



UNIVERSIDAD MAYOR DE SAN SIMÓN
FACULTAD DE CIENCIA Y TECNOLOGÍA
INGENIERIA INFORMÁTICA



**SISTEMA DE VIDEO VIGILANCIA INTELIGENTE PARA LA ALERTA INMEDIATA
ANTE SITUACIONES DE PELIGRO EN EL HOGAR**

Proyecto de Grado Presentado para optar el grado en Ingeniera Informática

Presentado por: Sergio Rodrigo Cárdenas Rivera

Tutor: Jorge Orellana Araoz

COCHABAMBA - BOLIVIA
Diciembre - 2020

Dedicatoria

Dedico con todo mi corazón el presente proyecto a mis padres porque sin ellos no lo hubiera logrado. Su bendición a diario a lo largo de mi vida me protege y me lleva por el camino del bien. Por eso les entrego este trabajo en ofrenda por su paciencia y amor infinito. Los quiero mucho.

Agradecimientos

Agradezco a esta prestigiosa institución por darme una oportunidad más para poder poner en práctica el conocimiento que me ayudaron a descubrir. A mi familia que me impulsa y ayuda a superar todos los obstáculos que se presentan en mi camino sin importar las adversidades. Agradezco también a la vida por todas aquellas personas que por azares del destino llegué a conocer, con las cuales he pasado inolvidables momentos.

Índice general

| | |
|--|------------|
| Dedicatoria | I |
| Agradecimientos | III |
| 1. Introducción | 1 |
| 1.1. Antecedentes | 2 |
| 1.2. Descripción del Problema | 2 |
| 1.2.1. Definición del problema | 2 |
| 1.3. Objetivos del Proyecto | 2 |
| 1.3.1. Objetivo General | 2 |
| 1.3.2. Objetivos Especificos | 3 |
| 1.4. Justificación | 3 |
| 1.5. Alcances y límites | 3 |
| 2. Marco Teórico | 5 |
| 2.1. Sistema de video vigilancia | 5 |
| 2.2. Inteligencia Artificial | 6 |
| 2.3. Machine Learning (Aprendizaje Automático) | 7 |
| 2.3.1. Métodos de Machine Learning | 8 |
| 2.4. Deep Learning (Aprendizaje profundo) | 9 |
| 2.4.1. Redes Neuronales | 9 |
| 2.5. Visión por Computadora | 9 |
| 2.5.1. Aplicaciones | 10 |
| 2.5.2. OpenCV | 10 |
| 2.6. Protocolos de red | 11 |
| 2.6.1. TCP/IP | 11 |
| 2.6.2. HTTP | 11 |
| 2.7. Video Streaming | 12 |
| 2.7.1. Formatos | 12 |
| 2.8. Aplicaciones Móviles | 12 |
| 2.8.1. Android | 12 |
| 2.8.2. Firebase | 12 |
| 2.8.3. Exoplayer | 12 |
| 2.9. Python | 12 |
| 2.10. Metodología de desarrollo Cascada | 12 |

| | |
|--|-----------|
| 3. Seguridad en el hogar | 13 |
| 3.1. Introducción | 13 |
| 3.2. Seguridad | 13 |
| 3.3. Ausencia en el hogar | 13 |
| 3.3.1. Ausencias cotidianas | 14 |
| 3.3.2. Ausencias de termino medio | 14 |
| 3.3.3. Ausencias prolongadas | 14 |
| 3.4. Situaciones de riesgo | 15 |
| 3.4.1. Presencia de intrusos | 15 |
| 3.4.2. Fuego y humo | 15 |
| 3.5. Sistemas de seguridad | 16 |
| 3.5.1. Alarmas | 16 |
| 3.5.2. Sensores | 17 |
| 3.5.3. Cámaras | 17 |
| 4. Inicialización y Planificación | 19 |
| 4.1. Identificación de Requerimientos | 19 |
| 4.2. Identificación de Subsistemas | 19 |
| 4.3. Comunicación de Sistemas | 19 |
| 4.3.1. Sockets | 19 |
| 4.3.2. ExoPlayer | 19 |
| 4.4. Planificación | 19 |
| 5. Implementación | 21 |
| 5.1. Módulo Cámara | 23 |
| 5.1.1. Modelo de clases | 23 |
| 5.1.2. RapsBerricam | 23 |
| 5.1.3. webCam | 23 |
| 5.1.4. captura de frames | 23 |
| 5.1.5. Comunicacion de los nodos | 23 |
| 5.2. Módulo Servidor | 23 |
| 5.2.1. Sockets | 23 |
| 5.2.2. Frames | 23 |
| 5.2.3. HTTP | 23 |
| 5.3. Módulo Cliente - Aplicación Móvil | 23 |
| 5.3.1. Android | 23 |
| 5.3.2. ExoPlayer | 23 |
| 5.3.3. Notificacion FireBase | 23 |
| 5.3.4. Disenio de Interfaz | 23 |
| 5.3.5. Historial de notificaciones | 23 |
| 6. Pruebas | 25 |
| 6.1. Pruebas de integracion | 25 |
| 6.2. Prueba de transmision | 25 |
| 6.3. Prueba de transmision en vivo | 25 |
| 7. Conclusiones | 27 |

| | |
|--|-----------|
| Referencias | 29 |
| Anexos | 30 |
| Anexo A: Manual de instalacion de la camara | 33 |
| Anexo B: Instalación del servidor | 35 |
| Anexo C: Instalación de la aplicación | 37 |

Índice de figuras

| | |
|--|----|
| 2.1. Sistema actual de videovigilancia Fuente: Web | 5 |
| 2.2. Proyección del mercado de la videovigilancia Fuente: MarketsAndMarkets(web) . | 6 |
| 2.3. Campo de acción de la Inteligencia Artificial. Fuente: Web | 7 |
| 2.4. Diferencias entre programación clásica y M.L. Fuente: Deep Learning with Python | 8 |
| 2.5. Neurona artificial Fuente: Web | 9 |
| 2.6. Logotipo de la librería Fuente: Web | 10 |
| 3.1. Ilustración de un ladrón | 14 |
| 3.2. Ilustración de un ladrón | 15 |
| 3.3. Ilustración de un ladrón | 15 |
| 3.4. Ilustración de un ladrón | 16 |
| 3.5. Ilustración de un ladrón | 17 |
| 3.6. Ilustración de un ladrón | 17 |
| 3.7. Ilustración de un ladrón | 17 |
| 3.8. Ilustración de un ladrón | 18 |

Índice de tablas

| | |
|--|----|
| 4.1. Título de la tabla | 19 |
| 5.1. Titulo de tabla multipágina | 21 |

Capítulo 1

Introducción

Seguridad es un término usado para referirse a la ausencia de riesgo o a la confianza en algo o alguien; pero este panorama toma diversos sentidos según el campo en el que se referencia la seguridad. Aunque su objetivo consista en reducir el riesgo a niveles aceptables, el mismo es inherente a cualquier actividad o situación y nunca podrá ser eliminado.

Desde la aparición del hombre sobre la faz de la Tierra siempre prevaleció su instinto de supervivencia surgiendo la necesidad de obtener y brindar seguridad ante cualquier peligro que ponga en riesgo su integridad física y la de sus seres más cercanos. Cuando las primeras sociedades se formaron, una de las principales tareas del estado fue administrar justicia y brindar seguridad. Por estas razones surge la necesidad de obtener o ofrecer seguridad para minimizar los riesgos ante cualquier peligro.

En el ámbito de la seguridad, la video vigilancia llega a ser el acto de observar una escena o escenas en busca de comportamientos específicos que podrían ser anormales o podrían indicar una posible emergencia o la existencia de un comportamiento impropio (Norman, 2017). Los sistemas de video vigilancia de la actualidad se han convertido en una herramienta esencial de la seguridad para mantener “observado” un espacio muy importante para el que requiere el sistema; donde el mismo esta compuesto por un conjunto de cámaras, monitores y grabadoras donde estos elementos forman parte esencial del sistema. Estos sistemas pueden ser instalados tanto en interiores como en exteriores de una propiedad o establecimiento especialmente en lugares que se desea mantener una vigilancia constante.

La tecnología actual ha permitido automatizar la mayoría de las tareas que los humanos realizan y la video vigilancia no es la excepción. Con los continuos avances tecnológicos cada vez se desarrollan sistemas más robustos y avanzados, permitiendo incrementar su eficacia y confiabilidad; por ejemplo la capacidad de poder vigilar en la oscuridad gracias a la tecnología de visión nocturna. Pero el campo más fascinante dentro de estos avances es el de la Inteligencia Artificial y específicamente la rama de la “Visión por Computadora”. Gracias a las técnicas utilizadas en este campo de investigación una computadora con el apoyo de redes neuronales tiene la capacidad de identificar objetos, siluetas y/o elementos dentro de una escena captada por una cámara.

Estas nuevas capacidades pueden ser explotadas en un sin fin de actividades diarias donde necesaria la supervision del ojo humano permitiendo aún más una automatización inminente. Un rápido uso de estos avances se ven en el campo de la seguridad, específicamente en los sistemas de video

vigilancia permitiendo un reconocimiento de los elementos que se encuentran en una escena de forma automática. El problema a afrontar a partir de este punto es evaluar si lo que esta siendo identificado en una escena representa un peligro para las personas.

1.1. Antecedentes

En la actualidad es común que empresas e instituciones tengan instalados sistemas de seguridad en sus ambientes como ser: oficinas, sitios de producción, almacenes, entradas, recepción, etc. pero realmente no solo las empresas tienen algún riesgo de situación de peligro o robo, si no también las personas en sus respectivos hogares.

Con el continuo crecimiento del mercado de la seguridad, el precio de los equipos de video vigilancia tendieron a decrecer. Este hecho asociado con el incremento de la inseguridad independientemente de cada país, promueve los siguientes escenarios: un incremento en el uso de sistemas de video vigilancia, sistemas con varias cámaras funcionando al mismo tiempo siendo monitoreadas solo por un usuario el cual no esta disponible todo el tiempo y la no capacidad de estos sistemas en el reconocimiento de elementos en una escena para su análisis de forma automática.

1.2. Descripción del Problema

Cuando el responsable de una casa esta ausente, nadie esta vigilando su hogar de manera que la preocupación de que esté todo normal en su hogar esta presente. Si en el peor de los casos llegase a ocurrir algo en su hogar, esta persona solo se enteraria si algún vecino se comunica con él para avisarle lo sucedido o enterarse directamente a su regreso. Un sistema de video vigilancia con la capacidad de identificar movimiento y situaciones de peligro como ser: presencia de intrusos, fuego y humo; podria disminuir los daños efectuados por las situaciones descritas por medio de una acción inmediata por parte del usuario a partir de una notificación inmediata y una visualización en tiempo real de lo que estan captando las cámaras.

1.2.1. Definición del problema

Dificultad para advertir de forma inmediata situaciones de peligro en el hogar.

1.3. Objetivos del Proyecto

A continuación se presentan el objetivo general y los objetivos específicos.

1.3.1. Objetivo General

Facilitar la alerta inmediata ante situaciones de peligro en el hogar por medio de un sistema de video-vigilancia inteligente.

1.3.2. Objetivos Especificos

1. Describir todos los factores que implican el proceso de transmisión de datos por la red.
2. Especificar el proceso de análisis y procesamiento de imágenes con inteligencia artificial.
3. Proveer una red neuronal para el reconocimiento y análisis de video.
4. Identificar las partes que conforman el proceso de transmisión de video.
5. Describir medios para la interacción entre la transmisión y el análisis de imágenes.
6. Proveer el medio de acceso y notificación entre el sistema y el usuario.

1.4. Justificación

El riesgo de que un suceso ponga en peligro la integridad física y material de las personas esta presente cada día y en cualquier lugar. A pesar de que esta posibilidad es imposible de eliminar, se puede buscar mecanismos para poder contrarrestar el impacto que pueden ocasionar dichos sucesos donde queremos evitarlos. Las situaciones más comunes que representan un peligro para la integridad física y material del hogar son: la presencia de intrusos en ausencia del encargado del hogar y la presencia de fuego y/o humo en el interior y/o exterior del hogar.

Los sistemas de video vigilancia permiten visualizar en tiempo real lo que las cámaras estan captando, pero se necesita de una persona que revise constantemente dicha transmisión para poder identificar y alertar sobre las situaciones que se acaban de describir. Si la cantidad de cámaras es considerable la eficacia del operador del sistema disminuye al tener que revisar la transmisión de varias cámaras. Aprovechando la tecnología actual se plantea la implementación de un prototipo de sistema de video vigilancia inteligente que permita retransmitir de manera remota lo que estan captando las cámaras, alertando al usuario sobre los sucesos antes descritos, despues de ser identificados por medio de técnicas de visión por computadora y redes neuronales, para poder actuar disminuyendo el impacto de estos sucesos en el hogar.

1.5. Alcances y límites

- El servicio de transmisión en vivo será implementado en un servidor en línea.
- Se desarrollara un aplicación móvil para la notificación de alguna situación de peligro.
- Se identificará: fuego, humo, personas no identificadas, y acciones violentas.
- Será posible poder ver en vivo lo que se esta trasmitiendo desde el hogar.
- Se procesará el video para reconocer situaciones de peligro.
- Se proveerá una red neuronal para procesar imágenes.

Capítulo 2

Marco Teórico

2.1. Sistema de video vigilancia

La videovigilancia consiste en la instalación de cámaras de vídeo que sirven como grabadoras, las cuales guardan su contenido en un almacén digital el cual puede ser visto en un monitor central. Un sistema de video vigilancia consiste en una instalación de seguridad cuya finalidad es el control y supervisión visual en tiempo real de instalaciones locales y remotas, mediante el uso de múltiples cámaras de vigilancia, así como de sistemas de visualización, grabación y archivo. Estos sistemas ayudan a proteger a las personas, bienes y recursos, mantienen una alerta activa y poseen un gran efecto disuasorio (Wikipedia, 2020).

El sistema captura imágenes y vídeos, que pueden ser comprimidos, almacenados, o enviados por una red de comunicación y pueden ser instalados en cualquier ambiente. En la figura 2.1 se visualiza el conjunto de elementos que forman un sistema de video vigilancia. Este sistema compone de un conjunto de cámaras que estan conectados directamente a un (NVR - Network Video Recorder) grabador de video en red, el cual permite la visualización de lo que las cámaras estan captando en un monitor local y por medio de una conexión a un punto de acceso a internet, permite la visualización de esta transmisión en dispositivos externos a la red local



Figura 2.1: Sistema actual de videovigilancia

Fuente: Web

La creciente demanda en el mercado de la vigilancia ha reducido costos en este tipo de sistemas, lo cual permitió que desarrolladores y fabricantes diseñen nuevas implementaciones de sistemas de video vigilancia agregándoles diversas capacidades dependiendo de la tecnología utilizada en su

desarrollo. En la figura 2.2 se muestra como el mercado global de la video vigilancia fue avaluado en 42.9 billones de dólares en 2019 y esta proyectado alcanzar a los 69.1 billones de dólares hasta el 2026, registrando una tasa de crecimiento anual compuesta del 10 % desde el 2020 al 2026. (MarketsAndMarkets, 2020)



Figura 2.2: Proyección del mercado de la videovigilancia

Fuente: MarketsAndMarkets(web)

El aspecto más importante a resaltar en el mercado de la videovigilancia es la potenciación de funcionalidades de estos sistemas gracias a la Inteligencia Artificial (I.A.) y la escalabilidad por servicios basados en la nube. Las ramas de inteligencia artificial como el Machine Learning(Aprendizaje Automático) y el Deep Learning(Aprendizaje profundo) permitiran potenciar las capacidades de este tipo de sistemas.

Para el desarrollo del prototipo propuesto se implementan todos los componentes involucrados en el sistema de videovigilancia como ser:

- Cámaras (Nodos)
- Servidor TCP
- Servidor Web
- Aplicación Movil (Cliente)

A continuación se detalla los componentes que forman parte del prototipo del sistema de video vigilancia inteligente propuesto.

2.2. Inteligencia Artificial

La Inteligencia Artificial (I.A.), es una tecnología innovadora que en los últimos tiempos no esta reservado solo para la investigación si no más bien ha ido formando parte en el desarrollo de la sociedad. El cerebro es el órgano más increíble del cuerpo humano; establece la forma en la que

percibimos las imágenes, sonido, olores, sabores y el tacto; por lo tanto permite al ser humano almacenar recuerdos, experimentar emociones e incluso soñar. Sin él, el ser humano sería un organismo primitivo, incapaz de otra cosa que el más simple de los reflejos. Por lo tanto el cerebro es lo que hace a este ser, un ser inteligente.

Durante décadas se ha investigado para construir máquinas inteligentes con cerebros como el del ser humano; asistentes robotizados para limpiar los hogares, coches que se conducen por solos, microscopios que detecten enfermedades automáticamente. Pero en la construcción de estas máquinas artificialmente inteligentes se presentan problemas computacionales complejos; problemas que el cerebro humano puede resolver en una fracción de segundos. Las formas de analizar y resolver este tipo de problemas, es el campo de estudio de la Inteligencia Artificial.

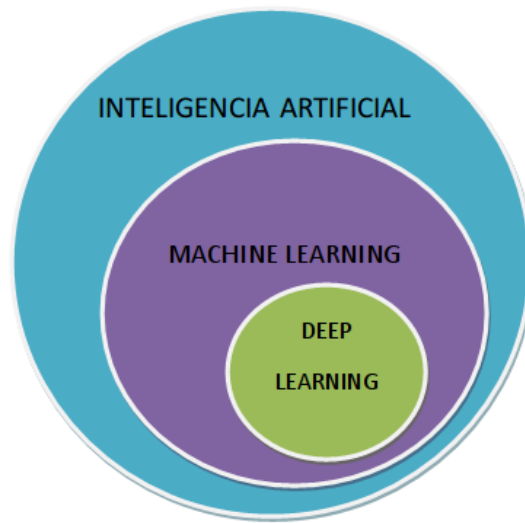


Figura 2.3: Campo de acción de la Inteligencia Artificial.
Fuente: Web

A menudo los términos Inteligencia Artificial, Aprendizaje Automático (Machine Learning) y Aprendizaje Profundo (Deep Learning) son usados de manera indistinta, pero se debe tener en cuenta su significado diferente. Por los años '80 la Inteligencia Artificial era una característica que se alcanzaba al definir un conjunto de reglas que decían que hacer en un determinado momento, de esta manera un sistema 'inteligente' solo obedecía reglas de acción programadas (Banda, 2017). En la figura 2.3 se ilustra como la Inteligencia Artificial engloba a sus subcampos de estudio como ser el Machine Learning y el Deep Learning.

2.3. Machine Learning (Aprendizaje Automático)

Es un subcampo de la Inteligencia Artificial cuyo objetivo es entender la estructura de la información y ajustar estos datos en modelos que puedan ser entendidos y utilizados por las personas (Tagliaferri, 2017).

A diferencia de la computación tradicional, donde los algoritmos resuelven problemas específicos, los algoritmos de Machine Learning entrenan a las computadoras con datos de entrada y emplean

análisis estadístico para generar valores de salida que se clasifican según a un rango específico. Por eso el Machine Learning facilita a las computadoras construir modelos a partir de datos ejemplo para automatizar el proceso de toma de decisiones basados en estos datos.

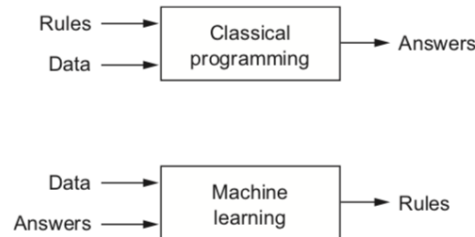


Figura 2.4: Diferencias entre programación clásica y M.L.

Fuente: Deep Learning with Python

En la figura 2.5 se aprecia la diferencia y similitud entre la programación clásica de la inteligencia artificial de los años '80 y las novedosas técnicas del aprendizaje automático. La programación clásica necesita de reglas y datos de entrada para que esta funcione como un sistema inteligente y pueda dar una respuesta, mientras que el Machine Learning necesita de datos y sus respectivas respuestas esperadas, para identificar patrones que los relacionen; y de esta manera permitiendo desarrollar reglas que generarán respuestas para nuevos datos.

2.3.1. Métodos de Machine Learning

En el Machine Learning, las tareas son generalmente clasificadas en grandes categorías, las cuales estan basadas en el modo en el que el “aprendizaje” es ejecutado.

Los métodos más adoptados en el Machine Learning son: el aprendizaje supervisado, que entrena un algoritmo basado en un ejemplo de entrada y salida el cual esta categorizado por un humano, y el aprendizaje no supervisado, que proporciona el algoritmo sin ningún dato categorizado permitiendo encontrar una estructura dentro de los datos de entrada.

Aprendizaje Supervisado

La computadora esta provista con entradas de ejemplo las cuales están categorizadas con sus respectivas salidas esperadas. El propósito de este metodo consiste en que el algoritmo pueda 1 “aprender” comparando la actual salida con las salidas esperadas para encontrar errores y en consecuencia modificar el modelo. El aprendizaje supervisado por lo tanto usa patrones para predecir valores categorizados en datos no categorizados.

Aprendizaje No Supervisado

La información provista a la computadora no está categorizada, por lo que los algoritmos de aprendizaje buscan similitudes entre los datos de entrada. Como los datos no etiquetados son

más abundantes que los datos etiquetados, los métodos de aprendizaje automático que facilitan el “aprendizaje” pasan a ser más importantes.

2.4. Deep Learning (Aprendizaje profundo)

Según la figura 2.3, el aprendizaje profundo es un subcampo dentro del Machine Learning, el cual hace uso de distintas redes neuronales para lograr el “aprendizaje” de sucesivas capas de representación que son relevantes para los datos.

El término Deep “profundo”, hace referencia a la cantidad de capas de representación que se utilizan en un modelo; en general es posible utilizar decenas incluso cientos capas de representación, los cuales aprenden de forma automática a medida que el modelo es entrenado con los datos (Briega, 2015).

2.4.1. Redes Neuronales

Son un modelo computacional basado en un gran número de unidades (neuronas simples), de forma similar de lo que se ha observado en los axones de las neuronas de un cerebro biológico.

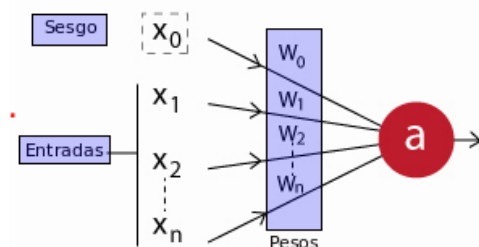


Figura 2.5: Neurona artificial
Fuente: Web

2.5. Visión por Computadora

La visión por computadora es una técnica de recolección de información que surge por la inspiración en el sistema visual humano, el cual es la principal fuente de información para el cerebro. Su meta es de modelar y automatizar el proceso de reconocimiento visual de objetos en la vida real.

De los cinco sentidos que poseen las personas, la vista es la más importante. Por lo tanto la visión, es una tarea de procesamiento de información; pero tiene un grado de complejidad elevado, ya que para saber que es lo que hay en el mundo nuestros cerebros deben ser capaces de representar esta información en toda su abundancia de color, forma, movimiento, detalle y belleza. (Briega, 2015)

Por lo tanto, la visión por computadora o visión artificial compone de un conjunto de herramientas y métodos que permiten obtener, procesar y analizar imágenes del mundo real, con el objetivo de

ser tratadas por una computadora. Estos métodos van a permitir automatizar un amplio conjunto de tareas al aportar a las computadoras información que es necesaria para la toma de decisiones en sus tareas asignadas. La visión por computadora trata de imitar a la visión humana, usando geometría y un enfoque estadístico para tratar el problema.

2.5.1. Aplicaciones

Esta rama de la Inteligencia Artificial aún sigue en investigación y mejoras donde sus aplicaciones más comunes son:

- **Reconocimiento óptico de caracteres:** Detección automática de símbolos que pertenecen a un alfabeto.
- **Inspección robotizada:** Revisión rápida de piezas para garantizar la calidad de componentes fabricados.
- **Modelado 3D:** Construcción de modelos 3D a partir de fotografías.
- **Imágenes médicas:** Análisis de radiografías.
- **Conducción segura:** Detección de obstáculos por medio de un sistema de conducción asistida por cámaras.
- **Vigilancia:** Monitoreo de intrusos, análisis del tráfico vial, monitoreo de piscinas, etc.
- **Detección de rostros:** Mediante algoritmos de reconocimiento facial se reconocen rostros usados en métodos de biometría.

2.5.2. OpenCV

Es una biblioteca de uso libre para el desarrollo de aplicaciones usando visión artificial desarrollada por Intel. Esta librería reúne diversas características que la hacen popular, por ejemplo:

- Permite su uso para fines comerciales y de investigación.
- Se encuentra disponible par varias plataformas como ser GNU/Linux, Mac OS, Windows y Android.
- Documentación completa y explicada, con una comunidad de desarrolladores activa.



Figura 2.6: Logotipo de la librería
Fuente: Web

Esta biblioteca permite:

- El procesamiento de imágenes en su escalado, eliminación de ruido y formateo de imagen y video.
- El uso y modificación de sus 2500 modelos pre-optimizados que son incluidos en la librería, acorde a las necesidades del usuario.
- El uso del estado del arte de modelos de visión por computadora como también de aprendizaje de máquina (Machine Learning).
- El desarrollo de modelos en varias categorías de investigación como ser: reconocimiento facial, detección y seguimiento de objetos, extracción de modelos 3D, etc.

Una de las características mas interesantes de OpenCV es el reconocimiento facial. OpenCV, en su extensa biblioteca de funciones, brinda las capacidades para realizar las tareas de preprocesamiento sin ningún problema, así como los algoritmos de predicción. Además de usar el algoritmo de detección de objetos, es posible usar el seguimiento de objetos, para identificar rostros en una transmisión de video. OpenCV incluso posee funciones para configurar fácilmente el modelo en una transmisión en vivo, como en un video pregrabado (TheResearchNest, 2020).

2.6. Protocolos de red

Un protocolo es un método estándar que permite la comunicación entre procesos (que potencialmente se ejecutan en diferentes equipos) y un conjunto de reglas y procedimientos que deben respetarse para el envío y la recepción de datos a través de una red.

2.6.1. TCP/IP

El Protocolo de Control de Transmisión es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973-1974 por Vint Cerf y Robert Kahn. Este es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). Como es un protocolo orientado a conexión permite que dos máquinas que están comunicadas controlen el estado de la transmisión. Las principales características del protocolo TCP son las siguientes: Da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP, SSH y FTP. Permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.

2.6.2. HTTP

(Protocolo de transferencia de hipertexto) es el protocolo más utilizado en Internet. Es el protocolo usado en cada transacción de la Web (WWW). El propósito del protocolo HTTP es permitir la transferencia de archivos (principalmente, en formato HTML) entre un navegador (el cliente) y un servidor web (denominado, entre otros, http en equipos UNIX). HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición- respuesta

entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante una cadena de caracteres denominada dirección URL. Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

2.7. Video Streaming

2.7.1. Formatos

HLS

DASH

2.8. Aplicaciones Móviles

2.8.1. Android

2.8.2. Firebase

2.8.3. Exoplayer

2.9. Python

Python es un lenguaje de programación interpretado cuya filosofía hace hincapié en la legibilidad de su código. Se trata de un lenguaje multiparadigma, ya que soporta parcialmente la orientación a objetos, programación imperativa y, en menor medida, programación funcional. Es un lenguaje interpretado, dinámico y multiplataforma.

Python usa tipado dinámico y conteo de referencias para la administración de memoria. Una característica importante de Python es la resolución dinámica de nombres; es decir, lo que enlaza un método y un nombre de variable durante la ejecución del programa (también llamado enlace dinámico de métodos).

2.10. Metodología de desarrollo Cascada

Capítulo 3

Seguridad en el hogar

3.1. Introducción

La seguridad en el hogar es un asunto especialmente sensible y delicado de tratar, principalmente por ser el más sensible de todos los espacios vitales del ser humano. Sea del tipo que sea, en un hogar se fraguan los vínculos más íntimos y personales, contiene a quien más amamos y lo que más deseamos proteger.

La presencia de una persona en el hogar es un factor de seguridad de gran importancia; la mayoría de percances como intrusiones, allanamientos y robos se producen durante su ausencia. Los motivos para dejar un hogar vacío son distintos y variados: desde ausencias prolongadas a salidas más o menos puntuales, o regulares y diarias. Una vivienda vacía es más vulnerable que otra ocupada y esto se debe tomar en cuenta en el diseño de un sistema de seguridad para el hogar que ofrezca las máximas garantías en sus capacidades.

3.2. Seguridad

3.3. Ausencia en el hogar

Evidentemente, incluso las personas más retraídas y amantes de la soledad y el aislamiento deben, en un momento u otro, salir de su residencia habitual, algo que se convierte en largas horas de ausencia en la mayoría de los casos (evidentemente por trabajo, obligaciones académicas y otros menesteres cotidianos), y ocasionalmente, con mayor o menor asiduidad, por otras razones menos frecuentes (viajes, vacaciones, escapadas...).

Hemos tratado de sintetizar estas posibilidades en función del tiempo de ausencia, estableciendo distintos casos con peculiaridades específicas en lo que se refiere a la seguridad y los riesgos que se afrontan, y empezando por exponer las medidas de protección más básicas y elementales que siempre se deberían tomar en consideración, tales como contratar un seguro para la vivienda (especificando algunos elementos importantes que figuran en toda póliza de esta índole para facilitar su elección y contratación).

Referenciando a la figura 3.8.



Figura 3.1: Ilustración de un ladrón

Fuente: Adaptada de Apellido, N. (2000) *Nombre del libro*. Editorial o universidad que lo publicó.

3.3.1. Ausencias cotidianas

El primero de los casos supuestos es el más frecuente y cotidiano: las ausencias diarias de horas o minutos que brindan oportunidades a asaltantes atentos. Aquí, se tendrán en cuenta medidas de protección sencillas y sin complicaciones que cualquiera puede llevar a cabo apenas sin inversión alguna. Asegurar los cierres de los accesos a la vivienda, disimular las ausencias o evitar proporcionar información sobre nuestros hábitos son algunas de las medidas que se exponen para evitar intrusiones no deseadas en el hogar.

Como situación perteneciente a este grupo de supuestos, pero con riesgos añadidos y particularidades propias que obligan a prestarle una atención especial, se tratará aparte el caso de ausencias puntuales dejando en la vivienda a niños, personas mayores o dependientes sin nadie a su cargo. Evidentemente, aquí se tratarán amenazas y riesgos internos de la vivienda, tales como manipulaciones indebidas de instalaciones y componentes de especial peligrosidad, o la atención a emergencias que puedan suceder durante ausencias breves.

3.3.2. Ausencias de termino medio

Al salir de casa debemos saber si volveremos al cabo de pocas horas, de unos días o de semanas, ya que cada caso (como hemos comentado) presenta peculiaridades y riesgos específicos que tenemos que afrontar de distintos modos. El segundo supuesto, tras las ausencias cotidianas, será el caso de ausencias de pocos días, especialmente en fines de semana, puentes festivos y vacaciones cortas.

En estas situaciones convergen la necesidad de contar con alarmas y avisadores técnicos, con la de disponer de sistemas de alarma y dispositivos antiintrusión los cuales, como veremos, pueden ser de muy diversa índole.

3.3.3. Ausencias prolongadas

Las vacaciones y las estancias de cierta duración en lugares alejados de nuestras residencias habituales ofrecen oportunidades únicas a posibles asaltantes. No ofrecer información sobre nuestro paradero, tratar de evitar el efecto de vivienda vacía, contar con la supervisión regular de alguien de confianza en nuestra ausencia y mantener a buen recaudo bienes u objetos de valor serán, en

estos casos, las principales prioridades (sobre todo en el caso de las segundas residencias, una cuestión que también consideraremos detalladamente como caso diferenciado).

3.4. Situaciones de riesgo

3.4.1. Presencia de intrusos

Referenciando a la figura 3.8.



Figura 3.2: Ilustración de un ladrón

Fuente: Adaptada de Apellido, N. (2000) *Nombre del libro*. Editorial o universidad que lo publicó.

3.4.2. Fuego y humo

Referenciando a la figura 3.8.



Figura 3.3: Ilustración de un ladrón

Fuente: Adaptada de Apellido, N. (2000) *Nombre del libro*. Editorial o universidad que lo publicó.

Referenciando a la figura 3.8.



Figura 3.4: Ilustración de un ladrón

Fuente: Adaptada de Apellido, N. (2000) *Nombre del libro*. Editorial o universidad que lo publicó.

3.5. Sistemas de seguridad

En el mercado, existen un sinnúmero de posibilidades al alcance para proteger nuestros hogares frente a casi cualquier tipo de amenaza, tanto interna como externa. Los más eficaces y eficientes, sin duda, son los sistemas electrónicos de seguridad, de los que ya hablamos detalladamente en la guía Hogares y negocios seguros

No obstante, sea cual sea la opción elegida a la hora de proteger nuestra vivienda durante ausencias más o menos prolongadas, debemos tener en cuenta los siguientes riesgos y amenazas:

Allanamientos, intrusiones y vandalismo: riesgos procedentes del exterior, que se pueden mitigar fácilmente instalando cierres de alta seguridad en los accesos a la vivienda, alarmas antiintrusión u otros mecanismos disuasorios.

Accidentes domésticos: riesgos procedentes del interior de hogar que pueden poner en riesgo la integridad física y/o moral de sus habitantes, tanto personas como mascotas, así como los bienes que contienen e incluso la misma infraestructura. Las alarmas técnicas (avisadores de fugas y escapes) y de emergencia son, para estos casos, los sistemas más adecuados para proteger una vivienda. También es preciso tomar las medidas oportunas para proteger los componentes más sensibles del hogar (instalaciones de suministros y otros elementos de riesgo) de manipulaciones indebidas, golpes y otro tipo de percances que pueden ocasionar accidentes o situaciones indeseables.

3.5.1. Alarmas

Referenciando a la figura 3.8.



Figura 3.5: Ilustración de un ladrón

Fuente: Adaptada de Apellido, N. (2000) *Nombre del libro*. Editorial o universidad que lo publicó.

3.5.2. Sensores

Referenciando a la figura 3.8.



Figura 3.6: Ilustración de un ladrón

Fuente: Adaptada de Apellido, N. (2000) *Nombre del libro*. Editorial o universidad que lo publicó.

3.5.3. Cámaras

Referenciando a la figura 3.8.



Figura 3.7: Ilustración de un ladrón

Fuente: Adaptada de Apellido, N. (2000) *Nombre del libro*. Editorial o universidad que lo publicó.

Referenciando a la figura 3.8.



Figura 3.8: Ilustración de un ladrón

Fuente: Adaptada de Apellido, N. (2000) *Nombre del libro*. Editorial o universidad que lo publicó.

Seguridad y vigilancia son aspectos que se requieren en todo el mundo; gobiernos, empresas, instituciones financieras, organizaciones de salud necesitan cierto grado de medidas de seguridad y como resultado se generó un dramático incremento en la demanda de aplicaciones de seguridad como por ejemplo video vigilancia, monitoreo y grabación de: fronteras, puertos, transporte, hogares, corporaciones, instituciones educativas, lugares públicos, edificios, etc.

Sistemas de videovigilancia inteligente La técnica clave del reconocimiento de la acción humana basada en la visión por computadora consiste en describir y comprender los comportamientos humanos por medio de la visión por computadora.

Este proceso es una tarea complicada e integra algunos campos de investigación que incluyen el procesamiento de imagen, aprendizaje automático, reconocimiento de patrones, etc.

La detección de un objeto móvil consiste en separar las áreas de cambio en el video es decir en las imágenes de fondo que comprenden el video, dicho de otra manera, separar correctamente las áreas y contornos del objeto móvil. Es crítico para el siguiente procesamiento la segmentación efectiva

Capítulo 4

Inicialización y Planificación

4.1. Identificación de Requerimientos

Tabla 4.1: Título de la tabla

| | Columna 1 | Columna 2 | Columna 3 |
|--------|-----------|-----------|-----------|
| Fila 1 | item | item | item |
| Fila 2 | item | item | item |
| Fila 3 | item | item | item |

Nota. Extraída de Apellido, N. (2000) *Nombre del libro*. Editorial o universidad que lo publicó.

4.2. Identificación de Subsistemas

4.3. Comunicación de Sistemas

4.3.1. Sockets

4.3.2. ExoPlayer

4.4. Planificación

Capítulo 5

Implementación

Tabla 5.1: Titulo de tabla multipágina

| | Columna 1 | Columna 2 | Columna 3 | Columna 4 |
|--------|--|--|--|--|
| Fila 1 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |
| Fila 2 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |
| Fila 3 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |
| Fila 4 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |
| Fila 5 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |
| Fila 6 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |
| Fila 7 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |

Continúa en la siguiente página.

Tabla 5.1 – Continuación de tabla previa

| | Columna 1 | Columna 2 | Columna 3 | Columna 4 |
|----------------|--|--|--|--|
| Fila 8 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |
| Fila 9 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |
| Fila 10 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |
| Fila 11 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |
| Fila 12 | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. | Lorem ipsum dolor sit amet, consectetur adipiscing elit. |

Nota. Extraída de Apellido, N. (2000) *Nombre del libro*. Editorial o universidad que lo publicó.

5.1. Módulo Cámara

5.1.1. Modelo de clases

5.1.2. RapsBerricam

5.1.3. webCam

5.1.4. captura de frames

5.1.5. Comunicacion de los nodos

5.2. Módulo Servidor

5.2.1. Sockets

5.2.2. Frames

5.2.3. HTTP

5.3. Módulo Cliente - Aplicación Móvil

5.3.1. Android

5.3.2. ExoPlayer

5.3.3. Notificacion FireBase

5.3.4. Disenio de Interfaz

5.3.5. Historial de notificaciones

Capítulo 6

Pruebas

6.1. Pruebas de integracion

6.2. Prueba de transmision

6.3. Prueba de transmision en vivo

Capítulo 7

Conclusiones

Concluimos que...

Referencias

- Banda, H. (2017, Abril). Inteligencia artificial: Principios y aplicaciones. *Research Gate*, 50. Recuperado de https://www.researchgate.net/publication/262487459_Inteligencia_Artificial_Principios_y_Aplicaciones
- Briega, R. E. L. (2015, Septiembre). *Libro online iaar*. Recuperado de <https://iaarbook.github.io/>
- MarketsAndMarkets. (2020, Noviembre). *Video surveillance market with covid-19 impact analysis*. Recuperado de <https://www.marketsandmarkets.com/Market-Reports/video-surveillance-market-645.html>
- Norman, T. L. (2017). Chapter 6 - electronics elements: A detailed discussion originally from integrated security systems design. thomas norman: Butterworth-heinemann, 2015. updated by the editor, elsevier, 2016. , 95-137. Recuperado de <https://www.sciencedirect.com/science/article/pii/B9780128044629000063> doi: <https://doi.org/10.1016/B978-0-12-804462-9.00006-3>
- Tagliaferri, L. (2017, Septiembre). An introduction to machine learning. *Digital Ocean*. Recuperado de <https://www.digitalocean.com/community/tutorials/an-introduction-to-machine-learning>
- TheResearchNest. (2020, Abril). *Computer vision tools and libraries*. Recuperado de <https://medium.com/the-research-nest/computer-vision-tools-and-libraries-52bb34023bdf>
- Wikipedia. (2020, Diciembre). *Videovigilancia ip*. Recuperado de https://es.wikipedia.org/wiki/Videovigilancia_IP

Anexos

Anexo A: Manual de instalacion de la camara

Contenido de Anexo A

Anexo B: Instalación del servidor

Contenido de Anexo B

Anexo C: Instalación de la aplicación

Contenido de Anexo C