UNIVERSIDAD PRIVADA ANTENOR ORREGO

FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIO DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

TESIS PARA OPTAR POR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

SISTEMA DE RECONOCIMIENTO FACIAL PARA EL CONTROL DE ACCESO EN LA I. E. 81585 SAGRADO CORAZÓN DE JESÚS DE CARTAVIO – ASCOPE – LA LIBERTAD EN EL SEGUNDO Y TERCER BIMESTRE DEL AÑO LECTIVO 2022

Área de Investigación

Sistemas Inteligentes

Autor:

asana Raymundo Fernando Rafael

Jurado evaluador:

Presidente: Ullon Ramirez, Agustin

Secretario: Infantes Quiroz, Freddy Henrry

Vocal: Gaytan Toledo, Carlos Alberto

Abanto Cabrera, Heber Gerson

Código Orcid: https://orcid.org/0000-0001-9320-806X

TRUJILLO – PERÚ

2022

Fecha de sustentación: 2022/11/18

UNIVERSIDAD PRIVADA ANTENOR ORREGO

FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIO DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

TESIS PARA OPTAR POR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

SISTEMA DE RECONOCIMIENTO FACIAL PARA EL CONTROL DE ACCESO EN LA I. E. 81585 SAGRADO CORAZÓN DE JESÚS DE CARTAVIO – ASCOPE – LA LIBERTAD EN EL SEGUNDO Y TERCER BIMESTRE DEL AÑO LECTIVO 2022

Área de Investigación

Sistemas Inteligentes

Autor:

Casana Raymundo Fernando Rafael

Jurado evaluador:

Presidente: Ullon Ramirez, Agustin

Secretario: Infantes Quiroz, Freddy Henrry

Vocal: Gaytan Toledo, Carlos Alberto

Asesor:

Abanto Cabrera, Heber Gerson

Codigo Orcid: https://orcid.org/0000-0001-9320-806X

TRUJILLO – PERÚ

2022

Fecha de sustentación: 2022/11/18

SISTEMA DE RECONOCIMIENTO FACIAL PARA EL CONTROL DE ACCESO EN LA I. E. 81585 SAGRADO CORAZÓN DE JESÚS DE CARTAVIO – ASCOPE – LA LIBERTAD EN EL SEGUNDO Y TERCER BIMESTRE DEL AÑO LECTIVO 2022

JURADO CALIFICADOR

……

MS. AGUSTIN ULLON RAMIREZ

CIP: 137602

PRESIDENTE

……..

MS. FREDDY HENRRY INFANTES QUIROZ

CIP: 139578

SECRETARIO

…….

MS. CARLOS ALBERTO GAYTAN TOLEDO

CIP: 84519

VOCAL

……..

MS. HEBER GERSON ABANTO CABRERA

CIP: 106421

ASESOR

DEDICATORIA

A Dios, mis padres y mi hermana. Señor por estar conmigo en cada paso del camino, cuidándome y dándome fuerzas para seguir adelante, mis padres que me han cuidado toda la vida, dándome una buena educación, porque me apoyaron todo el tiempo, a mi hermana por poner su fe en cada desafío que se me presentó sin dudar de mi inteligencia y habilidades. Gracias a ellos, soy quien soy ahora.

AGRADECIMIENTO

Agradecido con Dios por guiarme en el camino de la felicidad hasta ahora; en segundo lugar, a cada uno de los que son parte de mi familia a mi PADRE

, mi MADRE

A mi hermana; por siempre haberme dado su fuerza y apoyo incondicional hasta en los momentos más difíciles que me han ayudado y trasladado hasta donde estoy ahora.

Al Ms. Abanto Cabrera Heber que gracias a sus consejos y saber académico, pude plasmar en esta investigación.

RESUMEN

La presente tesis titulada Sistema de Reconocimiento Facial para el control de acceso en la I. E. 81585 Sagrado Corazón de Jesús de Cartavio – Ascope – La Libertad en el segundo y tercer bimestre del año lectivo 2022 de autoría del bachiller Fernando Rafael Casana Raymundo, cuyo problema ha sido la falta de un control de acceso efectivo y eficiente. Actualmente el control de acceso de personal y alumnado de la I. E. Sagrado Corazón de Jesus no ofrece la confiabilidad necesaria lo cual implica que exista la posibilidad de la suplantación de identidad en el momento de ingresar y salir por ello, en esta investigación se tiene como objetivo el desarrollo de un sistema de reconocimiento facial que permita un control de acceso superior al que tiene la I. E.

Un sistema de reconocimiento facial consta de tres fases básicas: adquisición de imágenes, procesamiento de imágenes, extracción de características e identificación de personas, ya que al tener identificada a la persona se posee menos riesgo de que ingresen personas desconocidas.

Para solucionar este problema se seleccionó el mejor método de acuerdo a los requerimientos de la I. E., se utilizó OpenCV que es una librería de visión artificial, que nos permite procesar imágenes, así obteniendo las características esenciales de los rostros para así poder identificarlas haciendo uso del modelo Eingenfaces, el cual será entrenado con las imágenes del personal y alumnado de la I. E. Finalmente, las personas identificadas tuvieron un rectángulo verde encerrando su rostro y su nombre en la parte superior del rectángulo con su valor de confianza.

El desarrollo de este sistema utilizando PCA, Eingenfaces y las librerías de Open CV permitió elaborar un sistema con reconocimiento facial para el control de acceso, el cual permitió mejorar las entradas y salidas de las personas de la I. E. en la cual se puede visualizar las imágenes de prueba así mismo se pudo ver que el software de reconocimiento facial reconoce a las personas con seguridad.

Palabra Claves: Control de acceso, Reconocimiento facial, seguridad.

ABSTRACT

This thesis entitled Facial Recognition System for access control in the I. E. 81585 Sagrado Corazón de Jesús de Cartavio - Ascope - La Libertad in the second and third bimester of the 2022 school year by the bachelor Fernando Rafael Casana Raymundo, whose problem has been the lack of effective and efficient access control. Currently the access control of staff and students of the I. E. Sagrado Corazón de Jesus does not offer the necessary reliability which implies that there is the possibility of identity theft at the time of entering and exiting for it, in this investigation it has as objective the development of a facial recognition system that allows access control superior to that of the I.E.

A facial recognition system consists of three basic phases: image acquisition, image processing, feature extraction and person identification, since by having the person identified there is less risk of unknown persons entering.

To solve this problem, the best method was selected according to the requirements of the I.E., OpenCV was obtained, which is an artificial vision library, which allows us to process images, thus obtaining the essential characteristics of the faces in order to be able to identify them using the Eingenfaces model, which will be disturbed with the images of the staff and students of the I. E. Finally, the identified people had a green rectangle enclosing their face and their name in the upper part of the rectangle with their trust value.

The development of this system using PCA, Eingenfaces and the Open CV libraries was able to develop a system with facial recognition for access control, which was able to improve the entrances and exits of people from the I. E. in which the test images can be viewed, as well as it was possible to see that the software of facial recognition recognizes people safely.

Keywords: Access control, Facial recognition, security.

PRESENTACIÓN

Señores miembros del jurado:

De conformidad y en cumplimiento con los requisitos estipulados en el reglamento de Grados y Títulos de la Universidad Privada Antenor Orrego, pongo a vuestra disposición la presente tesis titulada: "**SISTEMA DE RECONOCIMIENTO FACIAL PARA EL CONTROL DE ACCESO EN LA I. E. 81585 SAGRADO CORAZÓN DE JESÚS DE CARTAVIO – ASCOPE – LA LIBERTAD EN EL SEGUNDO Y TERCER BIMESTRE DEL AÑO LECTIVO 2022"** para obtener el título profesional de Ingeniero en Computación y Sistemas con la confianza de obtener una calificación y evaluación justas, por favor perdónenme de antemano los posibles errores involuntarios en su elaboración.

TABLA DE CONTENIDOS

Contenido

INDICE DE TABLAS

INDICE DE FIGURAS

I INTRODUCCION

1.1 Problema de Investigación

a) Descripción de la realidad problemática

Hoy en día, es fundamental crear un entorno seguro en oficinas gubernamentales, empresas privadas, etc. La forma más común de hacer esto es contratar personal de seguridad, esto es muy útil en el caso ideal, pero como sabemos aquí aplica una prueba subjetiva y la seguridad, en gran medida, depende de la honestidad de la persona encargada de permitir acceso. Estudios recientes muestran que un gran número de organizaciones sufren de falta de seguridad, ya sea por robo o destrucción de sus activos.

Muchas de estas formas de seguridad son engorrosas, lo que hace imposible que los clientes realicen sus tareas a la perfección, lo que genera vulnerabilidades en el sistema de seguridad.

Los sistemas de control de acceso han proliferado en las organizaciones de servicios a lo largo de los años a medida que sus aplicaciones se expandieron desde monitorear el acceso de las personas a áreas específicas. Hoy, gracias a una combinación de diferentes tecnologías, las empresas pueden monitorear su personal y sus procesos. En el Perú existe una clara migración de los sistemas tradicionales a los de tecnología avanzada. Actualmente, las necesidades del mercado están orientadas a la integración de distintas tecnologías, con el objetivo de construir sistemas que den soluciones integrales al control de acceso y asistencia, y al área de seguridad. Es tan así, que no sólo las empresas corporativas están requiriendo de estas herramientas, sino también las grandes industrias.

El sistema de control de acceso propuesto surge con la finalidad de desarrollar una innovación tecnológica que permita facilitar el acceso y brindar mayor control de acceso a la I. E. La tecnología de reconocimiento facial que utiliza OpenCV (una biblioteca gratuita) es perfecta para este proyecto, ya que es fácil de implementar. Además, se puede mejorar la seguridad del control de acceso.

b) Descripción del problema

La principal dificultad que encontramos dentro de la I E. en lo que respecta al control de acceso es que no cuenta con personal específico de seguridad, tan solo cuenta con dos auxiliares que están en la puerta. Actualmente en la I. E. no cuenta con un control de acceso del personal apropiado, para el ingreso se debe registrar la hora de entrada y salida manualmente en hojas de control que hacen los profesores cuando los alumnos ingresan a las aulas lo cual implica que exista la posibilidad de tener diferentes tipos de errores ejemplo la suplantación.

Durante mucho tiempo se descuidó el control de los alumnos que ingresaban al colegio Sagrado Corazón de Jesús - Cartavio, los docentes tomaban apuntes al inicio de cada sesión de clase como un registro único, es por ello que el reconocimiento facial automático será la posible solución a tal problema.

Las soluciones tecnológicas, como la biometría, nos permiten, mediante un dispositivo de lectura de rostros, comparar la foto original de los estudiantes tomada antes de la asistencia, con estas fotos se determinará cada persona que desea ingresar al centro educativo, que está siendo identificado en base a la base de datos biométricos. Aquí, en este ámbito, el trabajo de esta tesis se centra en la forma en que una organización puede identificar a las personas que ingresan a sus instalaciones.

c) Formulación del problema

¿Cómo mejorar el control de acceso del personal y alumnado de la I. E. Sagrado Corazón de Jesús - Cartavio - Ascope?

1.2 Objetivos

1.2.1 Objetivo General

Desarrollar un sistema de reconocimiento facial para el control de acceso en la I. E. 81585 Sagrado Corazón de Jesús de Cartavio – Ascope – La Libertad en el segundo y tercer bimestre del año lectivo 2022.

1.2.2 Objetivos Específicos

1. Investigar y almacenar información sobre técnicas de reconocimiento facial y cómo funciona.
2. Definir los requisitos necesarios de diseño del sistema de reconocimiento facial con base en las condiciones de acceso a una escuela.
3. Escoger la técnica de reconocimiento facial que permita tener en cuenta las condiciones previamente definidas.
4. Implantar el sistema de reconocimiento facial.
5. Elaborar los resultados y las conclusiones del proyecto.

1.3. Justificación del estudio

Las tecnologías de autenticación biométrica ahora se han convertido en la solución principal para prevenir el robo de identidad. En él, el reconocimiento facial es una forma segura, rápida y cómoda de comprobar si el personal y los alumnos llegan a IE a tiempo, reemplazando el uso manual de registros en libretas de control.

El desarrollo de esta investigación plantea la inexistencia de un sistema de reconocimiento para controlar el acceso a las personas que ingresen a la I. E.

1.3.1. Justificación Metodológica

El presente estudio se enfocará en el desarrollo de un sistema de reconocimiento facial funcional para el control de acceso para el ingreso de personas en la I. E. Sagrado Corazón de Jesús – Cartavio – Ascope – La Libertad, ya que permitirá aliviar los riesgos de seguridad desencadenados

del uso de mecanismos de reconocimiento de identidad para la entrada de individuos; en especial la de suplantar.

Se conseguirá mejorar la eficacia con la que se valida el ingreso de un individuo a la E.I. al asegurarse de que el individuo registrado en la entrada de video sea verificado, además, la entrada y salida de la persona puede ser monitoreada con precisión. Se sugiere su uso en escuelas que no cuentan con un gran presupuesto de inversión para poder elaborar otros sistemas que pueden ser muy caros, siendo este un sistema económico y muy efectivo para lo que se requiere.

1.3.2. Justificación Social

El desarrollo del sistema de reconocimiento se justifica con la colaboración directa en tareas de identificación y control de personas, con la premisa de incrementar la eficiencia en relación al tiempo de respuesta en estas tareas de control de las mismas, en beneficio de la seguridad dentro de las escuelas del país, cuyo precio de uso puede ser muy inferior; los casos que no consigan reconocerse por este medio deberán ser comprobados a través de seguridad física brindada por los empleados de seguridad.

Se busca beneficiar a la ciudadanía en cuanto al control de personas que ingresan o salen de la I E., ya que este puede estar ligado a la inseguridad dentro del plantel entre otros, esto para reducir el tiempo que involucra el proceso de búsqueda y hallazgo.

1.3.3. Justificación Tecnológica

Se propone desarrollar un sistema modelo para la identificación y reconocimiento de personas buscadas que nos permitirá aprovechar los diversos componentes tecnológicos existentes, dedicando el desarrollo de este proyecto a su aplicación en beneficio de la seguridad colectiva en la I.E.

II. MARCO DE REFERENCIA

2.1. Antecedentes del Estudio

2.1.1. Internacionales

Mosquera & Romero , (2016), en la tesis Titulado “Diseño de un Software Piloto de Reconocimiento Facial para el Control de Asistencia en la Escuela de Telecomunicaciones de la Universidad de Carabobo”, el cual brinda una confianza mayor gracias a su capacidad para detectar y reconocer los rostros de todos los trabajadores que laboran en el sitio, para ello , gracias a la librería OpenCV se utilizó la tecnología de visión artificial, la cual recopiló y comparó las imágenes, procesó digitalmente las imágenes y así identificar a la persona. Adicionalmente, con el uso del lenguaje de programación PYTHON, se ha creado una interfaz gráfica de usuario para administrar el software, realizando pruebas para evaluar su eficacia y eficiencia.

Caballero, Reyes, Sánchez, & Ríos (2017). En su trabajo de investigación “Reconocimiento facial por el método de Eigenfaces” Este artículo presenta una aplicación de reconocimiento facial Eigenfaces que utiliza Microsoft Visual Studio con varias herramientas de programación, como la biblioteca de la plataforma C# y Emgu CV combinados con OpenCV. El desarrollo de la solicitud se codifica en dos partes: una de registro y otra de acreditación. El programa se carga en computadoras de escritorio con sistema operativo Windows 8 y utiliza la cámara web incorporada. En la etapa de grabación, el individuo se para frente a la cámara para tomar tres fotografías en diferentes momentos. Durante la fase de identificación, el usuario aparece frente a la cámara y el sistema hace una comparación con todos los registros existentes en la base de datos, indicando si el usuario está registrado o no. Durante la fase de registro e identificación, se crean otros formularios para conectar los dos, utilizando las plantillas del explorador de soluciones de HaarCascade CANNY_PRUNING y el objetivo EigenObjectRecognizer. El proyecto se presenta a la sección de pruebas con un universo de diez usuarios, de los cuales ocho son hombres y dos mujeres, realizándose diez pruebas para cada

usuario, obteniendo una matriz de confusión con resultados, el resultado es 100 identidades incluso para usuarios no registrados.

2.1.2. Nivel Nacional

Mariño, 2018, en la tesis titulado "Aplicación móvil de reconocimiento facial en personas con trabajo previos de abuso sexual en la provincia de Andahuaylas, Apurímac - 2018", para optar de Ingeniero de Sistemas en la Universidad Nacional José María Arguedas, Apurímac. El desarrollo del sistema plantea la inexistencia de un sistema de reconocimiento para identificar a las personas que cometen estos actos delictivos en la ciudad de Andahuaylas en donde los acusados casi en su mayoría salen sin represalias de la justicia, entonces el objetivo principal es el de realizar un proceso de reconocimiento facial para identificar a los individuos que cuenten con antecedentes delictivos mediante el uso de un aplicativo instalado en un dispositivo móvil, ya con esta justificación la investigación se manejó con esta tecnología ya que está siendo de mucha efectividad en otros países además de mejorar los procesos de investigación analizada. Con la tecnología de desarrollo se tomó una muestra de 30 individuos y el mismo número de reportes fotográficos para realizar una sesión de pruebas del para detectar fallas en el aplicativo por el que el resultado fue el 100% de las nuestras fueron identificadas de manera eficiente y el 93% tiene consistencia y solo el 7% por factores externos ajenos al software no se generó el reconocimiento. En conclusión, el proyecto desarrollado es que el prototipo realiza el reconocimiento sin ser afectado por factores externos, adicionalmente realizaron en este proyecto la implementación de una base de datos al sistema para realizar mejor su efectividad para la búsqueda de posibles sospechosos.

Sandoval & Estela Villena, (2015). En la tesis titulado “detección de alumnos mediante mecanismos proactivos para el control de asistencia para la facultad de ingeniería y arquitectura de la universidad san Martin”, Utiliza la comunicación por bluetooth y la plataforma Android para generar una aplicación que sondea en intervalos de tiempo determinado a todos los equipos que se encuentran dentro de su alcance y permite el monitoreo constante de los personas en el salón de clases, este proyecto está en la etapa de un prototipo con la implementación de un software desarrollado en la plataforma Android para el personal docente y el estudiante. Este sistema será de gran utilidad ya que podrá conectarse con el sistema de la mencionada universidad para mostrar la ruta del alumno para que pueda seguirla en el momento de las clases. Los resultados muestran que en el proyecto mostró una disminución del 84,69%, en un salón de 108 personas, en la supervisión de la entrada al salón de clases

2.1.3. Nivel Local

Bautista Mendoza, Dennis, Miñano Pereira, Paulo Sergio (2019), en la tesis titulada “Análisis de la influencia del ángulo lumínico sobre el rendimiento de las técnicas de reconocimiento facial basadas en la apariencia lineal”, esta investigación propone el análisis de la influencia del ángulo lumínico sobre el rendimiento de las técnicas de reconocimiento facial basadas en la apariencia lineal con la finalidad de determinar el grado de asertividad de cada técnica a diferentes ángulos de luz. El estudio corresponde a una investigación aplicada y cuasi-experimental, cuya unidad de análisis es la captura de rostros con variaciones angulares de iluminación en el plano coronal.

2.2. Marco Teórico

2.2.1. Control de Acceso

Este es un concepto muy utilizado cuando se trata de la seguridad de cualquier lugar o instalación, es un factor muy vital ya que facilita el monitoreo y el control del flujo de individuos a través de instalaciones como puertas, ascensores, barandillas, accesos secundarios, etc.

El control de acceso se localiza en casi todas las industrias e instituciones donde se ve algún tipo de automatización y esto proviene de la obligación de preservar recursos, objetos o incluso la propia seguridad de la persona. Sobre esta base, se han desarrollado una secuencia de soluciones basadas en la tecnología existente en el mercado haciendo el uso de estándares y arquitecturas abiertas, de las que se considera como referencia el control de acceso en el ámbito de la seguridad.

Algunos de los rasgos principales del control de acceso son:

- Denegar el acceso a los sitios web por hora y usuario.
- Controlar el tránsito de personas por las áreas de la empresa.
- Registro de tiempo y asistencia.
- Controlar automáticamente el acceso a vehículos.
- Controlar a los individuos dentro del edificio.
- Establece un control preciso de los empleados sin necesidad de que los supervisores registren las entradas y salidas de los empleados.
- Protección de bienes.
- Sustitución guardias de seguridad.

2.2.2. TIPOS DE CONTROL DE ACCESO

Son sistemas automáticos que controlan de manera efectiva el movimiento de personas a través de áreas denegadas de acuerdo a algunos criterios de seguridad determinados por la empresa, comercio, organización o alguna otra institución. El control de acceso también permite guardar un registro automático de los movimientos de una o más personas en un espacio específico.

2.2.2.1 Sistemas de control de acceso autónomos.

Estos sistemas le aceptan controlar una o más puertas sin conectarse a una computadora o centro de monitoreo, lo que significa que este tipo de control de acceso no realiza un seguimiento de las puertas. Los controles de acceso autónomos más simples funcionan como una llave electrónica, esto significa que, identifican de forma única a un individuo y le admiten entrar y salir de las instalaciones.

La imagen que se presenta, tenemos algunos de los elementos imprescindibles para un sistema de control de acceso autónomo.

Fig.1 Sistemas de control de acceso autónomo

2.2.2.2. Sistema de control de acceso en red.

Estos sistemas son más complejos y tienen más funciones que los ya mencionados, porque están integrados mediante una computadora con un software que te permite llevar un registro de todos los individuos que ingresan y salen, puedes extraer todo tipo de datos como la hora, la fecha, también se han utilizado para la identificación, entre otras cosas. Estos sistemas de control de acceso son completamente configurables para cada cliente, con combinaciones complejas que brindan funciones a la medida de cada necesidad.

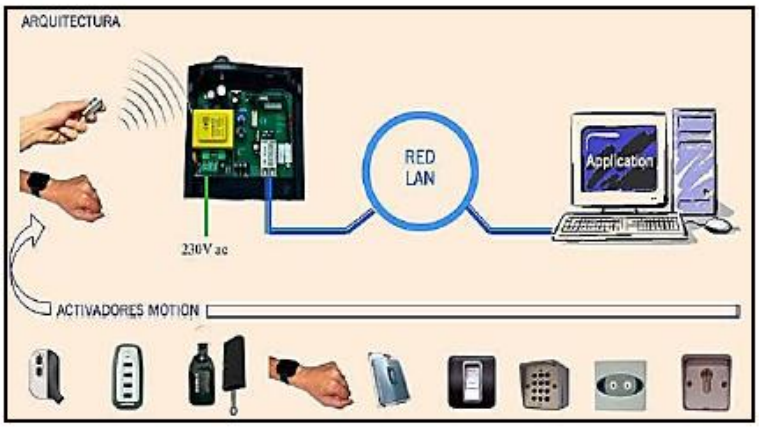


Fig. 2 Sistemas de control de acceso en red

2.2.3. MÉTODOS DE VERIFICACIÓN PARA EL CONTROL DE ACCESO

En cuanto al control de acceso, se utiliza una amplia variedad de métodos para comprobar que la persona no es un suplantador, además de dar acceso al propietario a todo lo que protege el control de seguridad, existen en el mercado muchos tipos de control de acceso, entre ellos lo más complejo, como la identificación biométrica en un puesto de control o el control mediante verificación de dígitos.

2.2.3.1. Verificación de dígitos.

Es un procedimiento tanto físico como digital y se utiliza para controlar el acceso a cerraduras, puertas, cajas fuertes, etc. Estos métodos de verificación de dígitos suelen ser dispositivos de teclado que ingresan algunos caracteres que verifican la entrada con una contraseña proporcionada por la persona principal y luego brindan acceso a una cerradura.

Fig. 3 Método de control de acceso por verificación de dígitos

2.2.3.2. Biometría.

Combinando estos conceptos con la tecnología, es posible brindar servicios seguros y confiables para el ingreso de los empleados a las áreas de la empresa que lo requieran. Un ejemplo es el uso de lectores de huellas dactilares en el control de acceso.

En la imagen, se ve en forma gráfica ciertos métodos de Biometría tales como Face recognition (Reconocimiento facial), Voice recognition (Reconocimiento de voz), y el touch ID (reconocimiento dactilar).

Fig. 4 Método de control de acceso por Biometría

2.2.3.3. Talanqueras o torniquetes.

Este es un modo de control de acceso que admite al usuario entrar y salir a través de las barras perpendiculares al armazón y tiene una separación entre la barra y barra el espacio necesario para su recorrido, lo que lo hace óptimo para el control de acceso de individuos que se identifican uno por uno, en la figura 5 se muestra la talanquera, este método es efectivo ya que se puede combinar con varios métodos como RFiD, huella digital de verificación o número de verificación, etc.

Fig. 5 Método de control de acceso torniquete

2.2.3.4. Reconocimiento ocular.

El reconocimiento de iris/retina es uno de los sistemas de reconocimiento más utilizados porque los patrones oculares tienen una posibilidad muy cercana de coincidir con una imagen anterior almacenada en la base de datos para comparar patrones oculares, por lo que es un sistema muy eficiente porque los ojos son los únicos humanos, órgano que, a pesar del tiempo, nunca envejece ni cambia de aspecto. Aun así, tiene algunos inconvenientes ya que al leer con láser será molestoso para la persona y si utiliza anteojos, su dueño se verá afectado y no podrá identificarse, por lo que la figura 6 muestra ciertas características del ojo humano.

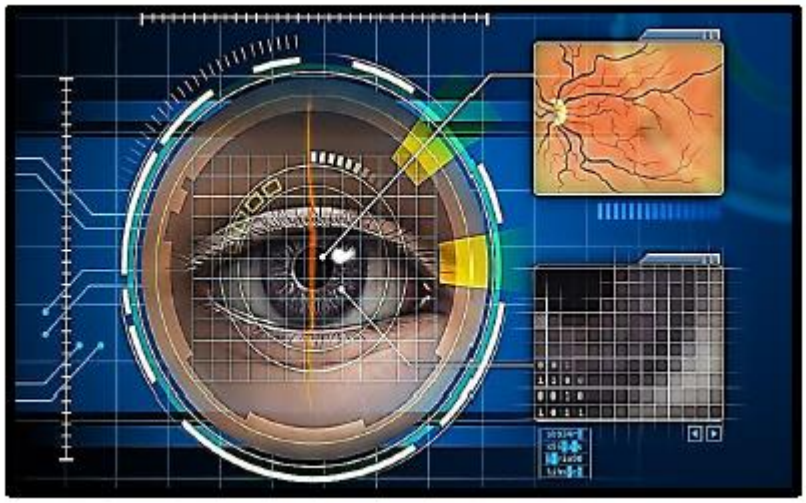


Fig.6 Método de control de acceso por reconocimiento ocular

2.2.3.5. Reconocimiento por huella dactilar.

La huella dactilar es uno de los criterios físicos para describir las características de un individuo, ya que tiene un buen efecto para establecer la identificación de una persona, pues se ha verificado que ninguna huella dactilar es parecida, ni siquiera entre mellizos o entre los dedos de un mismo individuo. La utilización de estas plantillas fue uno de los primeros en determinarse como plantilla de autenticación biométrica. Cuando la persona quiere validarse con el sistema, coloca su dedo en un área establecida. En este reconocimiento, se toma una imagen y luego se normaliza utilizando un sistema de espejo fino para enmendar los ángulos y es a partir de esta imagen normalizada que el sistema extrae los detalles más pequeños (cierto arco, bucle o remolino de la huella dactilar). comparará con lo que tiene en su base de datos, en la Figura 7, se destaca una huella digital.

Fig. 7 Método de control de acceso por reconocimiento dactilar

2.2.3.6. Reconocimiento facial.

El reconocimiento facial es una técnica que recientemente se ha abordado en varios campos del estudio como el análisis de imágenes, la extracción de características de archivos digitales, etc. Esto se debe a que este proceso tecnológico puede imitar la capacidad de los humanos para reconocer a los individuos en función de un patrón determinado en nuestro cerebro.

Fig. 8 Método de control de acceso por reconocimiento facial

2.3. Marco Conceptual

2.3.1. Imagen digital

Una imagen digital se compone de una agrupación de píxeles, cada uno con un valor de intensidad o brillo asociado. Una imagen digital se representa mediante una matriz bidimensional, de forma que cada elemento de la matriz se corresponde con cada píxel en la imagen.

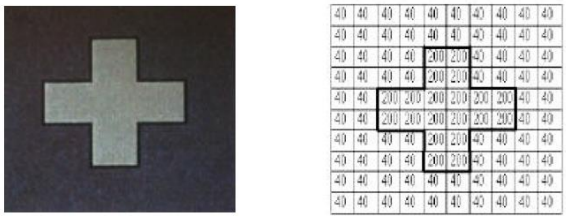


Fig. 9 Imagen original/ estructura matricial de la imagen

2.3.2. Procesamiento de la imagen

El objetivo principal de las técnicas de mejora de imágenes es procesar la imagen para hacerla más adecuada para una determinada aplicación o para un procesamiento posterior. Por tanto, depende del problema concreto a resolver mediante una técnica u otra. Los métodos de mejora de imágenes se pueden dividir en dos campos diferentes: métodos de dominio de frecuencia y métodos de dominio espacial. El primero se basa en modificar la transformada de Fourier de la imagen, mientras que el segundo se basa en operaciones directas sobre los píxeles de la imagen.

2.3.3. Visión artificial

La visión artificial tiene como objetivo recopilar información a partir de imágenes de muestra, utilizando equipos informáticos. El software de vision artificial trabaja sobre una imagen tomada de la realidad, proporcionando información sobre brillo, color, forma, etc. Estas imágenes suelen ser escenas tridimensionales estáticas o imágenes en movimiento.

2.4. Sistema de Hipótesis

Un Sistema de reconocimiento facial mejora el Control de acceso en la I. E. 81585 Sagrado Corazón de Jesús de Cartavio – Ascope – La Libertad

2.5. Variables e Indicadores

2.5.1 Variable Independiente

1. Sistema de reconocimiento facial

2.5.2. Variable Dependiente

1. Control de acceso en la I. E. 81585 Sagrado Corazón de Jesús de Cartavio – Ascope – La Libertad

Tabla 1. Cuadro de operacionalización de variable Independiente y Dependiente

VARIABLE	**DEFINICION CONCEPTUAL**	**DEFINICION OPERACIONAL**	**DIMENSIONES**	**INSTRUMENTOS DE RECOJO DE INFORMACION**
Independiente: - Sistema de reconocimiento facial	Aplicación dirigida por ordenador que identifica automáticamente a una persona en una imagen digital.	El reconocimiento facial necesita de un dispositivo que disponga de tecnología fotográfica digital, cámara, para generar y obtener las imágenes y datos necesarios para crear y registrar el patrón biométrico facial a través de algoritmos de la persona a identificar	Tiempo de detección (Objeto)	Medición de tiempo
			Precisión de detección (Objeto y movimiento)	Medición de valor de confianza
			Usabilidad	Juicio de expertos
Dependiente: Control de acceso en la I. E. 81585 Sagrado Corazón de Jesús de Cartavio – Ascope – La Libertad	Un control de acceso es aquel que permite o restringe la entrada de una persona o vehículo a la I. E. o a una zona determinada de la misma.	Forma de medir la eficacia y diferencia de tiempos que toman los procesos tradicionales con reconocimiento facial para un control eficiente	Tiempo de control de acceso	Medición de tiempo

III. METODOLOGÍA EMPLEADA

3.1. Tipo y Nivel de Investigación

Para esta investigación, el tipo es aplicada y el diseño que se utilizó en este estudio es correlacional, esto se debe a que existen indicadores medibles y los resultados son valores ante la aplicación de un Sistema de reconocimiento facial, haciendo una medición sobre el control de acceso de en la I. E. y con el tiempo de detección.

Correlacional porque se comparará el antes y el después del desarrollo del sistema de reconocimiento facial.
Para este estudio se manejó la variable independiente para ver su efecto con la variable dependiente.

3.2. Población y muestra de estudio

3.2.1 Población

En el presente estudio, la población se encuentra conformada por el personal administrativo, docentes, auxiliares y alumnado que conforma la I. E., que cuenta con un total de 402 según la información dada por la secretaria.

Tabla 2. Cantidad de personas de la I. E.

Descripción	Cantidad de Personas
Personal Administrativo	2
Personal Limpieza	2
Secretaría	1
Auxiliar	2
Alumnos 1° Grado sección A -B - C	62
Alumnos 2° Grado sección A -B - C	61
Alumnos 3° Grado sección A -B - C	63
Alumnos 4° Grado sección A -B - C	65
Alumnos 5° Grado sección A -B - C	60
Alumnos 6° Grado sección A -B - C	64
Docentes	20
TOTAL	402

3.2.2. Muestra

La muestra serán la docente y auxiliar para efectos de probar el sistema de reconocimiento facial.

3.3. Diseño de Investigación

El diseño de la investigación es experimental, tenemos nuestro objetivo general que es el probar que, con aplicando un sistema de reconocimiento facial basado en rasgos faciales nos permitirá mejorar el nivel de control de acceso a la I E. Sagrado Corazón de Jesús.

3.4. Técnicas e instrumentos de recolección de datos

- Observación: Para la determinación de patrones correspondientes.
- Post análisis: Se examina críticamente el proceso real de desarrollo y se contrasta con el proceso planificado para identificar aquellos aspectos del proceso que vale la pena conservar, profundizar, mejorar o eliminar.
- Cuestionarios: Se realizarán cuestionarios a los usuarios finales, para poder documentar su experiencia y sus opciones de mejora al sistema.

3.5. Procesamiento y análisis de datos

El sistema de recolección de información se implementará seleccionando las fuentes de información:

a) Resumir los datos y la información relacionada con el tema Reconocimiento Facial.

b) Preparar la muestra.

c) Determinación de los algoritmos necesarios para el reconocimiento facial

d) Verificar la metodología desarrollada.

IV. PRESENTACIÓN DE RESULTADOS

4.1. PROPUESTA DE INVESTIGACIÓN

Se ha desarrollado el trabajo de investigación, respondiendo al objetivo general y los específicos, un marco de trabajo que nos permita desarrollar un sistema de reconocimiento facial para mejorar el control de acceso a la I. E., iniciando con la recolección de información relacionada con el reconocimiento facial en libros, revistas científicas y otros documentos, de igual manera, se obtuvo información a partir de una población de administrativos y docentes, a los cuales se les realizó un cuestionario, lo cual facilitó determinar y especificar los requerimientos funcionales, el cual se aplicó durante el periodo que comprende segundo y tercer bimestre del año lectivo 2022.

Se desarrolló un prototipo del software, es decir, el desarrollo de los componentes y funcionalidades, implementación de estructuras de datos, elaboración de documentación técnica, la integración de la solución y las pruebas de verificación del prototipo desarrollado.

4.1.1. Investigar y almacenar información sobre técnicas de reconocimiento facial y cómo funciona

Para lograr el primer objetivo específico, se efectuó una búsqueda y compendio de información para entender el tema de reconocimiento facial, las técnicas y algoritmos.

4.1.1.1 Reconocimiento Facial

El reconocimiento facial es un sistema biométrico que tiene como objetivo reconocer a los individuos mediante la captura de una fotografía captada por una cámara digital, luego analizando las características físicas extraídas de la imagen y comparándola con una base de datos ya guardada.

Fig 10. Captura del rostro

El reconocimiento de patrones es un sistema que extrae datos, que establece procesos de reconocimiento, descripción, clasificación y restauración para catalogar un conjunto de patrones conocidos en dos o más categorías. Un patrón es un grupo de rasgos únicos de cada individuo. Para identificar patrones, se aconseja seguir las siguientes etapas: recopilación de datos, extracción de datos y toma de decisiones.

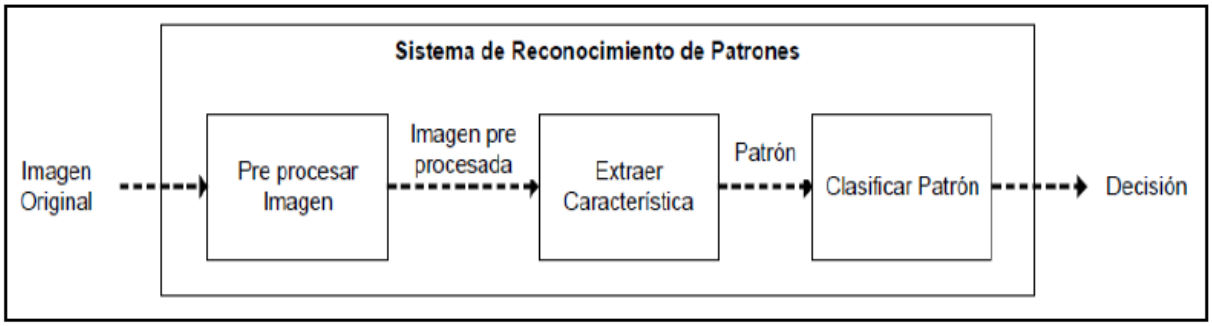


Fig 11. Diagrama de bloques de un sistema de reconocimiento de patrones

4.1.1.1.1. Etapas para el Reconocimiento Facial

1. **Detección de la cara:** detecta un rostro en la imagen sin identificar el rostro. Si es un vídeo, también podemos hacer seguimiento de rostros. Proporciona la posición y la escala en la que encontramos la cara.

2. **Análisis facial:** localizar los componentes del rostro y, mediante transformaciones geométricas, normalizarlo según propiedades geométricas, como el tamaño y la postura, así como propiedades fotométricas, como la luz. Para normalizar la imagen de la cara, diferentes reglas se pueden seguir como la distancia entre las pupilas, la posición del o la distancia entre las comisuras de los labios. También se debe especificar el tamaño de la imagen y la gama de colores. Usualmente, para reducir la carga computacional del sistema, es común usar imágenes pequeñas en escala de grises. A veces también se realiza la ecualización del histograma.

3. **Extracción de rasgos:** proporciona información para distinguir rostros de diferentes personas en base a variaciones geométricas fotométricas.

4. **Reconocimiento:** Los vectores de características extraídos se comparan con los vectores de características extraídos de las caras en la base de datos. Si encuentra uno con un alto porcentaje de similitud, devuelve la autenticidad del rostro; de lo contrario resulta que es una cara desconocida.

4.1.1.1.2. Aplicaciones con Reconocimiento Facial

Área	Aplicaciones Especificas
Biometría	Licencia de Conducir, Programas de Derecho, Inmigración, DNI, Pasaportes, Registro de Votantes, Fraude, Teléfonos inteligentes, Acceso a instalaciones restringidas.
Seguridad de la información	Inicio de Sesión, Seguridad en Aplicaciones, Seguridad en Bases de Datos, Cifrado de Información, Seguridad en Internet, Acceso a Internet, Registros Médicos, Terminales de Comercio Seguro, Cajeros Automáticos.
Cumplimiento de la ley y vigilancia	Video vigilancia Avanzada, Control CCTV, Control Portal, Análisis Post-event, Hurto, Seguimiento de Sospechosos, Investigación.
Tarjetas inteligentes	Valor Almacenado, Autenticación de usuarios.
Control de acceso	Acceso a Instalaciones, Acceso a Vehículos.

Tabla 3. Principales aplicaciones del reconocimiento facial

4.1.1.1.3. Arquitectura de un Sistema de Reconocimiento Facial

La arquitectura del sistema de reconocimiento facial consta de: una persona a reconocer, un objeto de fotografía digital (cámara digital), un aparato de procesamiento que almacena y compara la imagen (computadora) y finalmente una base de datos para almacenar los datos del usuario. La imagen muestra la arquitectura del sistema utilizando tecnología de reconocimiento facial.

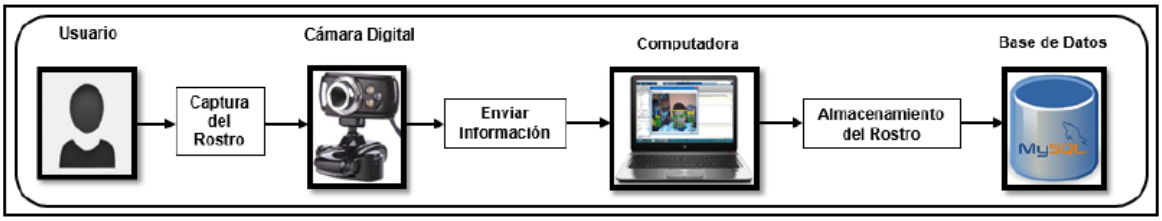


Fig. 12 Arquitectura de reconocimiento facial

4.1.1.1.4. Características del Reconocimiento Facial

El reconocimiento facial tiene características propias que lo distinguen de otros sistemas de reconocimiento biométrico, la variación que la afecta al detectar la imagen de una persona es: la luminosidad, inclinación, contraste, estado de ánimo, etc. Las características principales que se debe considerar para el reconocimiento facial sean eficientes es: singularidad, universalidad, permanencia, colectividad, aceptabilidad y resistencia a la elusión.

Las ventajas principales sobre sistemas similares son:

- Se puede utilizar a distancias fijas.
- Se puede utilizar en situaciones de difícil acceso, como quirófanos.
- Aceptabilidad alta, ya que las personas no ven detenido su flujo de acceso.
- Evitar el uso de tarjetas, claves, etc.

4.1.1.1.5. Objetivo de un Sistema de Reconocimiento de rostros

El objetivo del sistema de reconocimiento facial es proporcionar una imagen de un rostro, encontrar una imagen del mismo rostro en un conjunto de imágenes conocidas. La principal dificultad adicional es garantizar que este proceso se pueda realizar en tiempo real. El sistema reconocerá automáticamente el rostro presente en la imagen o video. Puede funcionar en dos modos:

- Verificar o Autentificar de rostro: compara una imagen de un rostro con otra imagen de un rostro cuya identidad deseas conocer. El sistema confirmará o rechazará el rostro.
- Identificación o Reconocimiento de rostros: Compara la imagen de un rostro desconocido con todas las imágenes de rostros conocidos en la base de datos para determinar su identidad.

4.1.1.1.6. Técnicas de Reconocimiento Facial

Existen dos familias de técnicas de reconocimiento facial: técnicas basadas en la apariencia y técnicas basadas en modelos. En cada una de estas familias, se encuentran distintos métodos para caracterizar la imagen, aunque en este estudio solo se tratarán algunos de los métodos basados en la apariencia.

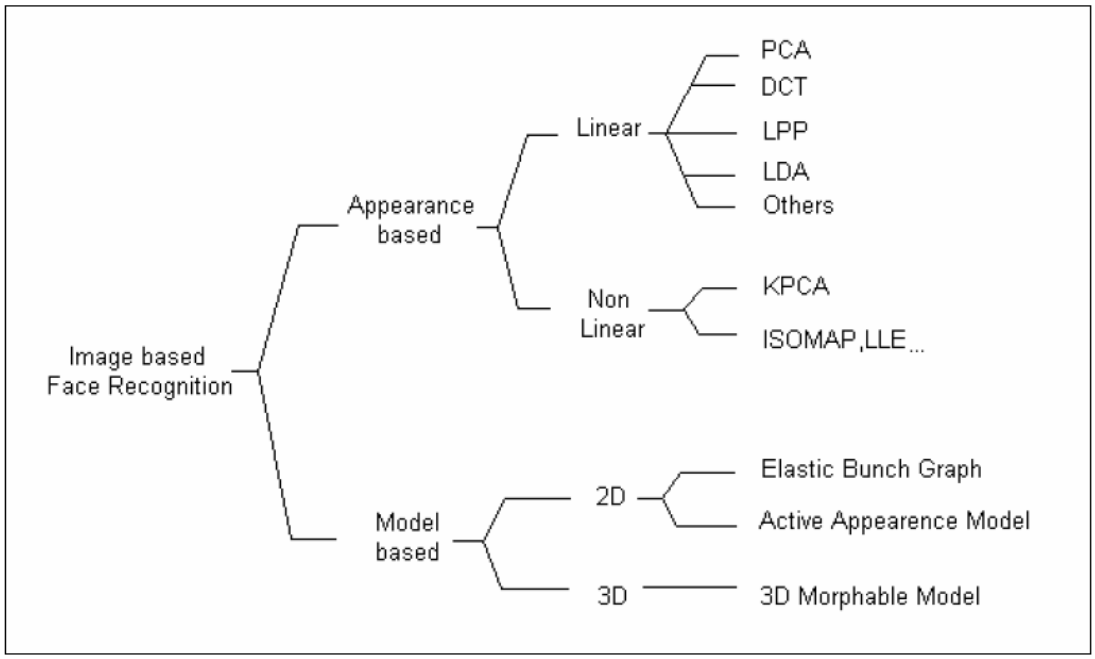


Fig. 13 Algunos métodos de clasificación

Los sistemas que se basan en la apariencia se usan directamente en las imágenes sin el uso de modelos 3D. Estos tipos de sistemas representan objetos basados en diferentes puntos de vista del objeto. En estos sistemas, cada imagen se representa como un punto en el subespacio vectorial, por lo que las comparaciones entre las imágenes de prueba y de referencia se realizan en el subespacio vectorial de rostros. El propósito de estos algoritmos es clasificar diferentes rostros en nuevos subespacios,

pero para hacerlo, el sistema debe entrenarse previamente con imágenes de diferentes rostros en diferentes vistas.

Por otro lado, existen sistemas basados en modelos que intentan crear modelos del rostro humano que sean lo más descriptivos posible que puedan encontrar con precisión las alteraciones del rostro.

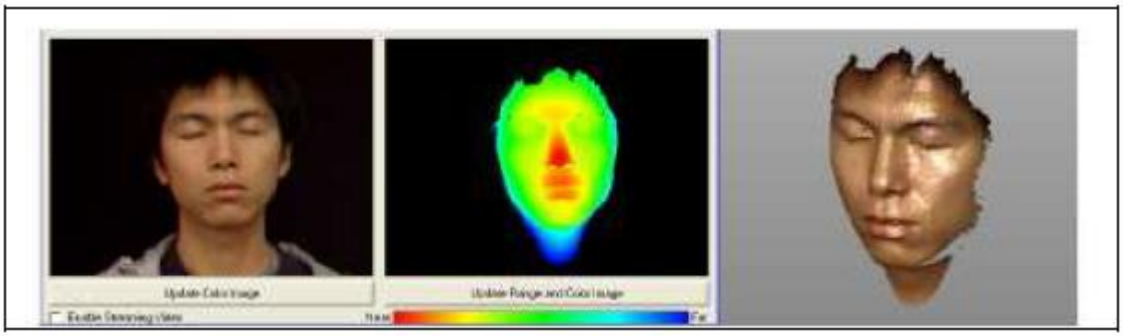


Fig. 14. Imagen en 2D, mapa de profundidad y representación 3D del modelo.

Estos sistemas tratan de obtener las características biométricas de las imágenes para efectuar el reconocimiento (la distancia entre los ojos, el grosor de la nariz...). Estos métodos suelen requerir imágenes de alta resolución.

4.1.1.1.7. Técnicas basadas en la apariencia

4.1.1.1.7.1 PCA (Principal Component Analysis)

Esta es una técnica de reconocimiento de patrones de datos que se utiliza para distinguir semejanzas y diferencias mediante combinaciones lineales entre imágenes adquiridas y guardadas. La ventaja del PCA es que la información necesaria para la identificación se reduce en un factor de 1000 a 1 en comparación con los datos mostrados. PCA comúnmente usa caras propias y fue creado por Kirby y Sirovich en 1988. Las imágenes deben normalizarse al mismo tamaño para que los ojos y la boca se alineen, como se muestra en la Figura 15.

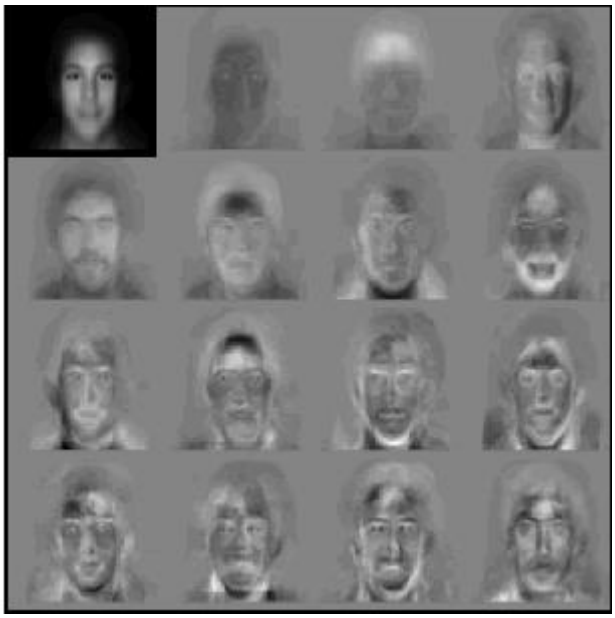


Fig. 15 Alineación y normalización de imágenes utilizando Eigenfaces

Esta técnica se utiliza para reducir la dimensión del conjunto de datos correspondiente al número de vectores propios utilizados, al reducirse la dimensión de la imagen se quitarán datos que no son útiles. El resultado es una estructura de caras que contiene componentes ortogonales (correlacionados) conocidos como Eigenfaces. Por lo tanto, la imagen proyectada por PCA tendrá un tamaño de valor d, como se muestra en la imagen 16. Estos autovectores representan las componentes principales que son más comunes en imagen de diferentes caras.

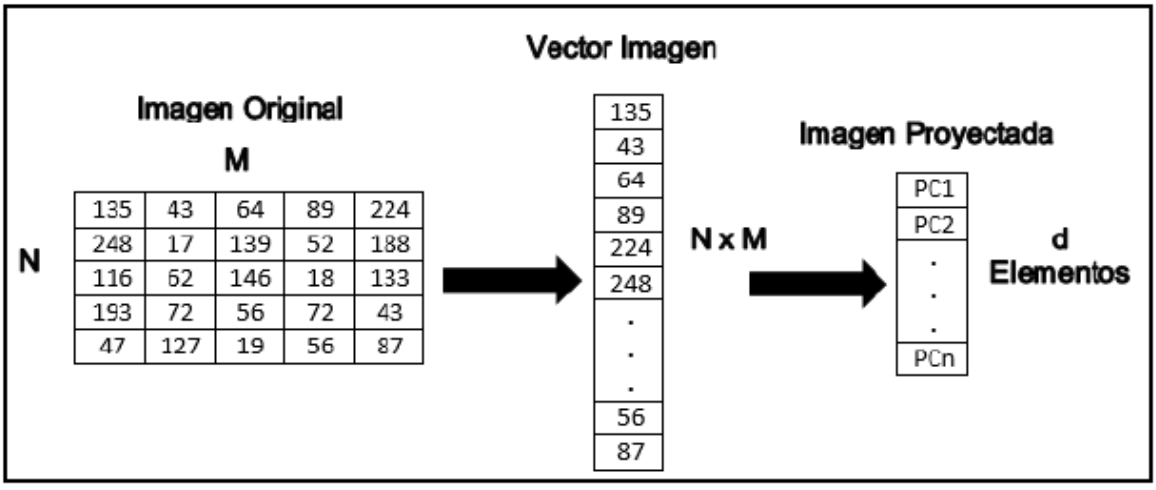


Fig. 16. Ejemplo de reducción dimensional al aplicar PCA

El propósito de este método se basa en la representación de la imagen en el sistema de coordenadas, reduciendo así el número final de elementos de la imagen. Entre todos los métodos de reconocimiento facial existentes, PCA es uno de los mejores métodos disponibles en este campo.

4.1.1.1.7.2 Análisis discriminante lineal: LDA.

Esta técnica es un enfoque estadístico para organizar muestras de clases o grupos que no se conocen. Esta técnica tiene como objetivo minimizar la varianza entre clases que se conocen y maximizarla sobre clases desconocidas. De esta forma se garantiza la máxima diferencia entre clases. Una de las limitaciones que tiene LDA es que tienen matrices de dispersión no singulares, porque el tamaño de la imagen a veces es mucho más grande que el número de imágenes en la base de datos, lo que genera problemas de matriz singular.

Fig. 17 Ejemplo de 6 clases distintas usando LDA

4.1.1.1.7.3 LPP (Locality Preserving Projections)

Al ser un algoritmo lineal, es útil para aplicaciones rápidas y prácticas. Una característica que difiere de PCA es que, en lugar de mantener una estructura global de datos, mantiene una estructura local. De este modo los ‘vecinos’ para un dato en concreto serán los mismos en el espacio original, de alta dimensionalidad, y en el nuevo subespacio de baja dimensionalidad. Al preservar la estructura local de los datos, las imágenes que pertenecen al mismo individuo estarán más cerca y más alejadas de las imágenes de otros individuos. Es decir, hay una distinción entre clases.

Para mantener la estructura local de los datos, se utiliza un gráfico de adyaciencias, que contiene información sobre la estructura de los datos. Este gráfico consiste en crear una matriz de tamaño NxN, donde N es el número de imágenes a las que se asignan pesos en función de si los elementos iyj son adyacentes o no.

En el momento de crear este grafo cabe la opción de crearlo de manera automática (caso no supervisado), utilizando métodos de búsqueda de ‘vecinos’ como K nearest neighbors o e-neighborhoods, o hacerlo de manera manual (caso supervisado) asignando manualmente quienes son o no vecinos.

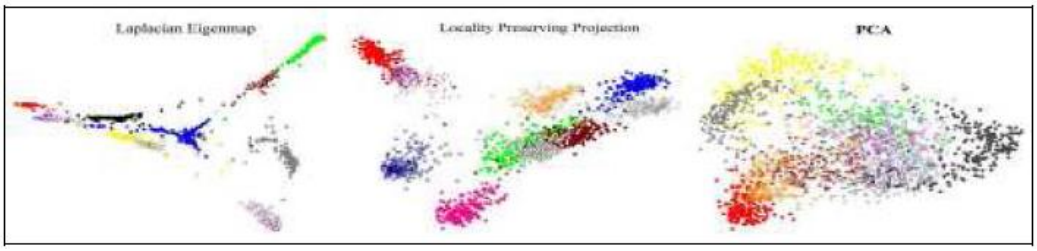


Fig. 18 En esta imagen podemos ver como a diferencia de PCA, en LPP se conserva la estructura local de los datos

Este método tiene diferentes ventajas:

- Los mapas están diseñados para reducir algunos de los criterios objetivos derivados de los métodos lineales clásicos.
- LPP conserva la estructura local de los datos, por lo que el sistema tiene el mismo "vecindario" en el espacio de baja dimensionalidad que en el de alta.

- LPP es un método lineal, por lo que es rápido y conveniente para aplicaciones prácticas.
- LPP se define para todos los casos, a diferencia de los métodos de reducción no lineal, que se definen solo para el conjunto de datos de entrenamiento, por lo que, si LPP tiene nueva información, puede representarla en un nuevo subespacio sin calcular matrices de predicción.

4.1.1.1.7.4 DCT (Discrete Cosine Transform)

La DCT es una transformación que representa una serie finita de datos como la suma de una secuencia de funciones cosenoidales fluctuando a varias frecuencias. Este método se usa ampliamente en aplicaciones de procesamiento de señales, desde compresión de audio e imágenes hasta métodos espectrales para resolver numéricamente ecuaciones diferenciales. Uno de sus usos es el reconocimiento facial.

4.1.1.1.8. Tecnicas basadas en modelos

Correspondencia entre Agrupaciones de Grafos Elásticos (Elastic Bunch Graph Matching, EBGM)

Este método, a diferencia de otros métodos que se basan en el análisis lineal de imágenes, se basa en características tales como cambios en la iluminación, la postura y la expresión de la persona.

EBDM utiliza la transformación de Gabor, se crea un patrón que se proyecta sobre la superficie de la celda elástica, que rastrea el comportamiento de la imagen con un solo píxel, como se muestra en la figura 19. Esto se logra combinando la imagen con un filtro Gabor, ya que se emplea para el reconocimiento de patrones y la extracción de características a través del procesamiento de imágenes.

Se logran varias características de zonas diferentes que permiten ubicar las similitudes y las diferencias de las imágenes de entrenamiento, estas secciones se fraccionan en 6 regiones las cuales se reunen en:

- 2 regiones para los ojos
- 2 regiones para las cejas
- 1 región para la sección que rodea la boca

- 1 región para las fosas nasales

Fig. 19 Correspondencia entre agrupaciones de grafos elásticos

4.1.1.1.8.1 Patrones binarios locales (Local Binary Pattern, LBP)

Un patrón binario local es un descriptor de textura en la imagen alrededor del cual se examina cada píxel (p). Para cada píxel a su alrededor, debemos establecer si el valor de intensidad es mayor o menor que el valor de intensidad de píxel (p). Si el valor es mayor se le asigna 1, en caso contrario se le asigna 0.

4.1.1.1.8.2 Modelo oculto de Markov (Hidden Markov Models, HMM)

Un modelo oculto de Markov es un modelo estadístico que asume que el sistema que se está modelando es un proceso de Markov con características que no se conocen. El objetivo es establecer las características que no se conocen de esta cadena a partir de las características observables. El modelo oculto de Márkov se utiliza específicamente para el reconocimiento de patrones temporales, como reconocimiento de voz, línea, gestos, marcado gramatical o en bioinformática.

4.1.1.1.8.3 Métodos Basados en Imágenes 3D

Se han creado distintos softwares utilizando modelos faciales 2D y 3D. La toma de fotografías de la cara se realiza con varias cámaras y un escáner especial. Estas investigaciones se realizan puesto que con el modelo del rostro en 3D del usuario se puede desarrollar comparaciones menos sensibles a factores como: la iluminación, estado de ánimo y la posición del rostro.

4.1.1.1.8.4 Análisis de componentes Independientes (Independent Component Analysis, ICA)

ICA es un método para calcular los vectores base de un área que son estadísticamente independientes. Está considerado como un descendiente de PCA, además ICA se enfoca en la transformación lineal para reducir la dependencia estadística entre los vectores base. Los vectores principales del subespacio de proyección obtenidos por análisis de componentes independientes no son ortogonales ni están ordenados por ningún criterio en comparación con los obtenidos por PCA.

El análisis de componentes principales intenta capturar una representación de entrada de variables correlacionadas, mientras que ICA intenta capturar una representación de variables estadísticamente independientes. Las imágenes de bases de datos obtenidas con ICA almacenan más información espacial que las obtenidas con PCA. A pesar de ello, el tiempo de entrenamiento para ICA es mucho más largo que para PCA.

4.1.2. Definir los requisitos necesarios de diseño del sistema de reconocimiento facial con base en las condiciones de acceso a una escuela.

Definición de requerimientos

- El centro educativo tiene un horario establecido que se debe intentar cumplir, excepto por aquellos motivos de fuerza mayor.
- Registro de las personas ajenas que acceden al centro (personal de servicios, visitas, etc.) y del motivo del acceso.
- El horario establecido de entrada es de 7:30 a 8:00 am para alumnado y profesores
- Prohibido acercarse a lugares potencialmente peligroso y/o prohibidos
- Rondas periódicas por parte del auxiliar al interior y antes y después del cierre de cada jornada, verificando que no haya quedado nadie en el colegio
- Infórmese y regístrese si así lo amerite en casos excepcionales ausencias de alumnos antes del horario o dentro del horario escolar activo.
- La profesora de cada aula sale en orden con sus alumnos en fila a la puerta de salida a las 12:15 pm en donde le espera la auxiliar quien llama a los padres de esa

sección que se acerquen, los padres llaman a sus hijos y la auxiliar debe cerciorarse que en efecto es el padre, madre o familiar del alumno y deja que se vaya.

Definir los requerimientos imprescindibles para la adaptación del control de acceso en la I. E. como:

● Dejar entrar a la escuela tras identificación.

● El detalle de recientes alumnos o personal al sistema del control de acceso.

Las condiciones típicas de acceso al sistema se determinan teniendo en cuenta varios aspectos, por ejemplo:

● Confirmar el acceso al identificar.

● Restringir acceso si el sistema no identifica al individuo.

● Reconocer las situaciones de acceso típicas y de entorno controlado

● Las condiciones climáticas.

Requerimientos No funcionales.

- El sistema debe funcionar en tiempo real, lo que significa que la efectividad de la técnica de reconocimiento facial debe ser alta para que los procedimientos computacionales se elaboren en un tiempo razonable.

4.1.3. Escoger la técnica de reconocimiento facial que permita tener en cuenta las condiciones previamente definidas.

Tabla 4. Ventajas y desventajas de las técnicas de reconocimiento facial

Técnica	Ventajas	Desventajas
PCA	Reduce la dimensionalidad de un conjunto de dato. Se utiliza para distinguir las semejanzas y las diferencias mediante combinaciones lineales entre la imagen obtenida y la guardada. Algoritmo sencillo Se implementa fácilmente Sistema para desarrollar en tiempo real	Dificultada al trabajar en ambientes no controlados. La brillosidad en las imágenes lo que dificulta el reconocimiento

	Trabaja con base de datos pequeñas Es la técnica principal de todas Utiliza Eigenfaces	
LDA	Minimiza la varianza entre clases conocidas Maximiza la varianza entre clases desconocidas	Tienen problema de matrices singulares. Es dificultuoso al restablecer los datos originales.
EBGM	Utiliza la transformación de Gabor, es decir solo puntos de referencia. La posición, expresión y la iluminación no afecta.	La ubicación precisa de los puntos característicos de referencia.
LPP	Rápido para aplicación practicas Reduce la dimensión de los datos	Dificultad al recuperar los datos originales No trabaja con vectores ortogonales Es un método supervisado

A continuación, pasaremos a desarrollar los criterios de selección para poder definir los puntos sobre los cuales seleccionaremos al método más adecuado para el desarrollo del
presente proyecto.

Criterios de selección

Para la selección del modelo de control de acceso, se tomará en cuenta los siguientes criterios que mencionaremos a continuación los cuales tendrán una ponderación numérica:

Algoritmo sencillo → 1
La iluminación no lo afecta →2
El reconocimiento es simple y efectivo →3
Trabaja con base de datos pequeñas →4
Facilidad de implementación →5

Reduce la dimensionalidad de un conjunto de datos →6

Normalizar los rostros de entrenamiento respecto al rostro promedio. →7

Utiliza Eigenfaces →8

Tabla 5. Calificación de las técnicas de reconocimiento facial a través de criterios

	TECNICAS DE RECONOCIMIENTO FACIAL			
CRITERIOS	**PCA**	**LDA**	**EBGM**	**LPP**
Algoritmo sencillo	1			
La iluminación no lo afecta		2	2	2
Trabaja con base de datos pequeñas	4			
Facilidad de implementación	5			
Reduce la dimensionalidad de un conjunto de datos	6			6
El reconocimiento es simple y efectivo	3			
Normalizar los rostros de entrenamiento respecto al rostro promedio.	7			
Utiliza Eigenfaces	8			
Puntaje total	**34**	**2**	**2**	**8**

Se escogió la técnica que está más acorde a las condiciones típicas que requiere el sistema en este caso será el PCA

4.1.4. Implantar el sistema de reconocimiento facial.

4.1.4.1 Herramientas de desarrollo

La implementación de esta investigación demanda la utilización de varias herramientas de software diseñadas para lograr un objetivo específico, todas las herramientas utilizadas en este proyecto se enumeran a continuación.

Biblioteca de visión por computador OpenCv

(Open Source Computer Vision Library) OpenCV es una biblioteca de software de aprendizaje automático. OpenCV se desarrolló para facilitar un soporte en común para aplicaciones de visión artificial y agilizar el uso de la visión artificial en productos comerciales. Al ser un producto con licencia gratuita, OpenCV posibilita a las organizaciones utilizar y modificar el código.

Estos algoritmos se usan para encontrar e identificar caras, reconocer cosas, catalogar acciones de personas en video, rastrear objetos cuando estos se mueven, extraer modelos 3D de objetos, generar nubes de puntos 3D desde cámaras estéreo. La biblioteca se utiliza a menudo en empresas, grupos de estudio y autoridades.

OpenCV se profundiza principalmente hacia las aplicaciones de visión en tiempo real. Tiene interfaces C ++, Python, Java y MATLAB y es compatible con Windows, Linux, Android y Mac OS.

PYTHON

Es un excelente lenguaje para programar, es interactivo, interpretable y dirigido a objetos. Python combina un alto rendimiento con una sintaxis muy clara. Tiene módulos, excepciones, clases y tipos de datos dinámicos. Hay interfaces para varias bibliotecas y para llamar al sistema, así como para varios sistemas de ventanas. Este es el lenguaje en el que se utilizan las herramientas de OpenCV para el reconocimiento facial, así como para la identificación de los puntos de referencia fáciles. Los recientes módulos integrados se escriben fácilmente en C o C ++ (u otros lenguajes, basándose en la implementación escogida).

NUMPY

NumPy es una biblioteca de lenguaje de programación PYTHON que admite la creación de grandes matrices y vectores multidimensionales junto con un amplio conjunto de funciones matemáticas de alto rendimiento para operar con ellas. NumPy es un software de código abierto y cuenta con muchos colaboradores.

SUBLIME TEXT

Sublime Text es un editor de texto y editor de código fuente, está escrito en C++ y Python para los plugins. Se puede descargar y valorar de forma gratuita. La versión de evaluación funciona totalmente completa y no tiene fecha de vencimiento.

* **EIGENFACES**

Eigenfaces son un grupo de vectores propios utilizados para la identificación facial elaborado por Lawrence Sirovich y Robert Kirby.

EigenFace es un grupo de vectores propios, por lo que la palabra al momento de descomponerla completa significaría grupo de vectores aplicados a la cara, ya que la cara tiene vectores y ángulos.

La gran característica de este concepto en el área de la identificación facial es que cuando un conjunto de imágenes ya está integrado en la base de datos, EigenFace junta estas imágenes en un tamaño bastante más pequeño y facilita su lectura o comparación con un algoritmo.

EigenFace es un grupo de vectores, y dichos vectores junto con las imágenes son la consecuencia de la matriz de covarianza de la distribución de probabilidad en el espacio vectorial de alta dimensión de imágenes de rostros.

Se utilizó Haar Cascades de OpenCV.

La detección de objetos mediante clasificadores en cascada basados en funciones de Haar es un método eficaz de detección de objetos propuesto por Paul Viola y Michael Jones en su artículo, "Detección rápida de objetos mediante una cascada potenciada de funciones simples" en 2001. Es un enfoque basado en el aprendizaje automático en el que una función de cascada se entrena a partir de muchas imágenes positivas y negativas. Luego se usa para detectar objetos en otras imágenes.

Inicialmente, el algoritmo necesita muchas imágenes positivas (imágenes de rostros) e imágenes negativas (imágenes sin rostros) para entrenar al clasificador. Luego necesitamos extraer características de él.

OpenCV proporciona un método de entrenamiento o modelos previamente entrenados, que se pueden leer mediante el método cv::CascadeClassifier::. Los modelos preentrenados se encuentran en la carpeta de datos en la instalación de OpenCV.

Las etapas para el reconocimiento facial son las siguientes:

1. **Detección de la cara:** Para la detección de rostros se empleó la librería de OpenCV apoyada de un haar cascade, en este caso el haar cascade frontalface. Con la finalidad de detectar en primera instancia un rostro. Se tuvo en cuenta también la aplicación de filtros para facilitar la detección de los rostros, los filtros aplicados en la captura de imagen fueron los siguientes:

   • Blanco y Negro: Su aplicación dentro del proyecto es de preprocesamiento. Para facilitar la detección con el haar cascade empleado.

• Recorte: Se aplica un recorte en el área resultante del filtro haar, con la finalidad de obtener un plano de rostro antes de ser procesado.

Fig. 20. Detección de la cara

Posteriormente, la detección se realiza mediante el método cv::CascadeClassifier::detectMultiScale , que devuelve rectángulos de contorno para los rostros detectados.

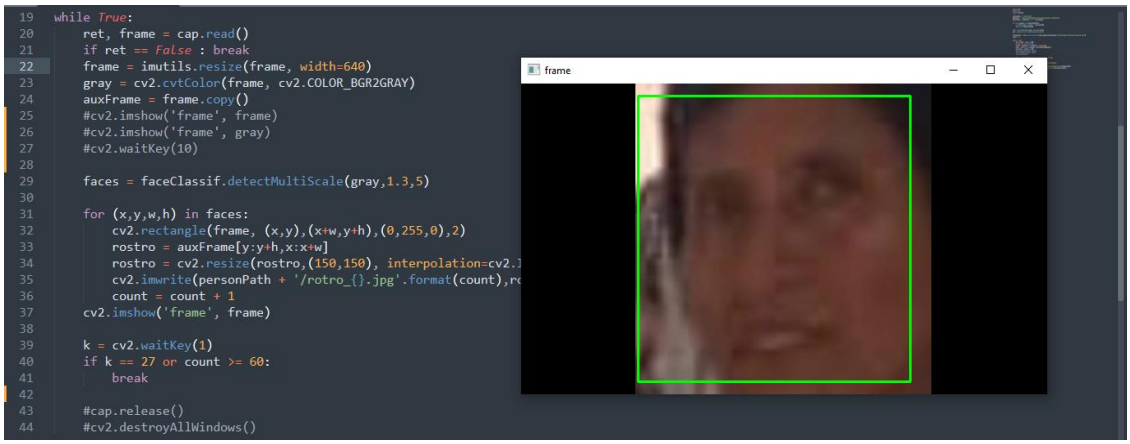
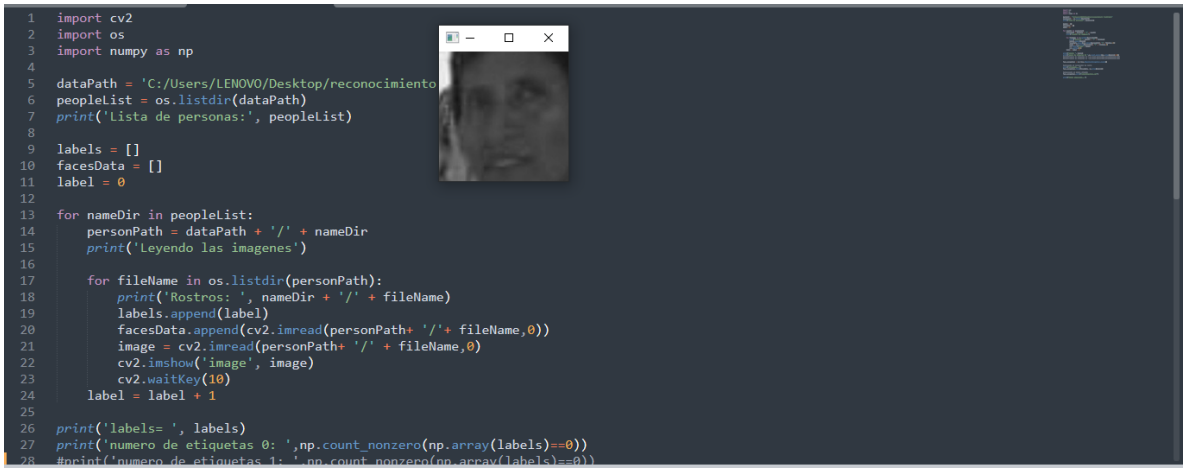


Fig. 21 Detección con detectMultiScale

2. **Análisis facial:** localizar los componentes del rostro y, mediante transformaciones geométricas, normalizarlo según propiedades geométricas, como el tamaño y la postura. También se especifica el tamaño de la imagen y la gama de colores. Usualmente, para reducir la carga computacional del sistema, se usa imágenes pequeñas en escala de grises.

3. **Extracción de rasgos:** proporciona información para distinguir rostros de diferentes personas en base a variaciones geométricas fotométricas.



```python
import cv2
import os
import numpy as np

dataPath = 'C:/Users/LENOVO/Desktop/reconocimiento
peopleList = os.listdir(dataPath)
print('Lista de personas:', peopleList)

labels = []
facesData = []
label = 0

for nameDir in peopleList:
    personPath = dataPath + '/' + nameDir
    print('Leyendo las imagenes')

    for fileName in os.listdir(personPath):
        print('Rostros: ', nameDir + '/' + fileName)
        labels.append(label)
        facesData.append(cv2.imread(personPath+ '/'+ fileName,0))
        image = cv2.imread(personPath+ '/' + fileName,0)
        cv2.imshow('image', image)
        cv2.waitKey(10)
    label = label + 1

print('labels= ', labels)
print('numero de etiquetas 0: ',np.count_nonzero(np.array(labels)==0))
#print('numero de etiquetas 1: ',np.count_nonzero(np.array(labels)==0))
```

Fig. 22. Analisis facial/ Extracción de rasgos

4. **Reconocimiento:** Los vectores de características extraídos se comparan con los vectores de características extraídos de las caras en la base de datos. Si encuentra uno con un alto porcentaje de similitud, devuelve la autenticidad del rostro; de lo contrario resulta que es una cara desconocida.

```python
import cv2
import os

dataPath = 'C:/Users/LENOVO/Desktop/reconocimiento facil/data'
imagePaths = os.listdir(dataPath)
print('imagePaths=',imagePaths)

face_recognizer = cv2.face.EigenFaceRecognizer_create()

#Leyendo el modelo
face_recognizer.read('modeloEigenFace.xml')

cap = cv2.VideoCapture('C:/Users/LENOVO/Desktop/reconocimiento facil/imagenes y videos/auxiliar-profesora.mp4')

faceClassif = cv2.CascadeClassifier(cv2.data.haarcascades+'haarcascade_frontalface_default.xml')

while True:
    ret, frame = cap.read()
    if ret == False : break
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    auxFrame = gray.copy()

    faces = faceClassif.detectMultiScale(gray,1.3,5)
```

Fig 23. Leyendo el modelo que se quiere reconocer

```
    for (x,y,w,h) in faces:
        rostro = auxFrame[y:y+h,x:x+w]
        rostro = cv2.resize(rostro,(150,150), interpolation= cv2.INTER_CUBIC)
        result = face_recognizer.predict(rostro)

        cv2.putText(frame, '{}'.format(result),(x,y-5),1,1.3,(255,255,0),1,cv2.LINE_AA)

        #EigenFaces
        if result[1] < 1000:
            cv2.putText(frame, '{}'.format(imagePaths[result[0]]),(x,y-25),2,1.1,(255,255,0),1,cv2.LINE_AA)
            cv2.rectangle(frame, (x,y),(x+w,y+h),(0,255,0),2)
        else:
            cv2.putText(frame, 'Desconocido'.format(imagePaths[0]),(x,y-20),2,0.8,(0,0,255),1,cv2.LINE_AA)
            cv2.rectangle(frame, (x,y),(x+w,y+h),(0,0,255),2)


    cv2.imshow('frame',frame)
    k = cv2.waitKey(1)
    if k == 27:
        break

```

Fig. 24. Comparación de imágenes

Fig. 25. Reconocimiento facial

Las etapas para el reconocimiento facial son las siguientes:

1. **Detección de la cara:**

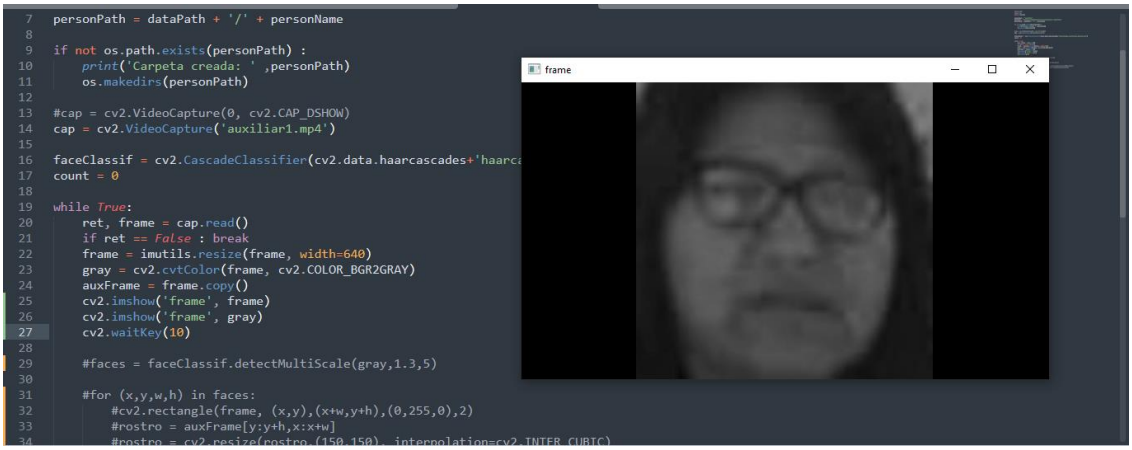


Fig. 26. Detección cara de auxiliar

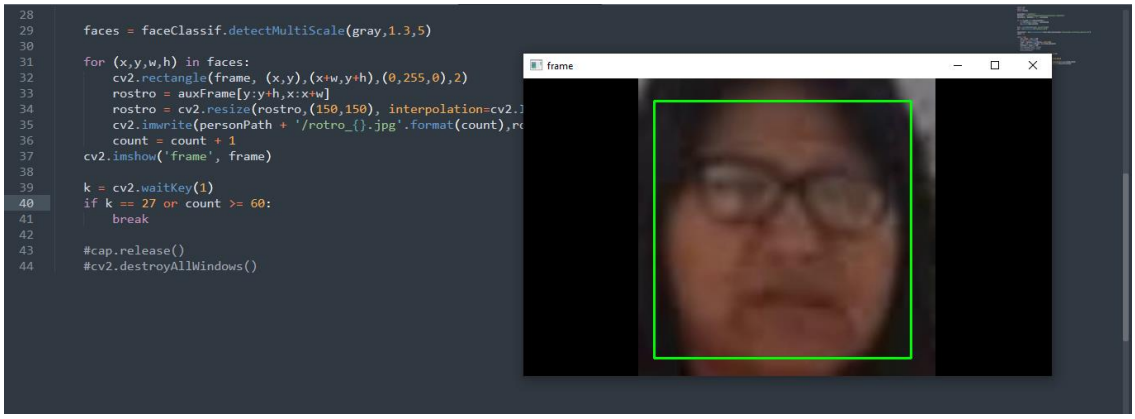


Fig. 27 Detección con detecMultiScale de la cara de auxiliar

2. **Análisis facial:**
3. **Extracción de rasgos:**

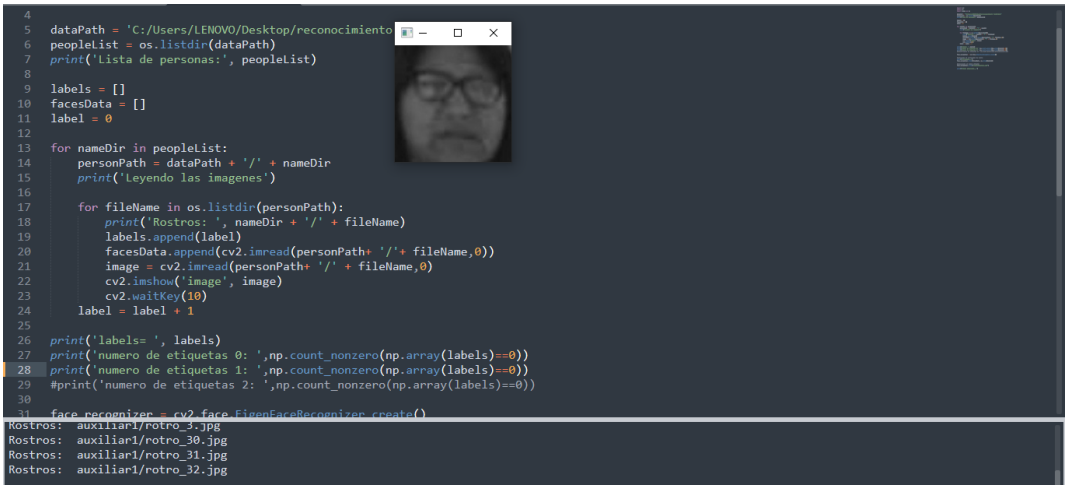


Fig. 28 Analisis facial/ Extracción de rasgos de auxiliar

4. **Reconocimiento:**

Fig. 29. Reconocimiento facial profesora y auxiliar

Las etapas para el reconocimiento facial son las siguientes:

1. **Detección de la cara:**

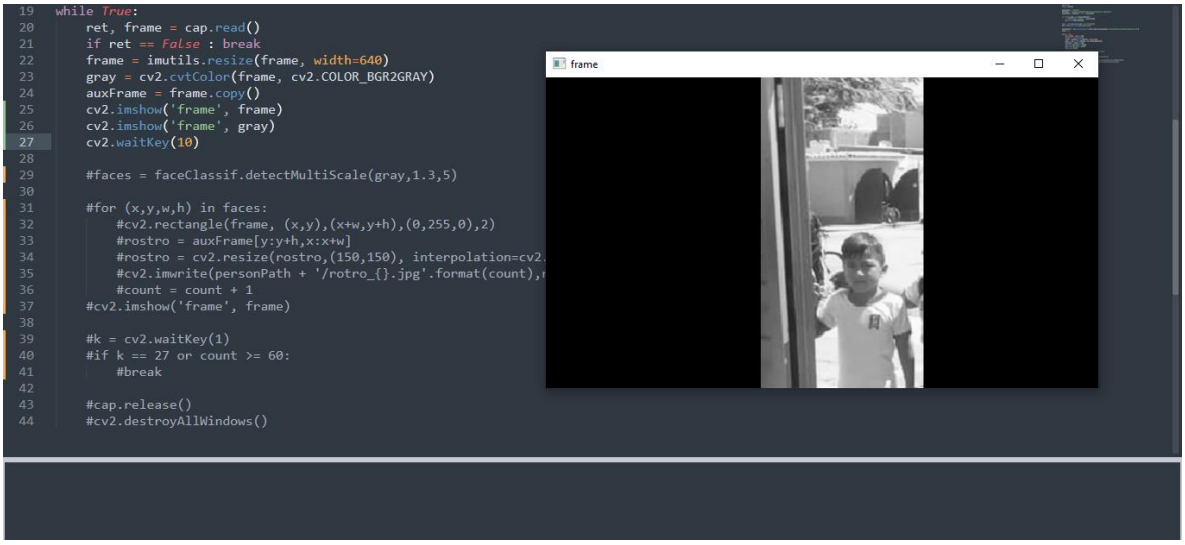


Fig. 30. Detección cara del alumno

.

Fig. 31. Detección con detecMultiScale de la cara del alumno

2. **Análisis facial:**
3. **Extracción de rasgos:**

Fig. 32 Analisis facial/ Extracción de rasgos de auxiliar

4. **Reconocimiento:**

Fig. 33. Reconocimiento facial completo (auxiliar, profesora y alumno)

4.1.5. Elaborar los resultados del proyecto.

Para este paso y poder verificar el resultado si el nivel de control de acceso mejora con desarrollo y posterior implantación de un sistema de reconocimiento facial, se realizarán dos (2) análisis de los resultados empleados los cuales se presentan a continuación.

4.1.5.1 Primer Análisis – Encuestas de eficacia antes del test

Para esto se trabajó un formato de test inicial, siendo los 22 usuarios quienes, con sus respuestas, se lograron los siguientes resultados, que se presentan, se ha elaborado de acuerdo a la escala de Likert se maneja la puntuación de 1 a 5 para verificar el nivel de eficacia con las preguntas en la encuesta aplicada.

Tabla 6 Pre – test: antes de las pruebas con el sistema de reconocimiento facial

N	Preguntas	Nada Eficaz	Poco Eficaz	Neutral	Muy Eficaz	Totalmente Eficaz
		1	2	3	4	5
1	¿Qué opina sobre el control de acceso en la Institución Educativa?	3	8	10	1	0
2	¿Qué opina sobre la labor de las auxiliares que controlan el acceso cuando entran o salen los alumnos?	1	10	9	2	0
3	¿Qué opina sobre la reacción del personal cuando alguien burla el control de acceso?	2	9	10	1	0
4	¿Qué tan eficiente es la identificación de alguien desconocido que entra a la I. E.?	5	7	8	2	0
5	¿Qué tan buena es la verificación de las personas	4	10	7	1	0

	que entran o salen de la I. E.?					
6	**¿Cree usted que el monitoreo actual en el control en la entrada y salida es eficiente?**	**5**	**10**	**6**	**1**	**0**

Tabla 7 Resumen PRE - TEST

Nivel de eficacia	Porcentaje
Nada eficaz	15%
Poco eficaz	41%
Neutral	38%
Muy eficaz	6%
Totalmente eficaz	0%
Total	100%

4.1.5.2 Segundo Análisis – Encuestas de eficacia después del test

Para esto se ejecutó el mismo formato de encuesta inicial, siendo los 22 usuarios quienes, con sus respuestas, se obtuvieron los siguientes resultados (*tabla 8*), que se presentan a continuación, se ha elaborado de acuerdo a la escala de Likert se maneja la puntuación de 1 a 5 para verificar el nivel de eficacia con las preguntas en la encuesta aplicada.

Tabla 8. Post – test: después de las pruebas con el sistema de reconocimiento facial

N	Preguntas	Nada Eficaz	Poco Eficaz	Neutral	Muy Eficaz	Totalmente Eficaz
		1	2	3	4	5
1	¿Qué opina sobre el control de acceso en la Institución Educativa?	0	0	5	9	8
2	¿Qué opina sobre la labor de las auxiliares que controlan el acceso cuando entran o salen los alumnos?	0	0	4	10	8
3	¿Qué opina sobre la reacción del personal cuando alguien burla el control de acceso?	0	0	5	10	7
4	¿Qué tan eficiente es la identificación de alguien desconocido que entra a la I. E.?	0	0	2	9	11
5	¿Qué tan buena es la verificación de las personas que entran o salen de la I. E.?	0	0	1	8	13
6	¿Cree usted que el monitoreo actual en el control en la entrada y salida es eficiente?	0	0	3	9	10
TOTAL		0	0	20	55	57

Tabla 9. Resumen POST - TEST

Nivel de eficacia	Porcentaje
Nada eficaz	0%
Poco eficaz	0%
Neutral	17%
Muy eficaz	41%
Totalmente eficaz	42%
Total	100%

Como podemos observar en ambas tablas de acuerdo a la comparación de resultados de los test se comprueba la eficacia del sistema de reconocimiento facial.

4.1.5.3 Validación del sistema (Cualidades evaluadas por expertos)

VARIABLE INDEPENDIENTE: sistema de reconocimiento facial

Los resultados de la evaluación del sistema de reconocimiento facial a través de la opinión de expertos.

Para obtener las siguientes puntuaciones del sistema de reconocimiento facial propuesta se expuso a tres expertos los atributo o características.

Tabla 10 Puntuación de Atributos por Expertos

	Atributo	Experto 1	Experto 2	Experto 3	Promedio
1	Tiempo de detección	**18**	**17**	**19**	**18**
2	Precisión de detección	**16**	**18**	**19**	**18**
					18

Validación del instrumento de recolección de datos:

Alfa de Cronbach

Se trata de un índice de consistencia que toma valores entre 0 y 1 y que sirve para comprobar si el instrumento que se está evaluando recopila información defectuosa y por tanto nos llevaría a conclusiones equivocadas o si se trata de un instrumento fiable que hace mediciones estables y consistentes.

Su fórmula es:

$$\alpha = \frac{k}{k-1}\left[1 - \frac{\sum V_i}{V_t}\right]$$

Donde:

$\alpha = Alfa\ de\ Crombach$

$K = Número\ de\ Items$

$V_i = Varianza\ de\ cada\ Item$

$V_t = Varianza\ del\ total$

ITEM		EXPERTO1	EXPERTO 2	EXPERTO 3	VARIANZA
1	Tiempo de detección	19	18	19	0.222222222
2	Precision de detección	18	16	17	0.666666667
	TOTAL	37	34	36	

$$\alpha = \frac{k}{k-1}\left[1 - \frac{\sum V_i}{V_t}\right]$$

K=	2
V_i =	0.88888889
V_t =	1.55555556
α=	0.85714286

Este coeficiente nos indica que entre más cerca de 1 este α, más alto es el grado de confiabilidad, en este caso, el resultado nos da un valor de 0,857, entonces se puede determinar que el instrumento empleado tiene un alto grado de confiabilidad.

4.2. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Tabla 11. Resultados de Encuestas Inicial y Final

Resultados de Encuestas		
Grado de eficacia	**Inicial**	**Final**
Nada eficaz	15%	0%
Poco eficaz	41%	0%
Neutral	38%	17%
Muy eficaz	6%	41%
Totalmente eficaz	0%	42%

El tiempo de respuesta de la aplicación se encuentra alrededor de 0.5 segundos. Las pruebas demostraron un porcentaje de coincidencia cercano al 97%, para los casos en los que la imagen objetivo y la imagen fuente no coinciden se presentó como resultado desconocido, importante destacar que el sistema fue construido para hacer una identificación basada en una toma frontal del rostro pues la detección automática del mismo se diseñó de esta forma.

4.3. Prueba de Hipótesis

En la presente investigación se confirma la veracidad de la hipótesis porque mediante la comparación de resultados tanto del primer cuestionario como el final, así como la validación por parte de expertos se comprueba in situ que el desarrollo y posterior implantación del sistema de reconocimiento facial es eficaz para el control de acceso.

- **CONCLUSIONES**

Al hacer la recopilación de información de las técnicas de reconocimiento facial se determinó que se usaría la técnica de reconocimiento facial PCA junto al EigenFaces, debido a varios motivos que la priorizan. Estos se deben a su baja complejidad computacional y bajo uso de recursos de imagen. Esto proporciona tiempos de respuesta muy aceptables y una detección precisa. No solo es uno de los algoritmos más representativos y confiables en la colectividad de investigadores, sino que también se puede combinar con otros métodos para mejorar el entrenamiento en imágenes de referencia.

En el marco de la elaboración de requerimientos de cómo debería ser el sistema de reconocimiento facial, todas ellas se fundamentaron en el ambiente de trabajo en la que se elaboró el sistema, por este motivo se tuvieron en cuenta cualidades propias de la I. E.; estas cualidades pueden afectar el funcionamiento aceptable si estas no se tienen en cuenta para la construcción de dicho sistema, ya que este alcanzaría a tener fallas o inclusive ocasionar que el reconocimiento facial no sea una técnica segura para el control de acceso.

Los valores de reconocimiento vistos en las pruebas están supeditados grandemente de las imágenes de entrenamiento que se efectúen, entre más fotos y más poses se realicen, superior será el reconocimiento facial.

Esta investigación aunque elaborado para su utilización en una I. E., no está exceptuado de usarse en otros sectores como banco, agroindustria, etc., donde el sistema de seguridad debe ser confiable, no obstante para estas ocasiones se deberían hacer indagaciones previas antes de elaborar este sistema en otros lugares, ya que el sistema presentado tiene rasgos particulares como: el mínimo de personas que tiene el sistema, la base de datos está ordenada solo por el nombre del individuo, la base de datos y el procesamiento del dispositivo esta proporcionado por la placa de desarrollo que se use.

El sistema presentado es óptimo para su elaboración en la I. E. y prometerá seguridad y bienestar a la hora de instalarlo como control de acceso.

- **RECOMENDACIONES**

Se recomienda implementar un sistema de control de acceso de los individuos que estudian y trabajan con reconocimiento facial ya que se basa en los rasgos de cada persona. Esto ayuda a evitar el robo de identidad al registrar la entrada y la salida.

Ejecutar el mantenimiento de la base de datos de las caras de los docentes y alumnos en un espacio de tiempo (3 años) para no pasar dificultades a la hora del reconocimiento facial, debido a que con el pasar de los años cambian las características físicas de las personas.

Se debe poner en marcha la elaboración de una fuente de alimentación ininterrumpida para proporcionar electricidad en caso de una falla del servicio y no afectar al sistema de reconocimiento facial.

Se recomienda que los administradores del sistema tengan estudios elementales de administración de software para poder manejar adecuadamente la información de los docentes, alumnado y personal administrativo registrada en el sistema.

- **REFERENCIAS BIBLIOGRÁFICAS**

Apaza, R., & Charaja , G. (2013). "*Sistema para detección y reconocimiento facial utilizando técnicas híbridas en imágenes y secuencias de video Puno 2013".* Repositorio Institucional UNAP, Puno. Obtenido de https://renati.sunedu.gob.pe/handle/sunedu/2905700

Mosquera & Romero, (2016). "*Diseño de un Software Piloto de Reconocimiento Facial para el Control de Asistencia en la Escuela de Telecomunicaciones de la Universidad de Carabobo*", Carabobo, Venezuela

Mariño, (2018). "*Aplicación móvil de reconocimiento facial en personas con trabajo previos de abuso sexual en la provincia de Andahuaylas, Apurímac - 2018*"

Caballero, Reyes, Sánchez, & Ríos (2017). "*Reconocimiento facial por el método de eigenfaces*". Tecnológico Nacional de México, México.

Cáceres, E. (2018). *Aplicación móvil de reconocimiento facial en personas con antecedentes de abuso sexual en la provincia de Andahuaylas, Apurímac - 2018.* Obtenido de https://renati.sunedu.gob.pe/handle/sunedu/2894847

Castano, D. L., & Alonso, J. D. (2019). *Sistema de reconocimiento facial para control de acceso a viviendas.* Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/24032/1/Final%20Trabajo%20de%20grado.pdf

Conde, R. (2017). *The new way to deliver technology.*

Espinoza, E. (2018). *La hipótesis en la investigación.*

Ipanaqué, J. (2020). *Análisis comparativo de técnicas de reconocimiento facial en ambientes no controlados para optimizar el proceso de registro de personal de la ugel ferreñafe.* Obtenido de https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/6964/JOS%C3%89

%20JES%C3%9AS%20IPANAQU%C3%89%20CASANOVA.pdf?sequence=1&isAllowed=y

Larcher, L., Biasoni, E., Cattaneo, C., Ruggeri, A., & Herrera, C. (2011). Algoritmo para Detección de Bordes y Ulterior Determinación de Objetos en Imágenes Digitales. Obtenido de https://cimec.org.ar/ojs/index.php/mc/article/view/3955

Calles Carrasco, M. F. (2019). "*Sistema informatico de reconocimiento facial para el registro y control de asistencia de los socios de la coperativa de taxis y camionetas Puyo.* Puyo - Ecuador.

Castro Arias, Romel D. (2016) *Sistema de control de acceso al personal de la lavadora de Jeans Fashion mediante reconocimiento facial.* Ambato, Ecuador.

Conde, R. (2017). *The new way to deliver technology.*

Martinez, Rafael Cazorla. Software para la detección y el reconocimiento de rostros. Universitat Autònoma de Barcelona, Barcelona 2016. https://ddd.uab.cat/pub/tfg/2016/tfg_49339/Software_para_la_deteccio_n_y_el_reconocimiento_de_caras.pdf

Meneses Alvaro, Vargas Cristian (2016). *Diseño e Implementación de un Prototipo para el Control de Acceso en la Sede de Ingeniería de la Universidad Distrital Francisco José de Caldas Mediante el Uso de Torniquetes Controlados por Carnet con Tegnología NFC y Lector Biométrico de Huella Dactilar*. (Tesis de grado). Universidad Distrital Francisco José de Caldas, Bogotá, Colombia. https://repository.udistrital.edu.co/bitstream/handle/11349/3430/VargasGarciaCristianGerman2016.pdf;jsessionid=56C215D7068215056DE7452D248A54C5?sequence=1

Espinoza, E. (2018). *La hipótesis en la investigación.*

Larcher, L., Biasoni, E., Cattaneo, C., Ruggeri, A., & Herrera, C. (2011). Algoritmo para Detección de Bordes y Ulterior Determinación de Objetos en Imágenes Digitales. Santa Fe, Argentina.

R. G. Hernández, *Estudio de técnicas de reconocimiento facial*, Barcelona, España, 2010. https://upcommons.upc.edu/bitstream/handle/2099.1/9782/PFC_RogerGimeno.pdf

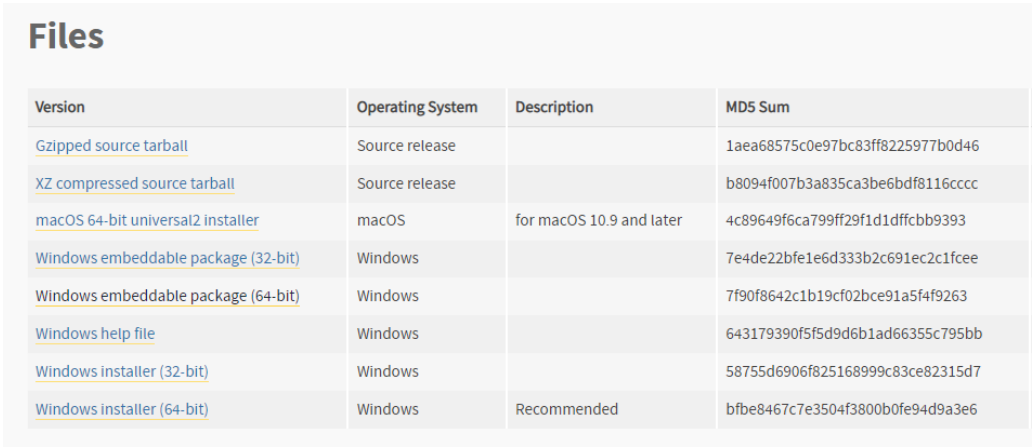
VEGA Luna, J. I., Sánchez-Rangel, F. J., Salgado-Guzmán, G., & Lagos-Acosta, M. (2018). Sistema de acceso usando una tarjeta RFiD y verificación de rostro. https://www.redalyc.org/journal/5055/505555586010/html/#:~:text=El%20alcance%20de%20lectura%20de,ms%20usando%20310%20fotograf%C3%ADas%20entrenadas.

ANEXOS

Instalación de Pyhton:

1. Ingresar a https://www.python.org/downloads/
2. Ir a Downloads luego clic en windows

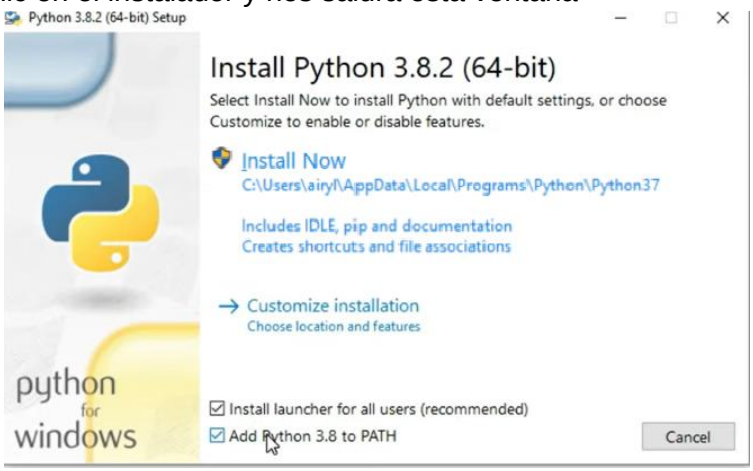
3. Clic en la versión para Windows de 64 bits



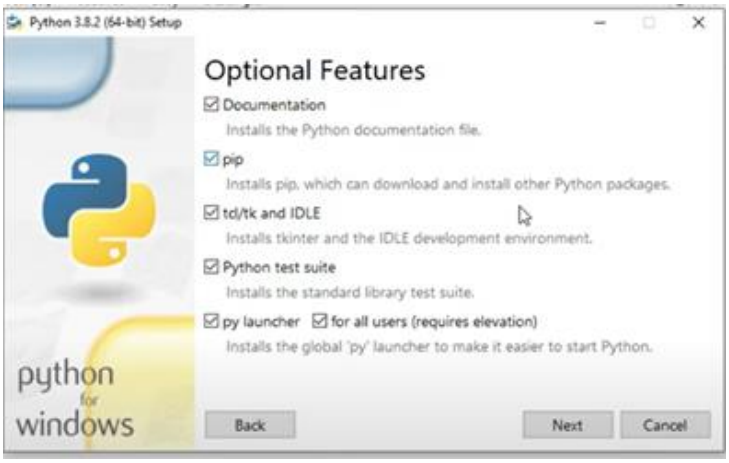
Files

Version	Operating System	Description	MD5 Sum
Gzipped source tarball	Source release		1aea68575c0e97bc83ff8225977b0d46
XZ compressed source tarball	Source release		b8094f007b3a835ca3be6bdf8116cccc
macOS 64-bit universal2 installer	macOS	for macOS 10.9 and later	4c89649f6ca799ff29f1d1dffcbb9393
Windows embeddable package (32-bit)	Windows		7e4de22bfe1e6d333b2c691ec2c1fcee
Windows embeddable package (64-bit)	Windows		7f90f8642c1b19cf02bce91a5f4f9263
Windows help file	Windows		643179390f5f5d9d6b1ad66355c795bb
Windows installer (32-bit)	Windows		58755d6906f825168999c83ce82315d7
Windows installer (64-bit)	Windows	Recommended	bfbe8467c7e3504f3800b0fe94d9a3e6

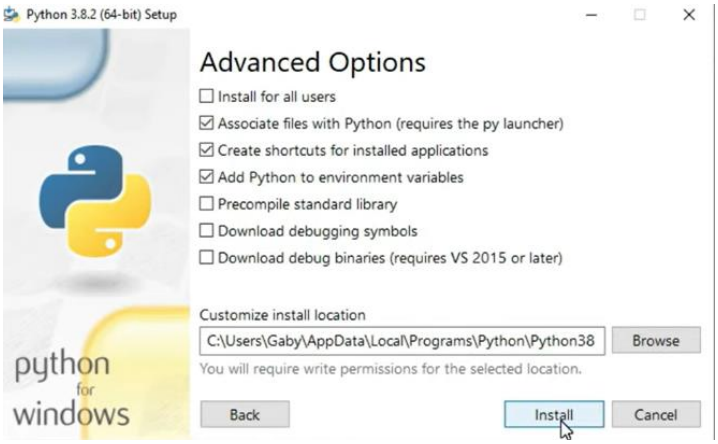
4. Clic en el instalador y nos saldrá esta ventana



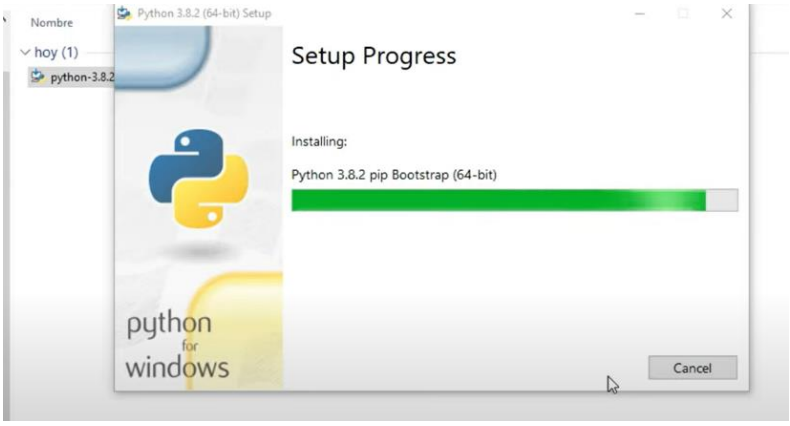
5. Clic en Customize installation – saldrá esta ventana, clic en pip y luego en Next



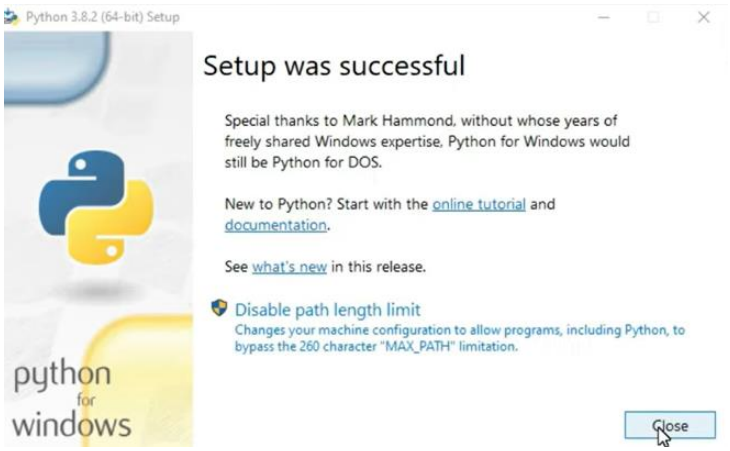
6. Clic en Next



7. Comenzará la instalación

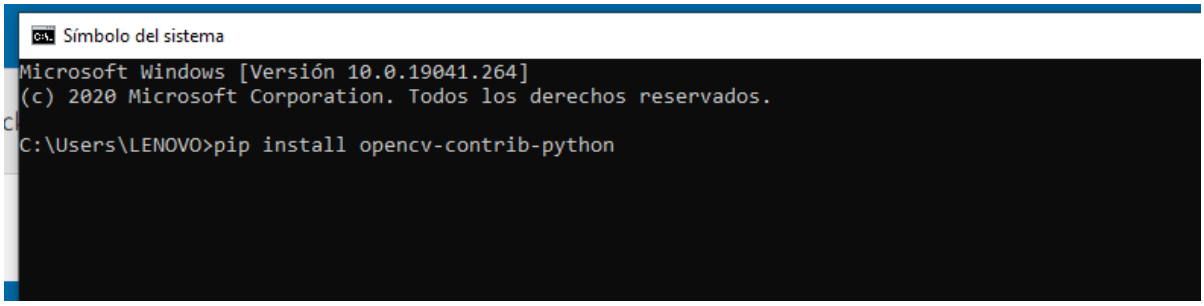


8. Finalizacion de instalación, clic en close

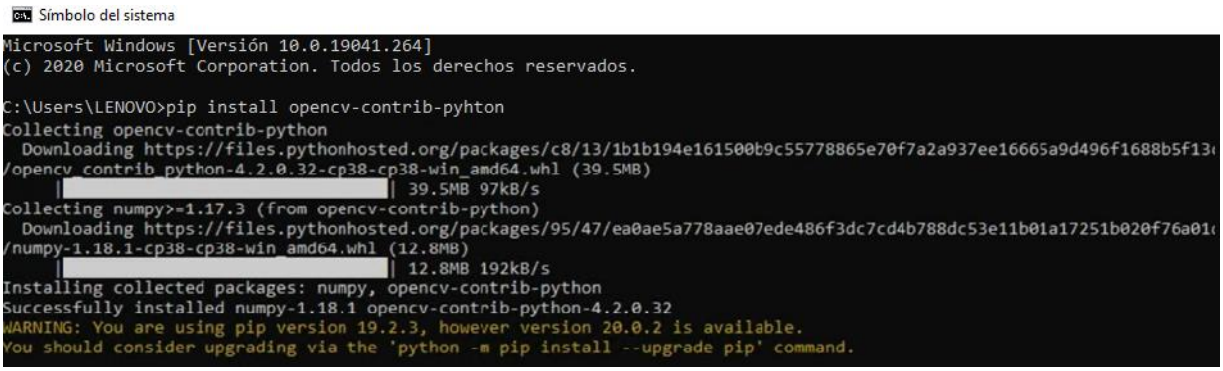


Instalación de OPENCV

1. Escribimos en el símbolo del sistema pip install opencv-contrib-pyhton y damos enter



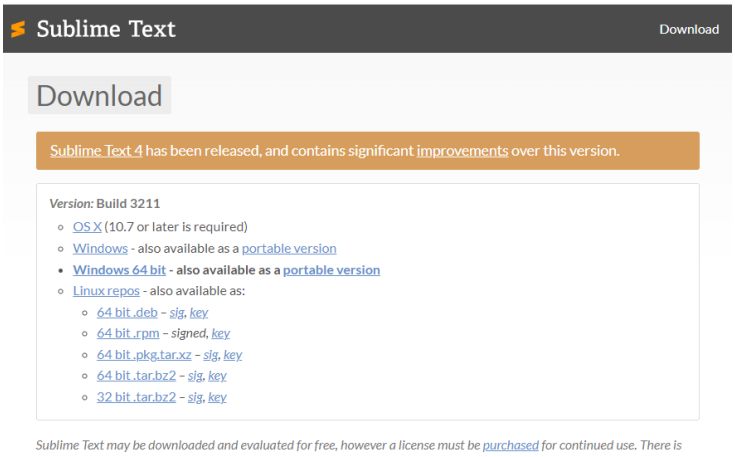
2. Esperamos que se instale



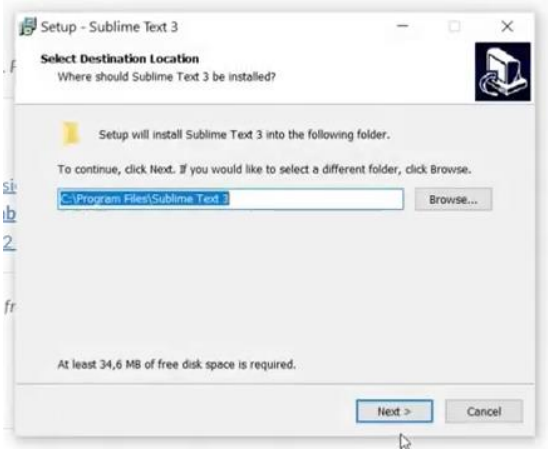
Instalacion de Sublime text

1.Nos vamos a https://www.sublimetext.com/3

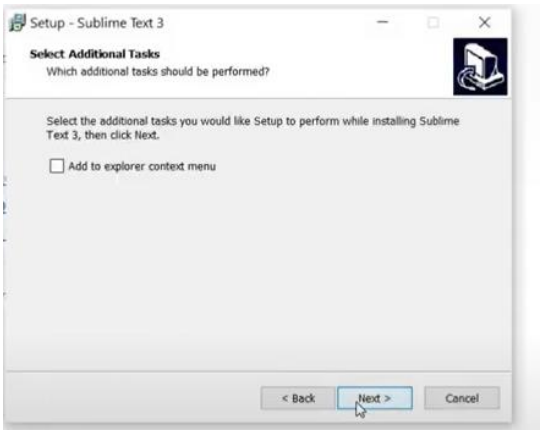
2. Clic en Windows de 64 bits



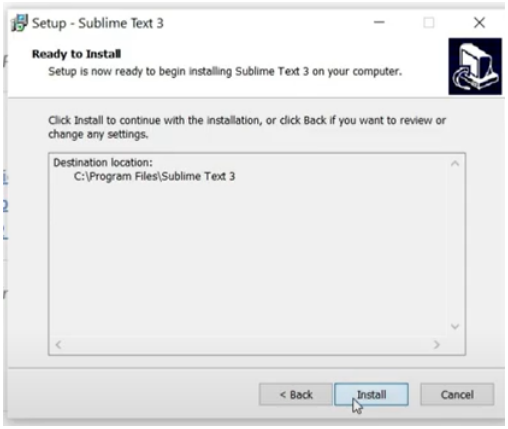
3. Clic en el instalador, luego en Next



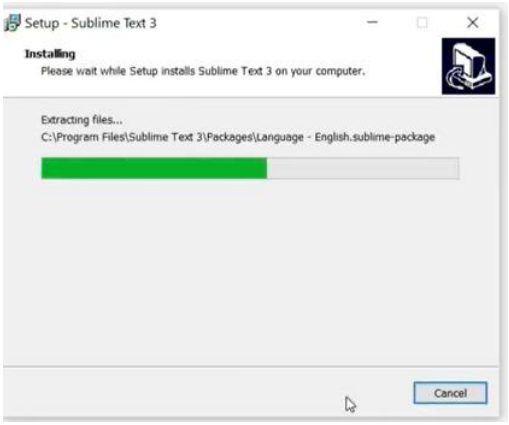
4. Clic en Next



5. Clic en Install



6. Se instalará



7. Clic Finalizar