Polo del Conocimiento

Pol. Con. (Edición núm. 60) Vol. 6, No 7
Julio 2021, pp. 935-956
ISSN: 2550 - 682X
DOI: 10.23857/pc.v6i7.2900

Desarrollo de un sistema de alarma domiciliaria con reconocimiento facial y alerta temprana. Caso de estudio: vivienda del Barrio Corazón de María, Cantón Cuenca, Provincia del Azuay

Development of a home alarm system with facial recognition and early warning. Case study: house in the Corazón de María neighborhood, Cuenca city, Azuay

Desenvolvimento de um sistema de alarme domiciliar com reconhecimento facial e aviso antecipado. Estudo de caso: Habitação do coração de Mary Bairro, Canton Cuenca, Província de Azuay

Galo Fabián Suárez-Pesántez [I]
gfsuarezp97@est.ucacue.edu.ec
https://orcid.org/0000-0003-1384-8791

Jenny Karina Vizñay-Durán [II]
jviznay@ucacue.edu.ec
https://orcid.org/0000-0001-7557-5034

Correspondencia: gfsuarezp97@est.ucacue.edu.ec

Ciencias técnicas y aplicadas
Articulo de revisión

*__Recibido:__ 22 de mayo de 2021 *__Aceptado:__ 20 de junio de 2021 __* Publicado:__ 05 de julio de 2021

I. Estudiante de la carrera de Ingeniería en Sistemas, Universidad Católica de Cuenca, Cuenca, Ecuador.

II. Ingeniera de Sistemas, Docente de la Unidad Académica de Tecnologías de la Información y Comunicación (TIC), Unidad Académica de Tecnologías de la Información y Comunicación Universidad Católica de Cuenca Grupo de Investigación Simulación, Modelado, Análisis y Accesibilidad (〖SMA〗^2), Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

En Ecuador las cifras de robos y hurtos domiciliarios crece exponencialmente cada año, muchos de ellos quedan en la impunidad por falta de evidencia para presentar una denuncia; es por ello que el presente trabajo investigativo demuestra la posibilidad de crear alternativas de seguridad de bajo costo y fácil instalación en una casa modelo. El objetivo de este artículo se centra en: 1). el desarrollo de un sistema de seguridad con reconocimiento facial y alerta temprana con el uso de componentes disponibles en el mercado local, como: placa de desarrollo Rasberry Pi 3, sensores de movimiento PIR y sensor magnético de contacto; y, 2). en base a los requisitos de seguridad especificados para la casa modelo, el desarrollo de un aplicativo móvil que permite al propietario la activación o desactivación del sistema, recepción de alertas en tiempo real de los sensores de la vivienda y la recepción de la fotografía cuando no exista el reconocimiento de la persona, otorgando así al propietario herramientas de protección domiciliaria y en caso de que el delito se cometa, la generación de evidencia fotográfica.

En la etapa de prueba se aplicaron tres métodos de valoración, el sistema respondió de forma óptima a todas las variables de validación establecidas, haciendo un preciso reconocimiento y emitiendo en un tiempo promedio de tres segundos las notificaciones a sus destinatarios. El método LBPHFaceRecognizer es el que mayor confiabilidad presentó con un 96.67% de eficiencia, con un rango de desempeño óptimo considerado entre los 40 a 150 centímetros.

Palabras claves: Reconocimiento Facial; Visión Artificial; Alerta Temprana; Evidencia.

Abstract

In Ecuador, the number of robberies and home thefts grow exponentially every year, many of them remain in impunity due to lack of evidence to file a complaint; That is why this research work demonstrates the possibility of creating low-cost and easy-to-install security alternatives in a model house. The objective of this article focuses on: 1). the development of a security system with facial recognition and early warning with the use of components available in the local market, such as: Rasberry Pi 3 development board, PIR motion sensors and magnetic contact sensor; and, 2). Based on the security requirements specified for the model house, the development of a mobile application that allows the owner to activate or deactivate the system, receive alerts in real time from the house's sensors and receive photographs when not there is recognition of the person, thus granting the owner

tools for home protection and, in the event that the crime is committed, the generation of photographic evidence. In the test stage, three evaluation methods were applied, the system responded optimally to all the validation variables established, making a precise recognition and issuing the notifications to its recipients in an average time of three seconds. The LBPHFaceRecognizer method is the one with the highest reliability with 96.67% efficiency, with an optimal performance range considered between 40 to 150 centimeters.

Keywords: Facial Recognition; Computer Vision; Early Warning; Evidence.

Resumo

No Equador, as figuras de roubo de casa e roubos crescem exponencialmente todos os anos, muitos deles continuam a impunidade por falta de evidências para apresentar uma queixa; É por isso que o presente trabalho investigativo demonstra a possibilidade de criar alternativas de segurança de baixo custo e fácil instalação em uma casa modelo. O objetivo deste artigo se concentra em: 1). O desenvolvimento de um sistema de segurança com reconhecimento facial e aviso antecipado com o uso de componentes disponíveis no mercado local, como: placa de desenvolvimento de Rasberry Pi 3, sensores de movimento pir e sensor de contato magnético; e 2). Com base nos requisitos de segurança especificados para a casa do modelo, o desenvolvimento de uma aplicação móvel que permite ao proprietário a ativação ou desativação do sistema, recepção de alertas em tempo real dos sensores de habitação e a recepção da fotografia quando não há o Reconhecimento da pessoa, concedendo assim as ferramentas de proteção residencial do proprietário e, caso o crime seja cometido, a geração de evidências fotográficas.

Três métodos de avaliação foram aplicados no estágio de teste, o sistema respondeu otimamente a todas as variáveis de validação estabelecidas, fazendo um reconhecimento preciso e emitindo notificações para seus destinatários em um tempo médio. O método LBPHfacerecognizer é a maior confiabilidade apresentada com eficiência de 96,67%, com uma faixa de desempenho ideal entre 40 a 150 centímetros.

Palavras-chave: reconhecimento facial; Visão artificial; Aviso prévio; Evidência.

Introducción

En toda sociedad se presentan fenómenos de violencia y delincuencia, en América Latina, los más destacados son los robos y hurtos. El número de personas afectadas por este tipo de delitos es alto,

los dueños de los inmuebles no solo pierden sus bienes materiales, sino también la tranquilidad de sentirse a salvo. Además, en muchos de los casos no se presenta la denuncia correspondiente por no disponer de evidencias y así el proceso investigativo es entorpecido.

Si bien es cierto, en el mercado actual existen soluciones dirigidas hacia la seguridad del inmueble, pero la mayoría son costosas y su instalación requiere la intervención de personal capacitado, por esta razón la mayoría de propietarios no cuentan con sistemas de seguridad, es así que en el presente proyecto se ha desarrollado un sistema de seguridad de bajo costo, basado en software y hardware libre.

Se inicia con el diseño y construcción de un sistema de seguridad con reconocimiento facial y alerta en tiempo real, que proporcione al propietario de herramientas para proteger su domicilio, ya que cuando una persona no sea reconocida por el sistema enviará una notificación al propietario, quien podrá activar una sirena de forma disuasiva, o comunicar del particular a familiares, autoridades o personas de su interés, además quedará registrada la fotografía del intruso que podría servir para una investigación de carácter legal.

El desarrollo del proyecto se ha divido en tres etapas: 1). Levantamiento de requisitos funcionales y no funcionales, 2). Codificación del software para la detección de movimientos, apertura de puertas y reconocimiento facial, desarrollados con Python versión 3.7 y utilizando la librería OpenCV para determinar el método más fiable para el reconocimiento; el aplicativo móvil orientado a dispositivos Android ha basado su desarrollo en Java en el Ide Android Studio, 3). Construcción e implementación del sistema de seguridad en la casa modelo teniendo en cuenta los requisitos expresados por el propietario; los dispositivos utilizados se adquieren fácilmente en el mercado local, éstos son la placa de desarrollo Raspberry Pi 3 (cerebro del sistema) que recibe la información entregada por los sensores de apertura y por los sensores de movimiento PIR (Passive Infrared).

Desarrollo

Conceptos relacionados

Sistemas de seguridad .- Son grupos de dispositivos instalados e interconectados entre sí que su principal función es de prevenir, detectar o actuar ante intrusiones, intentos de robos, tradicionalmente se asocia a los “Sistemas de seguridad” con alarmas antirrobo, sin embargo, éstos se han convertido

en las soluciones modernas que las personas han implementado como medidas de protección (Verisure , s.f.).

Dependiendo del grado de seguridad que se desee obtener se pueden clasificar en: grado uno es de bajo riego y solo emite señales acústicas, el grado dos es de riesgo medio y se encuentran conectadas a una central y permiten un control remoto; el grado tres es de riego alto, son complejas y se encuentran conectadas a centrales de gestión (Alarmas, s.f.).

Inteligencia Artificial (IA).- Es la composición de algoritmos creados con el fin de diseñar máquinas que imiten las destrezas que el ser humano realiza como el pensar y razonar (Identification, 2020). Los expertos Stuart Russell y Peter Norvig identifican varios tipos de IA como son: (Iberdrola)

Sistemas que piensan como humanos: Realizan actividades mediante la automatización, como la resolución de problemas y la toma de decisiones, podemos tener como ejemplo las redes neuronales.

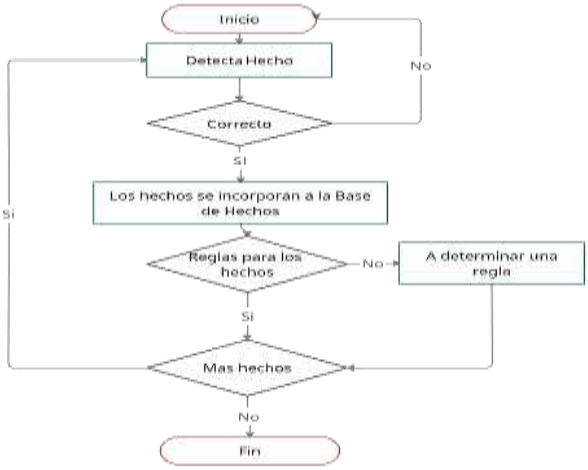
- ***Sistemas que actúan como humanos:*** Son ordenadores que realizan tareas repetitivas de forma similar como lo hacen los humanos, como son los robots.
- ***Sistemas que piensan racionalmente:*** Pretenden simular el pensamiento lógico racional de las personas, por ende, que sean capaces de percibir, razonar y actuar (Sistemas Expertos).
- ***Sistemas que actúan racionalmente:*** Son aquellos que tratan de imitar de forma racional el comportamiento humano, como un software que simula ser un jugador en un juego de computadora.

Sistemas Expertos (SE).- Se puede considerar un sistema que maneja el conocimiento humano capturado en una computadora para solucionar situaciones que requieren de expertos humanos. Son programas que capturan el conocimiento de un experto y trata de imitar su razonamiento cuando resuelven los determinados problemas que pertenece a su área de conocimiento (Ruiz M. E., 2004).

Componentes de un Sistema Experto

- ***Base de hechos:*** Es una memoria auxiliar que contiene las experiencias del usuario, es decir que compone la memoria de trabajo del sistema.
- ***Proceso lógico de Carga de Hechos.*** **-** Se detectan los hechos y se incorporan a la base de hechos (Ilustración 1).

Ilustración 1: Proceso Lógico de Carga de la Base de Hechos



Fuente: Autoría Propia

- ***Base de conocimiento:*** Contiene las experiencias introducidas por el experto, se representa mediante reglas.

If <premisa > then <conclusión >

Las reglas componen la base de conocimiento, las mismas que se relacionan proporcionando lugar a nuevos hechos.

- ***Motor de Inferencia:*** Es el encargado de manejar, controlar y utilizar los conocimientos adquiridos en la base, el paradigma del motor de inferencia es la estrategia utilizada para la producción del conocimiento demandado.

Visión Artificial.- Se puede definir la "Visión Artificial" como parte de la "Inteligencia Artificial" (IA) que, por medio de la utilización de técnicas, permiten a las maquinas ver, identificar y procesar las imágenes de la misma manera que lo hiciera un ser humano, en la actualidad se está utilizando esta tecnología en vehículos autónomos, reconocimiento facial, atención sanitaria, pues las ventajas que presentan son muy superiores a otras tecnologías (Centro de la formación técnica para la industria, 2021).

Sus principales usos dentro de la seguridad:

- ***Videovigilancia:*** Se lo aplica la visión artificial en la vigilancia de espacios, tanto abiertos como cerrados, lo que nos permite tener sistemas de video vigilancia inteligentes los cuales son capaces de detectar y alertar comportamientos anormales.

- ***Control de acceso:*** Es la capacidad de reconocer a las personas para permitir o no el ingreso a un determinado lugar, para esto se encuentra técnicas como el reconocimiento facial y el reconocimiento de iris.

Reconocimiento facial.- Es la capacidad de identificar o verificar a una persona por medio de una imagen, video o cualquier medio audiovisual de su rostro, es una forma de identificación biométrica se lo puede utilizar en: desbloqueo de teléfonos celulares, acceso a servicios online, acceso a inmuebles, etc. (Pascual, 2019).

Métodos de reconocimiento facial.- Uno de los factores prioritarios para la identificación de los rostros es la calidad de la imagen, lo que permitirá que el algoritmo funcione de mejor manera, el algoritmo tiene que tener en cuenta otros factores con los cuales se dificulta el proceso de detección como son: estado anímico de la persona, ubicación del rostro, accesorios (lentes, barba, gorros, mascarillas, etc.), condiciones lumínicas y cantidad desconocida de caras en la imagen (López Pérez & Toro Agudelo, 2017).

En la actualidad existen varios métodos para la detección de rostros como son:

- ***Métodos basados en rasgos faciales:*** Para la identificación la imagen se procesa y se extrae los rasgos faciales como los ojos, boca o nariz, se calcula las relaciones geométricas entre los puntos faciales para la obtención de un vector (García, 2019).
- ***Métodos basados en la imagen:*** En este método se aplica diversos algoritmos para de reconocimiento de patrones para la generación de un modelo a partir de un grupo de fotografías de entrenamiento, se trabaja con las fotografías de forma completa o parcial, en la cual no se buscan rasgos faciales de forma localizada.

OpenCV (Open Source Computer Vision Library).- Es una biblioteca de código abierto que brinda funciones y algoritmos para la utilización de visión artificial, procesamiento de imágenes y algoritmos numéricos, proporciona herramientas para el procesamiento de imágenes incluyendo el reconociendo de objetos en fotografías y videos (caras, figuras de personas, textos, etc.) (Svitla Team, 2019), esta biblioteca incorpora 3 métodos con los que se puede realizar reconocimiento facial como son:

- ***EigenFaces.*** Es una técnica que determina, mediante la ortogonalidad dimensional, identifica que vectores brindan más información a un grupo de datos de dimensión N, el reconocimiento se realiza proyectando la imagen del rostro en el subespacio formado por eigenface y comparando la posición con los rostros conocidos (Esparza Franco, Tarazona Ospina, Sanabria Cuevas, & Velazco Capacho, 2015).

- ***FisherFaces.*** Es un método que se encarga del reconocimiento de rostros, teniendo en cuenta como refleja la luz y las expresiones faciales (Tesillo, 2016)
- ***Local Binary Patterns Histograms (LBPH).*** Se basa en la comparación directa de imágenes, extrayendo características importantes de cada imagen. (Tesillo, 2016)

Rasberry Pi .- Es un ordenador de bajo costo y de reducido tamaño de porte de una tarjeta de crédito, que puede ser conectado a un monitor o un televisor, se puede utilizar con periféricos estándar (ratón y teclado). Es un ordenador capaz de correr sistemas operativos de distribuciones de Linux (Raspberry Pi Documentation , s.f.).

FireBase .- Según Miguh Ruiz (Ruiz M. , 2017) define como un conjunto de herramientas orientadas a la creación de aplicaciones de alta calidad. Se describe la plataforma como una suite de diferentes aplicaciones que harán más fácil el desarrollo de las aplicaciones. Firebase permite programar aplicaciones compatibles con Android, iOS, Java Script, Node JS.

Firebase Cloud Messaging.- Es una herramienta multiplataforma de mensajería que permite enviar mensajes de forma segura, con la que se puede reemitir mensajes de notificaciones (Developers, Google, s.f.).

Firebase Realtime Database .- Se define como una base de datos NoSql alojada en la nube, los datos se encentran almacenados en formato JSON y se sincronizan en tiempo real (Developers, Google, s.f.).

Evidencia digital.- Es un registro de información almacenado o distribuido a través de sistemas informáticos que pueden ser utilizados como pruebas en un proceso legal. Es cualquier tipo de información digital que puede relacionarse con un delito con su víctima o el autor del mismo. Para que una evidencia sea válida debe cumplir con varios principios como son: admisible, auténtica, completa, confiable y creíble (Ochoa, 2018).

Trabajos Relacionados

En el año 2015, se realizó una investigación que tuvo como objetivo el desarrollar un prototipo de un sistema de seguridad para los automóviles, el mismo que se basa en la identificación facial del dueño del vehículo y de quienes están autorizados para su uso, para el reconocimiento emplearon la técnica de Análisis de Componentes Principales (PCA), el cual obtiene e identifica las características faciales más importantes de la imagen capturada, que posteriormente será comparada con las características

de los usuarios autorizados y determinar si la persona está registrada para la utilización del vehículo, al finalizar, se concluyó que el nivel de confiabilidad del sistema se ve comprometido ya que la iluminación afecta los resultados pues estos durante el día tiene una confiabilidad del 71,45 % y durante la noche tiene 65,84% (Amaya Arcos, 2015).

En el año 2016, se aplicó una investigación que tuvo como objetivo principal el desarrollo de un sistema control de seguridad biométrico de reconocimiento facial para el ingreso y egreso a la Área Administrativa de la Facultad de Ingeniería de la UCSG, el mismo que utilizó dos herramientas y una librería OpenCV que permite la detección de rostros bajo la aplicación de la técnica Haar y el uso del API Kairos. Se obtuvo como conclusión que la utilización que del sistema de detección es ventajoso debido a la veracidad de un registro detallado, de igual forma se pudo visualizar que se solventó situaciones tales como robos, hurtos, infiltraciones, etc.; llevando un control de registros de personas que frecuentan el lugar (Solis Calvopiña & Puga Torres, 2016).

En el año de 2019, una investigación realizada tuvo como finalidad el desarrollo de un sistema de reconocimiento facial el cual permitió el control de acceso a los domicilios, con la utilización de una innovadora metodología de reconocimiento facial-Eigen-faces junto al PCA, ya que presentaba una baja complejidad computacional y su poca utilización de recursos de la imagen lo que presenta una respuesta óptima, se realizaron pruebas en diversos escenarios tanto con luz artificial como con luz natural también lo realizaron con accesorio: gafas, gorras, aretes y pañoletas. El reconocimiento fue de un 97% preciso (Casteño Saavedra, 2019).

Metodología

La presente investigación se ha fundamentado en los siguientes pasos:

- ***Levantamiento de requerimientos:*** Determinación de los requerimientos funcionales y no funcionales del sistema de seguridad domiciliaria con reconocimiento facial.
- ***Diseño:*** En base los requerimientos funcionales y no funcionales se determinan las características del sistema, acorde a las capacidades y características del hardware. El diseño considera: detección de movimiento y apertura de puertas, reconocimiento facial, interface de usuario, base datos alojada en la nube con sincronización y envío de notificaciones en tiempo real, con arquitectura de hardware centralizada y software cliente – servidor.
- ***Codificación:*** El sistema de seguridad se encuentra dividido en 2 componentes:

- Software para detección de movimientos, apertura de puertas y reconocimiento facial, perteneciente a la placa de desarrollo Rasberry Pi 3.
- Aplicativo móvil (Android) para el control del sistema de seguridad.

- ***Pruebas:*** Aplicación de pruebas simultaneas a nivel de software y hardware, comprobando la operatividad del proyecto y tomando en consideración el tiempo de respuesta ante las aperturas de las puertas y su notificación a los dispositivos, para la detección de los movimientos se consideran diversos ambientes para medición de la eficiencia en la detección, el reconocimiento facial toma en cuenta la distancia y la identificación mediante la utilización de 3 métodos; y, por último la validación del aplicativo móvil, instalando en los diversos dispositivos Android de los residentes de la vivienda, midiendo la facilidad de uso de la aplicación.

Resultados

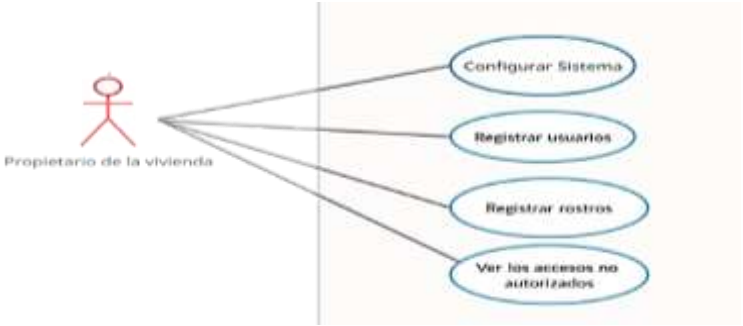
Etapa de requerimientos

Para la recopilación de los requerimientos se ha tomado como modelo una vivienda tradicional estándar ubicada en el Barrio Corazón de María, Provincia del Azuay, Cantón Cuenca, posee dos plantas de construcción, acceso de puerta de garaje en la que se incluye un ingreso peatonal, es así que el portón de ingreso de la vivienda contiene dos puertas adicionales de acceso.

Por ser una zona residencial antigua principalmente sus residentes son adultos mayores que generalmente se encuentran solos en sus residencias, lo cual los convierte en un grupo de riesgo.

Para determinar los requerimientos del sistema se inicia con el diseño de un diagrama de caso de uso que muestra el rol del propietario frente al sistema de seguridad, ver ilustración 2.

Ilustración 2: Caso de uso del propietario

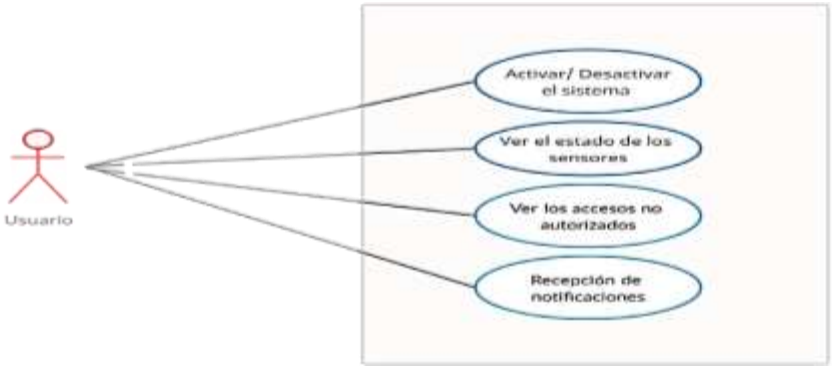


Fuente: Autoría Propia

Propietario de la vivienda. El responsable de implementar, configurar, registrar el sistema de seguridad.

A continuación, la ilustración 3, expone mediante un diagrama de casos de uso el rol del usuario frente al sistema de seguridad.

Ilustración 3: Caso de uso del usuario



Fuente: Autoría Propia

Usuario: Puede activar o desactivar el sistema, constatar el estado de los sensores y la recepcion de notificaciones en tiempo real.

Requerimientos funcionales.- "Son declaraciones de los servicios que debe proporcionar el sistema, de la manera en que éste debe reaccionar a entradas particulares y de cómo se debe comportar en situaciones particulares" (Sommerville, 2005).

Tabla 1: Requerimiento de seguridad

Nombre	Alerta de seguridad.
Descripción	Detectará la apertura de puertas y movimientos en las áreas protegidas.
Entrada	Sensores de puertas y detectores de movimiento.
Salida	Notificaciones en tiempo real.

Fuente: Autoría Propia

Tabla 2: Identificación de personas

Nombre	Reconocimiento facial.
Descripción	Se identificará a las personas que ingrese a la vivienda.
Entrada	Rasberry Pi 3
Salida	Notificaciones en tiempo real de ingreso de persona no identificada.

Fuente: Autoría Propia

Tabla 3: Interface de Usuario

Nombre	Aplicativo móvil.
Descripción	Los usuarios podrán acceder a la información del domicilio mediante la aplicación móvil (Android).
Entrada	Proporcionar una aplicación móvil acorde a la casa modelo.
Salida	Acceder a la información a través de la aplicación.

Fuente: Autoría Propia

Requerimientos no funcionales.- "Como indica su nombre, son requerimientos que no se relacionan directamente con los servicios específicos que el sistema entrega a sus usuarios. Pueden relacionarse con propiedades emergentes del sistema, como fiabilidad, tiempo de respuesta y uso de almacenamiento" (Sommerville, 2005). Estos aspectos están relacionados con factores externos sobre los que no se tiene control directo.

Tabla 4: Compatibilidad

Nombre	Versión del sistema operativo Android
Descripción	El Aplicativo móvil se encuentra desarrollado para dispositivos Android, que cuenten con versión 5.0 (Lollipop) o superior.
Tipo	Compatibilidad.
Prioridad	Alta.

Fuente: Autoría Propia

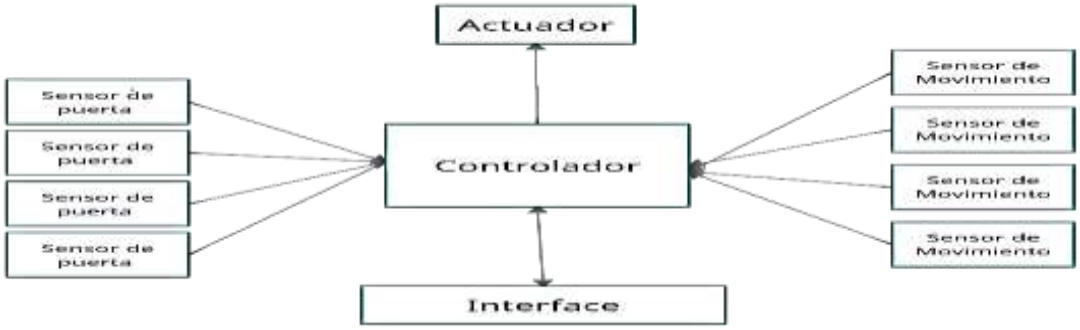
Etapa de diseño

Teniendo en cuenta los requerimientos establecidos para la detección a través de los sensores se ha procedido a elaborar un diseño bajo las características mencionadas a continuación:

- Características del sistema.- El proyecto consiste en el diseño de un Sistema de Seguridad Domiciliario de bajo costo basado en:
- Detección de movimiento y apertura de puertas.
- Reconocimiento facial.
- Interface de usuario (Aplicativo móvil) desarrollada en Android Studio.
- Una base datos alojada en la nube con sincronización en tiempo real.
- Envió de notificaciones en tiempo real.

Arquitectura del hardware. Arquitectura centralizada, que es un sistema que consta de un controlador, en vía la información a los actuadores e interfaces, de igual forma recibe la información de los sensores como se puede observar en la ilustración 4.

Ilustración 4: Arquitectura de hardware

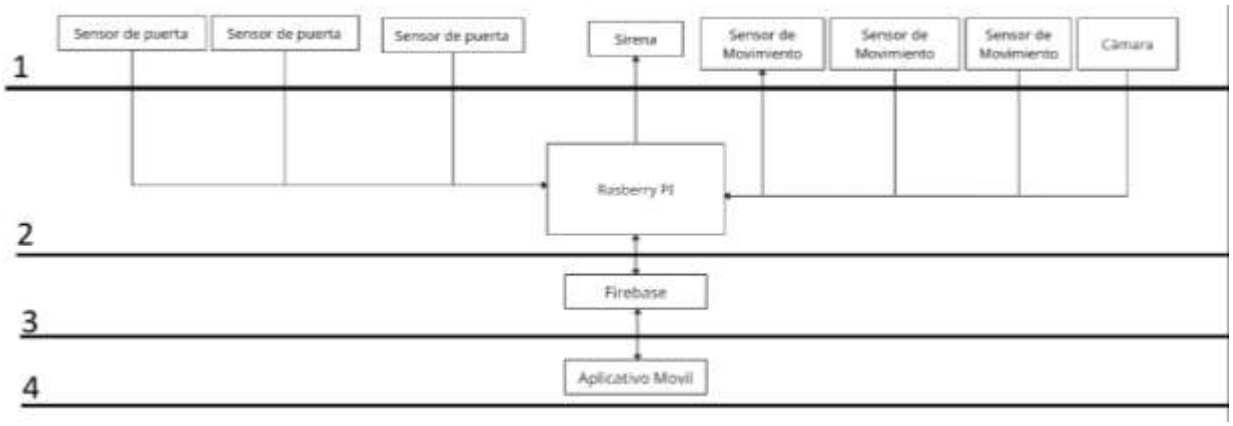


Fuente: Autoría Propia

Descripción de bloques funcionales hardware.- Para un correcto funcionamiento del sistema, el hardware se encuentra dividido en varios bloques, como muestra la ilustración 5, en el primer bloque se encuentran los sensores de movimiento, apertura de puertas, cámara web y actuadores (sirena) instalados en lugares estratégicos dentro de la vivienda y conectados con el segundo bloque que corresponde a la placa de desarrollo Rasberry Pi 3, siendo ésta la encargada de procesar las señales recibidas, enviar las notificaciones y realizar la actualización del estado de los sensores, atreves de la tercera sección.

En el último bloque se ubica la interface de usuario (Aplicativo Móvil) en el que se ve reflejado el estatus de los sensores, la recepción de las notificaciones y la visualización de las fotografías captadas.

Ilustración 5: Bloques funcionales

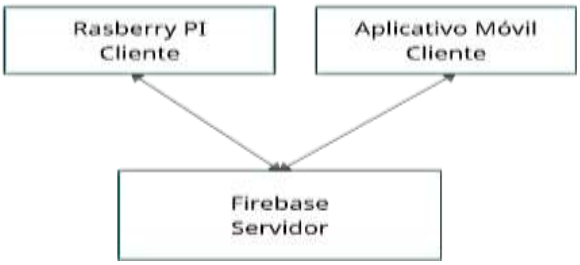


Fuente: Autoría Propia

Arquitectura del Software.- Arquitectura Cliente – Servidor, que es un modelo de aplicación distribuida en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados servidores y los demandantes, llamados clientes. Las aplicaciones Clientes realizan peticiones al Servidor. (Marini, 2012).

Las aplicaciones se han desarrollado bajo esta arquitectura, las tareas que realiza el sistema se reparten entre los diversos recursos provistos por Firebase, como se puede observar en la ilustración 6.

Ilustración 6: Arquitectura Cliente- Servidor



Fuente: Autoría Propia

Etapa de codificación

El sistema de seguridad es encuentra dividido en 2 componentes: el software que recopila la información del reconocimiento facial, detección de apertura de puertas, movimientos y el aplicativo móvil .

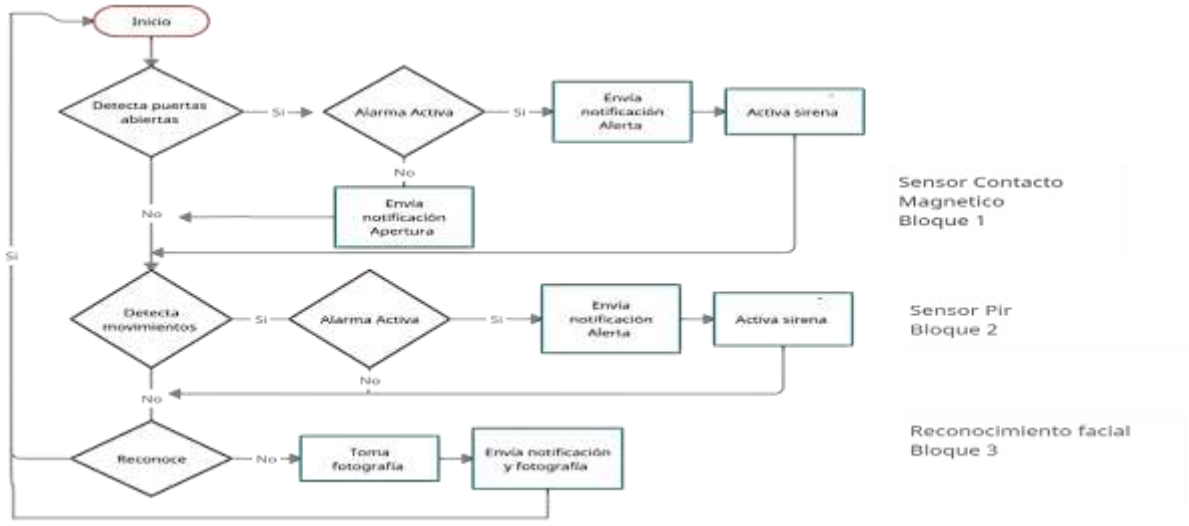
Desarrollo de aplicación para la detección de movimiento, apertura de puertas y reconocimiento facial.- Su desarrollo considera dos etapas: La primera etapa es la Interface para el ingreso de nuevos reconocimientos faciales (Ilustración 7) en la cual se fotografía a la persona autorizada para el ingreso, el mismo que fue desarrollado en Python en su versión 3.7.3. y la utilización de la librería OpenCv, que se encarga de la captura de las fotografías y el reconocimiento.

Ilustración 7: Agregar rostros autorizados

Fuente: Autoría Propia

En la segunda etapa se consideran 3 bloques, en el primer bloque como se puede observar en la ilustración 8 se encuentra la detección de la apertura de las puertas y actualización del estado de puertas (Firebase Realtime Database), el sistema comprueba la información entregada por los sensores, siendo "0" que la puerta se encuentra cerrada y un "1" si la puerta se encuentra abierta, en el segundo bloque se encuentran los detectores de movimiento (sensor PIR) que al detectar movimiento darán un pulso en alto "1" actualizando el estado. Si en los bloques 1 o 2 se activan los sensores magnéticos (apertura de puertas), o detectan movimiento estando el sistema activo, éste envía las notificaciones de alerta pertinentes por medio de Firebase Cloud Messaging; en el tercer bloque, se encuentra el reconocimiento facial, cuando una persona ingresa a la vivienda y no es reconocida, se almacena la fotografía en Firebase Storage e inmediatamente envía la notificación y fotografía a los dispositivos móviles.

Ilustración 8: Diagrama de procesos detención y reconocimiento



Fuente: Autoría Propia

Desarrollo de aplicación Móvil.- Aplicativo móvil que permite al usuario interactuar con el sistema, es decir activar o desactivar el sistema, acceso a ver el status de las puertas o si existe algún movimiento dentro de la vivienda como se puede observar en la ilustración 9, siempre y cuando el usuario este autentificado. Para esta etapa se ha utilizado el servicio de Firebase Realtime Database que corresponde a la información subida por los sensores (Hardware).

Ilustración 9: Estado de alarma desactivado y activado

Fuente: Autoría Propia

Cuando el aplicativo móvil este corriendo en segundo plano mostrará las notificaciones como se observa en la ilustración 10, cuando exista la apertura de puertas o detección movimiento.

Ilustración 10: Notificaciones

Fuente: Autoría Propia

Los usuarios pueden acceder a las fotografías de las personas no identificadas por el sistema en el apartado de fotografías (Ilustración 11), pueden ser descargadas y usadas como evidencia en caso de denuncia de un delito, como se puede observar en la ilustración 12.

Ilustración 11: Fotografías

Fuente: Autoría Propia

Ilustración 12: Fotografía de evidencia

Fuente: Autoría Propia

Etapa de pruebas

La toma de información se realizó por medio de la observación en tres áreas, la primera de ellas en un periodo de tiempo de 72 horas se tomó el tiempo de reacción entre la apertura de la puerta y la llegada de la notificación, la segunda se realizó con los sensores de movimientos se tomó 25 muestras en cada locación y la tercera se realizó en forma controlada, pues la toma del reconocimiento facial se realiza en tiempo real. El primer estadístico se obtuvo al registrar el número de aperturas de puertas y su registro, su detección y envío de notificaciones, la certeza fue alta debido a la simplicidad de sensor, para el segundo se registraron las detecciones de movimiento al circular por el domicilio y al igual que en el caso anterior, la certeza es alta, pese que hay puntos ciegos, pero que por la ubicación de los detectores de movimiento en algún momento los registraron hasta llegar a esa ubicación. La tercera toma de información se la realizó de forma controlada, pues se tenía que determinar las distancias a las que la cámara lograba un reconocimiento. Las técnicas usadas fueron tres LBPHFaceRecognizer, Eigenfaces y FisherFace. Pertenecientes a la librería utilizada (OpenCV).

Apertura de puertas.- En la apertura de puertas por tratarse de un sensor magnético de contacto de alta confiablidad la prueba demostró un resultado del 100% de confiabilidad con un tiempo máximo de 3.3 segundos como tiempo de reacción entre la apertura de la puerta y la llegada de la notificación al dispositivo.

Tabla 5: Resultado de apertura de puertas

Puertas	Dia 1	Día 2	Día 3	Tiempo de reacción	Notificaciones recibidas	Porcentaje de fallo	Falsos positivos
Principal	18	22	17	3.3 segundos	57	0%	0
Medio	1	3	2	2.3 segundos	6	0%	0
Calle	18	22	16	2.7 segundos	56	0%	0
Garaje	2	4	2	3.2 segundos	8	0%	0

Fuente: Autoría Propia

Detección de movimiento.- La observación se realizó en una secuencia de 25 muestras en cada espacio físico, con resultados superiores al 80% y en alguna zona siendo el 100% dando un promedio del 90.4%. Este porcentaje permite certificar con un grado de certeza aceptable. Podemos añadir a esta información que la observación se realizó con los sensores por separado, pero por tratarse de áreas cercanas muchos puntos son cubiertos por sensores aledaños lo que maximiza la eficiencia del sistema.

Tabla 6: Resultado de detección de movimientos

Detección de movimiento				
Lugar	**Numero de movimientos**	**Movimientos detectados**	**Movimientos no detectados**	**Porcentaje de certeza**
Sala	25	23	2	92%
Estancia	25	20	5	80%
Cocina	25	24	1	96%
Comedor	25	21	4	84%
Lavandería	25	25	0	100%
Porcentaje de éxito				90.4%

Fuente: Autoría Propia

Reconocimiento Facial.- Tuvo un comportamiento bastante claro, utilizando los tres métodos con los que se realizaron las mediciones, dieron una ineficiencia del 100 % cuando las distancias eran inferiores a los 30 centímetros, una certeza del 100% a partir de los 40 cm hasta aproximadamente los 100 cm, siendo este el rango que más confiabilidad entrega, siendo el método LBPHFaceRecognizer el que mejores resultados presentó, pero las tres reflejan un promedio de confiabilidad de 90.00% con un rango de seguridad entre 81.67 a 96,67%

Tabla 7: Reconocimiento facial

	Distancia	Número de intentos	Válidos	No válidos	Porcentaje de fallo	Porcentaje de aciertos
LBPHFaceRecognizer	40 - 60 cm	20	20	0	0%	100%
	61-100 cm	20	20	0	0%	100%
	101-150 cm	20	18	2	10%	90%
					Promedio	96.67%
EigenFaces	40 - 60 cm	20	20	0	0%	100%
	60-100 cm	20	20	0	0%	100%
	100-150 cm	20	15	5	25%	75%
					Promedio	91.67%
FisherFace	40 - 60 cm	20	18	2	10%	90%
	61-100 cm	20	18	2	10%	90%
	101-150 cm	20	13	7	35%	65%
					Promedio	81.67%

Fuente: Autoría Propia

Aplicativo móvil.- Por tratarse de un prototipo, se envió vía WhatsApp a los usuarios un APK (instalador) y un manual de usuario (PDF) como instructivo para la instalación, su lenguaje sencillo facilita la compresión del mismo, permitiendo a los participantes la instalación sin dificultad y creando un ambiente amigable para el uso de la aplicación.

Existe una absoluta concordancia en el número de notificaciones emitidas y las recibidas en los dispositivos que disponen la aplicación, teniendo una eficiencia total y las personas que probaron la app e interactuaron con ella, expresaron que lo hicieron sin ninguna dificultad y satisfactoriamente, moviéndose entre las diversas opciones del sistema.

Tabla 8: Aplicativo móvil

Aplicativo móvil				
	Login	Activación / Desactivación	Descargar fotografías	Ajustes
Persona 1	✓	✓	✓	✓
Persona 2	✓	✓	✓	✓
Persona 3	✓	✓	✓	✓
Persona 4	✓	✓	✓	✓

Fuente: Autoría Propia

Conclusiones

Al terminar la investigación y haber realizado la implementación y prueba del sistema, se concluye que:

- El rápido crecimiento de robos y hurtos a nivel país crea una necesidad de protección domiciliaria que parten desde alarmas sencillas de apertura y sensores de movimiento, hasta el uso de alarmas más completas.
- Las alarmas disponibles en el mercado no proporcionan evidencia probatoria en el caso del cometimiento de un delito, razón por la cual muchos hechos delictivos quedan en la impunidad.
- Es posible construir eficientes sistemas de seguridad domiciliaria de bajo costo, fácil instalación y que permitan emitir evidencia fotográfica que cumpla los requisitos de la cadena de custodia para procesos legales de denuncia, con un valor de construcción de 105.10 dólares (Mercado libre) .
- Las alarmas domiciliarias de bajo costo construidas en el proyecto proporcionan un grado de eficiencia del 96.67% en reconocimiento facial en un rango de entre 40 a 150 cm., el uso de los sensores magnéticos presenta un 100 % de confiabilidad, los detectores de movimiento una eficiencia del 90.40%, el sistema presenta una eficacia promedio del 97.2%. y proveyeron la información pertinente para el envío de las notificaciones cuando el caso era pertinente.
- La fotografía captada con una resolución 640*360, podrá ser utilizada como ante el presunto delito, ya que cumple con las características de evidencia digital: admisible, auténtica, completa, confiable y creíble .
- La experiencia de realizar este trabajo se traduce haber descubierto un amplio campo de oportunidades de innovación en el campo de la inteligencia artificial pudiendo renovar productos viejos o crear nuevos. La aplicación de los conocimientos del aula más la experimentación e investigación propia se convierten en la herramienta para un futuro emprendimiento.

Agradecimiento

Quiero agradecer a mis padres Galo y Ana, por el apoyo y los consejos que me han brindado durante toda mi vida, a mis hermanas Andrea y Mónica gracias a sus locuras y ocurrencias me ayudaron a salir adelante.

Referencias

1. Alarmas, M. P. (s.f.). Movistar Prosegur Alarmas. Recuperado el 7 de Abril de 2021, de https://blog.prosegur.es/niveles-de-seguridad/
2. Amaya Arcos, A. B. (2015). Sistema alternativo de seguridad vehicular basado en reconocimieto facial. Ambato.
3. Casteño Saavedra, D. L. (2019). Sistema de reconocimiento facial para el control de acceso a viviendas. Bogota.
4. Centro de la formación técnica para la industria. (15 de Mayo de 2021). Aula21. Recuperado el 8 de Mayo de 2021, de https://www.cursosaula21.com/que-es-la-vision-artificial/
5. Developers, Google. (s.f.). Firebase Documentation. Obtenido de https://firebase.google.com/docs/cloud-messaging?hl=es
6. Developers, Google. (s.f.). Realtime Database. Recuperado el 8 de Mayo de 2021, de https://firebase.google.com/docs/database
7. Esparza Franco, C. H., Tarazona Ospina, C., Sanabria Cuevas, E. E., & Velazco Capacho, D. A. (17 de 04 de 2015). Reconocimiento facial basado en eigenfaces, lbhp y fisherfaces en la beagleboard-xm. Bucaramanga, Colombia.
8. Fernández, D. R. (2014). Desarrollode Aplicaciones para Android II. Ministerio de Educación de España.
9. García, G. (15 de Enero de 2019). Naps Tecnología y educación. Obtenido de https://n9.cl/robak
10. Iberdrola. (s.f.). Recuperado el 8 de Mayo de 2021, de https://n9.cl/eq8f5
11. Identification, E. (27 de Julio de 2020). Electronic Identification. Recuperado el 8 de Mayo de 2021, de https://www.electronicid.eu/es/blog/post/como-funciona-reconocimiento-facial/es
12. López Pérez, N., & Toro Agudelo, J. J. (2017). Diseño y implementación de un sistema de seguridad vehicular mediante reconocimiento facial atraves de vision artificial. Cuenca, Ecuador.
13. Marini, E. (2012). El Modelo Cliente/Servidor. Obtenido de https://www.linuxito.com/docs/el-modelo-cliente-servidor.pdf

14. Ochoa, P. (2018). EL TRATAMIENTO DE LA EVIDENCIA DIGITAL, UNA GUÍA PARA SU ADQUISICIÓN. Economia y politica.
15. Pascual, J. A. (24 de Agosto de 2019). Computer Hoy. Recuperado el 8 de Mayo de 2021, de https://computerhoy.com/reportajes/tecnologia/inteligencia-artificial-469917
16. Raspberry Pi Documentation . (s.f.). Raspberrypi. Recuperado el 7 de Diciembre de 2021, de https://www.raspberrypi.org/documentation/usage/gpio/
17. Ruiz, M. (09 de Agosto de 2017). OpenWebinars. Recuperado el 7 de Diciembre de 2020, de https://openwebinars.net/blog/que-es-firebase-de-google/?cv=1
18. Ruiz, M. E. (2004). Sistemas expertos para realización de diagnóstico parálisis facial con electromiografía: parfac. Lima, Peru.
19. Solis Calvopiña, L. N., & Puga Torres, L. R. (2016). Control de Seguridad Biométrico de Reconocimiento Facial como Caso de Estudio Implementación en el Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil. Guayaquil.
20. Sommerville, I. (2005). Ingenieria de Software . En Ian. Madrid: PEARSON ADD.
21. Svitla Team. (12 de Novimbre de 2019). Svitla. Recuperado el 10 de Mayo de 2021, de https://svitla.com/blog/overview-of-modern-computer-vision-tools
22. Tesillo, C. M. (2016). Análisis comparativo de los algoritmos fisherfaces y lbph para el reconocimiento facial en diferentes condiciones de iluminación y pose, Tacna - 2015. Tacta, Peru.
23. Verisure . (s.f.). Verisure Smart Alarms.