Sistemas Operativos

Proyecto:

Detección automática de ingreso de la Universidad Católica del Uruguay

Alumnos:

* Brian Morat
* Agustín Negreira
* Alfonso Rodriguez

Profesores:

* Julio Motañes

2024 – URUGUAY

Implementación de un Sistema de Reconocimiento Facial para Control de Acceso en una Universidad

Para controlar el acceso, hemos integrado la funcionalidad de puertas automáticas que se abren automáticamente para los estudiantes, funcionarios e invitados para que puedan ser reconocidos por el sistema. Los estudiantes y el personal autorizado pueden acceder al campus sin necesidad de interactuar con el personal de seguridad.

En el caso de que una persona no esté registrada en el sistema, nuestro sistema permite al personal de seguridad agregarla manualmente. Esto se logra capturando su rostro y asociándolo con su nombre en la base de datos del sistema.

Nuestro proyecto no solo mejora la seguridad en el campus universitario, sino que también agiliza el proceso de control de acceso y registro de estudiantes y personal. Además, proporciona una solución escalable y eficiente que puede adaptarse a las necesidades de cualquier institución educativa.

Nuestro sistema opera en varias etapas clave:

Detección de Rostros:

Se utilizan hilos para ejecutar de forma paralela la detección de rostros en las imágenes capturadas por la cámara del sistema.

Reconocimiento Facial:

Hilos separados se encargan de realizar el reconocimiento facial de los rostros detectados, comparándolos con los perfiles previamente registrados en la base de datos.

Control de Acceso:

Mediante el diseño de procesos, se coordina el acceso de los estudiantes y personal autorizado a través de las puertas automáticas. Los semáforos se utilizan para evitar condiciones de carrera y garantizar un acceso seguro y ordenado.

Registro de Nuevos Usuarios:

La captura de rostros y el registro de nuevos usuarios se realizan de manera concurrente utilizando hilos, permitiendo un proceso fluido y eficiente.

La utilización de hilos y semáforos en este proyecto ofrece varias ventajas significativas:

1. Paralelismo y concurrencia:

Hilos: Permite ejecutar múltiples tareas simultáneamente, lo que es especialmente útil en un sistema de reconocimiento facial donde se pueden realizar varias operaciones al mismo tiempo, como la captura de imágenes, detección de rostros y reconocimiento facial.

Semáforos: Facilita el control de acceso a recursos compartidos, garantizando que los diferentes procesos se ejecuten de manera ordenada y sin interferencias, evitando condiciones de carrera y asegurando la consistencia de los datos.

1. Mejora de la eficiencia y rendimiento:

Al utilizar hilos, se puede aprovechar al máximo la capacidad de procesamiento de la CPU al realizar múltiples tareas en paralelo, lo que puede conducir a una ejecución más rápida del sistema.

Los semáforos permiten gestionar eficientemente la concurrencia, evitando bloqueos y maximizando la utilización de los recursos del sistema.

1. Respuesta en tiempo real:

El uso de hilos permite que el sistema responda de manera más rápida a eventos externos, como la detección de un rostro o una solicitud de acceso, lo que mejora la experiencia del usuario al reducir los tiempos de espera.

Los semáforos garantizan una gestión eficiente de los recursos compartidos, lo que contribuye a una respuesta más rápida y consistente del sistema.

1. Escalabilidad:

La implementación de hilos y semáforos facilita la escalabilidad del sistema, ya que permite gestionar eficientemente un mayor número de solicitudes de acceso y procesamiento de datos sin comprometer el rendimiento.

Esto es especialmente importante en entornos universitarios donde puede haber un gran número de personas accediendo al sistema simultáneamente.

En resumen, la utilización de hilos y semáforos en este proyecto proporciona una mayor eficiencia, rendimiento y capacidad de respuesta del sistema, lo que contribuye a una experiencia de usuario más fluida y una gestión más eficiente de los recursos del sistema.

Planificación de criterios

Captura de Imágenes:

Criterio de Planificación: Round Robin

Justificación: Dado que la captura de imágenes depende de eventos externos el algoritmo de Round Robin podría ser útil para garantizar un acceso equitativo a todas las cámaras en caso de múltiples solicitudes simultáneas.

Procesamiento de Imágenes:

Criterio de Planificación: SJF (Shortest Job First)

Justificación: Dado que el procesamiento de imágenes puede variar en complejidad según la cantidad de personas presentes y la precisión requerida, el algoritmo SJF podría ser útil para minimizar el tiempo de respuesta al procesar las tareas más cortas primero.

Almacenamiento de Datos:

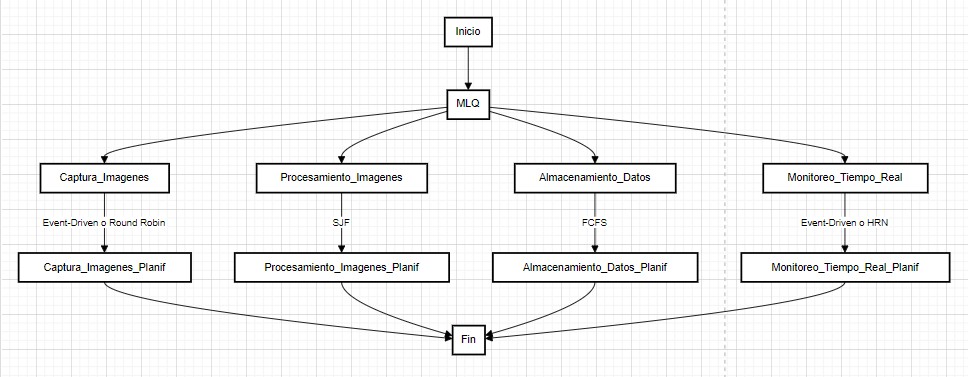
Criterio de Planificación: FCFS (First-Come, First-Served)

Justificación: Ya que el almacenamiento de datos implica acceder a dispositivos de almacenamiento, un enfoque simple como FCFS puede ser adecuado para garantizar un acceso equitativo a los recursos.

Monitoreo en Tiempo Real:

Criterio de Planificación: Event-Driven

Justificación: El monitoreo en tiempo real implica responder a eventos y alertas de manera rápida y eficiente, un enfoque basado en eventos sería apropiado para manejar estas tareas de manera oportuna.



Una identificación preliminar de los recursos y procesos involucrados en la solución.

Recursos físicos:

Como recursos físicos tenemos a las cámaras de seguridad en primer lugar que se necesitaran colocarlas en las entradas y las cámaras PTZ para los pasillos y espacios comunes.

Para el almacenamiento de datos y el procesamiento de las imágenes necesitaremos una sala de servidores con amplio espacio de almacenamiento y estaciones de trabajo, a raíz de tener este factor deberíamos contar con una sala de contingencia por cualquier catástrofe.

Además del almacenamiento en la sala de servidores y en la sala de contingencia el equipo de almacenamiento de coincidir con los videos (HVRs) que permiten la grabación y gestión de imágenes de cámaras IP y analógicas.

Procesos:

Captura de imágenes: Proceso de captura de imágenes faciales por parte de las cámaras instaladas en las entradas, pasillos y espacios comunes.

Procesamiento de imágenes: Análisis de las imágenes capturadas para el reconocimiento facial, que implica comparar las características faciales con una base de datos de personas autorizadas.

Identificación y verificación: Proceso de identificación de personas autorizadas y verificación de su acceso al edificio.

Monitoreo en tiempo real: Supervisión continua de las imágenes de las cámaras y las identificaciones faciales en el centro de monitoreo.

Almacenamiento y gestión de datos: Grabación y almacenamiento de las imágenes capturadas para su posterior revisión y análisis.

Respuesta a eventos: Acciones tomadas en respuesta a eventos detectados, como alertar al personal de seguridad o tomar medidas preventivas.

Priorización de personas embarazadas y/o discapacidades: Acceso VIP al edificio para aquellas personas ya registradas en la base de datos del sistema como personas con acceso exclusivo.

Una descripción de los distintos criterios de optimización que podrían usarse.

Tiempo de Respuesta:

Es crucial garantizar que el sistema responda rápidamente a las solicitudes de acceso para proporcionar una experiencia fluida a los usuarios y minimizar los tiempos de espera en la entrada.

Precisión del Reconocimiento Facial:

La precisión en la identificación de estudiantes y personal autorizado es fundamental para garantizar la seguridad del campus y evitar accesos no autorizados.

Eficiencia en el Uso de Recursos:

Se busca optimizar el uso de recursos del sistema, como la CPU y la memoria, para garantizar un rendimiento óptimo y reducir los costos operativos asociados.

Priorización de eventos y tipos de público:

Implica dar prioridad al procesamiento de ciertos eventos o tipos de público sobre otros. Los criterios de optimización podrían incluir la asignación de recursos adicionales para el reconocimiento de personas VIP o con necesidades especiales, así como la reducción del tiempo de espera para estos grupos

Optimización del uso de recursos:

Distribución equitativa de recursos entre áreas de alto tráfico y bajo tráfico, así como la minimización del consumo de energía.

Seguridad y privacidad de datos:

Implementación de medidas de seguridad robustas, como el cifrado de datos y el control de acceso a los sistemas.

Un ordenamiento justificado de los criterios y una selección de los primeros que el equipo decida optimizar.

Las prioridades de optimización se determinarán en función de su relevancia directa con los objetivos del proyecto. Por lo tanto, daremos prioridad a aquellos aspectos cuya importancia es fundamental para el funcionamiento eficaz del sistema. Dependiendo de su relevancia, estos aspectos ocuparán los primeros lugares en nuestra lista de optimización.

Seguridad y privacidad de datos:

Este criterio es fundamental para proteger la integridad y la confidencialidad de la información personal recopilada por el sistema. La implementación de medidas robustas de seguridad y privacidad es crucial para evitar posibles violaciones. Esto incluiría la encriptación de datos, el control de acceso adecuado y la adopción de prácticas de seguridad cibernética.

Algoritmo de reconocimiento facial:

Antes de abordar la eficiencia operativa del sistema, es esencial garantizar que el algoritmo de reconocimiento facial sea preciso y confiable. Esto implica realizar pruebas exhaustivas del algoritmo en diversas condiciones y ajustarlo según sea necesario para minimizar los errores de identificación y mejorar la precisión general del sistema.

Optimización del uso de recursos:

Una distribución equitativa de recursos y la minimización del consumo de energía son importantes para garantizar la eficiencia operativa del sistema y reducir los costos a largo plazo.

La descripción de los distintos escenarios de prueba de la simulación y las mediciones que se realizarán.

Escenario de Prueba 1 - Precisión del Reconocimiento Facial:

* Utilizando un conjunto de datos diversos que incluya imágenes de estudiantes y personal autorizado, así como de posibles intrusos, se evaluará la precisión del sistema al identificar correctamente a las personas autorizadas y rechazar a los no autorizados.

Escenario de Prueba 2 - Tiempo de Respuesta:

* Se simulará el acceso de múltiples usuarios al sistema en un período de tiempo determinado.
* Se medirá el tiempo que tarda el sistema en procesar cada solicitud de acceso, desde la detección facial hasta la apertura de la puerta automática.

Escenario de Prueba 3 - Eficiencia en el Uso de Recursos:

* Se realizarán pruebas de carga para evaluar el uso de recursos del sistema bajo diferentes niveles de demanda.
* Se medirá el consumo de CPU y memoria durante las pruebas para garantizar un uso eficiente de los recursos del sistema.

Un bosquejo de la simulación que se efectuará. Arquitectura de la solución,

identificando hilos y principales procesos involucrados.

