

Pontificia Universidad Católica del Perú

Facultad de Ciencias e Ingeniería



PONTIFICIA
UNIVERSIDAD
CATÓLICA
DEL PERÚ

MEJORA E IMPLEMENTACIÓN DEL HARDWARE PARA UN SISTEMA DE ACCESO VEHICULAR A LA PUCP BASADO EN TECNOLOGÍA RFID Y DETECCIÓN DE PLACAS VEHICULARES

Tesis para optar el Título de Ingeniero Electrónico, que presenta el bachiller:

Alvaro Alonso Chavarri Freyre

ASESOR: Willy Eduardo Carrera Soria

Lima, noviembre del 2020

Resumen

El fin del presente trabajo de tesis es la implementación física de los elementos de hardware para un sistema de ingreso vehicular a la Pontificia Universidad Católica del Perú, enfocado en el uso adecuado de las herramientas tecnológicas vigentes para reducir las afecciones de tiempo, economía y de seguridad en el ingreso a la universidad.

El diseño del trabajo partió del que fue presentado por el Ing. Luis Gomero Vásquez, en su tesis, “Diseño de un sistema de acceso vehicular a la PUCP basado en tecnología RFID y procesamiento de placas vehiculares”, PUCP, 2017.

En el presente trabajo se realizaron mejoras del diseño inicial para prevalecer el enfoque mencionado inicialmente, reduciendo gastos en computadores y empleando bases de datos en Internet.

Para la labor se emplearon tecnologías como las tarjetas de radiofrecuencia para la identificación de los usuarios, cámaras web para la recopilación de imágenes, placa de desarrollo Arduino para el accionamiento de indicadores visuales y mecánicos; así como para la recepción de datos de las tarjetas electromagnéticas, data enviada a una base de datos mediante un módulo Ethernet. Además, una placa de desarrollo Raspberry para el procesamiento de imágenes y comunicación con servidores en Internet.

Dado que el proyecto parte del concepto de “internet de las cosas” o IOT, en el que los elementos realizan comunicación de datos con internet para la gestión de la información relevante y acciones ante la gestión de estos en la nube. Se emplearán circuitos adicionales para este fin, como es el caso de las placas Arduino Ethernet y el aprovechamiento de la integración del Raspberry Pi 3 a través de su placa Ethernet incorporada.

Del mismo modo, se hará mención a la lógica de recibo de datos en los servidores virtuales para que estos puedan interpretar la información recibida, y la recopilación de imágenes por las cámaras en el ingreso vehicular para su procesamiento; para lo cual no se entrará a detalle en los algoritmos y programación por no estar en el alcance del presente estudio. Pero sí será necesario explicarlo para entender la elección de los equipos del proyecto. Los cuales deben cumplir con los requisitos que la parte de software plantea.



Agradezco a Dios y a mi madre por su esfuerzo, confianza y amor, esto es de ambos. Gracias a cada persona que a su modo me apoyó e impulsó. Mil gracias a cada uno de manera especial.

"El que da, no debe volver a acordarse; pero el que recibe nunca debe olvidar." Proverbio judío.

ÍNDICE

INTRODUCCIÓN	1
<u>CAPÍTULO 1.- DESCRIPCIÓN DEL PROBLEMA</u>	
1.1. Descripción de la problemática en la seguridad del acceso vehicular	
1.1.1. Variables internas	2
1.1.2. Identificación de la problemática.....	3
1.2. Declaración del Marco problemático.....	4
<u>CAPÍTULO 2.- TECNOLOGÍAS EN EL CONTROL DE ACCESO VEHICULAR</u>	
2.1 Estado del Arte	
2.1.1 Presentación del asunto de estudio.....	5
2.1.2 Estado de la investigación.....	6
2.1.2.1 Sistemas de acceso vehicular existentes.....	6
2.1.2.2 Tecnologías de identificación para accesos vehiculares.....	10
2.1.2.3 Diferencias técnicas para tecnologías de identificación.....	13
2.1.2.4 Requerimientos para la implementación del acceso vehicular.....	14
2.1.3 Síntesis sobre el asunto de estudio.....	22
<u>CAPÍTULO 3.- IMPLEMENTACIÓN DEL SISTEMA</u>	
3.1. Objetivos	
3.1.1. Objetivos Generales.....	24
3.1.2. Objetivos Específicos.....	24
3.2. Alcances del Proyecto.....	24
3.3. Comparativo con el proyecto inicial	26
3.4. Explicación de cambios.....	27
3.5. Metodología de elección de componentes	
3.5.1 Diagrama de flujo del Algoritmo de control.....	27
3.5.1. Módulo de Control.....	28
3.5.1.1 Conveniencia del uso del Raspberry.....	31
3.5.1.2 Conveniencia del uso del Arduino Mega y placa Ethernet externa.....	33
3.5.2. Elevador de voltaje para salidas del computador: 3.3V a 5V.....	33
3.5.3. Cámara.....	35
3.5.4. Pantalla de control.....	40
3.5.5 Sensor RFID.....	43
3.5.6. Indicadores.....	44
3.5.7. Fuente de Poder.....	49
3.5.8. Etapa de Potencia.....	52
3.6 Costos.....	57

CAPÍTULO 4.- RESULTADOS

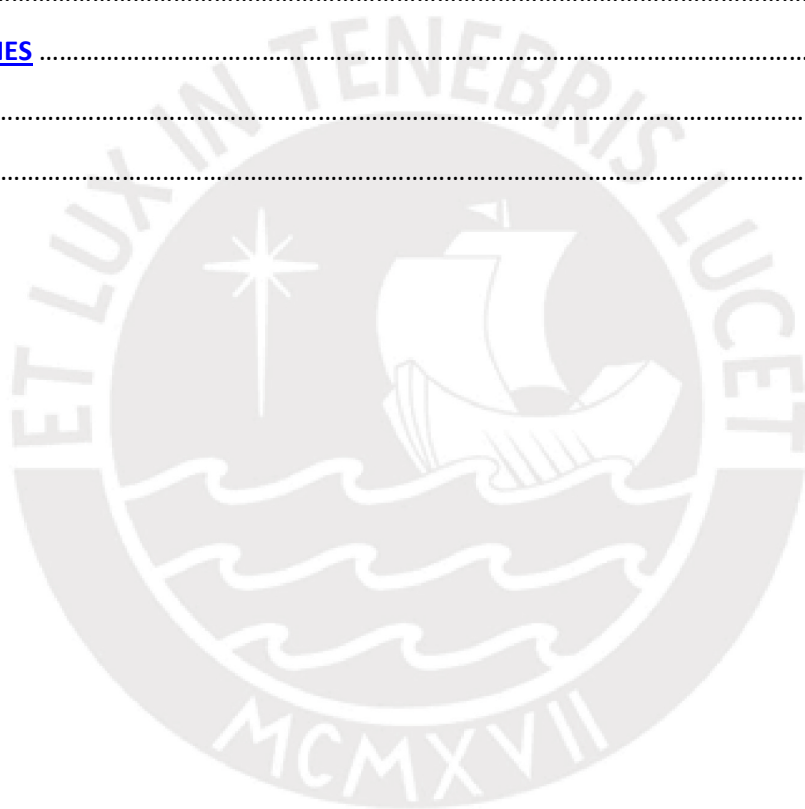
4.1. Envío y recepción de datos desde el módulo de control hacia la base de datos ubicada en Internet.....	59
4.1.1 Primera etapa: Arduino.....	59
4.1.2 Segunda etapa: Raspberry.....	62
4.2 Presentación de la interfaz del módulo de control.....	64
4.3 Integración: Datos Recibidos – Activación de Indicadores.....	65
4.4 Diagrama de bloques final.....	67

<u>CONCLUSIONES</u>	68
----------------------------------	----

<u>RECOMENDACIONES</u>	69
-------------------------------------	----

<u>BIBLIOGRAFÍA</u>	70
----------------------------------	----

ANEXOS.....	73
-------------	----



INTRODUCCIÓN

En la actualidad, la delincuencia en el país ha incrementado a niveles alarmantes; siendo, en el año 2014, elegidos como el país con mayor índice de delincuencia en Latinoamérica. Por tales motivos, la seguridad se ha convertido en un interés común e importante para todo ciudadano, y la mejor idea para contrarrestar este mal que acecha, es la prevención. [1] La infiltración de personas en diversos lugares de espacios públicos y no públicos, es una modalidad de robo muy común. Siendo el año 2015, un año anecdótico para la Pontificia Universidad Católica del Perú, tras sufrir un ataque e infiltración de personas a la entidad y robar sumas cuantiosas de dinero de la cafetería central.

De esta manera, la reducción de la posibilidad de un acceso de personas extrañas en un recinto, se debe de llevar a cabo con un sistema que involucre tecnología de reconocimiento; ya sea para el personal, alumnado y/o diversos miembros de una comunidad. Además de un registro digital de dicho ingreso, esto para el control de la seguridad ante alguna emergencia.

La presente tesis, parte de un proyecto para un sistema integral de entrada vehicular a la PUCP propuesto por la sección de Electricidad y Electrónica y mencionado en la tesis del Ing. Luis Gomero Vásquez, titulado “Diseño de un sistema vehicular a la PUCP basado en tecnología RFID y detección de placas vehiculares” (2016). Se desarrolló la implementación y mejora de hardware de este sistema integral.

La implementación de dicho hardware está compuesta por el módulo de identificación por RFID, la elección de un motor para activación de la tranquera, el uso de una pantalla de comunicación con el usuario, una cámara web que enviará las imágenes de la entrada, una fuente de alimentación para la parte de control y potencia del sistema, y el hardware de control de los periféricos mencionados anteriormente. El sistema estará interconectado con una base de datos, la cual permitirá almacenar los registros de ingreso de automóviles, tales como placa del vehículo, hora de ingreso, persona relacionada y otros datos requeridos para el reconocimiento exacto del ingreso. Asimismo, permitirá, al personal de seguridad pertinente, el manejo exclusivo de la información, para la manipulación de esta.

El desarrollo de la parte del software relacionado al sistema tales como algoritmos de reconocimiento de imágenes, código en QT para la interfaz de usuario en pantalla, configuración de redes de comunicación y administración de base de datos; no serán tratadas a detalle en la presente tesis; ya que su desarrollo abarca temas específicos que es necesario sean cubiertos por una siguiente tesis. Sin embargo, se hará mención de algunas de las etapas; ya que la elección de componentes se realizó teniendo en cuenta los lineamientos de requisitos básicos que demandan las configuraciones. Esto tomando en consideración el esquema que se presentará en capítulos posteriores.

CAPÍTULO 1

DESCRIPCIÓN DEL PROBLEMA

El capítulo primero desarrolla la situación actual en la Pontificia Universidad Católica del Perú, e identifica los problemas y posibles causas de éstos.

1.1. Descripción de la problemática materia de estudio

1.1.1. Variables Internas

En este bloque evaluaremos el proceso actual para el ingreso del personal con vehículo a las instalaciones de la PUCP. Asimismo, adjuntaremos los posibles problemas que se tiene en ciertas etapas. [Ver Diagrama 1]

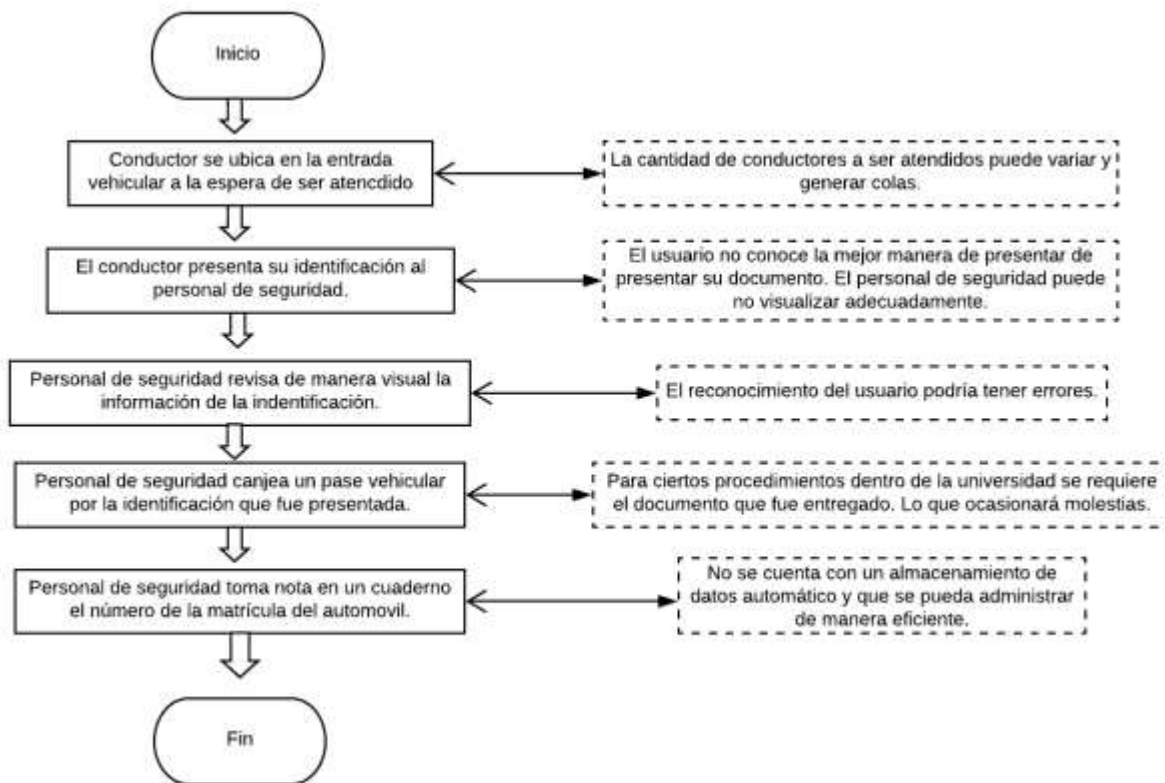


Diagrama 1. Proceso actual de identificación para el acceso vehicular en la PUCP

Fuente: Elaboración Propia

1.2.1. Identificación de la problemática

A continuación, mostraremos una tabla descriptiva referente a los posibles problemas encontrados en el proceso actual de identificación para el ingreso vehicular en la PUCP. [Tabla 1]

Tabla 1.

Problemas y características del proceso de ingreso vehicular

Problemas	Características y causas
La atención de los conductores puede tardar.	Debido a que el método actual es realizado por personal humano, el cual puede tardar si intentara realizar la búsqueda del usuario de manera manual. Lo puede generar tiempos de espera no establecidos.
El reconocimiento del usuario puede tener errores	El cotejo de la información presentada en la identificación, queda bajo el criterio visual del personal de seguridad en la puerta. El error humano es latente en esta etapa; ya se por defectos de visión, cansancio, estrés u otro motivo.
Inconvenientes al entregar documentos en el ingreso.	Una de las formas de mantener el control en el ingreso de personas a la universidad, es la recepción de algún documento de identificación. Esto complica el requerimiento en otros servicios dentro de la universidad. Como puede ser el caso de requerir presentarlo en tesorería, para realizar una gestión administrativa o inclusive para labores dentro de la biblioteca.
No se cuenta con una base de datos virtual.	La recolección de información del ingreso vehicular, no es ni rápida, ni fácil de administrar. Los datos almacenados, solo pueden ser observados in situ. Solo se cuenta con datos limitados acerca del ingreso: Nombre del usuario, código y matrícula.

Nota. Fuente: Elaboración Propia

1.2 Declaración del Marco problemático

En la actualidad, la PUCP cuenta con dos ingresos vehiculares, los cuales son controlados por guardias de seguridad. El método para dar el acceso vehicular usado es simple: Identificación con documento de identidad o carnet universitario y la entrega de un pase vehicular para el usuario por parte de seguridad.

La identificación del usuario, se lleva a cabo de manera visual por el personal de seguridad, el cual está expuesto al error humano, estrés, cansancio u otros factores. Este punto traería, como consecuencia, la infiltración de personas no deseadas en el campus universitario.

Un punto importante para contar con una correcta seguridad, es la recolección de pruebas. Las pruebas permiten identificar las causas. La demostración de la veracidad de un hecho. [9] De no contar con un registro de las pruebas de ingreso vehicular por usuario adecuado, se corre el riesgo de error o fraude respecto a los datos que se obtengan. Almacenar estas pruebas en una base de datos apropiada, mejorará la condición actual del registro de pruebas en el momento del ingreso de un usuario a la PUCP. [12]

Otro aspecto problema acerca del sistema de seguridad de ingreso vehicular, es que se requiere la entrega del documento que se presenta para el ingreso. Esto a manera de garantía ante algún problema relacionado con el usuario al que se dio acceso. Esta acción, puede ocasionar molestias para los usuarios, ya que en ocasiones requieren estos documentos para realizar trámites dentro de la universidad.

Finalmente, el tiempo promedio que demanda la atención actual para cada usuario que intente ingresar con automóvil al campus universitario es de aproximadamente siete segundos, lo cual, en horas de afluencia vehicular, puede ocasionar congestión en el ingreso de la universidad. Con lo cual se generarán molestias, retrasos en las actividades de los usuarios y congestión en las avenidas principales que colindan con la universidad.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Estado del Arte

2.1.1 Presentación del asunto de estudio

La Pontificia Universidad Católica del Perú, cuenta con un área de 413,902 m², en la cual alberga once facultades, esto sin mencionar las áreas comunes, edificios administrativos y espacios recreativos, en los cuales la afluencia de personas es constante en todo el horario de labor de la universidad. Esta afluencia de población estudiantil y no estudiantil, implica un control estricto para el ingreso de las personas al recinto universitario.

La universidad cuenta con dos ingresos principales de acceso vehicular. Estos ingresos son controlados por guardias de seguridad que se encargan de dar el acceso vehicular a los estudiantes, profesores o personal administrativo cuando estos se identifiquen con el carnet o pase relacionado. Sin embargo, la filtración de alguna persona extraña con un carnet falsificado, no identificado, o con un carnet que no sea de su propiedad, quedará bajo el criterio de dicho personal de seguridad, el cual podría cometer errores.

Un camino eficiente, y que es aplicado en los mejores recintos alrededor del mundo, es el uso de tecnologías de reconocimiento para la identificación de personas. Entre ellas se encontramos tecnologías como la detección biométrica, el uso de tarjetas o tags de radiofrecuencia o RFID por sus siglas en inglés (Radiofrequency Identification), reconocimiento de firmas, el reconocimiento óptico de código de barras para carnets, entre otros.

Partiendo del concepto de seguridad como el "crear las condiciones de paz y tranquilidad, para que las personas puedan desarrollar sus actividades sin sobresaltos y seguros de que su familia y sus bienes no corran riesgo frente a las acciones delictivas", se trabajará un sistema que permita garantizar esta. [2] Se buscará adecuar dichas tecnologías para cumplir el beneficio requerido.

Para que un plan de seguridad sea adecuado, deberá ser coherente con los objetivos generales consignados en el plan estratégico de la empresa, que es el que articula toda la actividad y evolución de la entidad, y tomar las siguientes pautas:

- Viabilidad: ha de ser factible y realista; su consecución debe ser algo posible.
- Claro y delimitado: Tiene que ser patente y debe tener claro que es lo que se pretende, así como totalmente coherente con su política.
- Medible: Debe estar formulado de manera que sea posible medir el grado en el que han sido alcanzados.
- Temporalizado: Ha de establecerse un periodo de tiempo para su consecución
- Flexible: Para adaptarse a las contingencias que se vayan presentando
- Motivador: Para que los involucrados, encargados de su ejecución, se sientan implicados en el logro.

De esta forma, en el trabajo de implementación que se planteará, se busca guardar estas pautas anteriores para un correcto desempeño de una nueva estrategia de seguridad.

2.1.2 Estado de la investigación

2.1.2.1 Sistemas para el acceso vehicular comerciales

El diseño e implementación de los accesos vehiculares, en la actualidad, parten de la necesidad de tener control de los vehículos que circulan por un espacio público o privado. De esta forma aseguran el paso de vehículos permitidos, y restringen el de aquellos que no están autorizados. Estos sistemas son implementados para viviendas, hoteles, condominios, industrias, bancos, ministerios, entidades públicas y empresas. Para este servicio, existen diversas tecnologías integradas con mecanismos electromecánicos para habilitar el ingreso, toma de imágenes, sistemas de identificación electrónicos y bases de datos de los usuarios. Siendo las más actuales, los sistemas integrados que ofrecen servicios electrónicos automatizados.

Accesos vehiculares con tecnologías UHF

Este tipo de identificación variará en torno a cómo se realice esta identificación, dado que el usuario puede identificarse mediante una tarjeta electromagnética o el automóvil mismo puede ser identificado por el sistema mediante la colocación de pegatinas especiales con transmisión electromagnética. En ambos casos, se cuenta con una comunicación de información entre un circuito electromagnético y un transductor ubicado en el ingreso. Una vez identificado el usuario el acceso se activará dando pase al automóvil.

El uso de tarjetas o tags, es ampliamente usado en muchos ingresos vehiculares, por su simplicidad. El usuario deberá acercarse al transductor instalado en el ingreso, bajar la ventana, presentar la tarjeta o tag y se realiza el acceso.

Las pegatinas electromagnéticas, son adhesivos con identificación electromagnética que son pegados en el parabrisas. Estos pueden ser reconocidos hasta 5 metros de distancia del transductor ubicado en el ingreso. Con esta forma de identificación, se obtiene diversos beneficios:

- El usuario no requiere bajar la ventanilla en condiciones adversas en el clima. Sea lluvia, bajas temperaturas u otra condición que identifique al usuario.
- El usuario no requiere detener el vehículo completamente para realizarse la detección. Esto beneficia al contribuir con la fluidez del tránsito vehicular.
- Las tarjetas de proximidad pueden extraviarse, mientras que las pegatinas son de un solo uso, y están adheridas al vehículo.
- La complicación común de las tarjetas es que requiere tenerlas al alcance al momento del ingreso. Para esto deberá buscarla en su cartera con posibilidad de no encontrarla en el momento, caer debajo del asiento o presentarse otro problema; con las pegatinas, no.
- En caso de que exista un flujo constante vehicular, podría disminuir el tiempo de ingreso de los vehículos gracias a los beneficios anteriores.

Adicionalmente, existe un método que combina el uso de estas pegatinas de identificación en los autos, con el uso de tarjetas o tags electromagnéticos para elevar el

grado de seguridad del ingreso de los usuarios. Para el caso, se realiza una doble identificación mediante el recurso presentado por la pegatina del auto y la información extraída de la tarjeta tipo RFID en un transductor al ingreso. [21][22] En la figura 1 se puede apreciar un esquema de funcionamiento para la identificación de estas pegatinas electromagnéticas con un transductor ubicado en el ingreso



Figura 1. Identificación de la pegatina o sticker electromagnético por el transductor

Fuente: Empresa Biotrack

Tecnologías como la mencionada anteriormente se vienen ofreciendo y desarrollando como soluciones para aparcamientos, tal es el caso de la empresa QUATUM Systems que lanzó al mercado un potente sensor de proximidad vehicular llamado MOD.MAXIPROX5375 (Ver Figura 2), este consigue detectar el vehículo hasta 7 metros de distancia



Figura 2. Sensor MOD.MAXIPROX5375 de Quantum Systems

Fuente: <http://www.quantumsystems.com.mx/>

Accesos vehiculares con tecnologías biométricas

Este tipo de identificación se realiza mediante una lectura huella dactilar por un sensor instalado en un pedestal cercano al ingreso vehicular. El usuario deberá acercar su dedo al sensor (usualmente el dedo índice), el cual reconocerá el patrón y enviará la información recabada en bits al sistema para cotejar los datos. Estos sistemas manejan un nivel de seguridad muy eficaz.

Asimismo, vienen integrados con teclados matriciales o lectoras de tarjetas de proximidad, estos pueden ser programados para obtener otro tipo de seguridad del ingreso (Ver Figura 2).



Figura 3. Pedestal y detector de huellas digital

Fuente: Empres Doltech

Estos sistemas de identificación se interconectan con una base de datos. Así se cotejarán los datos extraídos para verificar el ingreso de los usuarios. De esta forma, al ser el acceso positivo, un sistema electromecánico ubicado en el ingreso dará el acceso.

Entre los sistemas electromecánicos comerciales que habilitan el acceso, encontraremos a las tranqueras o barreras, bolardos o pilones y puertas corredizas o de apertura. Todos estos sistemas, son ofrecidos y son integrados con los métodos de acceso vehicular comerciales.

De igual forma, se cuenta con cámaras de vigilancia de grabación continua para contar con las imágenes de los hechos suscitados ante cada ingreso. [6]

Accesos vehiculares con tecnologías ópticas

Este tipo de identificación está basado en la identificación de patrones en documentos de identificación. Por medio de un láser consigue realizar un escaneo de un patrón de líneas o cuadros. Va orientado al reconocimiento de manera más rápida de patrones ordenados como los de los códigos de barra o código QR.

Un ejemplo de uso de este tipo de tecnología es el que se usa actualmente para el ingreso vehicular en la Universidad de Lima. Para el reconocimiento del usuario emplea la tarjeta universitaria de sus estudiantes y personal, el cual lleva un código de barras registrado. Este es enlazado con los datos vehiculares que el usuario declara con anterioridad. [24] (Universidad de Lima, 2012)

“... () Procedimiento para el uso del estacionamiento

1. Verificar que el semáforo esté de color verde.
2. Acercar su tarjeta de aproximación a la lectora óptica.
3. Esperar que la tranquera se levante.
4. Ingresar a una velocidad moderada (máximo 20 km/h). ...()”

2.1.2.2 Tecnologías de identificación para accesos vehiculares

Mediante un Sistema de Control de Acceso Vehicular podemos llevar y obtener un pormenorizado registro de Ingresos y Salidas (con fecha y hora) de cada unidad que ingresa a un edificio, Ministerio, Estacionamiento público o privado, etc.

Si bien los Sistemas de Tranqueras o Barreras Vehiculares en estacionamientos existen hace mucho tiempo la tecnología se ha hecho más flexible, eficiente y económica para implementar con nuevos elementos anteriormente no disponibles, tales como los Lectores de Tarjetas de Proximidad de Largo Alcance – entre 1 y 100 metros, según el

estándar elegido – con los cuales el chofer no necesite sacar la mano por la ventanilla del vehículo para que la tarjeta pueda ser leída; como tampoco que el auto reduzca la velocidad hasta detenerse. Ya que ciertos sistemas son capaces de identificar los vehículos incluso con el auto en movimiento. Lo cual significa un impacto positivo para el tránsito afluente en el ingreso a la institución, así como para la seguridad del usuario y del recinto

Por lo demás, la tecnología IP permite ahora administrar el Sistema de Control de Acceso Vehicular incluso de manera remota y ya no únicamente desde la Garita de Control sino a través de la red LAN o desde el INTERNET. A continuación, un ejemplo de un ingreso vehicular usando tecnologías actuales [Ver Figura 4].



Figura 4. Ingreso vehicular aplicando tecnología RFID implantada en el automóvil

Fuente: IPSOLUTIONS company

En el punto anterior, se mostró las tecnologías más usadas en los ingresos vehiculares para la identificación del usuario, ahora se explicará cómo funcionan estas tecnologías usadas para la identificación.

Identificación Biométrica

En las tecnologías de la información (TI), la autenticación biométrica es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para su autenticación, es decir, “verificar” su identidad.

Las huellas dactilares, la retina, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas). La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento.

Asociada a otras tecnologías de restricción de accesos, la biometría garantiza uno de los niveles de autenticación menos franqueables en la actualidad. Además, los inconvenientes de tener que recordar una contraseña o un número de PIN de acceso serán pronto superados gracias al uso de los métodos biométricos, debido a que estos últimos presentan notables ventajas: están relacionados de forma directa con el usuario, son exactos y permiten hacer un rastreo de auditorías.

La utilización de un dispositivo biométrico permite que los costos de administración sean más pequeños, ya que sólo se debe realizar el mantenimiento del lector, y que una persona se encargue de mantener la base de datos actualizada. Otro beneficio: las características biométricas de una persona son intransferibles a otra. [20]

Identificación mediante código de barras

El código de barras, es un código basado en la representación de un conjunto de líneas paralelas de distinto grosor y espaciado que en su conjunto contienen una determinada información, es decir, las barras y espacios del código representan pequeñas cadenas de caracteres. De este modo, el código de barras permite reconocer rápidamente un artículo de forma única, global y no ambigua en un punto de la cadena logística y así poder realizar inventario o consultar sus características asociadas. Actualmente, el código de barras está implantado masivamente de forma global. [20]

Identificación mediante RFID o Radiofrecuencia

RFID (siglas de *Radio Frequency IDentification*, en español identificación por radiofrecuencia) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados tags RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (*automatic identification*, o identificación automática).

Las etiquetas RFID (RFID Tag, en inglés) son unos dispositivos pequeños, similares a una pegatina, que pueden ser adheridas o incorporadas a un producto, un animal o una persona. Contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren. Una de las ventajas del uso de radiofrecuencia es que no se requiere visión directa entre emisor y receptor; asimismo, la falsificación de estos, es de mucha dificultad. [5]

2.1.2.3 Diferencias técnicas para tecnologías de identificación

En el apartado anterior, se mencionó las características y avances de tres de las más comunes tecnologías de identificación automática que poseen los sistemas de acceso en la actualidad. Entre sus características técnicas podemos encontrar el cambio de información que tienen internamente, el precio por cada dispositivo de identificación o la seguridad que brindan de la autenticidad del usuario. Asimismo, existen otros métodos, que no fueron mencionados anteriormente, pero que se describirán sus características técnicas a continuación, a fin de demarcar las principales diferencias con las más comunes. Se muestra una tabla comparativa en la siguiente imagen de las diferencias técnicas. [Ver Tabla 2]

Tabla 2

Tabla comparativa de distintas tecnologías de identificación

	Código de Barras	Banda Magnética	Memoria de Contacto	Sistemas Biométricos	RFID Pasivo	RFID activo
Modificación de la información	No Modificable	Modificable	Modificable	No Modificable	Modificable	Modificable
Seguridad de los Datos	Mínima	Media	Alta	Alta	Variable (baja a alta)	Alta
Capacidad de Almacenamiento de datos	-Lineales(8-30 caracteres) - 2D hasta 7.200 caracteres	Hasta 128 bytes	Hasta 8MB	No aplica	Hasta 64 KB	Hasta 8MB
Precio	Bajo	Medio-Bajo	Alto (cerca de US\$1 por memoria)	Alto	Medio (menos de US\$0.50 por tag)	Muy Alto (US\$10 a US\$100 por tag)
Estándares	Estables	Estables	Propietarios, no estándar	No estándar	Evolucionando hacia estándar	Propietario y en evolución hacia estándar
Ciclo de Vida	Corto	Mediano	Largo	Indefinido	Indefinido	Depende de la batería (3 a 5 años)
Distancia de Lectura	Línea de vista y (hasta 1.5m)	Requiere contacto	Requiere contacto	Depende del biométrico	No requiere línea de vista ni contacto Hasta 10m.	No requiere línea de vista ni contacto Hasta 100 m. y mayores
Interferencia Potencial	Cualquier modificación en las barras y objetos entre el código y el lector	Bloqueo del contacto	Bloqueo del contacto	Puede ser bloqueo del contacto, o bloqueo de línea de vista e inclusive el ruido.	Ambientes o campos que afecten la transmisión de radio frecuencia	La interferencia es muy limitada, debido a la potencia de transmisión.

Nota. Fuente. Tesis de Luis Gomero Vásquez. [23] [Luis Gomero Vásquez (2016). Diseño de un sistema de acceso vehicular a la PUCP basado en tecnología RFID y procesamiento de placas vehiculares (tesis de pregrado). Pontificia Universidad Católica del Perú, Lima, Perú]

2.1.2.4 Requerimientos para la implementación de un acceso vehicular

Los aspectos para la implementación de un sistema integral de entrada vehicular, basándonos en la tecnología actual, abarcará cuatro puntos fundamentales. Estos son (i) la tecnología que se usará para la identificación de los usuarios con ingreso vehicular,

(ii) el empleo de algoritmos para el procesamiento de imagen relacionado con la identificación de las matrículas de los automóviles, (iii) la gestión de la base de datos para almacenar la información proveniente del módulo físico de identificación; (iv) la comunicación entre el módulo de identificación de usuarios y la base de datos;(v) los actuadores, que serán la salida de nuestra planta y actúan en respuesta a la información que se recibió en la entrada; y el (vi) control del sistema integrado. Así como la aplicación del internet de las cosas. Con lo cual, valiéndose de máquinas virtuales, se podrán controlar y manejar la información vía web.

(i)Módulo de identificación vehicular usando Radio Frecuencia

En este tipo de identificación, para el acceso vehicular, trabaja mediante radiofrecuencia (RF). Se brinda a cada usuario un “tag” (Tarjeta electromagnética), la cual lo identificará como un usuario. Este elemento se acercará a una antena RFID ubicada en un módulo. Esta antena enviará pulsos electromagnéticos hacia el tag; el cual responderá si su frecuencia de trabajo es igual a la de la antena. Es así que, luego de un breve momento, el tag brindará un valor al módulo de identificación ubicado. Este valor será analizado por una computadora, la cual certificará si el usuario está autorizado. [5][6] A continuación se presenta el diagrama de bloques para el acceso. [Ver Figura 5]

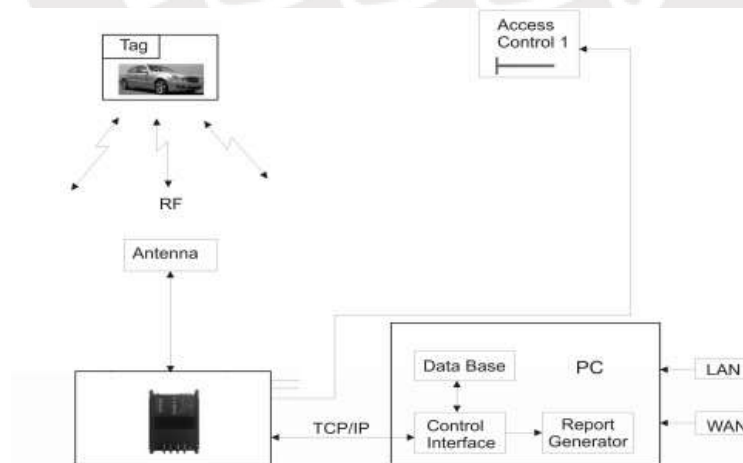


Figura 5. Diagrama de bloques del control de acceso vehicular mediante RFID

Fuente: DESIGN AND IMPLEMENTATION OF A VEHICULAR ACCESS CONTROL USING RFID (D. L. Almanza-Ojeda, 2016)

(ii)Procesamiento de Imágenes para la identificación de las matrículas de los automóviles

Para poder crear una relación entre el usuario y el automóvil con el que intenta acceder, se requiere de un reconocimiento e identificación del vehículo. Esto se consigue gracias al procesamiento de imagen que se ejecuta a la matrícula.

Se definen seis pasos principales para el procesamiento de imagen. El primero es la adquisición, en el cual la imagen es capturada por una cámara instalada en la ubicación adecuada; el segundo, es el preprocesamiento, en el cual se corrigen los errores y defectos que pueda tener la primera imagen obtenida, se le da una limpieza de imagen; como tercer paso, se define la segmentación, en la cual se divide la imagen, para separar de ella los atributos que son necesarios para obtener el número de placa; el cuarto paso, es la extracción de los atributos, se obtiene los atributos del patrón establecido. Finalmente, se obtiene un valor de acuerdo a los atributos extraídos, y se almacena en un banco de datos. Se pueden visualizar las etapas definidas. [Ver figura 6]

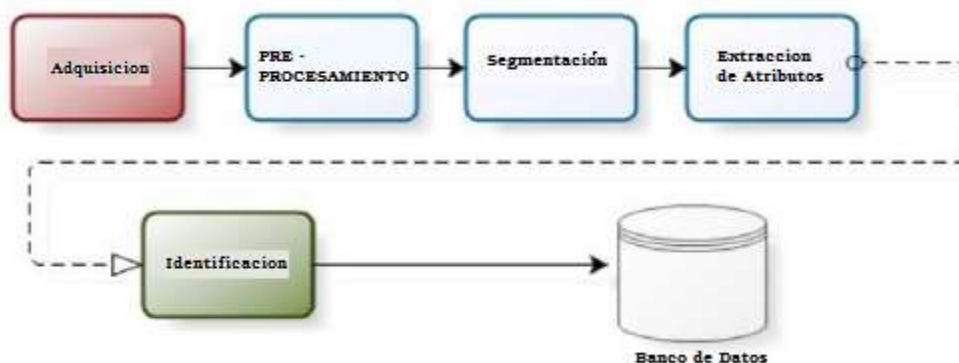


Figura 6. Etapas de un sistema de procesamiento de imágenes típico

Fuente: Development of Control Parking Access Using Techniques Digital Image Processing And Applied (E. Cavalcanti, 2015)

Para la extracción de los atributos son utilizadas técnicas de inteligencia computacional aplicada, esto para identificar los caracteres de las placas.

Como ejemplos, en la detección de los bordes de los objetos de las imágenes, se suele utilizar convoluciones bidimensionales en la imagen, utilizando mascarar específicas.

Para el filtraje de ruido en las imágenes, la utilización de un filtro Canny es requerido. Este consta de un algoritmo de suavización para así minimizar la probabilidad de error en la detección. [7].

En síntesis, el empleo de esta tecnología estará constituido por:

1. Cámara web para la adquisición de imágenes.
2. Iluminación artificial en caso de requerirse para la mejor captura de imágenes.
3. Equipo de procesamiento de imágenes.
4. Algoritmo en el cual se ingrese una imagen y se obtenga a la salida un valor.

(iii) Bases de Datos

La forma más eficaz de almacenar tamaños grandes de información es almacenarlo en servidores dedicados. La primera opción son los servidores físicos, para los cuales se cuenta con módulos computacionales en los que se almacenará esta información. Sin embargo, su mantenimiento, instalación, el lugar que tienen que ocupar, así como el costo del mismo módulo, que debe ser una computadora de gran capacidad y velocidad, significa un costo alto para los usuarios.

Como segunda opción, se tiene a los “Servidores en la Nube”, los cuales abarcan una variedad de opciones y funciones a pedido. La función de un servidor en la nube, es similar a la de un servidor físico en su función principal de almacenaje y administración de información. No obstante, un servidor en la nube, puede llegar a ser más económico, además de ser elegido de acuerdo a las necesidades específicas de información del usuario. En la actualidad, existen distintos proveedores, siendo los más populares Microsoft Azure, Google Cloud y Amazon Web Services.

La elección de un servidor en la nube, será evaluada como la adquisición de una máquina virtual; en la cual un proveedor entrega un espacio de su servidor a un cliente o usuario. Brindándole una serie de especificación en torno a espacio de almacenamiento, memoria RAM, y los servicios del CPU para realizar las tareas de administración de datos. Gracias a estas variables, se obtendrá la capacidad de almacenamiento, y la velocidad de

comunicación de los datos. [9]. Se presenta un esquema de un servidor en la nube. [Ver Figura 7]

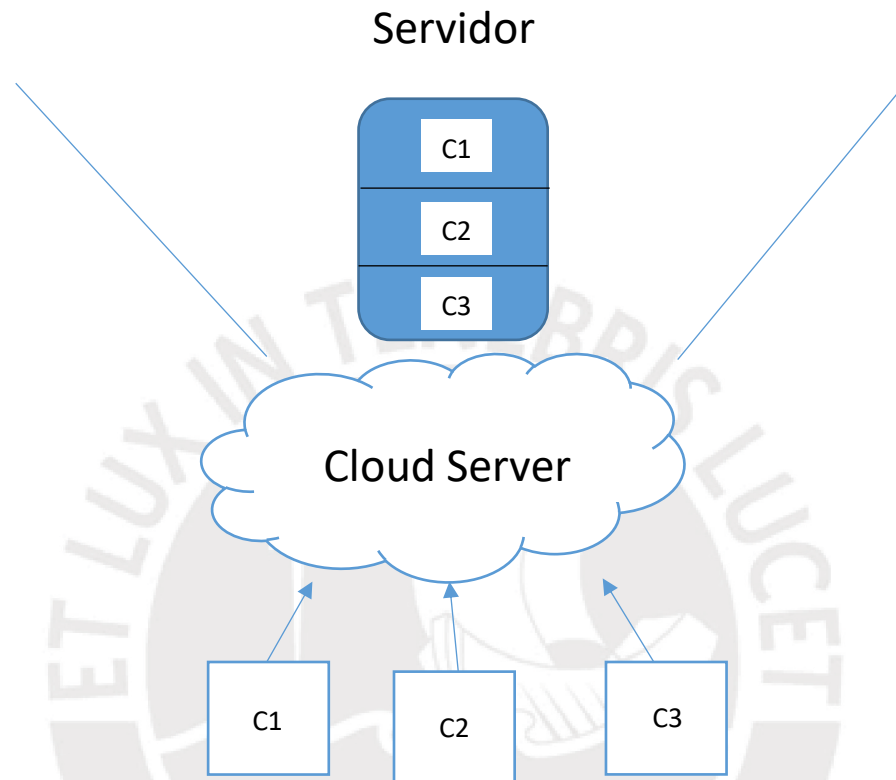


Figura 7. Esquema del Servidor en la Nube

Fuente: Elaboración propia

La Gestión de estos servidores, debe ser llevada a cabo por los denominados Gestores de Base de Datos, o SGBD (siglas en ingles). Estos gestores se encargarán del almacenamiento y administración de la información en los servidores.

Entre ellos encontraremos una variedad de software relacionado que nos permitirán tener una interfaz de usuario para la programación y administración de la información. Entre los más populares, se encuentran el Microsoft SQL Server y el Database Oracle. Esta administración, tendrá en consideración, también, la seguridad de la información con la que trabaje. [10]

Los servidores, en la actualidad, cuentan con una infraestructura que abarca el sistema operativo, el servidor web, el gestor de base de datos y el lenguaje de programación.

(iv)Comunicación

Para el acceso a la red, se requiere que un módulo sea identificable ante los elementos de interconexión a la red, tales como un Switch, elemento que administra, protege contra la intrusión y enlaza con los Router los diversos dispositivos conectados a una red local. La identificación, se da gracias a la IP, la cual es la dirección con la cual se encuentra cualquier elemento dentro de una red. [11]

Un Router, es un elemento que trabaja en la capa 3 de la capa OSI, nivel de red. Realiza su funcionamiento encaminando paquetes de datos a través de la red formada con otras subredes, o de manera directa hacia el destinatario final, la figura 8 permite visualizar como se da esta comunicación entre máquinas de usuarios [Ver figura 8]. Para el enrutamiento, se vale de etiquetas que le permiten identificar paquetes de datos para que puedan llegar a su destino, y ser reconocidas por los elementos de llegada (posiblemente otro Router). Asimismo, requiere de una configuración específica para el enrutamiento, estas pueden ser:

- Enrutamiento estático: Es de tipo predeterminado y específico, es establecido por el administrador.
- Enrutamiento dinámico: los encaminadores podrán elegir el camino para transmitir los paquetes valiéndose de un protocolo, previamente, configurado por el administrador. Por ejemplo, camino más corto, rutas publicadas por pares, u otra.
- RIP: Se vale de la comunicación entre routers vecinos para obtener información de mejores rutas para enviar paquetes. Para esto se vale de una métrica de saltos para el envío de información. [15]

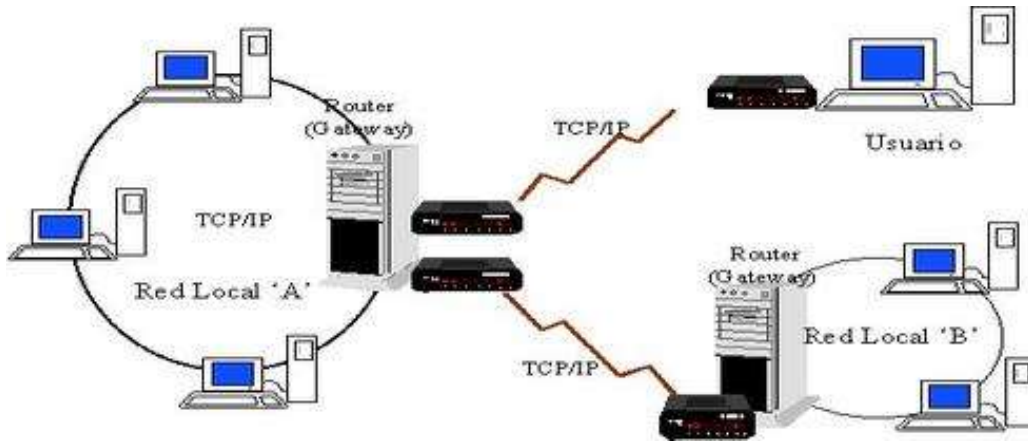
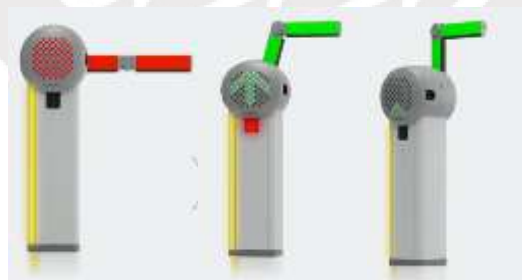


Figura 8. Esquema de interconexión entre routers.
Fuente: <https://redes-informatic-2.wikispaces.com>

(v) Actuadores de Potencia

En este punto se establece la etapa de potencia de un sistema de entrada vehicular. Siendo los más utilizados el uso de barreras vehiculares que van desde el control manual hasta activación mediante sensores administrados por el jefe de seguridad o automáticos. Un ejemplo es la barra periférica utilizada por la empresa SKIDATA para su sistema de ingreso, su activación puede ser de forma automática o manual por medio de un botón instalado. Cuenta con un brazo que puede llegar a elevarse hasta 4.5m, asimismo cuenta con iluminación desde su interior y brinda orientación a los usuarios mediante la muestra de diversos símbolos. [Ver figura 9]



A) B) C)

Figura 9. Módulo de acceso vehicular a) En espera para una entrada de usuario. b) Abertura de la barrera e indicadores de esperar a que finalice el proceso. c) Finalización de la apertura y autorización de ingreso.

Fuente: <http://www.intellisoftparking.com/>

(vi)Control

El control de accesos vehiculares, debe ser llevado a cabo por un controlador inteligente, automatizado y programable. Que permita definir los parámetros para cumplir los requisitos del ingreso. Entre estos, encontraremos dos empresas de ordenadores populares, que brindan los requerimientos básicos para un correcto control electrónico: eficiente, de fácil uso y con características mínimas de desempeño.

Raspberry Pi

Entre sus productos, encontramos Raspberry Pi 3B en sus diferentes versiones. Se trata de un ordenador de placa reducida con un procesador central quad-core ARMv8 con capacidad de hasta 1.4GHz. Un procesador gráfico (GPU) VideoCore IV, y 1GB de memoria RAM. No cuenta con un disco duro, pues trabaja con tarjeta SD para el almacenamiento de la información. Asimismo, tampoco incluye fuente de alimentación propia, por lo que su carga se realiza mediante una fuente externa. En la actualidad el Raspberry Pi 4 es el modelo de última generación con 1.5GHz de procesamiento y siendo seguido en procesamiento por sus versiones Raspberry Pi 3A y 3B con 1.4GHz; y Raspberry Pi 3 con 1.2GHz. Asimismo, referente a la tarjeta gráfica, existe un cambio de Broadcom VideoCore IV hacia VideoCore V en la última versión Pi 4.

De igual manera, el Raspberry, cuenta con la capacidad de conexión Ethernet configurable, y de 10-100 Mbps. Siendo capaz de realizar conexiones inalámbricas sin la necesidad de adaptador alguno dada la incorporación de un módulo de bluetooth en el equipo.

La mayor parte de la programación y configuración que se realiza en este computador de placa reducida se lleva a cabo en el ambiente Python.

Estos beneficios y simplezas, hacen que el Raspberry Pi pueda ser ideal para establecer comunicación red y brindar una interfaz gráfica para ser atendido. [18]

Arduino

Por otro lado, encontramos a la familia Arduino con una variedad de elementos, tales como el Arduino Mega, Leonardo y el Uno/ Genuino Uno. Siendo este último uno de los más comerciales por su tamaño pequeño y simpleza en la programación de sus terminales. Consta de una placa electrónica basada en el ATmega328P. Cuenta con 14 pines digitales de entrada / salida (de los cuales 6 se podrán utilizar como salidas PWM), 6 entradas analógicas, un cristal de cuarzo de 16 MHz, una conexión USB, un conector de alimentación, una cabecera ICSP y un botón de reinicio. Contiene todo lo necesario para apoyar el microcontrolador; basta con conectarlo a un ordenador con un cable USB o la corriente con un adaptador de CA a CC o una batería para empezar.

La plataforma de Arduino, permite una adaptación de módulos de circuitos integrados para la obtención de otras capacidades que no están incluidas en un producto inicial. Tales como módulos bluetooth, interfaces gráficas, módulos Ethernet, etc. [19]. El tipo de programación de este computador embebido se lleva a cabo en la plataforma Arduino IDE, la cual se programa en un lenguaje tipo C, y es apoyado por librerías en el mismo lenguaje para realizar otro tipo de configuraciones predeterminadas. Plataformas como GitHub, se encargan de mantener actualizadas las librerías de Arduino, así como brindar códigos libres.

2.1.4 Síntesis sobre el asunto de estudio

Existen diversos tipos de identificación para ingresos vehiculares, entre los más resaltantes la identificación biométrica (la cual incluye reconocimiento de retina, huellas dactilares, o reconocimiento de firmas), resaltante por su alto nivel de seguridad, pero complejo en la detección; lectores de tarjetas mediante código de barras, una manera simple de identificación, pero que no garantiza la protección a falsificación; y RFID, la cual resulta una forma sencilla de identificación, pues no es requerido que el usuario se encuentre a poca distancia del sensor para la detección. Asimismo, es un método de identificación de difícil suplantación.

Para el diseño e implementación de la identificación vehicular, en la actualidad, se toman en cuenta diversos mecanismos de automatización. Entre estos se encuentran: el módulo de identificación, una base de datos para reservar la información, la comunicación entre estos anteriores, procesamientos de imagen de fotogramas tomados al usuario o a su vehículo, el control del sistema integrado; e inclusive, la capacidad de configurar los elementos de hardware por separado para transmitir hacia una central de procesamiento de datos en Internet.



CAPITULO 3

IMPLEMENTACION DEL SISTEMA

3.1. Objetivos

3.1.1. Objetivo General

Implementación y rediseño de hardware del sistema de acceso vehicular a la PUCP usando las tecnologías RFID y detección de placas vehiculares.

3.1.2. Objetivos Específicos

1. Rediseño e implementación del hardware para el sistema de entrada vehicular.
2. Comprobar mejora de tiempo con respecto al sistema actual de ingreso vehicular.
3. Posibilitar el almacenamiento de la data de ingreso en la nube.
4. Comprobar mejora de costos con el diseño original del hardware.

3.2 Alcances de la Tesis

La seguridad dentro del campus universitario de la PUCP, en particular, la seguridad frente a la delincuencia, responde a una serie de factores y eventos que se suscitan cotidianamente. Algunos de estos, pueden ocurrir por el descuido de las víctimas. Sin embargo, existen otros, que pueden evitarse con la prevención e implementación de métodos eficaces que disminuyan la probabilidad de ocurrencia de estos hechos, un sistema de ingreso vehicular integrado en la PUCP, permitiría esta disminución. Esto, implementando, tanto identificación, como una correcta administración de la información recabada del ingreso.

La extracción de la información al ingreso vehicular, debe contener la mayor cantidad de datos presentes en este instante. Para el caso serían: La placa del auto, la identificación del usuario, la imagen del usuario y la hora exacta del ingreso.

Para verificar que el ingreso está aprobado, debe contar con una base de datos estática que envíe estos permisos, esta deberá ser administrada previamente al ingreso.

Asimismo, debe permitir almacenar la información nueva extraída al momento del ingreso del vehículo: Base de datos dinámica.

El módulo de identificación y toma de imágenes, será elaborado y mejorado gracias a medios electrónicos, como la construcción de tarjetas electrónicas e instalación de cámaras que permitan la correcta toma de datos de imagen y de las tarjetas RFID con las que se presenten los usuarios. Asimismo, el módulo incluirá una tranquera que restringirá el acceso, así como de una interfaz gráfica para la interacción con la persona que desee acceder. En la figura 11, se puede apreciar un diagrama de bloques referente a todo el sistema.

Por otro lado, se requiere que el manejo de información se realice en la nube, esto para facilitar la administración de los recursos de manera más eficiente, simplificando el proceso que reciben estos datos a 3 pasos resumidos. [Ver Figura 10]

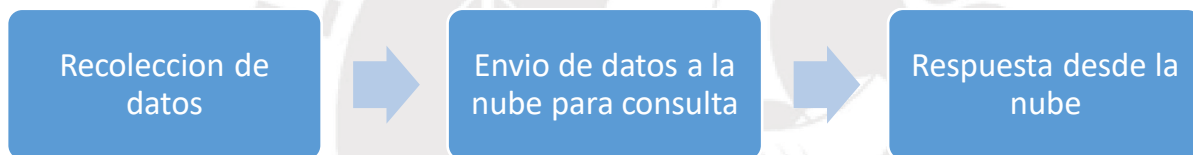


Figura 10. Proceso que reciben los datos extraídos en el ingreso.

Un concepto empleado en la presente tesis es la de “el Internet de las cosas”. Los módulos contarán con transmisión de datos hacia internet y comunicación con una base de datos en la nube. Esto se consigue con módulos adicionales. Placa adicional Ethernet en el caso del Arduino Mega y sus periféricos relacionados; y en el caso del Raspberry y sus periféricos relacionados, el módulo ethernet integrado que posee. Mencionar que también cuenta con un módulo wifi incorporado, el cual podría también emplearse. El presente trabajo desarrolla el hardware del sistema mencionado.

3.3 Comparativo con el diseño inicial

A continuación, se mostrará el diagrama de bloques referido al funcionamiento del sistema integral de ingreso vehicular que se implementará en la entrada de la Pontificia

Universidad Católica del Perú [Ver Figura 11]. El usuario es considerado como la fuente, y el inicio su registro en la garita o planta.

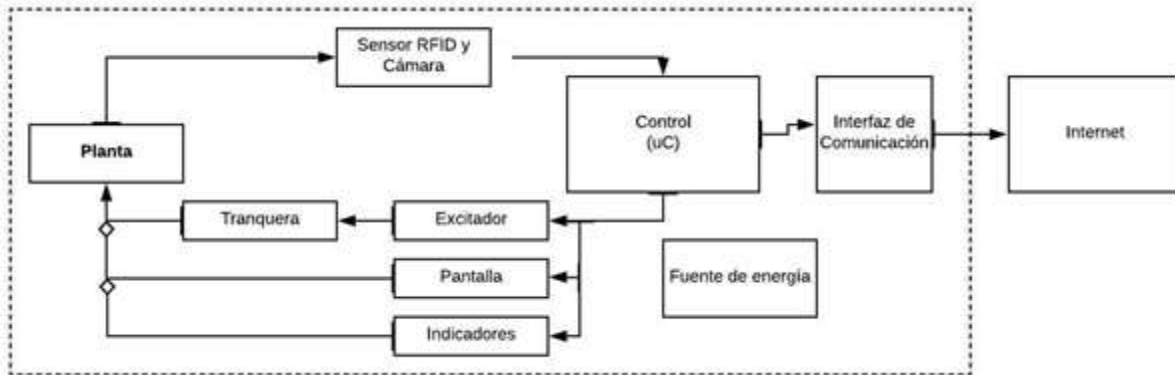


Figura 11. Diagrama de bloques para el proyecto de implementación
Fuente Propia

En comparativa, se presenta el diagrama de bloques para el diseño que fue inicialmente planteado [Ver figura 12].

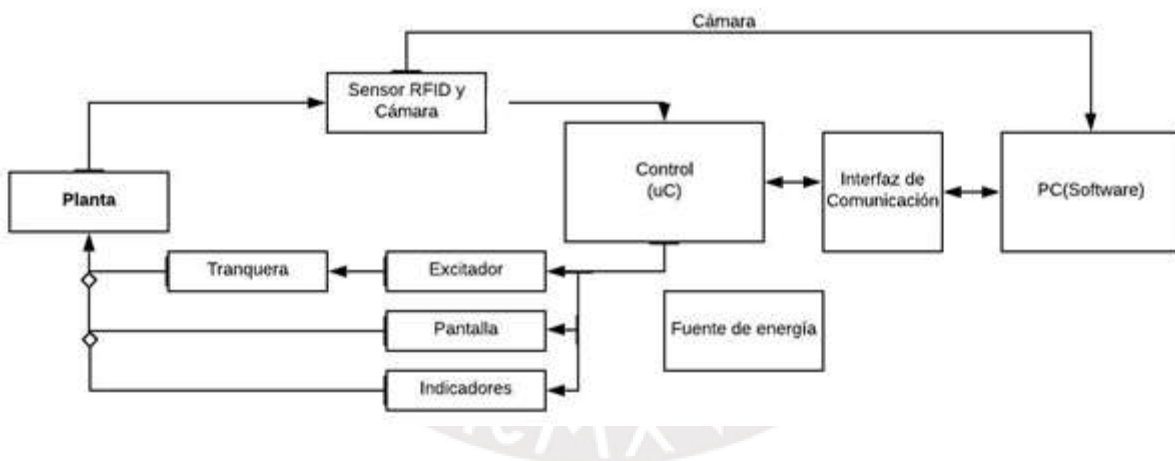


Figura 12. Diagrama del proyecto inicial
Fuente: Tesis de Luis Gomero Vásquez

La etapa de tranquera es la misma etapa de potencia establecida en el proyecto inicial. Asimismo, se establece como planta el sistema físico que se ubica en el ingreso de la universidad

Sin embargo, la información de los sensores y cámara ahora pasarán ambas a un computador de placa reducida, que enviará la información hacia Internet. (imagen procesada de número de placa y código RFID). De esta forma obtendrá una respuesta

positiva o negativa desde este respecto al usuario. Según este resultado, el computador brindará la respuesta en excitador, indicador y pantalla.

3.4 Explicación de cambios

La presente implementación provee el desarrollo relacionado con el nuevo entorno de comunicación que obtiene la etapa de control: comunicación con Internet, siendo esta su característica más resaltante, por lo cual se procedió a realizar los cambios tanto en software como en hardware. De esta forma, obtuvimos una interacción con una base de datos instalada en internet, brindar rapidez en la comunicación y seguridad para los datos. En el presente trabajo se explicará la etapa de hardware implementado.

Entre los elementos de cambio, se procedió a incorporar nuevos componentes para la etapa de control, los cuales permitieran una conexión simplificada y centralizada. Es así que se insertó un computador de placa reducida, el elegido fue el Raspberry Pi 3, en el siguiente punto se explicará el porqué de su elección entre la diversidad de productos en el mercado.

Este componente permitió conseguir una salida hacia la nube o Internet, recepción de datos de sensores, una comunicación con los actuadores y la conveniente proyección de los datos para una pantalla de usuario, la cual será instalada en el módulo ubicado en el acceso para uso del guardia encargado. A continuación, se aprecia la distribución del Raspberry Pi 3, procesador de placa reducida usado. [Ver figura 13]

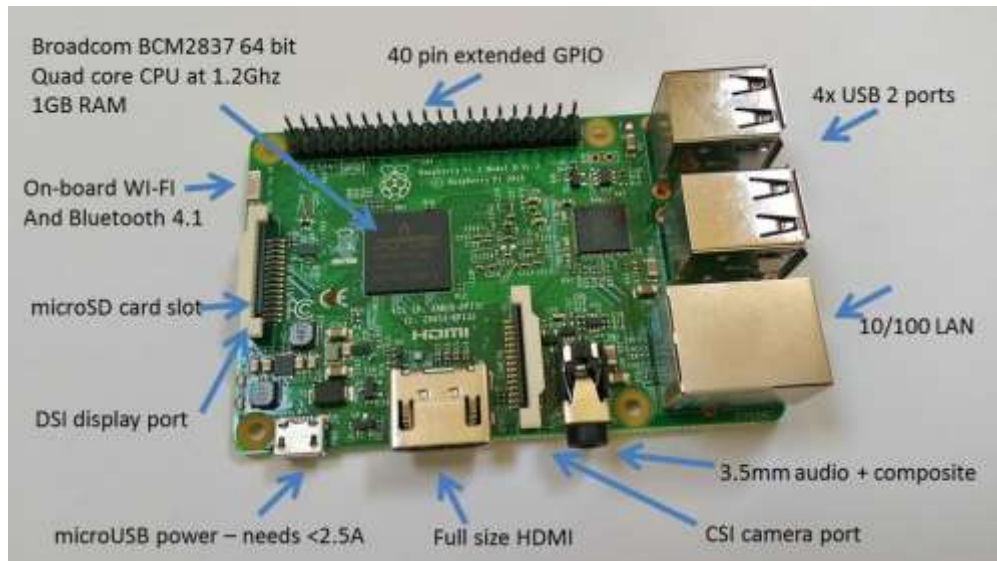


Figura N°13

Fuente. <http://tech.scargill.net/raspberry-pi-3-grand-opening/>

Además, se añadió la separación de alimentaciones para la tranquera y la parte de sensores, control y comunicación. La etapa de potencia contará con su propia fuente de alimentación, y será activada por una señal separada mediante un circuito de aislamiento, como se propuso en el diseño inicial.

Estos cambios, entre otras cosas, permitirán mantener la rapidez necesaria para continuar con el mismo sistema de seguridad para el registro de usuarios; actualizándolo con esta nueva cualidad de registro y cotejo de datos en la Internet. Lo cual evita la necesidad de almacenar datos en módulos o computadoras sensibles a desperfectos, así como la facilidad de actualización de estos datos de forma externa.

3.5 Metodología de elección de componentes

3.5.1 Módulo de Control

Para el trabajo del control, como ya antes se mencionó, se realizó un cambio sustancial: el de usar un computador de placa reducida para controlar la información proveniente de los sensores, y la recepción de información de los indicadores, así como el envío al actuador instalado para el movimiento de la tranquera.

Este cambio, supone una reducción en el espacio ocupado, así como la cantidad de módulos usados, dado que ya no se trabajará con una PC instalada sumado al microcontrolador Arduino.

Asimismo, el costo se reduce de manera considerable, como se verá en la tabla a continuación. Primero veamos el costo de computadores de placa reducida en el mercado. [Tabla N°3]

Tabla N°3
Costos de Computadores de placa reducida

	Raspberry Pi 3	BeagleBone Black	Banana Pi	Odroid	Pine A64
Costo	S/.118.3	S/.152.1	S/.111.54	S/.135.2	S/.101.4

Nota. Tabla extraída de las páginas webs de las marcas mencionadas.
Tipo de cambio dólar a sol a octubre del 2019: 3.38

En la tabla anterior, se tomaron en cuenta diversas marcas de ordenadores de placa reducida. Cada uno capaz de ser programado como controlador, así como hacer labores de procesador para etapas como la del procesamiento de imagen, o el envío de información a la nube. Se puede observar que el precio de estos tiene un costo promedio de 123 soles, a comparación del costo de una portátil para la instalación, más el costo de un computador embebido como el Arduino Uno o edición que se obtenga. Podemos visualizar los costos de una portátil o laptop en el mercado local a continuación [Ver Figura 14].



Figura N° 14. Precios de Portátiles en el mercado local

Fuente. Página Web Importaciones Hiraoka

Además del costo del computador de placa reducida para el proyecto también se incluye una pantalla táctil para el uso del guardia, el costo de este asciende a 60 dólares, o 202.8 soles.



Figura N°15 Pantalla Raspberry Pi

Fuente. <http://www.xataka.com/accesorios/la-raspberry-pi-ya-tiene-pantalla-tactil-oficial-hazte-con-ella-por-60-dolares>

Siendo el costo aproximado de 300 soles en conjunto, a diferencia de un promedio de 2000 soles de una portátil.

Vale la pena mencionar estos detalles; ya que, si bien se ha realizado el cambio para conseguir la comunicación con Internet en este nuevo diseño, el diseño anterior incluye un computador o portátil. La cual tiene la capacidad de realizar una comunicación externa hacia Internet; sin embargo, por motivos de eficiencia en torno al costo, espacio modular

y centralización de las interfaces, se optó por una mejor opción que es el uso de computadores de placa reducida.

De igual manera, se resolvió el problema del almacenamiento de información de la placa vehicular y tarjetas RFID empleando servidores web.

3.5.5.1 Conveniencia del uso del Raspberry Pi

Como requisitos mínimos que tenemos para la elección del computador de placa reducida, será una capacidad de comunicación a internet, un mínimo de 10 pines de salida para controlar periféricos (indicadores, actuadores, etc.) y capacidad para realizar proyección de imágenes en una pantalla, así como recibir indicaciones desde esta.

A continuación, compararemos dos de los computadores de placa reducida populares en la actualidad por su velocidad de procesamiento, así como su trabajo con 64bits; lo cual los acerca mucho al trabajo de una portátil o PC. [Ver Tabla 4]

Tabla 4

Comparativa entre RPi 3B+ y Pine A64

	Raspberry Pi 3 B+	Pine A64 + 2GB
Fabricación	Reino Unido	EE.UU.
Procesador	1.4GHz 64-bit quad-core ARMv8	1.2Ghz Allwinner A64 ARM Cortex A53 Quad-Core 64Bit
Velocidad de Comunicación Ethernet	10/100MB	10/100MB
RAM	1GB LPDDR2	2GB DDR3 SDRAM
Batería	Ninguna	AXP803
Pines de salida	40	84
Puertos USB	4	2
Capacidad de memoria	Micro SD (64GB)	Micro SD (256GB)
Precio	35\$	29\$

Nota. Fuente propia

La placa Raspberry Pi, nos ofrece la posibilidad de trabajar con software open source, con lo cual nos garantiza la simplicidad de trabajar con el que más nos adecuemos, siendo el sistema operativo Raspbian (adaptación del Debian), el idóneo y más usado para el trabajo en esta plataforma. Se trata de una interfaz simple y adecuada para que los usuarios puedan programar lo necesario en diversos softwares, en los que resalta el Python como el más conveniente para la plataforma, ya que permite configurar de forma directa los pines GPIO, comunicación serial, comunicación Ethernet y demás aplicaciones que posee el dispositivo. Sin embargo, en comparación con la mayoría de computadores de placa reducida no supondría una gran ventaja con la variedad que existen. Es por eso que el factor popularidad o soporte que ofrece será su principal ventaja.

Raspberry, nos ofrece un gran soporte en torno a actualizaciones, códigos o configuraciones desde su página web; así como una comunidad muy grande que ofrece ayuda y comparte diversas inquietudes. Gracias a esta comunidad, Raspberry cuenta con diversos tutoriales de fácil acceso que incluyen videos en la web, los cuales facilitan el trabajo y una adecuada programación. Además, podemos encontrar diversos códigos libres en plataformas como GitHub.

Con respecto a las interfaces necesarias para el trabajo que se desarrolla, Raspberry cuenta con todas las necesarias: interfaz gráfica, conexión a cámara web con cable flat o USB, conexión Ethernet hasta 100Mbps; y una capacidad de procesamiento de 1.2GHz a 64-bits, con lo que garantizamos un trabajo rápido para nuestros fines.

Mencionar que, al ser el equipo de placa reducida de mayor comercialización al momento, permite reducir los costos de envío del equipo. Otros modelos tienen un precio de envío más elevado.

Sobre su procesador de video, Raspberry Pi 3 el procesador que incluye, un VideoCore IV 400 MHz, es de la rama de procesadores diseñados también para celulares en la modernidad; lo que involucra menor gasto de energía, soporte de cámara de gran resolución y procesamiento más rápido de gráficos. Lo que suma positivamente para el procesamiento de imágenes.[29]

Por último, y de gran importancia, el Raspberry Pi 3, nos ofrece un bajo consumo de energía de aproximadamente 500mA en funcionamiento del GUI o interfaz de usuario. Con lo que garantizamos su funcionamiento prolongado evitando un consumo excesivo de energía.

3.5.5.2 Conveniencia del uso del Arduino Mega y placa Ethernet externa

En referencia al uso del módulo RFID, los datos son recibidos por un módulo Arduino. El cual, para su programación, cuenta con librerías libres las cuales facilitan bastante el manejo de la información que genera cada tarjeta de radiofrecuencia. El uso del módulo RFID con Arduino se hace sencillo gracias a que posee una amplia comunidad de desarrolladores. De igual forma, hay que destacar sus bajos precios en el mercado que son de 15 dólares en promedio.

Asimismo, se requerirá realizar envío de la información recabada a la base de datos. Es por esto que se procede a añadir la placa Ethernet de Arduino, la cual está basado en el chip Ethernet Wiznet W5100.

Debido a que la tarjeta Arduino Ethernet requiere varios de los pines de la placa de Arduino en donde se encuentra nuestro procesador principal, se eligió el Arduino Mega entre la gran cantidad de módulos Arduino existentes; ya que este cumple con la cantidad de pines necesarios para también poder trabajar con el módulo de RFID a la par.

En comparación con otros productos en el mercado, como los desarrollados con el microcontrolador ESP8266, Arduino nos permite con la cantidad de pines disponibles, conectar mayor cantidad de actuadores. De igual forma, al trabajar con 5 Voltios y 3.3 Voltios, nos permite el uso de una variedad de sensores y actuadores que trabajen con cualquiera de estos valores, como es el caso del módulo RFID (5 V). De igual forma, al poseer desarrollo libre, la variedad de librerías, facilitará su configuración.

3.5.2 Elevador de voltaje para las salidas 3.3v a 5v

Esta etapa es requerida debido a que el computador elegido trabaja con voltajes de salida en cada uno de sus pines GPIO con 3.3 Voltios; sin embargo, existen otros módulos que requieren comunicación con este que utilizan voltajes de 5 Voltios, como por ejemplo el

módulo de potencia, el cual recibirá una señal de accionamiento, en el cual este módulo se comportará como excitador.

El circuito conversor de 3.3V a 5V consiste en un circuito pequeño compuesto por un mosfet BS170 y una resistencia de 10 k Ω . El circuito usado es mostrado en la imagen siguiente [Figura 16], que no es más que la repetición para siete entradas y salidas que puede utilizar el controlador.



Figura N°16 Conversor 3.3 – 5V

Fuente <https://es.aliexpress.com/store/product/Raspberry-Pi-8-road-level-conversion-module-3-3-V-and-5-V>

El diagrama esquemático del circuito se muestra en la figura 17, cuenta con un mosfet canal N de pequeña señal, una resistencia de 10K y las fuentes fijas de 3.3V (Gate) y 5V conectados a través de la resistencia. En la entrada podemos tener 3.3V o 0V provenientes del controlador; de esta forma, para entradas de 3.3V, debido a que para la conducción del mosfet se requiere que exista un voltaje Gate-Source positivo, no conducirá; con lo que la salida toma el valor de 5V. En caso contrario, cuando la entrada sea 0V, el voltaje Gate-Source será positivo, por lo que el mosfet conducirá, obteniendo en la salida 0V.

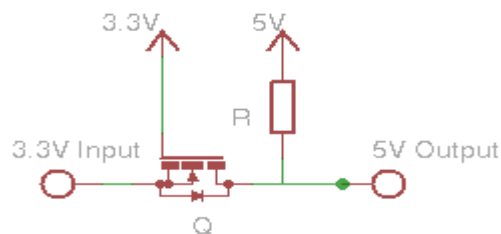


Figura N°17 Diagrama del circuito para cada par IN/OUT

Fuente. <https://findeprehistoria.wordpress.com/2010/07/29/interfaz-de-3-3v-a-5v-y-visceversa/>

3.5.3 Cámara

El uso de la cámara es para realizar la captura de imagen de la placa de los autos en el ingreso. Una vez capturada la imagen, esta pasará al computador, el cual ejecutará un procesamiento de imagen mediante algoritmo libre en el entorno de programación Python. Por tal motivo, y según los criterios de diseño establecidos en la tesis de Luis Gomero Vásquez [Luis Gomero Vásquez (2016). Diseño de un sistema de acceso vehicular a la PUCP basado en tecnología RFID y procesamiento de placas vehiculares (tesis de pregrado). Pontificia Universidad Católica del Perú, Lima, Perú], esta será ubicada a 0.5 metros del suelo y a una distancia de 4.25 metros de la puerta del chofer. Con lo que, en promedio, la distancia de la matrícula será 2.5 metros. Por lo que, inicialmente, en el diseño se planteó el uso de una Life-Cam HD 3000 debido a sus características y bajo costo a comparación de otras marcas (Ver tabla 5). Asimismo, el Raspberry Pi, nos permite trabajar con una variedad de cámaras en las que se encuentran las del modelo Life-Cam de Microsoft. El presente trabajo de tesis no cubrirá el trabajo realizado para al procesamiento de imágenes a detalle, pero se nombrarán las etapas para fines de entendimiento. Se identifican las siguientes etapas:





-Adquisición de la imagen: Se realizará una toma continua de imágenes de la ubicación. Al brindarse la señal de que se realizó el registro en el módulo RFID, utilizará la última toma para procesar la imagen. De ser alta en probabilidad de error, tomará una siguiente imagen, y así reiterativamente sea el caso.

-Acondicionamiento: Como siguiente paso para el procesamiento, se ejecuta en el computador una serie de primeros filtrados que permitan ejecutar el análisis de imágenes. Estos filtros son por ejemplo el uso de la imagen en escala de grises para un procesamiento más eficiente, filtros gaussianos para definir las líneas o filtro Canny para la detección de los bordes de la imagen.

-Análisis de la imagen: Una vez definidos los filtros, el sistema de procesamiento es capaz de hacer la lectura de los datos, y expresarlos de manera binaria para que se pueda interpretar como una serie de valor numéricos. Esto se conseguirá realizando una comparación con una base de datos en la que se tengan los números y letras con los que comparar.

Tabla N°5

Comparación cámaras en el mercado

Características/ Modelo	Cámara Web pro C920	Genius Eye 110	DCS-3715	Life-Cam HD 3000
Resolución	1080p – 720p	640x480 px	Full HD 16:9	720 p
Conectividad	USB 2.0	USB 1.1	Ethernet	USB 2.0
Fabricante	Logitech	Genius	D-link	Microsoft
Precio(S/.)	369.90	70.00	1090.00	150.00
Equipo	 [3.1]	 [3.2]	 [3.3]	 [3.4]

Nota. Fuente. Tesis Luis Gomero Vázquez [Luis Gomero Vázquez (2016). Diseño de un sistema de acceso vehicular a la PUCP basado en tecnología RFID y procesamiento de placas vehiculares (tesis de pregrado). PUCP, Lima, Perú]

Es así que, para la implementación, se utilizó una cámara de 720 píxeles, como es la Life-Cam HD. Sin embargo, después de las pruebas realizadas, se estimó una tasa de error del 12.5% (1 error cada 8 pruebas), un error en detección de la placa debido a la distorsión o “blur” debido a la resolución de este tipo de cámara. Es por esto que para reducir el error obtenido se recomienda utilizar una cámara de captura de 1080 píxeles, como es el caso de la cámara web C920 de Logitech, que además es soportada por el sistema operativo que se empleó en el computador Raspberry: el Raspbian. Lo que mejorará la calidad de la imagen captada por el computador, y obtener un mejor resultado en el procesamiento. Además, una lista completa de cámaras web que son soportadas por el Raspberry puede ser encontrada en la página de asistencia de Linux. (http://elinux.org/RPi_USB_Webcams)

La conexión de la cámara es directa a cualquiera de los puertos USB en los periféricos del Raspberry Pi, el cual permite una alimentación de 5 Voltios para cualquier elemento que se conecte por estos.

Elección de iluminación

Para una correcta recopilación de imágenes, se requiere una iluminación apropiada en diversos escenarios climatológicos. Como es el caso de las horas nocturnas. (Ver Figura 18)

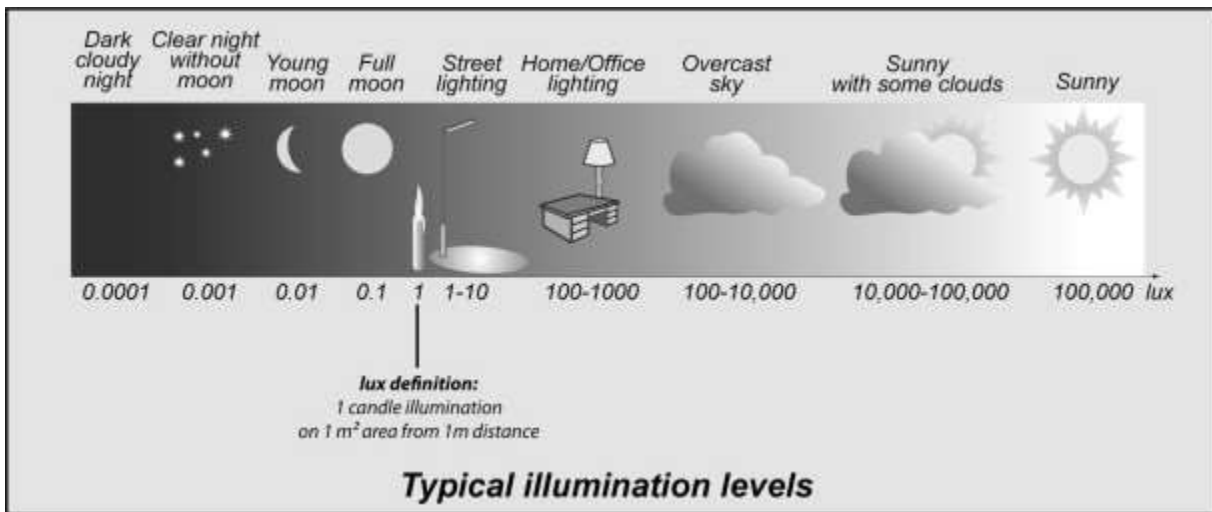


Figura 18. Niveles típicos de iluminación. (Damjanovski, 2014)

Para el trabajo apropiado de la cámara se tomará el valor de 500 lux. Este valor nos proporciona una correcta iluminación en la placa vehicular. Este valor se obtuvo gracias a mediciones realizadas por el National Optical Astronomy Observatory (NOAO) en la cual hacen referencia a la iluminación requerida en entradas para trabajos en parqueaderos y considerando una iluminación adecuada hacia la placa (Figura 19).

Specialty Areas	
Dining Areas	150-200
Kitchens	500
Outleased Space	500
Physical Fitness Space	500
Child Care Centers	500
Structured Parking, General Space	50
Structured Parking, Intersections	100
Structured Parking, Entrances	500

Figura. 19 (National Optical Observatory Astronomy, 2015)

*Valores en unidad Lux

Las dimensiones que se consideran para el espacio entre placa y foco de luz son las siguientes:

Medidas de área de placa 300mm x 150mm (Ver Figura 21) y la distancia entre la fuente de iluminación 2000 mm (Ver Figura 20). Además, asumiremos que la fuente está de manera perpendicular al objetivo (la placa).

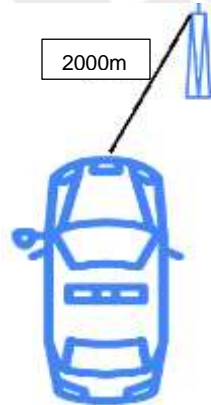


Figura 20. Distancia entre luminaria y placa vehicular. Fuente propia.



Figura 21. Medidas placa vehicular Fuente: Ministerio de Transportes.

El área mínima iluminada debe ser un poco mayor a la superficie de la placa a efectos de dar un margen de error. Por lo que se asumen los valores 300mm de longitud x 500mm de altura (placa), a una distancia de 2000mm del automóvil.

De este modo, podemos realizar la elección de nuestra luminaria revisando los datos que diversos fabricantes nos proporcionan. Se mostrará uno como ejemplo. (Ver Figura 22)



Figura 22. Luces led Marca AKSI. Tipo direccional. (AKSI, s.f.)

En la imagen el proveedor nos indica que a una distancia de 2.5 metros, se puede enfocar un área con un diámetro de 1.20 metros la cantidad de 446 lux [Figura 23]. Valores suficientes para aseverar que la luz abarcará toda la superficie de la placa. Además, al encontrarse a 2.00 metros, se entiende que la cantidad de lux será mayor a 500, dada la proporción que se encuentra en los datos de la imagen del fabricante, en la que cada 0.5 metros hay una variación aproximada de 130 luxes [Figura 22]. Valor que era necesario para ingresos en parqueaderos según datos de NOAO.

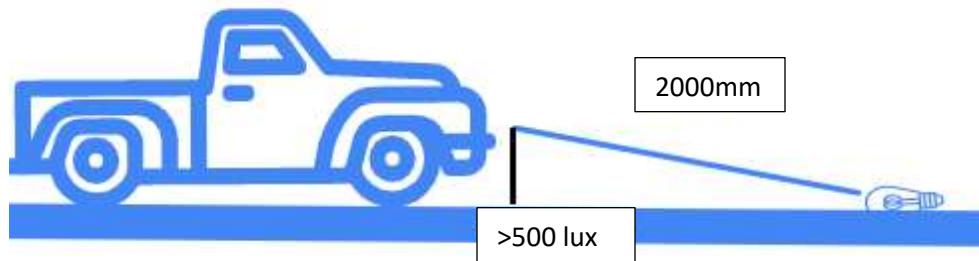


Figura 23. Ejemplo de incidencia de luz en la placa con luminaria

3.5.4 Pantalla de control

La pantalla de control es incluida en esta implementación debido al cambio y exclusión de la pc o portátil incluida en el proyecto inicial. Esta pantalla es requerida para que el miembro de seguridad pueda tener control de lo que sucede en el ingreso.

Las funciones con las que contará la pantalla serán el de denegar el acceso si el guardia de seguridad decide que hay algún error con el ingreso de la persona en auto. De esta forma, se eligió una pantalla táctil para que se pueda enviar comandos desde esta. La conveniencia de que

metros; lo que es equivalente a una pantalla de 10 pulgadas. [Ver Figura sea táctil, será para simplificar la acción y hacer más rápida la decisión del miembro de seguridad.

Se considera que el miembro de seguridad tenga la pantalla a la altura de su rostro al estar parado para que pueda ejercer la movilidad habitual [Figura 19]. Hay que recordar que el sistema implementado es automático, y el miembro de seguridad solo tendrá que estar cerca a la pantalla ante algún hecho que considere extraño.

La recomendación de la SMPTE (Society of Motion Picture and Television), es que la distancia mínima del usuario a la pantalla sea al menos el doble de la dimensión de la pantalla. Por esto, considerando una distancia de 0.5 metros a la cual estará el guardia de la pantalla, optaremos por una pantalla de tamaño de 0.2524]



Figura 24. Dimensiones para la ubicación de la pantalla
Fuente Propia

Entre las pantallas habilitadas para el uso con el Raspberry, tenemos una variedad, de la cual podemos separarlas de acuerdo al método de conexión que tienen con este. El tipo de conexión podrá ser vía HDMI, cable flat o por Wifi, realizando transmisión de datos en red. Sin embargo, la mejor calidad de comunicación de datos nos la brinda la conexión por cable flat según el fabricante. A continuación, veremos una comparación entre dos opciones que tenemos para una pantalla táctil compatible con el Raspberry Pi 3 [Tabla 6].

Tabla 6

Comparación entre pantalla Tablet y pantalla de Raspberry Pi para el control del Raspberry

	Pantalla Raspberry Pi	Tablet Advanced AT - 6141
Tamaño de Pantalla	10 pulgadas	9.1 pulgadas
Tipo de Conexión	Cable Flat	HDMI/Red-Vía Wifi
Transmisión de datos	Tanto de envío como recepción vía cable Flat en puertos configurados para pantalla de Raspberry	Envío y recepción en configuración del Raspberry en la versión HDMI 1.4. Sí permite vía Wifi
Precio	S/ 202.28	S/ 676

Nota. Fuente Propia

Para este cometido, la mejor opción es el uso de la pantalla original con la que cuenta el Raspberry Pi [Figura 25]. Esto debido a la garantía que nos da el mismo fabricante y a la facilidad de conexiones e instalación, lo que simplificaría el mantenimiento en caso de algún problema con este módulo.



Figura 25. Pantalla para Raspberry Pi

Fuente. <http://www.xataka.com/accesorios/la-raspberry-pi-ya-tiene-pantalla-tactil-oficial-hazte-con-ella-por-60-dolares>

Asimismo, en dicha pantalla se visualizaría la siguiente interfaz [Figura 26]. Interfaz planteada en el diseño de Luis Gomero Vásquez.



Figura 26. Interfaz que se incluirá en la pantalla de control
Fuente. Tesis Luis Gomero Vásquez

3.5.5 Sensor RFID

El sensor RFID cumple la función de identificar a cada usuario mediante la detección del campo magnético recibido desde una tarjeta electromagnética cuya información será procesada por el computador para el cotejo.

En esta etapa se hizo uso de tarjetas de 13.56 MHz. La elección es debida a la distancia de hasta dos metros que se puede conseguir a esta frecuencia para el registro, distancia más que suficiente para que el conductor pueda acercar su tarjeta o tag al módulo.

El sensor usado es el MFRC 522 [Figura 27], debido a su facilidad de configuración, conexión y precio. Sin embargo, existen otros tipos de sensores más robustos en torno al material de fabricación y protección al ambiente que poseen, como el sensor RFID USB de Windows, pero por temas de costo se optó por el antes mencionado.

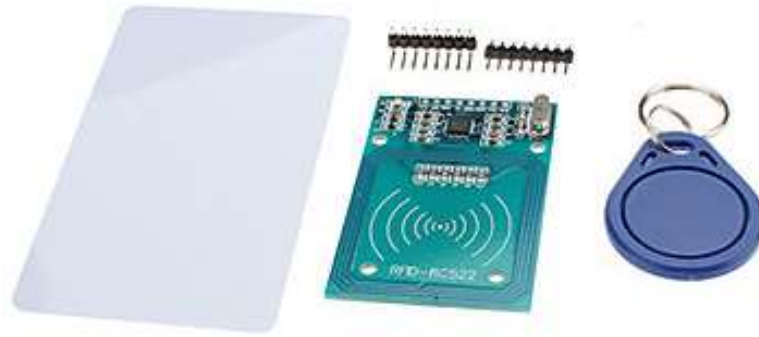


Figura 27. Lector RFID MFRC 522

Fuente: http://www.nxp.com/documents/data_sheet/MFRC522.pdf

3.5.6 Indicadores

El trabajo de los indicadores será el de informar al usuario en el acceso si está registrado en la base de datos. Según este criterio, se empleó una bocina, un conjunto de leds y una matriz LCD para que el usuario tenga conocimiento de su estado [Ver Figura 28].



Figura 28. Indicadores Funcionales

Fuente Propia

Bocina

La función de esta bocina será el de emitir diversas combinaciones de sonido programadas, de acuerdo a sí el acceso del usuario es permitido o no.

Para el diseño inicial, se optó por el uso de una bocina de 0.5 W que trabajaba con 5 V, la cual se puede ver en la imagen siguiente [Ver Figura 29]. Sin embargo, no permite realizar diversas tonalidades de sonidos, por lo que se incorporó una nueva opción de bocina. Esta incorpora un pequeño circuito que facilita el trabajo con corrientes bajas de control provenientes de las salidas del controlador a una frecuencia deseada.



Figura 29. Buzzer 0.5W

Fuente. Tesis Luis Gomero Vásquez

Se usa una bocina de 0.3W para limitar la corriente que se entregue, y por ser una potencia suficiente para que la información sonora sea transmitida al usuario.

La bocina utilizada, como se mencionó, es un buzzer de 0.3 Watts alimentado a 5 Voltios. Se puede apreciar la bocina con el circuito [Ver Figura 30].



Figura N°30 Bocina 0.3 Watts

Fuente Propia

Asimismo, el esquemático del circuito anterior se puede apreciar en la figura 31. [Ver Figura 31]

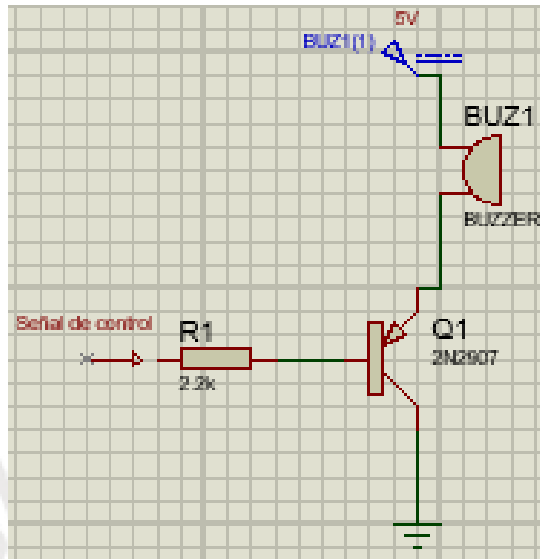


Figura N°31 Esquemático del circuito para una bocina
Fuente propia

La señal de control de la bocina es un pin del computador a la frecuencia a la cual se quiere que esta suene. El circuito con el transistor trabajará en corte y saturación a la frecuencia de la señal de control. Se requiere de un transistor BJT de canal P dado que se busca que los pines de control no entreguen corrientes, se recomienda el uso de un transistor 2N2907, dada su comercialización y su entrega de hasta 600mA, considerando la bocina consumirá 60mA, mientras que la corriente en base, considerando una caída de tensión insignificante en el buzzer, será de 2.2mA. Lo cual significará que el transistor puede soportar la carga. La alimentación que recibe el buzzer, es entregada por el módulo del Arduino que puede entregar 5 Voltios por uno de sus pines, y la variación de la tonalidad se puede garantizar configurando su salida como una señal PWM.

Leds:

El uso de los leds será similar al de la bocina: Emitir una combinación de luces de acuerdo al estado del usuario que intente ingresar con su vehículo.

Por motivos de simplificar la circuitería, reducir el consumo de energía, trabajo con voltajes menores y costo; se optó por trabajar con diodos leds de 5 mm de alta luminosidad y voltaje de conducción de 1.2V (Según hoja de datos) [Ver Figura 32].



Figura N°32. Diodo led alta luminosidad
Fuente propia

A continuación, realizamos el análisis para el consumo de corriente [Figura 33]. La conexión de estos leds fue usando como fuente el mismo pin de salida del controlador, antecedido por una resistencia de 180 Ohmios.

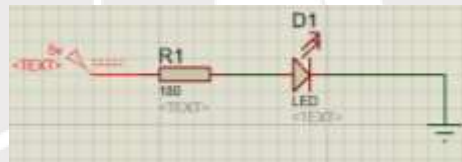


Figura 33. Circuito diodos led de alta luminosidad
Fuente propia

Debido a que el voltaje en el diodo será de 1.2 V en su funcionamiento, entre la resistencia obtenemos una diferencia de potencial de 3.8 V, con lo que aplicando la fórmula de la ley de Ohm $V= I * R$, obtenemos una corriente de 21mA que viaja por el circuito del diodo. Como consideración para la resistencia $P=3.8*0.021=0.08W$. Con lo que lo recomendable es utilizar una resistencia de 180 Ohmios y ½ Watt.

Para la implementación, se utilizaron dos de estos para facilitar la identificación (Uno color verde y otro color rojo).

Pantalla indicadora:

La pantalla indicadora, permite brindar un mensaje de bienvenida o un texto al usuario que ingresará, incluido su nombre si así se requiera. Todos estos parámetros controlados mediante el manejo del algoritmo de control en el computador.

Como requerimiento, de esta forma, se necesita una matriz suficiente para ingresar palabras como “denegado” (8 letras) o “bienvenido” (10 letras). De igual forma, existen diversos tipos de pantallas, para nuestro propósito nos limitaremos a una pantalla simple para letras, debido a que solo requerimos un saludo.

Entre las principales opciones, encontramos pantallas a color y de fondo azul. Una breve comparación se puede observar en la tabla 7. (Ver Tabla 7)

Tabla 7

Comparación de pantallas indicadoras

	Nextion HMI	Pantalla Oled	Pantalla 1602 LCD
Colores	Full color	Fondo azul y letras blancas	Fondo azul y letras blancas
Resolución	480 x 268	128x64	16x2
Costo	27\$	2.62\$	2.20\$

Nota. Fuente propia

Para la implementación, se utilizó una matriz de 16 x 2, suficiente para incluir el nombre de algún usuario, y/o un mensaje de bienvenida corto. El consumo de este es de 25 mA con la luz de fondo activada según hoja de datos. Por tanto, tiene un consumo bajo de energía.

La conexión se realizó mediante un circuito integrado I2C que permite una conexión con menor cantidad de pines a la matriz LCD usando la comunicación I2C incluida en el computador y elegida mediante software.

A continuación, se muestra el diagrama de conexiones para el funcionamiento [Ver Figura 35].

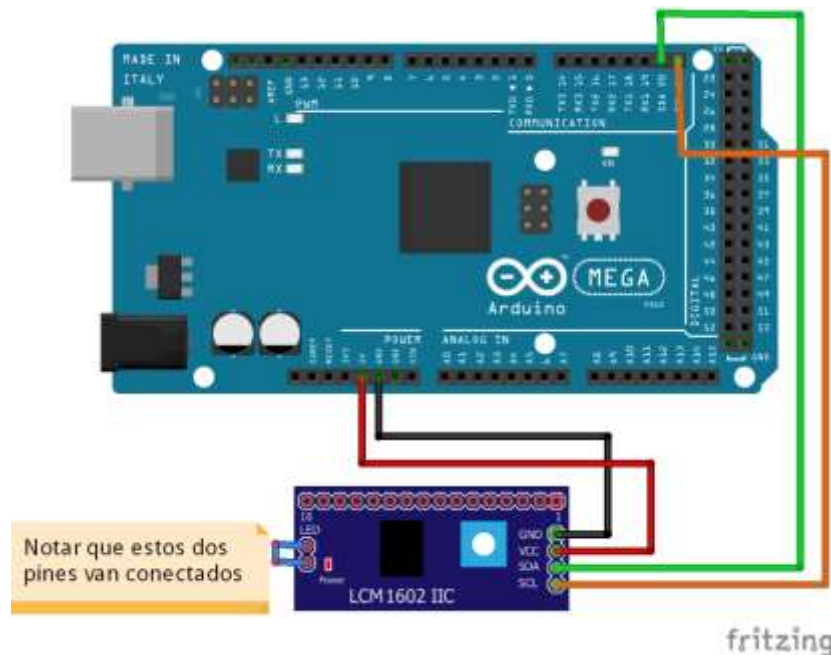


Figura N°35 Conexión Raspberry Pi – Circuito adaptador I2C – Matriz 12 x 2 LCD
 Fuente. <https://parzibyte.me/blog/2018/02/02/obtener-direccion-modulo-i2c-lcd-arduino/>

Las entradas del circuito I2C son:

- VCC: Alimentación de 5Voltios
- GND: Tierra o potencial de referencia
- SDA: Pin para la información serial
- SCL: Pin de control para la comunicación

3.5.7 Fuente de Poder

En lo respectivo al consumo de energía, como el diagrama del proyecto mostró (Figura 9), se alimentará cada uno de los bloques en desarrollo exceptuando el consumo que requiera la tranquera o etapa de potencia. Por tal motivo, y teniendo en cuenta cada uno de los consumos de cada módulo, se procedió a usar una fuente con un límite de corriente superior al requerido; para así tener un factor de seguridad que nos confirme que cada módulo recibe correctamente la energía que necesita. Se muestra el consumo de cada módulo en cuestión. [Ver Tabla 8]

Tabla 8.

Consumo de módulos de baja potencia Raspberry Pi

Módulo	Voltaje	Corriente Consumida (mA)
Cámara	5 V	125 mA
Raspberry Pi 3 (GUI + Wifi)	5V (Fuente externa)	1250 mA
Total		1 375 mA

Nota. Fuente Propia

Con los resultados obtenidos en funcionamiento y valores máximos, se pasó a usar una fuente tipo cargador con conector micro USB, dado que el Raspberry Pi requiere de este tipo de conector (Figura 36). La capacidad de este es de 5 Voltios y 2.5 Amperios en la salida, con conexión de entrada a 220 Voltios directo a la red eléctrica, con lo que se aseguró una correcta alimentación a la carga. Esto dado que el computador distribuirá la energía a cada módulo conectado a sus interfaces (Sensor RFID y Circuito indicador). A continuación, se muestra una imagen de la fuente de alimentación seleccionada.



Figura 36. Fuente de voltaje para Proyecto
Fuente. Propia

Para el caso del Arduino se empleará un cargador de 9V y 1 A, con entrada de 220V. Esto debido al consumo que demanda el módulo Arduino y periféricos como se detalla en la Tabla 9 (Ver Tabla 9).

Tabla 9.

Consumo de módulos de baja potencia Arduino Mega

Módulo	Voltaje	Corriente Consumida (mA)
Sensor RFID	3.3 V (Extraído Arduino Mega)	26 mA
Arduino Mega	5V (Fuente externa)	93 mA
Circuito indicador: Matriz LCD 16x2, Bocina y leds indicadores	5V(Extraído del Arduino Mega)	206 mA
Shield Ethernet	5V(Extraído del Arduino Mega)	40mA
Total		365 mA

Nota. Fuente Propia

Esto será suficiente para los consumos del equipo, dado que el voltaje de funcionamiento está en el rango de 7V y 12V. Asimismo, aunque el consumo de corriente es menor a 1 A, se trata de un cargador comercial y económico. (Ver Figura 37)



Figura 37. Fuente de voltaje para Arduino Mega 2560

Fuente. https://articulo.mercadolibre.com.pe/MPE-430699718-cargador-fuente-9v-y-1a-compatible-para-arduino-_JM?quantity=1

3.5.8 Etapa de Potencia

Para la etapa de potencia, se requiere enviar una señal a un excitador que indique a la tranquera si el acceso es permitido o no, y realice la acción de elevarse o mantenerse en su lugar.

En la implementación realizada, se procedió a enviar una señal de 5 Voltios mediante el adaptador instalado a la salida del computador. Este adaptador o excitador es informado mediante uno de los pines GPIO instalados en el Raspberry y activado por la información recibida y procesada desde la base de datos.

El tipo de motor para activar la tranquera será un motor de torque 6.25 N.m, como se especifica en la tesis del diseño para el proyecto realizada por Luis Gomero Vásquez [Luis Gomero Vásquez (2016). Diseño de un sistema de acceso vehicular a la PUCP basado en tecnología RFID y procesamiento de placas vehiculares (tesis de pregrado). Pontifica Universidad Católica del Perú, Lima, Perú], después que realizó una comparación con servomotores disponibles en el mercado [Ver Tabla 7]. Para tal etapa, se utilizó el Servomotor BF HITEC HSR-5980SG [Ver imagen 37], sugerido en el diseño inicial, debido a su trabajo con voltajes desde 4.8V a 6 V que permite enviar señales de control de bajo voltaje; así como su bajo consumo de energía y menor valor pico de corriente de arranque por tratarse de un motor DC. Característica útil debido a la cantidad de ingresos que se presentan en un día. Se considera la corriente como un 1.5 x Corriente Nominal. Este módulo tendrá su propia fuente de alimentación dado que estará aislado de la parte de control. A continuación, se muestra una lista de servomotores en el mercado (Ver Tabla 9).

Tabla 9

Servomotores disponibles en el mercado

Característica /Modelo	BDG 70 – GREEN LED	Serie MOOVI 30	HSR5980 SG	Zebra barrera Vehicular
Tensión de Alimentación	220Vca	230 V	4.8V – 6V 2.5 A	230 VAC 50Hz, monofásica
Potencia Absorbida	45 VA	300 W	15 W	300W
Tiempo de apertura	1.3 s	3s	3.5 s	4s
Tipo de Motor	Servomotor	Servomotor irreversible	Servomotor	Servomotor
Longitud Brazo	2.5 m	2.5 m	2.6 m	3m

Nota. Fuente. Tesis de Luis Gomero Vásquez [Luis Gomero Vásquez (2016). Diseño de un sistema de acceso vehicular a la PUCP basado en tecnología RFID y procesamiento de placas vehiculares (tesis de pregrado). Pontificia Universidad Católica del Perú, Lima, Perú]



Figura 38. Servomotor BF HITEC HSR-5980SG

Fuente. <http://www.superrobotica.com/S330173.html>

Con respecto a la fuente que nos proporcionará el voltaje e intensidad requeridos por el servomotor, se seleccionó una fuente de 5 V y 5 A. Lo que cumple con el mínimo específico para trabajar con el motor seleccionado. (Ver Figura 39)



Figura 39. Fuente para etapa de potencia

Fuente. https://es.aliexpress.com/item/4000741932348.html?spm=a2g0o.productlist.0.0.2b1e5ef1NbIEQ9&s=p&ad_pvid=202005041121275618303133101760001993230_3&algo_pvid=3efef0f9-a990-47cf-ae2a-143a9c919aa6&algo_expid=3efef0f9-a990-47cf-ae2a-143a9c919aa6-2&btsid=0ab6fab215886164876183356e2fcc&ws_ab_test=searchweb0_0,searchweb201602_,searchweb201603_

La señal será acoplada mediante un relé, para esto se emplea el requisito de que la activación de dicho relé se active a 5V, que es el voltaje de salidas que permite el Arduino Mega, el cual controlará la acción. De igual forma, debe permitir como mínimo 5 A. de corriente que es la corriente pico a la cual trabajará el servomotor. Para esto se empleó un relé acoplador de 5V y 10A, el cual es de carácter comercial. Además de contar con una etapa de protección mediante optoacoplador para aislar etapa de control con potencia. (Ver Figura 40).



Figura 40. Relé de acoplamiento

Fuente. <https://es.aliexpress.com/i/32813096688.html>

3.5.1 Diagrama de Flujo del algoritmo de control

El trabajo realizado estuvo enfocado al hardware del producto final. Sin embargo, este cumple su funcionamiento debido a la correcta ejecución de órdenes enviadas y programadas en la computadora. A continuación, se mostrará el diagrama de flujo del programa principal. [Ver diagrama 2]

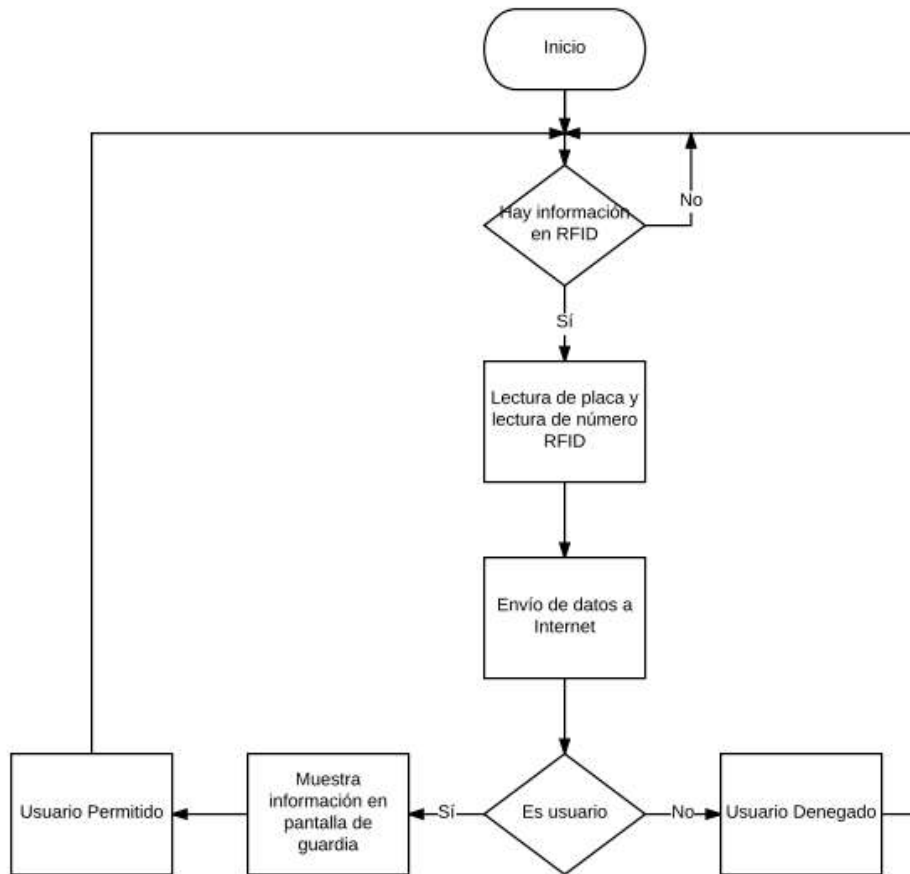


Diagrama 2. Programa Principal

Asimismo, se muestra los diagramas de bloques para las subrutinas de acceso negado, acceso aceptado y la interrupción generada si se activa algún comando en la pantalla de control del guardia.



Diagrama 3. Usuario Denegado



Diagrama 4. Usuario Permitido

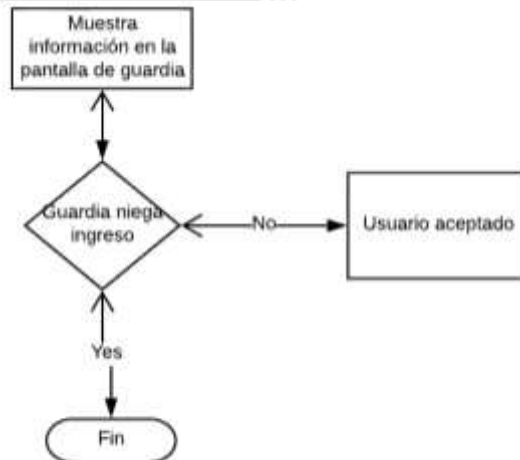


Diagrama 5. Interrupción en la pantalla de Control del Guardia de Seguridad

3.6 Costos

Los costos de la implementación se mostrarán en la tabla siguiente.

Tabla 10

Costos relacionados a la implementación de la Tesis

Elemento	Precio (S/.)
Raspberry Pi 3	160.00
Tablet Advance AT 61-41	700.00
Cables UTP con Conectores RJ45	10.00
Carcasa para proteger Pantalla	30.00
Indicadores + cableado	50.00
Arduino Mega + Shield Ethernet	150.00
Fuentes para circuitos embebidos	15.00
Fuente para potencia	30.00
Circuito acoplador 3.3V a 5V	5.00
Modem Switch	50.00
Estructura para montar componentes	100.00
Otros	50.00
Total	1,350.00

Nota. Fuente Propia

Comparativamente con los costos del proyecto inicial. (Ver tabla 11)

Tabla 11

Costos relacionados al diseño usando PC

Elemento	Precio (S/.)
Tablet Advance AT 61-41	700.00
Carcasa para proteger Pantalla	30.00
Indicadores + cableado	50.00
PC Laptop	2500.00
Cables UTP con conectores RJ45	10.00
Fuente para potencia	30.00
Modem Switch	50.00
Estructura para montar componentes	100.00
Otros	50.00
Total	3520.00

Nota. Fuente propia

Se encuentra una diferencia de 2170 nuevos soles entre ambos costos totales. Cifra sustancial.

CAPITULO 4

RESULTADOS

En este capítulo se mostrarán los resultados obtenidos luego de la implementación del sistema. Se establecieron 3 procedimientos para verificar el estado de todos los módulos: 1. Envío y recepción de datos desde el módulo de control hacia la base de datos ubicada en Internet, 2. Presentación de la interfaz del módulo de control y la Integración de los datos recibidos con la activación de los Indicadores; y 3. Respuesta del sistema al ingresar un usuario.

4.1 Envío y recepción de datos desde el módulo de control hacia la base de datos

El desarrollo de envío y recepción de datos entre Internet y el módulo tuvo dos momentos: Usando el módulo de Arduino Mega y usando el módulo de Raspberry Pi. El funcionamiento fue similar; sin embargo, por las limitaciones que posee el Arduino Mega al ser un microcontrolador y no un microprocesador, el procesamiento de imagen no se llevó a cabo en esta primera etapa, más sí en la etapa con el Raspberry Pi

4.1.1 Primer momento: Arduino Mega

El primer momento fue requerido debido a la necesidad de ejecutar las pruebas a la base de datos en la nube. La etapa de software necesitaba saber comprobar el envío y recepción de datos. Por motivos de simpleza en torno al manejo del Arduino, y debido al tiempo que demandaba el software, se optó por trabajar en una primera instancia de prueba con la plataforma Arduino. Además, gracias a este conjunto de pruebas se pudo comprobar la calidad del funcionamiento del módulo RFID.

En esta etapa, se usó el Arduino integrándolo con el módulo RFID vía la conexión serial SPI. De igual modo, se requirió una tarjeta integrada o shield Ethernet para brindar la conexión con Internet del Arduino. No obstante, las conexiones del módulo RFID y de la shield Ethernet requerían el uso de una conexión por los pines SPI, los cuales están

ubicados solamente en la parte central de la placa en plataformas como el Arduino Uno. Es por este problema de falta de conexiones, que se optó por el uso de un Arduino Mega de mayor cantidad de puertos de salida.

La instalación mecánica fue de forma simple: La tarjeta de expansión de Ethernet, se coloca por encima de la placa de Arduino haciendo coincidir los pines ICSP en la parte del medio [Ver Figura 40]. Mientras que la conexión del módulo RFID, se llevó a cabo realizando la conexión de los pines 5, 50, 51, 52, 53 y los de alimentación. Adicionalmente, se le añadió una bocina o buzzer como medio indicador del proceso. La conexión de este se llevó por medio del pin 3 para el control, así como de los pines de alimentación [Ver Figura 41].

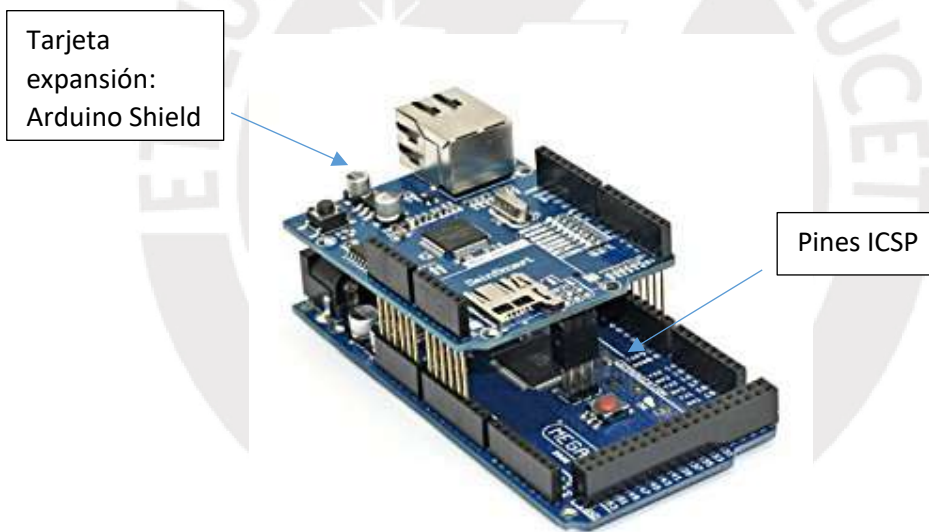


Imagen 40. Conexión entre placa Arduino Mega y Arduino Shield Ethernet

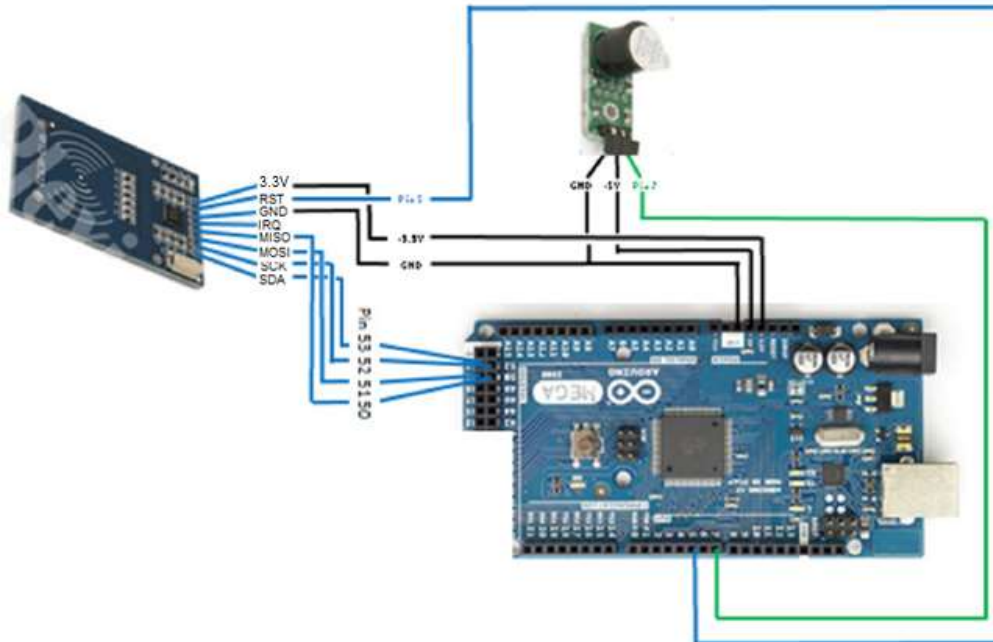


Imagen 41. Conexión placa Arduino Mega, módulo RFID y bocina indicadora

Posteriormente, las líneas programadas en el Arduino permiten interpretar la información brindada por el módulo de radiofrecuencia cuando una tarjeta electromagnética de 13.56Mhz se acercaba. Esta información se transmite en cinco paquetes de dos dígitos en el formato hexadecimal como se aprecia en la figura 42. De esta manera se garantiza la comunicación correcta de los datos extraídos en cada identificación.

```

pruebaLibreriaRFID | Arduino 1.0.5
Archivo  Editar  Sketch  Herramientas  Ayuda
COM23

El numero de serie de la tarjeta es :
EB 85 BE B4 64

El numero de serie de la tarjeta es :
EB 85 BE B4 64

El numero de serie de la tarjeta es :
EB 85 BE B4 64

```

Figura 42. Consola de conexión serial Arduino con recepción de datos del módulo RFID

De esta manera, los datos almacenados en una variable global serán posteriormente enviadas a otra parte del código encargada de enviar esta hacia la nube, mediante el método de envío de datos en HTTP: POST. El detalle de estos envíos no estará documentado por ser parte de la configuración de software.

Finalmente, tras realizar la cantidad de 300 pruebas en días distintos, se obtuvo que el módulo RFID captó la data correctamente. Cada tarjeta presentada, fue registrada con un código único invariante. Se emplearon 7 tarjetas RFID pasivas de 13.56MHz que se le presentaron para tomar la muestra. Sin embargo, la transmisión o llenado de la base de datos tuvo problemas relacionados a la velocidad de internet que se usaron para la experimentación (0.8Mbps para subida de datos). Esto se comprobó, ya que en pruebas con distintas conexiones podía variar la tasa de aciertos en el envío de datos a la nube.

4.1.2 Segundo momento: Raspberry Pi

Para esta segunda etapa, habiendo confirmado el trabajo correcto de recepción en la base de datos mediante los métodos de envío de datos de HTML, se procedió a replicar el proceso en la plataforma de Raspberry. Lo que significó una reducción en conexiones, debido a la conexión Ethernet incorporada que posee el Raspberry Pi. Con este conjunto de pruebas en esta segunda etapa, se consiguió obtener resultados en torno al funcionamiento de la cámara web instalada y al procesamiento posterior.

De esta forma, fue necesario conectar el módulo RFID y la cámara web LifeCam HD 3000. Por un lado, la cámara tiene una rápida conexión mecánica: mediante uno de los puertos USB periféricos del Raspberry Pi. No obstante, se tiene que habilitar el uso de cámaras web en la plataforma vía software, así como la actualización de la versión del programa Python y la instalación de la librería OpenCV, para lo cual no se entrará a detalle, pero será necesario su instalación para que se ejecute el correcto procesamiento de las imágenes.

En lo respectivo al algoritmo de procesamiento de imágenes, se utilizó el algoritmo libre ALPR planteado en el diseño inicial del tesista Luis Gomero Vásquez. [Luis Gomero Vásquez (2016). *Diseño de un sistema de acceso vehicular a la PUCP basado en*

tecnología RFID y procesamiento de placas vehiculares (tesis de pregrado). Pontificia Universidad Católica del Perú, Lima, Perú]

El módulo de procesamiento de imágenes [Ver Figura 43] entrega los resultados en formato de texto, el cual será almacenado en una variable que posteriormente será enviada hacia Internet.



Figura 43. Procesamiento de placa de autos aplicando los filtros

No obstante, a la distancia de 2.5m y utilizando una cámara web de resolución 720 píxeles, se obtuvo un porcentaje de errores (9%). Se puede visualizar la estadística de muestras en la figura 44 (Ver Figura 44). Es así que se adelantó que la calidad óptima se obtendría con una mayor resolución de la cámara. Por lo que, para realizar estas pruebas, se tomó el mejor escenario de recepción y se aceptó cualquier respuesta brindada por el procesamiento de imagen. El objetivo de esta etapa fue el envío de número de placa y código de usuario directamente extraídos de estos dos algoritmos de control que son la identificación del usuario y procesamiento de imagen.



Figura 44. Estadística entre muestras correctas y erradas

Elaboración Propia

4.2 Presentación de la interfaz del módulo de control

Para la elección de la pantalla de la interfaz se optó por el uso de la propuesta de una de la misma empresa Raspberry Pi. Sin embargo, para la implementación, por motivos de costo, se hizo uso de una Tablet AT-6141 de 10" [Ver Figura 44] para la simulación de la interfaz que tendrá el guardia de seguridad. En esta etapa, se inspeccionó el correcto envío de comandos desde la pantalla de control hacia el computador.

Para realizar la conexión de la Tablet con el computador, se aprovechó la capacidad de conectividad vía Wifi de ambos elementos (Tablet y Raspberry Pi 3). De esta forma, y realizando la configuración de red adecuada, la cual será revisada por el tesista César Nicolini, se pudo conseguir una comunicación entre ambos módulos.



Figura 45. Pantalla de Control

La pantalla instalada permite visualizar e inclusive enviar órdenes al controlador, si fuese necesario denegar el acceso al usuario.

Para el desarrollo de la interfaz de usuario, se trabajó en el programa QT el cual nos permite el manejo de una interfaz en Raspberry que envíe comandos, los cuales ejecutan acciones de acuerdo a la programación escrita. [Figura 45]

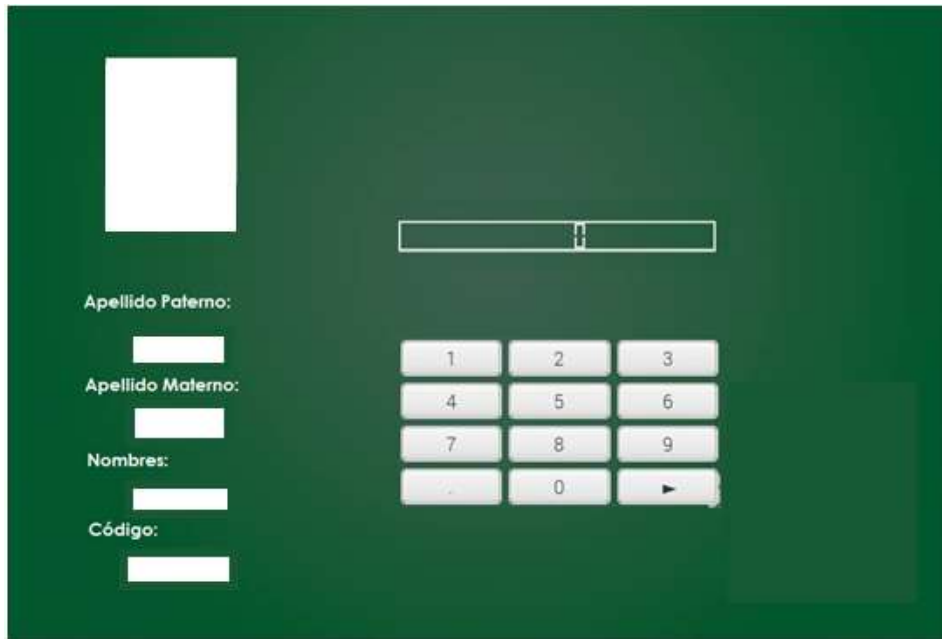


Figura 46. Interfaz de control creada en el programa QT

Para comprobar el correcto funcionamiento, habiendo culminado la interfaz gráfica, se procedió a llenar una variable de programación cada vez que se realizaba la digitación de uno de los botones. Experimentación que fue satisfactoria en un 100% de sus pruebas. Sin embargo, habrá que considerar, que por la conexión inalámbrica que se desarrolló, no podía haber un alejamiento de más de 30 cm entre la pantalla táctil de la Tablet y el módulo de control, dado que podía haber pérdida de datos o de conexión.

4.3 Integración: Datos recibidos – Activación de Indicadores

En esta última etapa, se procedió a la programación del controlador para el control de sus periféricos de salida, como son los indicadores. Desde la base de datos, mediante programación en lenguaje PHP, se recibió un mensaje de respuesta indicando si la persona que intentaba ingresar era un usuario permitido o no. Posteriormente, el microcontrolador procede a ejecutar una acción tras recibir la información de la base de datos.

Para la simulación de un registro errado, al computador Raspberry Pi 3 se le envía el comando “error” desde la base de datos.

Acciones:

- Luz de color Rojo activa
- Pantalla LCD envía mensaje: “Acceso Negado” [Figura 46]
- Sonido Buzzer a 250 Hz por 1 segundo

Mientras que para un ingreso aceptado se dispone a la recepción de un comando “aceptado”, el cual, de igual manera será enviado vía web.

Acciones:

- Luz de color verde activa
- Pantalla LCD envía mensaje: “Bienvenido PUCP”
- Sonido Buzzer a 3000 Hz por 1 segundo
- Activación de tranquera

De esta manera, se comprobó el funcionamiento de los indicadores para cada diferente ingreso de comandos. Siendo unas 100 pruebas las realizadas y con un 100% de envío positivo en su ejecución según el comando recibido.

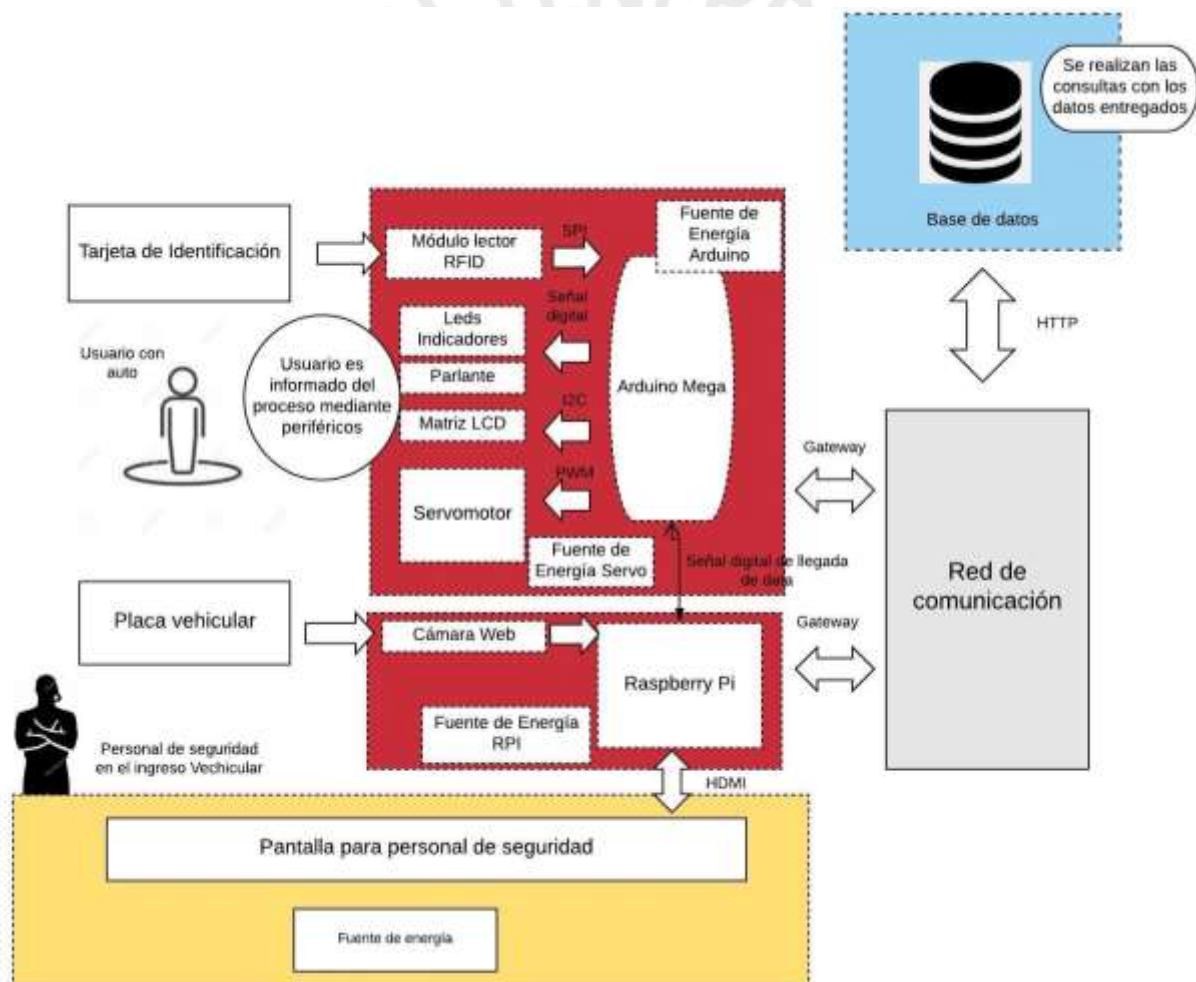


Figura 47. Indicadores para el acceso negado

4.4 Diagrama de bloques final

En el siguiente diagrama se puede visualizar cómo está constituido el sistema de ingreso vehicular a la PUCP.

La integración y pruebas de cada una de las partes que conforman el sistema, se pueden resumir como un módulo de control que tiene dos partes (Color Rojo), una constituida por el Arduino Mega, y otra por el Raspberry Pi; los cuales irán en comunicación con la base de datos en la nube (Color Celeste), y reciben información del usuario. A su vez el flujo de la información recibida y enviada está monitoreada por un personal de seguridad (Color Amarillo).



Finalmente, todo el proceso de registro y aceptación o negación para el ingreso del personal tuvo un retardo mínimo que se puede aproximar a los 3 segundos.

Conclusiones

-Se logró implementar de manera exitosa el trabajo que realizará el sistema de ingreso vehicular a la PUCP. Se realizaron pruebas a cada uno de sus módulos siendo el resultado:

- Módulo RFID: Funcionó en un 100% con la identificación
- Cámara web: Se planteó una nueva alternativa con una cámara de 1080p para mejorar la captura de imagen para el procesamiento.
- Indicadores: Funcionaron de acuerdo a lo esperado. Entregando las señales para que el usuario conozca su estado en el ingreso
- Activación de tranquera: En todos los casos donde se enviaba la señal para su activación estar respondía de forma correcta.

-En una evaluación económica, la principal diferencia con el diseño de hardware presentado en la tesis de Luis Gomero Vásquez, radica en el uso de placas embebidas en contraste de la computadora presentada inicialmente. Lo cual presentó un ahorro, y confirma la mejora económica con este uso.

-Gracias al uso de placas con conexión Ethernet en el proyecto, se proporcionó el agregado de una conexión del sistema con la web.

-Por último, se consigue una mejora de tiempo del proceso, dado que los datos se envían y reciben en tiempo real, con un retardo mínimo de 3 segundos, comparado con el proceso de revisión exhaustiva del ingresante que puede oscilar entre los 6 a 15 segundos, el mejor tiempo si se incluyeran a dos guardias realizando la identificación en conjunto. Esta mejora se debe gracias a su naturaleza digital.

Recomendaciones

-Para realizar la implementación y funcionamiento adecuado del sistema de detección de placas vehiculares, hay que tomar consideraciones de iluminación externa, si fuese el caso de realizarla en horas nocturnas o después de las 5 pm según horario en Lima-Perú. Se recomienda aumentar la iluminación en el ingreso vehicular mediante el uso de fuentes como focos que enfoquen el haz lumínico a la zona donde se ubican las placas vehiculares. Se expuso un foco con las características adecuadas para la iluminación. Sin embargo, se puede utilizar otra fuente teniendo las consideraciones de lúmenes expuesta en el punto 3.5.3 Cámara.

-Para garantizar una conexión “instantánea” para el envío de datos a Internet, hay que asegurarnos que esta esté en valores de 15Mbps para la velocidad de subida de datos.

-En la actualidad existen placas de desarrollo más modernas; en la familia de Raspberry, el Raspberry Pi4 que cuenta con una velocidad de procesamiento mayor en relación al procesador, memoria RAM adicional y GPU con los que cuenta. Lo cual es importante para el procesamiento de imágenes que desarrolla. Además de no diferir en mucho el costo del equipo. Por lo que es aconsejable realizar la implementación con este dispositivo.

-Para evitar el uso de un nuevo documento como es el de tarjetas RFID, se plantea la presentación del documento de identidad DNI. Con lo cual se obtiene un ahorro en la adquisición de tarjetas y practicidad, ya que este documento es de uso diario para los usuarios. Se recomienda cambiar el módulo RFID por un módulo óptico para el reconocimiento de DNI.

-Un ahorro adicional se puede generar cambiando la pantalla de presentación en la garita. De una Tablet a una pantalla con procesamiento limitado. Lo cual puede significar un menor precio. Tal es el caso de la pantalla para Raspberry Pi de 10 pulgadas HDMI LCD 1024x600 con un precio de 200 soles considerando el envío desde China.

-Se puede realizar la integración de envío de datos desde el módulo Raspberry: Datos de placa vehicular y código RFID relacionado. Reduciendo aún más la cantidad de equipos.

Bibliografía

[1]EL COMERCIO

2015 “Perú tiene la más alta tasa de delincuencia en Latinoamérica” [en línea]

[Consultado 15/05/2016]

<<http://elcomercio.pe/politica/actualidad/peru-tiene-mas-alta-tasa-delincuencia-latinoamerica-noticia-1805807>>

[2] Escuela de seguridad ciudadana

1999 Manual de organización y funciones. Bolivia.

[3]Félix Murazzo Carrillo

2013 Reflexiones sobre la seguridad ciudadana en el Perú. Perú

[4]Ángel Joel Chávez Hidalgo

2012 La estructura y funciones de la Policía Nacional del Perú bajo un enfoque moderno. Tesis Doctorado. Ciencias contables y Empresariales. U.N.M.S.

[5] D. L. Almanza-Ojeda, A. Hernández-Gutiérrez and M. A. Ibarra-Manzano.

2006 Design and implementation of a vehicular access control using RFID. Facultad de Ingeniería Mecánica, Eléctrica y Electrónica (FIMEE)

Universidad de Guanajuato

[6]Empresa DOINTECH

2016 “Control Acceso Vehicular” [En línea]

[Consultado 10/05/2016]

<<http://www.dointech.com.co/control-acceso-vehicular.html>>

[7] E. Cavalcanti Neto, E. S. Rebouças, J. L. Moraes, S. L. Gomes, P. P. Rebouças Filho

2015 Development of Control Parking Access Using Techniques Digital Image Processing And Applied Computational Intelligence. IEEE Latin American Transactions, VOL. 13, NO. 1

[8] Dr. Rosebrock, Adrian

2019. Raspberry Pi for Computer Vision 3rd Edition. PyImageSearch. EE.UU.

[9]Norton, Peter

2014 Introducción a la computación 6ª edición. [Libro Electrónico]. México

[10] Laura Silva, Yasin Nilton

2001 Administración de base de datos enfocado a la optimización para múltiples plataformas de base de datos. Tesis para obtener el título de Ingeniería de software.

PUCP.

- [11] CISCO
2013 "Switching and Routing". (Capítulos 1, 2, 9 y 10).
- [12] Poder Judicial
2016 "Teoría de las pruebas". [En línea]
Consultado [28/05/2016]
<https://www.pj.gob.pe/wps/wcm/connect/f79058004678c1b1a1ece793776efd47/Teor%C3%ADa+de+la+prueba.pdf?MOD=AJPERES&CACHEID=f79058004678c1b1a1ece793776efd47>
- [13] Kishan Prajapati
2015 Process Control and Monitoring using Arduino and Raspberry Pi. Tesis para obtener el título de Master. Telemark University College -Faculty of Technology.
- [14] Juan Diego Gauchat
2012 El gran libro de HTML5, CSS3 y Javascript. España.
- [15] Kurose, James. Ross, Keith
2008. Computer networking. Pearson. EE.UU.
- [16] Lancker, Luc Van
2013 HTML5 y CSS3 : domine los estándares de las aplicaciones web. España
- [17] Universidad Nacional de Educación a Distancia
2015 Apuntes sobre máquinas virtuales. España.
- [18] Raspberry
2016 Raspberry Pi. [En línea]
[Consultado 10/05/2016]
<https://www.raspberrypi.org/>
- [19] Arduino
2016 Arduino UNO. [En línea]
[Consultado 13/05/2016]
<https://www.arduino.cc/en/Main/ArduinoBoardUno>
- [20] Universidad del País Vasco
2016 Identificación Biométrica [En línea]
[Consultado 13/05/2016]
<http://www.sc.ehu.es/ccwqrom/transparencias/pdf-vision-1-transparencias/ident-biometrica-1.pdf>
- [21] Biotrack [En línea]
[Consultado 14/06/2016]
<http://www.biotracksoftware.com/esp/vehicular.htm>

[22] Ipsolutions [En línea]
[Consultado 14/06/2016]
<http://www.ipsolutions.com.pe/control-de-acceso-vehicular.html>

[23] Luis Gomero Vásquez
2016 Diseño de un sistema de acceso vehicular a la PUCP basado en tecnologías RFID y detección de placas vehiculares. Tesis para obtener el título de bachiller en Ingeniería Electrónica. PUCP.

[24] web ULIMA -
2019 “Procedimiento para solicitar ingreso vehicular alumnos de pregrado y posgrado ”
[En línea]
[Consultado 12/10/2019]
[http://www3.ulima.edu.pe/webulima.nsf/otrosweb/avisoinvsvehicular/\\$file/default.htm](http://www3.ulima.edu.pe/webulima.nsf/otrosweb/avisoinvsvehicular/$file/default.htm)

[25] Jiménez Llatas, Cinthya Lorena; Pretell Cabrera, Víctor Hugo
2013 Sistema inteligente de identificación y localización vehicular usando RFID en una red integrada Zigbee y GPRS. Tesis para obtener el título de licenciado en Ingeniería Electrónica. UPC.

[26] Dueñas Rodríguez, Abel Alejandro; Vadillo Vidal, Christian Edward
2013 Conteo de varillas de acero por procesamiento de imágenes. Tesis para obtener el título de licenciado en Ingeniería Electrónica. UPC.

[27] Gerardo Alfonso Joel Espinoza Vásquez
2014 Sistema de reconocimiento de patrones en placas vehiculares para el acceso automático de visitas a un edificio. Tesis para obtener el título de licenciado en Ingeniería Informática. PUCP.

[28] Diana Maribel Sánchez Chung
2008 Diseño de un Sistema de control de acceso vehicular en zonas residenciales. Tesis para obtener el título de licenciado en Ingeniería Electrónica. PUCP

[29] web Broadcom -
2020 “VideoCore IV - BCM28145” [En línea]
[Consultado 25/04/2020]
<https://web.archive.org/web/20130526115301/http://www.broadcom.com/products/Cellular/3G-Baseband-Processors/BCM28145-28155>

ANEXOS

1. Código Arduino de envío/recepción de datos desde la base de datos y alerta a Raspberry para inicio de lectura para pantalla de guardia.

```
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <SPI.h>
#include <MFRC522.h>
#include <Ethernet.h>

byte mac [] = {0xDE, 0xAD, 0xBE, 0xEF, 0xFF, 0xEE}; // Direccion MAC
IPAddress server(63,83,35,64); // Ip de la ubicacion de nuestra página
EthernetClient client;
int esperar=1;
int analog_pin = 0;
int activa_RPI= 5
int respuesta_RPI= 6
int tarjeta; //almacena la data de la tarjeta RFID
char c; //almacena respuesta de la base de datos

#define RST_PIN 9 // reset del RC522
#define SS_PIN 10 //Pin 10 para el SS (SDA) del RC522
MFRC522 mfrc522(SS_PIN, RST_PIN); //
LiquidCrystal_I2C lcd(0x3F,16,2);

const int led = 13; // del pin 13, obtendremos la señal de aprobacion de usuario
const int tranquera = 12 ; // del pin 12, saldrá la señal de activacion de la tranquera
int sonido_PWM = 44 ;//del pin 44 extraemos el sonido grave

int conectando=0; //variable de activación de periféricos

////////////////////////////////////
//Configuracion de periféricos de ARDUINO////////////////////////////////////
////////////////////////////////////

void setup() {
  // put your setup code here, to run once:
  esperar=1 ;// Variable que sólo cambia cuando entrega la respuesta la base de datos
  para pasar a una nueva consulta
  pinMode(led, OUTPUT);
  pinMode(tranquera, OUTPUT);
  pinMode(activa_RPI, OUTPUT);
  pinMode(respuesta_RPI, INPUT);
  lcd.init(); // Iniciar LCD
```

```

lcd.backlight(); //Enciende luz de fondo de la matriz
lcd.print("Bienvenido");

Serial.begin(9600); //Iniciamos la comunicación serial
SPI.begin(); //Iniciamos el Bus SPI
mfrc522.PCD_Init(); // Iniciamos el MFRC522

if(Ethernet.begin(mac)==0){
  Serial.println("Falló configuracion de Ethernet usando DHCP");
  for(;;)
  ;
}
delay(1000);
Serial.println("connecting...");

if (client.connect(server, 80) ) {
  Serial.println("connected");
  // Make a HTTP request:

}
else {
  // kf you didn't get a connection to the server:
  Serial.println("connection failed");

  Serial.println("A la espera");}
}
////////////////////////////////////
//Segmento de lazo infinito de programa////////////////////////////////////
////////////////////////////////////

void loop() {
  // put your main code here, to run repeatedly:
  digitalWrite(tranquera, LOW); //Baja tranquera siempre después de usarla
  digitalWrite(activa_RPI, LOW); // Desactivamos la alerta de lectura del RPI
  inicialmente
  // A la espera de algún TAG
  if ( mfrc522.PICC_IsNewCardPresent())
  {
    //Lee la tarjeta presentada
    if ( mfrc522.PICC_ReadCardSerial())
    {
      // Enviamos serialmente su UID
      Serial.print("Card UID:");
      for (byte i = 0; i < mfrc522.uid.size; i++) {
        Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
        Serial.print(mfrc522.uid.uidByte[i], HEX);
      }
    }
  }
}

```

```

        tarjeta=mfr522.uid.uidByte[i]; // almaceno data de tarjeta para
comparar con la info en base de datos
        //Enviamos lectura de tarjeta
        client.print("GET /tesis/comunicaciones/arduino/mysql.php?tarjeta="); // se
envía por método get el valor de la tarjeta
        //El valor de la tarjeta será comparado en la nube, y enviará una respuesta.
        client.print(tarjeta);
        client.println(" HTTP/1.0");
        client.println();

    }
    Serial.println();
    // Terminamos la lectura de la tarjeta actual
    mfr522.PICC_HaltA();

while(esperar==1){
if (client.available()) {
char c = client.read();
Serial.print(c);
esperar=0;
}}
// si el servidor se desconecta, terminar
if (!client.connected()) {
Serial.println();
Serial.println("disconnecting.");
client.stop();
}
}

if (String(c)=="aceptado") //Si base de datos acepta
{

digitalWrite(activa_RPI,HIGH); //Esta salida enviará la alerta al RPI para lectura desde
la nube
delay(2000);

if(respuesta_RPI==1) { //El Rpi enviará la alerta de si la placa es correcta con la
tarjeta presentada

activacion_periféricos();

}

if(respuesta_RPI==0) { //Si la placa no es correcta, desactiva los periféricos
desactivacion_periféricos();
}
}

```

```

    }
}
}

if (String(c)=="negado") // Si base de datos niega la tarjeta, desactiva los periféricos
{
    desactivacion_perifericos();
}
}

////////////////////////////////////
//Activacion de periféricos////////////////////////////////////
////////////////////////////////////
void activacion_perifericos(){
    //Activamos la matriz LCD
    lcd.setCursor(0,1);
    // Mensaje de Bienvenida
    lcd.print("Usuario Correcto");

    //Activamos leds
    digitalWrite(led, HIGH);
    //Sonido grave
    analogWrite(sonido_PWM, 80);
    //Activamos tranquera
    digitalWrite(tranquera, HIGH);

    delay(20000);
}
////////////////////////////////////
//Desactivacion de periféricos////////////////////////////////////
////////////////////////////////////

void desactivacion_perifericos(){
    //Activamos la matriz LCD
    lcd.setCursor(0,1);
    // Mensaje de negacion de usuario
    lcd.print("Usuario Incorrecto");

    //Activamos leds
    digitalWrite(led, LOW);
    //Sonido grave
    analogWrite(sonido_PWM, 180);
    //Activamos tranquera
    digitalWrite(tranquera, LOW);
    delay(3000);
}
}

```