
for i, resultado in enumerate(resultados):
if resultado:
nombre_encontrado = nombres[i]
break

# Mostrar el nombre en la ventana por 5 segundos
cv2.putText(frame, f'Nombre: {nombre_encontrado}', (50, 50),
cv2.FONT_HERSHEY_SIMPLEX, 1, (0, 255, 0), 2, cv2.LINE_AA)
cv2.imshow('Reconocimiento Facial', frame)
cv2.waitKey(5000) # Esperar 5 segundos
```

```
# Controlar el relé y el buzzer según la detección
if nombre_encontrado != "No encontrado":
GPIO.output(PIN_RELE, GPIO.HIGH) # Encender el relé
while GPIO.input(PIN_PULSADOR_APAGADO) == GPIO.HIGH:
pass # Esperar hasta que se presione el pulsador de apagado

GPIO.output(PIN_RELE, GPIO.LOW) # Apagar el relé cuando se presiona el pulsador
de apagado

else:
# Si no se detecta un rostro conocido, activar el buzzer durante 3 segundos
GPIO.output(PIN_BUZZER, GPIO.HIGH)
time.sleep(10)
GPIO.output(PIN_BUZZER, GPIO.LOW)

# Mostrar el frame en una ventana
cv2.imshow('Reconocimiento Facial', frame)

# Inicializar la cámara
cap = cv2.VideoCapture(0)

# Configurar la resolución de la cámara (ajustar según sea necesario)
cap.set(cv2.CAP_PROP_FRAME_WIDTH, 1280)
cap.set(cv2.CAP_PROP_FRAME_HEIGHT, 720)

# Lista de nombres y rutas de imágenes de referencia
nombres_referencia = ["Nando"] # Agrega más nombres según sea necesario
rutas_referencia = ["/home/pi/Desktop/codigos/img/nando.jpg"] # Rutas
correspondientes a las imágenes

# Cargar imágenes de referencia y sus nombres
encodings_referencia = []
nombres = []
for ruta in rutas_referencia:
imagen_referencia = face_recognition.load_image_file(ruta)
encoding_referencia = face_recognition.face_encodings(imagen_referencia)[0]
encodings_referencia.append(encoding_referencia)
nombres.append(ruta.split("/")[-1].split(".")[0]) # Extraer el nombre desde la
ruta

while True:
# Leer un frame de la cámara
ret, frame = cap.read()

# Verificar si el frame se leyó correctamente
if not ret:
print("Error al leer el frame.")
break

# Mostrar la vista de la cámara
cv2.imshow('Reconocimiento Facial', frame)

# Detectar persona solo cuando se presiona el pulsador de detección
if GPIO.input(PIN_PULSADOR_DETECCION) == GPIO.LOW:
```

```
detectar_persona(frame, encodings_referencia, nombres)

# Esperar hasta que se libere el pulsador antes de continuar
while GPIO.input(PIN_PULSADOR_DETECCION) == GPIO.LOW:
pass

# Salir si se presiona la tecla 'q'
if cv2.waitKey(1) & 0xFF == ord('q'):
break

# Liberar la cámara y cerrar la ventana al salir
cap.release()
cv2.destroyAllWindows()

# Limpiar configuración de pines GPIO
GPIO.cleanup()
```

Fuente: Autores.

3.6 Diseño del bloque de encendido

Como resultado del proceso de autenticación, el sistema procede con la activación del actuador cuando se reconoce un rostro autorizado.

En caso de que el rostro capturado no presente similitud con los almacenados, se procederá a activar el buzzer durante un periodo de tiempo predeterminado. Este buzzer actúa como una alarma, alertando que una persona no autorizada está intentando encender la motocicleta. Este mecanismo contribuye a la seguridad del sistema al identificar intentos no autorizados de uso.

Figura 3.23. *Código de activación del actuador o alarma según el reconocimiento facial.*

```
# Controlar el relé y el buzzer según la detección
if nombre_encontrado != "No encontrado":
GPIO.output(PIN_RELE, GPIO.HIGH) # Encender el relé
while GPIO.input(PIN_PULSADOR_APAGADO) == GPIO.HIGH:
pass # Esperar hasta que se presione el pulsador de apagado

GPIO.output(PIN_RELE, GPIO.LOW) # Apagar el relé cuando se presiona el pulsador
de apagado

else:
# Si no se detecta un rostro conocido, activar el buzzer durante 3 segundos
GPIO.output(PIN_BUZZER, GPIO.HIGH)
time.sleep(10)
GPIO.output(PIN_BUZZER, GPIO.LOW)

# Mostrar el frame en una ventana
cv2.imshow('Reconocimiento Facial', frame)
```

Fuente: Autores.

CAPÍTULO IV
PRUEBAS E INTERPRETACIÓN DE LOS RESULTADOS

4.1 Pruebas de validación

Después de configurar e integrar todos los componentes del sistema seleccionados, se procedió con la construcción del prototipo de manera externa para validar su funcionamiento correcto antes de la implementación en la motocicleta.

Figura 4.24. *Pruebas de validación con el sistema fuera del vehículo.*

Fuente: Autores.

Una vez ensamblado y el circuito, se probó la activación del relé, que cierra el circuito de contacto de la motocicleta al autenticar el rostro, permitiendo el encendido del vehículo. De manera correspondiente, si el rostro capturado no es reconocido, se activa el buzzer, generando una alerta sonora durante 10 segundos.

Con el sistema de seguridad concluido y resultados satisfactorios en las pruebas preliminares, se procede a la fabricación de cada una de las piezas diseñadas para su fijación en la motocicleta. Posteriormente, se llevará a cabo la instalación de todos los componentes y la realización de las pruebas respectivas una vez integrados en el vehículo.

Figura 4.15. *Pruebas de validación con el sistema implementado en el vehículo.*

Fuente: Autores.

4.2 Pruebas de encendido

4.2.1 Verificación de puesta en contacto del vehículo subcategoría L3.

Al poner en marcha el sistema de autenticación a través del reconocimiento facial y capturar el rostro del usuario autorizado, se produce la activación del relé. Este al activarse, cumple la función de cerrar el circuito de encendido de la motocicleta, permitiendo que entre en contacto sin requerir el uso de la llave. Posteriormente, el usuario puede presionar el botón de arranque para encender la motocicleta.

Figura 4.26. *Proceso de captura del rostro para la fase de reconocimiento facial.*

Fuente: Autores.

Figura 4.27. *Reconocimiento facial del usuario autorizado.*

Fuente: Autores.

Figura 4.28. *Verificación de activación, luego del proceso de reconocimiento facial.*

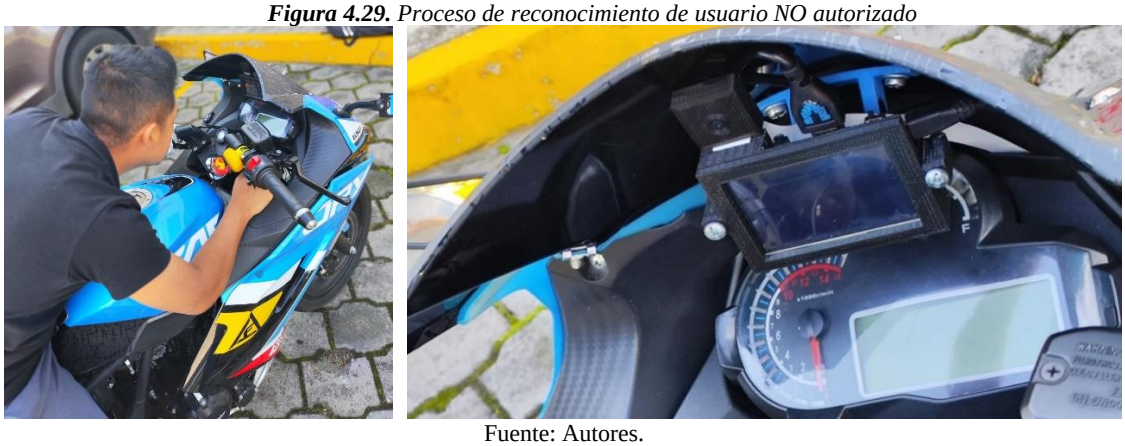
Fuente: Autores.

4.2.2 Prueba de funcionamiento

En el desarrollo de estas pruebas, el usuario autorizado inicia el proceso activando los componentes, comenzando con el encendido de la Raspberry y posteriormente ejecutando el sistema en el microcontrolador.

El usuario se posiciona frente a la cámara y presiona el botón destinado para capturar su rostro. En caso de ser el usuario autorizado, el sistema procede a validar la identificación y activa el relé, facilitando así el contacto de la motocicleta. En situaciones contrarias, donde el sistema no identifica al usuario, se despliega un mensaje en la parte superior izquierda indicando la falta de reconocimiento, al mismo tiempo que activa un buzzer que emite un pitido durante un período determinado.

Figura 4.29. *Proceso de reconocimiento de usuario NO autorizado*



Fuente: Autores.

Este proceso se repite secuencialmente en caso de que el usuario no esté autorizado. En el caso afirmativo, el sistema permite el contacto de la motocicleta, permitiendo al usuario ponerla en marcha para su conducción.

4.3 Tiempos de puesta en marcha del sistema

4.3.1 Tiempo de iniciación del sistema

El tiempo requerido para iniciar la ejecución del programa es de 1 minuto y 15 segundos. Cuando la cámara detecta un rostro previamente registrado y entrenado, el sistema de seguridad permite el encendido del vehículo de la subcategoría L3 en un periodo de 3 segundos.

El sistema de reconocimiento facial en la motocicleta presenta cierta complejidad debido al espacio limitado y la variabilidad en la posición del conductor, que no siempre es constante. Para abordar este desafío, se incorporó un pulsador destinado a capturar el rostro externo para su posterior comparación. Esta medida contribuye a la ejecución del sistema únicamente cuando sea necesario, evitando capturas erróneas en situaciones innecesarias.

4.3.2 Tiempo de respuesta del sistema en diferentes condiciones

La Tabla 3 presenta los intervalos de tiempo necesarios para la captación del rostro externo por parte del sistema, con el propósito de llevar a cabo la comparación con la base de datos. Estos tiempos se registraron bajo diversas condiciones externas de iluminación.

Tabla 3. *Tiempos de respuesta del reconocimiento facial en condiciones de día.*

	Tiempo de captura de rostro (segundos)		
	Iluminación alta	**Iluminación media**	**Iluminación baja**
Prueba 1	10	3	6
Prueba 2	9	4	5
Prueba 3	8	3	6
Prueba 4	10	5	7
Prueba 5	7	3	6
Promedio	8.8	3.6	6

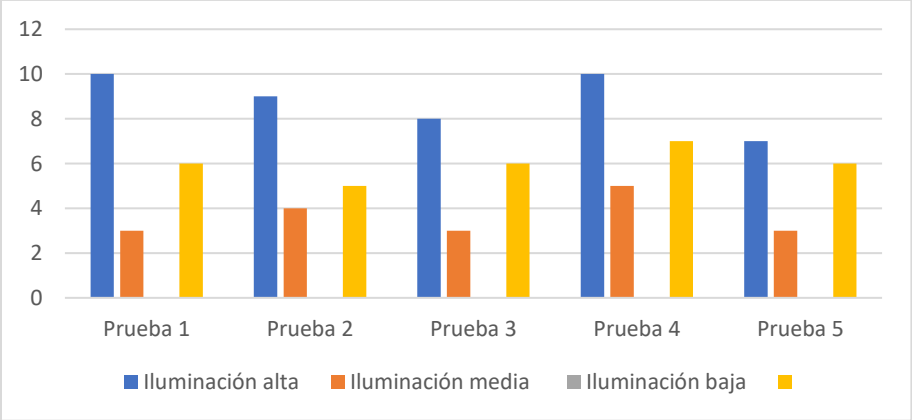
Fuente: Autores 2023

Según se observa en la Tabla 3, los tiempos de respuesta presentan variaciones debido principalmente a factores de iluminación del entorno, siendo particularmente mayor cuando las

condiciones de iluminación externa son altas. Se nota que el tiempo de respuesta se prolonga significativamente en entornos exteriores con una alta iluminación, especialmente cuando la luz solar es intensa.

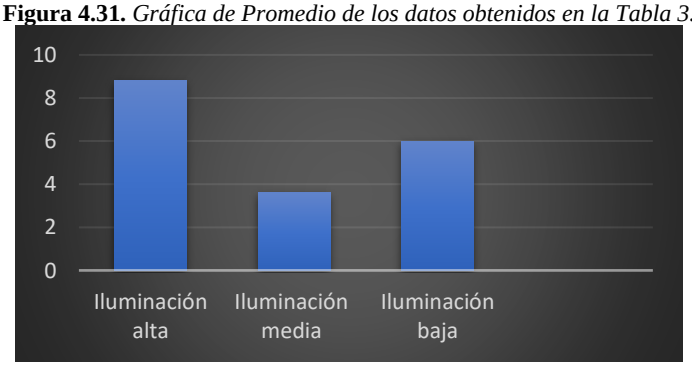
En estas circunstancias, el sistema experimenta un mayor tiempo de captación del rostro externo, el cual se utiliza posteriormente en la comparación con la base de datos para generar una respuesta.

Figura 4.23. *Tiempo de respuesta vs Calidad de Iluminación.*



Fuente: Autores.

Figura 4.31. *Gráfica de Promedio de los datos obtenidos en la Tabla 3.*



Fuente: Autores.

Según los resultados de la Figura 4.31, el tiempo de respuesta más corto se registra en entornos con iluminación moderada o cuando la motocicleta se encuentra con iluminación moderada bajo techo.

Esta situación resulta beneficiosa ya que reduce la influencia de la iluminación exterior o del resplandor del sol. En estos escenarios, la cámara logra captar de manera más efectiva el rostro,

permitiendo un perfilado más preciso de la red neuronal y la extracción de rasgos faciales de manera más concisa y específica.

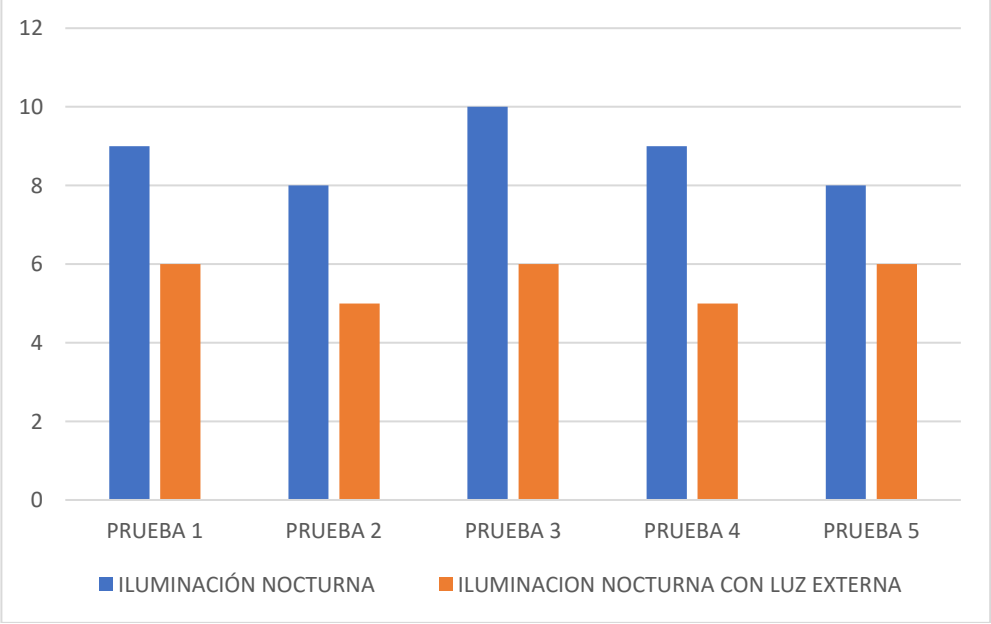
Tabla 4. *Tiempos de respuesta del reconocimiento facial en condiciones de noche.*

	Tiempo de respuesta (segundos)	
	Iluminación nocturna	**Iluminacion nocturna con luz externa**
Prueba 1	**9**	**6**
Prueba 2	8	5
Prueba 3	10	6
Prueba 4	9	5
Prueba 5	8	6
Promedio	8.8	5.6

Fuente: Autores.

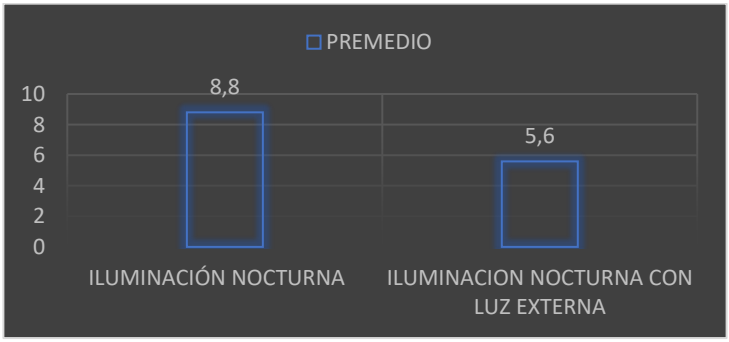
Según lo indicado en la Tabla 4, se observa que durante la noche, unicamente con la luz nocturna o alguna iluminacion presente, como la proveniente del alumbrado publico o la luz lunar en el lugar de estacionamiento de la moto, el tiempo de respuesta para la captacion del rostro es prolongado debido a la dificultad en la visibilidad facial. No obstante, en la noche, al incorporar una fuente adicional de ilumicacion, como una luz led situada sobre la pantalla y enfocada hacia el rostro, se evidencia una mejora considerable en la captura del rostro. Esta mejora se traduce a una visualizacion mas clara para la camara, facilitando asi su captación.

Figura 4.32. *Tiempo de respuesta: Iluminación Nocturna vs Iluminación Nocturna con iluminación extra.*



Fuente: Autores.

Figura 4.33. *Promedio de Pruebas: Iluminación Nocturna vs Iluminación Nocturna con Luz extra.*



Fuente: Autores.

De acuerdo con lo evidenciado en la figura 4.33, se destaca que el menor tiempo de respuesta para la captación del rostro durante la noche se alcanza cuando se dispone de una iluminación externa dirigida específicamente a facilita la iluminación facial. Es importante señalar que en ambas situaciones se logra la captura del rostro, pero para optimizar la eficiencia en cuanto a tiempo de lectura del rostro externo, se contempla la instalación de esta luz adicional.

4.4 Análisis de efectividad

En esta sección se llevarán a cabo exclusivamente pruebas focalizadas en la fase de reconocimiento facial, con el objetivo de evaluar la efectividad del sistema al identificar al usuario autorizado y a aquellos no autorizados para el encendido de la motocicleta. Este proceso de evaluación busca establecer la viabilidad de implementar el sistema en otras motocicletas.

Es importante destacar que, debido a la composición del sistema, que incluye una variedad de elementos, su aplicabilidad puede ser limitada en ciertos tipos de motocicletas. La razón principal radica en la necesidad de espacio para la instalación de todos los componentes. Por lo tanto, su efectividad está específicamente diseñada para motocicletas tipo ninja y pasolas, las cuales cuentan con un carenado amplio que permite ocultar todos los componentes, dificultando su manipulación indebida.

Para el desarrollo de las pruebas se consideró la participación de 2 personas: una de ellas debidamente autorizada y la otra no autorizada, adicionalmente se usó la fotografía de la persona autorizada. El propósito de estos tres escenarios es validar la efectividad del sistema para evaluar

su capacidad para distinguir entre usuarios autorizados y no autorizados, así como su desempeño ante posibles intentos de manipulación mediante el uso de fotografías.

4.4.1 Prueba de Reconocimiento de una persona autorizada

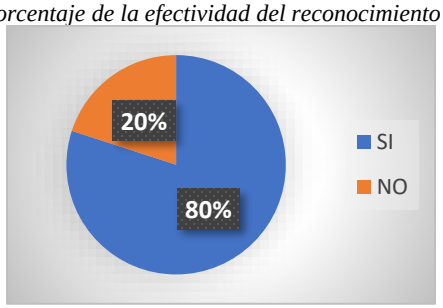
En este escenario se ejecutaron 20 pruebas las cuales se detallarán en la tabla 5 que evidencia el porcentaje de efectividad:

Tabla 5. *Pruebas de reconocimiento al usuario registrado.*

	RECONOCE AL USUARIO	
No. PRUEBA	**SI**	**NO**
1	X	
2	X	
3	X	
4	X	
5		X
6	X	
7	X	
8		X
9	X	
10	X	
11	X	
12		X
13	X	
14	X	
15	X	
16		X
17	X	
18	X	
19	X	
20	X	
TOTAL	16	4

Fuente: Autores.

Figura 4.34. *Gráfico de porcentaje de la efectividad del reconocimiento facial de la persona autorizada.*



Fuente: Autores.

Según los resultados de la Figura 4.34, el sistema presenta un nivel considerable de efectividad al reconocer el rostro de la persona autorizada para operar la motocicleta. Sin embargo, es importante señalar que esta efectividad no es absoluta, ya que en las pruebas se ven afectadas por diversas variables externas.

Factores como la posición para la captación del rostro, la iluminación del entorno, cambios físicos en el rostro, entre otras variables, influyen en los resultados del sistema, generando en ciertos casos respuestas diferentes a las esperadas.

4.4.2 Pruebas de Reconocimiento de una persona NO autorizada

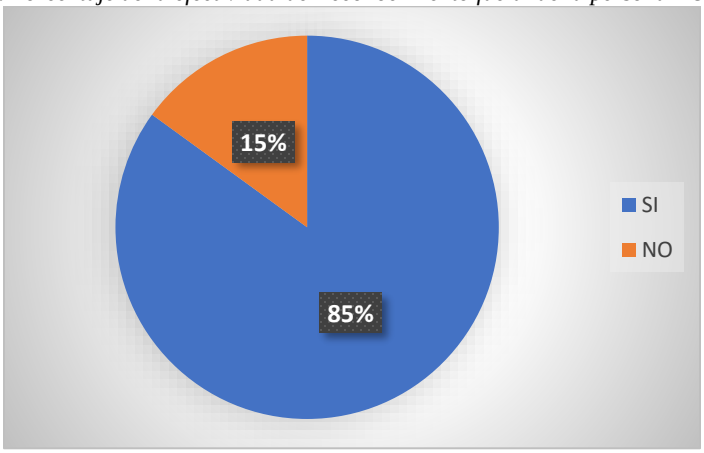
Al igual que en el escenario anterior, se realizaron un total de 20 pruebas las cuales se detallan en la tabla 6, con su respectivo porcentaje de efectividad:

Tabla 6. *Pruebas de reconocimiento al usuario registrado.*

	RECONOCE QUE ES UN USUARIO NO AUTORIZADO	
No. PRUEBA	**SI**	**NO**
1	X	
2	X	
3	X	
4	X	
5		X
6	X	
7	X	
8	X	
9	X	
10	X	
11	X	
12	X	
13		X
14	X	
15	X	
16	X	
17	X	
18	X	
19	X	
20		X
TOTAL	17	3

Fuente: Autores.

Figura 4.35. *Porcentaje de la efectividad del reconocimiento facial de la persona NO autorizada.*



Fuente: Autores.

En la Figura 4.35, se puede apreciar que el sistema presenta un alto grado de efectividad en la identificación del rostro autorizado, aunque no es absoluto. Se nota que en ciertas ocasiones se permitió el acceso a una persona no autorizada, y esto podría atribuirse a diversas variables, entre ellas, la iluminación que es un factor altamente influyente que podría afectar negativamente el reconocimiento facial al provocar tonalidades falsas en el rostro.

4.4.3 Prueba de Reconocimiento mediante la fotografía de una persona autorizada

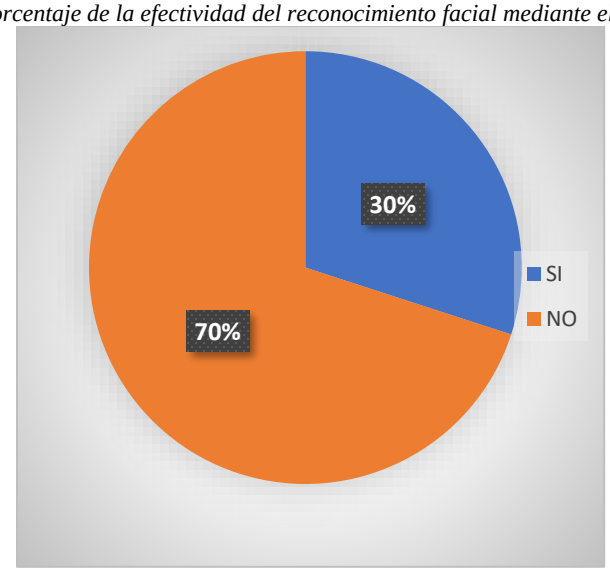
En el siguiente escenario se muestra el nivel de efectividad usando la fotografía de una persona autorizada. Como se observa en la tabla de resultados, el sistema puede ser muy vulnerable en estas circunstancias debido a que la cámara utilizada solo es capaz de distinguir características superficiales del rostro y no profundidades. Para lograr este nivel de detalle, se requeriría una cámara especial basada en rayos infrarrojos. A pesar de estas limitaciones, se el sistema mantiene un nivel significativo de efectividad:

Tabla 7. *Reconocimiento facial por medio de una fotografía.*

	RECONOCIMIENTO MEDIANTE UNA FOTOGRAFÍA	
No. PRUEBA	**SI**	**NO**
1	X	
2		X
3		X
4		X
5		X
6	X	
7		X
8		X
9		X
10	X	
11		X
12	X	
13		X
14		X
15		X
16	X	
17		X
18		X
19	X	
20		X
TOTAL	6	14

Fuente: Autores 2023.

Figura 4.36. *Porcentaje de la efectividad del reconocimiento facial mediante el uso de una fotografía.*



Fuente: Autores.

CONCLUSIONES

- El uso de la inteligencia artificial en el ámbito automotriz, revelan los importantes avances tecnológicos que abren una gama de alternativas y oportunidades para el desarrollo de soluciones efectivas e innovadoras en temas de ergonomía y de seguridad.

- El sistema de seguridad vehicular basado en reconocimiento facial requirió de la codificación, y el uso de bibliotecas y comandos avanzados de programación para llevar a cabo funciones fundamentales, como el entrenamiento de la red neuronal, la captura, procesamiento y comparación de rasgos faciales, asegurando así una autenticación precisa y rápida del usuario.

- La funcionalidad de un sistema de seguridad vehicular basado en autenticación por reconocimiento de requiere del uso de tarjetas programables con alta capacidad de procesamiento y almacenamiento que se traduce en la eficiencia y la precisión del procesamiento de información, minimizando posibles errores, así como vulnerabilidades del sistema.

- La exitosa integración de todos los elementos del sistema de seguridad en el sistema de arranque de un vehículo L3 posibilita la activación del encendido sin la necesidad de utilizar una llave, ya que la identificación facial de individuos autorizados cumple con esta función. Este sistema representa una alternativa innovadora que refuerza la protección contra el encendido no autorizado de la motocicleta y adicionalmente contribuye a simplificar el proceso de arranque.

- La realización de pruebas de desempeño, permitieron validar la efectividad del sistema considerando variaciones de iluminación del entorno. El sistema presenta un gran desempeño al autenticar a los usuarios autorizados, incluso en condiciones adversas de iluminación, lo cual sugiere su operatividad aun en condiciones ambientales no favorables.

RECOMENDACIONES

- Considerando que ningún sistema de reconocimiento facial puede garantizar una efectividad del 100%, ya que intervienen algunas variables, se sugiere atender las condiciones climáticas que son esenciales para una ejecución correcta del sistema.

- Para futuras versiones se sugiere realizar una comparativa de los componentes más avanzados y de altas prestaciones para perfeccionar el proceso de autenticación, priorizando los tiempos de captura de datos y la respuesta en los procesos de validación de las imágenes. Actualmente existen componentes que pueden mejorar aún más la efectividad del sistema implementado.

- Se recomienda realizar las pruebas de validación y efectividad del sistema de seguridad fuera de producción o en laboratorio, con la finalidad de optimizar la instalación posterior del prototipo evitando posibles fallos que pueden ocasionarse al estar trabajando con corrientes que pueden generar corto-circuitos y se requiera el reemplazo de componentes.

- Es importante tomar en cuenta la ubicación del sistema de seguridad, debido a que el espacio en una motocicleta es reducido, y esto puede limitar o dificultar la implementación en ciertos modelos de vehículos subcategoría L3.

REFERENCIAS BIBLIOGRÁFICAS.

Alex Nuñez, L. N. (2020). Reconocimiento Facial para el encendido automático de vehículos basados en Raspberry Pi. *Revista ODIGOS*, 1-2.

Calvo, L. (10 de Marzo de 2022). *GoDaddy Web site*. Obtenido de GoDaddy Web site: https://es.godaddy.com/blog/que-es-raspberry-pi/

Chávez, E. (14 de Abril de 2023). *autocosmos*. Obtenido de autocosmos: https://noticias.autocosmos.com.co/2023/04/14/bmw-iface-sistema-de-reconocimiento-facial-y-ocular-antirrobo-de-motos

Desarrolladores web. (18 de Mayo de 2023). *Desarrolladores Web site*. Obtenido de Desarrolladores Web site: https://desarrolladoresweb.org/python/que-es-python-y-para-que-sirve-caracteristicas-como-funciona-y-que-se-puede-hacer/

Electrositio. (2023). *Electrositio Web site*. Obtenido de Electrositio Web site: https://electrositio.com/que-es-un-transformador-de-corriente-funcionamiento-y-sus-aplicaciones/?expand_article=1

FayalsMotos. (5 de Septiembre de 2022). Obtenido de FayalsMotos: https://www.fayalsmotos.com/2022/03/robos-en-motos-aumentan-en-2022-en-el.html

Fiscalía General Del Estado, FGE. (08 de Julio de 2021). *Ecuador - Guía Oficial de Trámites y Servicios*. Obtenido de Ecuador - Guía Oficial de Trámites y Servicios: https://www.fiscalia.gob.ec/wp-content/uploads/2021/08/Cifras-robo-corte08072021.pdf

García, D. (4 de Mayo de 2023). Obtenido de MSMK The University of Science & Technology Web site: https://msmk.university/ciberseguridad/autenticidad

Hernández, R. G. (2012). *Estudio de técnicas de reconcimiento facial* (Vol. 4).

IBM. (20 de Abril de 2021). *IBM*. Obtenido de IBM: https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009740--htm

Ihalainen, P. (1 de Septiembre de 2016). *GlobalSign Web site*. Obtenido de GlobalSing Web site: https://www.globalsign.com/es/blog/what-is-biometric-authentication

InteractiveChaos. (2023). *InteractiveChaos Web site*. Recuperado el 14 de Octubre de 2023, de InteractiveChaos Web site: https://interactivechaos.com/es/manual/tutorial-de-machine-learning/tutorial-de-machine-learning

kaspersky. (15 de Enero de 2013). *kaspersky Web site*. Recuperado el 10 de Octubre de 2023, de kaspersky Web site: https://www.kaspersky.es/resource-center/definitions/what-is-facial-recognition

Lopez, R., Marañón, F., Erazo, G., & Reinoso, S. (2009). Sistema de seguridad mediante reconocimiento facial para la puesta en marcha de un Chevrolet... *Repositorio*, 1-2.

MCI Electronics. (2023). *MCI Electronics Web site*. Obtenido de MCI Electronics Web site: https://raspberrypi.cl/producto/pantalla-tactil-lcd-3-5-para-raspberry-pi-3b-3b-4b/#:~:text=Caracter%C3%ADsticas%3A%201%20Resoluci%C3%B3n%20320%20%C3%97%20480%202%20Control,oro%20de%20inmersi%C3%B3n%20de%20alta%20calidad%20M%C3%A1s%20elementos

MotoGruaSaccsa. (26 de Junio de 2018). *MotoGruaSaccsa Web site*. Obtenido de MotoGruaSaccsa Web site: http://moto-grua.com/blog/como-funciona-el-sistema-de-encendido-de-una-moto

MOTOYCASCO. (Junio de 2019). Obtenido de MOTOYCASCO: https://motoycasco.com/mejores-antirrobo-moto/

Moyens Staff. (2021). *Moyens Web site*. Obtenido de Moyens Web site: https://es.moyens.net/tec/4-de-los-mejores-sistemas-operativos-ligeros-para-raspberry-pi/

Muradas, Y. (25 de Febrero de 2020). *OpenWebinars Web site*. Obtenido de OpenWebinars Web site: https://openwebinars.net/blog/que-es-gradle/

Olabe, X. B. (2016). *Redes Neuronales Artificiales y sus Aplicaciones.* Escuela Superior de Ingeniería de Bilbao.

OneSpan. (3 de Octubre de 2019). *OneSpan Web site*. Recuperado el 10 de Octubre de 2023, de OneSpan Web site: https://www.onespan.com/topics/biometric-authentication

Pietikainen, M. (2010). Local Binary Patterns. *Scholarpedia*, *5*(3), 9775. https://doi.org/10.42.49/scholsrpedia.9775

Prado, K. S. (10 de Noviembre de 2017). *Medium Web site*. Obtenido de Medium Web site: https://towardsdatascience.com/face-recognition-how-lbph-works-90ec258c3d6b

Primicias, R. (15 de Noviembre de 2022). El robo de motocicletas subió 8% en Quito durante el 2022. *PRIMICIAS El periodismo comprometido.*, pág. 7.

ProSegur. (10 de Julio de 2022). Obtenido de PROSEGUR: https://blog.prosegur.es/sistemas-de-seguridad-para-la-moto/#:~:text=Los%20principales%20sistemas%20de%20seguridad%20para%20la%20motocicleta,vehicular.%20Anclaje%20para%20el%20garaje.%20Alarma%20antirrobo.%20Protectores.

RECFACES. (2021). *RECFACES Web site*. Recuperado el 10 de Octubre de 2023, de RECFACES Web site: https://recfaces.com/es/articles/autenticacion-biometrica

Redacción Vistazo. (26 de Septiembre de 2023). Obtenido de Revista Vistazo: https://www.vistazo.com/actualidad/nacional/alerta-y-preocupacion-por-robo-de-vehiculos-y-motocicletas-en-ecuador-cual-es-la-cifra-reportada-en-lo-que-va-del-ano-ED6027431

ResearchGate. (Julio de 2019). *ResearchGate*. Obtenido de ResearchGate: https://www.researchgate.net/figure/Illustration-of-LBP-approach_fig3_338359209

Rodríguez, H. (28 de Abril de 2021). *Crehana Web site*. Obtenido de Crehana Web site: https://www.crehana.com/blog/transformacion-digital/que-es-opencv/

Rossum, V. (2007). Lenguaje de Programación Python. *Conferencia Técnica Anual de USENIX*, *41*(1), 36.

Saavedra, J. A. (12 de Septiembre de 2023). *EBAC Web site*. Obtenido de EBAC Web site: https://ebac.mx/blog/que-es-javascript

Saini, Y. (2022). *OpenGenus IQ Web site*. Obtenido de OpenGenus IQ Web site: https://iq.opengenus.org/lbph-algorithm-for-face-recognition/

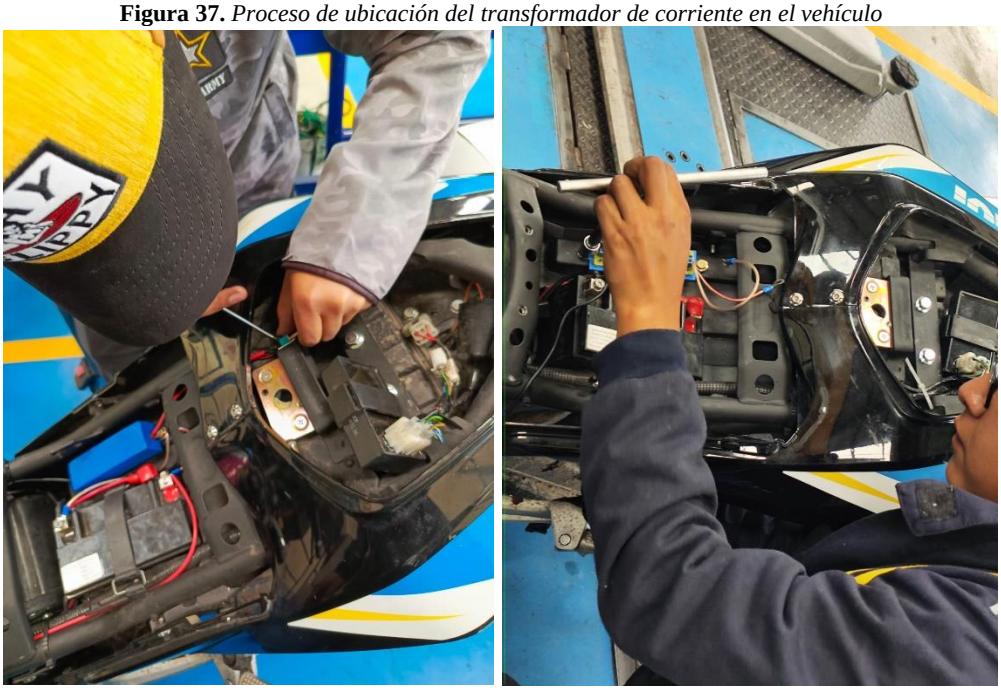
Sánchez, J. A. (2021). Desarrollo y validación de un algoritmo de reconocimiento facial para aplicaciones emotivas. Madrid, España. Obtenido de https://oa.upm.es/68968/1/TFG_JOSE_ANTONIO_ALONSO_SANCHEZ.pdf

Sánchez, M. L. (2022). Introducción a los sistemas de reconocimiento facial utilizando Deep learning. *ResearchGate*, 11..

Sotaquirá, M. (2 de Julio de 2018). *codificandobits Web site*. Obtenido de codificandobits Web site: https://www.codificandobits.com/blog/el-gradiente-descendente/#:~:text=El%20algoritmo%20del%20gradiente%20descendente%20es%20uno%20de,Convolucionales%2C%20Recurrentes%20y%20LSTM%2C%20hasta%20las%20Redes%20Transformer.

ANEXOS

Figura 37. *Proceso de ubicación del transformador de corriente en el vehículo*

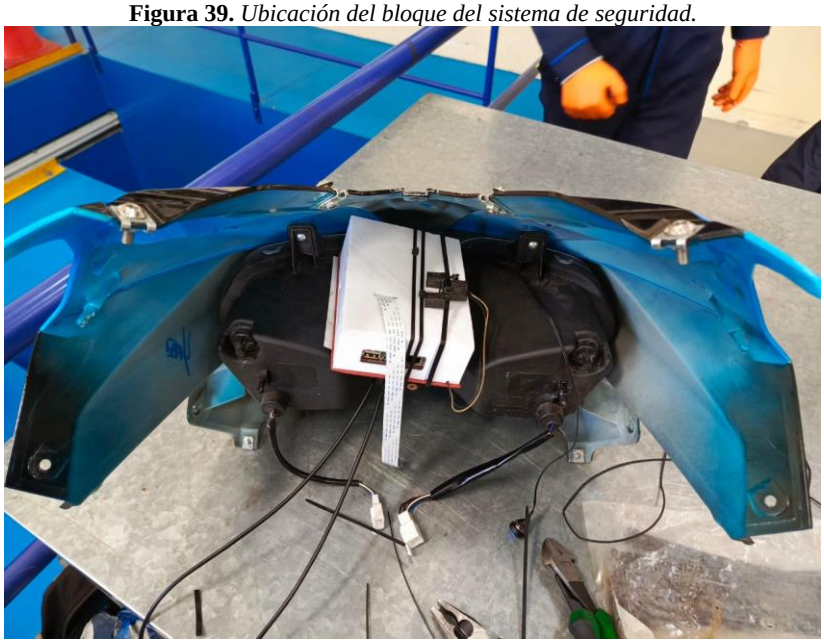


Fuente: Autores.

Figura 38. *Desarmado del carenado del vehículo para la implementación del sistema.*

Fuente: Autores.

Figura 39. *Ubicación del bloque del sistema de seguridad.*



Fuente: Autores.

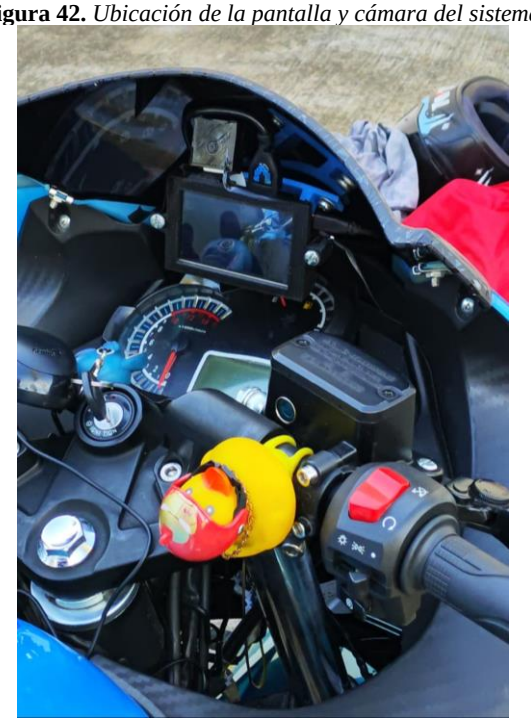
Figura 40. *Proceso de conexión del cableado.*

Fuente: Autores.

Figura 41. *Proceso de montaje del carenado con el sistema de seguridad implementado.*

Fuente: Autores.

Figura 42. *Ubicación de la pantalla y cámara del sistema.*



Fuente: Autores.