UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

SISTEMA DE AUTENTICACIÓN BIOMÉTRICA MEDIANTE TÉCNICAS DE APRENDIZAJE PROFUNDO EN EL COLEGIO INDUSTRIAL 32 DE PUNO

TESIS

PRESENTADA POR:

Bach. NELSON YOEL PHUÑO CAHUANA

Bach. DAYSI SAIMIRA MACHACA CONDORI

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO – PERÚ

2024

NELSON YOEL PHUÑO CAHUANA DAYSI SAIMIRA ...

SISTEMA DE AUTENTICACIÓN BIOMÉTRICA MEDIANTE TÉCNICAS DE APRENDIZAJE PROFUNDO EN EL COLEGIO IN...

tesis 20204

tesis 20204

Universidad Nacional del Altiplano

Detalles del documento

Identificador de la entrega
trn:oid:::8254:417213979

Fecha de entrega
18 dic 2024, 9:54 a.m. GMT-5

Fecha de descarga
18 dic 2024, 9:59 a.m. GMT-5

Nombre de archivo
04 - SISTEMA DE AUTENTICACIÓN BIOMÉTRICA MEDIANTE TÉCNICAS DE APRENDIZAJE PROFUND....pdf

Tamaño de archivo
1.8 MB

103 Páginas

18,796 Palabras

112,190 Caracteres

turnitin Página 1 of 107 - Portada Identificador de la entrega trn:oid:::8254:417213979

5% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 12 palabras)

Fuentes principales

4% Fuentes de Internet
0% Publicaciones
3% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.° de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Universidad Nacional del Altiplano
Firmado digitalmente por GOMEZ QUISPE Hugo Yosef FAU 20145496170 soft
Motivo: Soy el autor del documento
Fecha: 18.12.2024 10:00:58 -05:00

V°B°
Firmado digitalmente por SOTOMAYOR ALZAMORA Guina Guadalupe FAU 20145496170 hard
Motivo: Doy V°B°
Fecha: 18.12.2024 17:05:19 -05:00

turnitin Página 2 of 107 - Descripción general de integridad Identificador de la entrega trn:oid:::8254:417213979

DEDICATORIA

Este proyecto está dedicado a Dios, quien me ha dado la fortaleza y la sabiduría para superar cada obstáculo, permitiéndome llegar a este momento tan importante. A mi querida familia, que ha sido mi mayor apoyo, especialmente a mi madre por su amor incondicional y a mi hermana por su constante motivación y ánimo.

Nelson Yoel Phuño Cahuana

DEDICATORIA

A mi familia, que con sus enseñanzas y su ejemplo me formaron como la persona que soy hoy. Gracias por inculcarme valores y por estar siempre presentes en mi vida, apoyándome a cada paso del camino. Este logro también les pertenece.

Daysi Saimira Machaca Condori

AGRADECIMIENTOS

A la Universidad Nacional del Altiplano de Puno, a la Escuela Profesional de Ingeniería de Sistemas.

A todos nuestros docentes por los valiosos conocimientos que nos impartieron a lo largo de nuestra formación.

A los Jurados del presente trabajo de investigación, por su tiempo y dedicación en la evaluación y concreción de esta tesis.

A todas las personas, familiares y amigos, que nos apoyaron en diversos aspectos para la culminación de nuestra Carrera Profesional.

Nelson Yoel Phuño Cahuana

Daysi Saimira Machaca Condori

ÍNDICE GENERAL

Pág.

DEDICATORIA

AGRADECIMIENTOS

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

ACRÓNIMOS

RESUMEN 16

ABSTRACT 17

CAPÍTULO I

INTRODUCCIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA **19**

1.2. FORMULACIÓN DEL PROBLEMA **21**

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN **21**

1.4. OBJETIVOS DE LA INVESTIGACIÓN **22**

1.4.1. Objetivo general 22

1.4.2. Objetivos específicos 22

1.5. HIPÓTESIS DE LA INVESTIGACIÓN **23**

1.6. DELIMITACIÓN DE INVESTIGACIÓN **23**

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1 **ANTECEDENTES** 25

2.1.1. Antecedentes Locales 25

2.1.2. Antecedentes Nacionales 26

2.1.3. Antecedentes Internacionales 27

2.2. MARCO TEÓRICO 29

2.2.1. Aprendizaje Profundo para la Biométrica 29

2.2.2. Reconocimiento Facial Biométrico con Redes Neuronales Profundas 29

2.2.3. Autenticación Táctil Basada en la Nube con Aprendizaje Profundo..... 30

2.2.4. Modelos de Detección de Ataques Basados en Datos para Reconocimiento Facial 31

2.2.5. Avances en Biométrica Mediante Aprendizaje Profundo..... 31

2.2.6. Autenticación por Huella Dactilar con Redes Neuronales Convolucionales 32

2.2.7. Aprendizaje Automático para Aplicaciones Biométricas 32

2.2.8. Biometría de Voz Usando Redes Neuronales Profundas..... 33

2.2.9. Reconocimiento Facial en Entornos Educativos con Aprendizaje Profundo 33

2.2.10. Autenticación Biométrica en Escuelas: Retos y Soluciones 34

2.2.11. Autenticación Biométrica Suave para Plataformas de Aprendizaje en Línea..... 34

2.2.12. Sistemas Biométricos Basados en el Iris Usando CNN 35

2.2.13. Avances en Biometría Profunda y Aplicaciones..... 35

2.2.14. Análisis Comparativo de Modelos de Aprendizaje Profundo para Reconocimiento Facial..... 36

2.2.15. Blockchain Biométrico para la Seguridad de Datos Vehiculares 36

2.2.16. Estimación de Flujo Óptico con Aprendizaje Profundo. 37

2.2.17. Biometría Espectral Profunda: Desafíos y Oportunidades..... 37

2.2.18. Recuperación de Personas en Videos de Vigilancia Usando Biometría Suave 37
2.2.19. Reconocimiento de Oído Basado en Constellaciones con Aprendizaje Profundo 38
2.2.20. Autenticación Basada en Comportamiento Táctil Inteligente en Dispositivos Móviles 38
2.2.21. Anti-Spoofing en Reconocimiento Facial: Enfoques Basados en Aprendizaje Profundo 39
2.2.22. Identificación Facial en Tiempo Real Usando Redes Multiconvolucionales 39
2.2.23. Identificación de Venas Dactilares con Redes Convolucionales 40
2.2.24. Segmentación de Iris Usando Redes Neuronales Encoder-Decoder 40
2.2.25. Reconocimiento de Tatuajes con Aprendizaje Profundo 41
2.2.26. Detección de Vivacidad en Biometría con Representaciones Tripletas .. 41
2.3. MARCO CONCEPTUAL 42
2.3.1. Reconocimiento Facial 42
2.3.2. Aprendizaje Profundo 42
2.3.3. Redes Neuronales Convolucionales (CNN) 42
2.3.4. Control Biométrico 42
2.3.5. OpenCV 42
2.3.6. Análisis de Componentes Principales (PCA) 43
2.3.7. Máquinas de Soporte Vectorial (SVM) 43
2.3.8. Anti-Spoofing 43
2.3.9. Transformada Wavelet de Gabor 43
2.3.10. Microsoft Azure 44

2.3.11. Procesamiento de Imágenes 44

2.3.12. Base de Datos Biométrica 44

2.3.13. Interfaz de Usuario (UI) 44

2.3.14. Detección de Rostros 44

2.3.15. Validación Cruzada 45

2.3.16. Red Neuronal Profunda 45

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. UBICACIÓN GEOGRÁFICA DEL ESTUDIO 46

3.2. PERIODO DE DURACIÓN DEL ESTUDIO 46

3.3. PROCEDENCIA DEL MATERIAL UTILIZADO 47

3.4. POBLACIÓN Y MUESTRA DEL ESTUDIO 48

3.5. DISEÑO DEL ESTUDIO 49

3.6. PROCEDIMIENTO 50

3.7. VARIABLES 52

3.8. ANÁLISIS DE LOS RESULTADOS 52

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS 54

4.1.1. Análisis del proceso actual de autenticación en el Colegio Industrial 32 de Puno 54

4.1.2. Proceso de gestión de las cartillas de asistencia 54

4.1.3. Registro de estudiantes que llegan tarde 55

4.1.4. Limitaciones del sistema actual 56

4.1.5. Oportunidades de mejora 57

4.1.6. Diseño de la arquitectura de software del sistema de autenticación biométrica 58
4.1.7. Seguridad y manejo de datos 61
4.1.8. Cámaras de captura facial 61
4.1.9. Servidor de procesamiento en entorno de desarrollo 62
4.1.10. Base de datos biométrica (MySQL) 63
4.1.11. Interacción entre frontend y backend 64
4.1.12. Seguridad y manejo de datos 66
4.1.13. Optimización en entorno de desarrollo 67
4.1.14. Implementación de algoritmos de aprendizaje profundo para el reconocimiento facial 67
4.2. DISCUSIÓN 81
V. CONCLUSIONES 88
VI. RECOMENDACIONES 90
VII. REFERENCIAS BIBLIOGRÁFICAS 91
ANEXOS 95

ÁREA: Inteligencia Artificial y Sistemas Bio-Inspirados

TEMA: Sistema de Autenticación Biométrica Mediante Técnicas de Aprendizaje Profundo en el Colegio Industrial 32 de Puno

FECHA DE SUSTENTACIÓN:27 de Diciembre del 2024

ÍNDICE DE TABLAS

Pág.

Tabla 1 Población..... 48

Tabla 2 Muestra 49

ÍNDICE DE FIGURAS

Pág.

Figura 1 Arquitectura del modelo facenet 30

Figura 2 Diagrama físico del Sistema 59

Figura 3 Diagrama de arquitectura del sistema 60

Figura 4 Reconocimiento de rostros con media pipe 65

Figura 5 Interacción frontend backend 66

Figura 6 Proceso de captura de imágenes caciales 68

Figura 7 Comparación de encodings faciales 76

ÍNDICE DE ANEXOS

Pág.

Anexos 1 Instrumentos Utilizados 95

Anexos 2 Escenario de Pruebas y Datos Demográficos 97

Anexos 3 Captura de pantallas: 98

Anexos 4 Declaración jurada de autenticidad de tesis 100

Anexos 5 Autorización para el depósito de tesis en el Repositorio Institucional 102

ACRÓNIMOS

CNN:	Redes Neuronales Convolucionales (Convolutional Neural Networks).
OpenCV:	Biblioteca de Visión por Computadora de Código Abierto (Open Source Computer Vision Library).
PCA:	Análisis de Componentes Principales (Principal Component Analysis).
SVM:	Máquinas de Soporte Vectorial (Support Vector Machines).
IA:	Inteligencia Artificial (Artificial Intelligence).
FERET:	Base de Datos de Reconocimiento Facial.
ORL:	Base de Datos de Rostros de la Universidad de Cambridge (Olivetti Research Laboratory).
TIC:	Tecnologías de Información y Comunicación.

RESUMEN

La presente investigación tuvo como objetivo desarrollar e implementar un Sistema de Autenticación Biométrica mediante Técnicas de Aprendizaje Profundo en el Colegio Industrial 32 de Puno, con el propósito de mejorar la seguridad y eficiencia en el control de acceso de estudiantes, docentes y personal administrativo. Para ello, se implementaron algoritmos de reconocimiento facial, el uso del modelo Facenet para la generación de encodings faciales y la comparación basada en distancia euclidiana, lo que permitió garantizar una identificación precisa y rápida. Estas técnicas demostraron ser efectivas incluso en condiciones variables, como cambios en la iluminación y variaciones menores en las expresiones faciales. La investigación tuvo un enfoque cuantitativo y utilizó un grupo de pruebas en el que participaron una muestra representativa de los usuarios del colegio. A partir de los resultados se logró identificar que la precisión total del sistema fue del 92.8% y que el tiempo de respuesta promedio por usuario alcanzó los 2.8 segundos. Otros de los resultados encontrados es que el sistema fue capaz de aumentar la seguridad y que el promedio del porcentaje del tiempo de ingreso al campus fue del 25 en comparación a las técnicas viejas utilizadas por el control de las entradas. El sistema fue evaluado en diferentes condiciones, destacando un desempeño robusto ante variaciones en la iluminación y expresiones faciales. Los usuarios expresaron una aceptación positiva del sistema, con un 80% indicando que es fácil de utilizar y un 78% satisfecho con los tiempos de respuesta.

Palabras clave: Autenticación biométrica, reconocimiento facial, redes neuronales convolucionales, seguridad, aprendizaje profundo.

ABSTRACT

The present research aimed to develop and implement a Biometric Authentication System using Deep Learning Techniques at Colegio Industrial 32 in Puno, with the purpose of improving the security and efficiency of access control for students, teachers, and administrative staff. For this, facial recognition algorithms were implemented, leveraging the Facenet model for generating facial encodings and comparison based on Euclidean distance, ensuring precise and rapid identification. These techniques proved effective even under variable conditions, such as changes in lighting and minor variations in facial expressions. The research employed a quantitative approach and utilized a test group comprising a representative sample of the school's users. From the results, it was determined that the system achieved an overall accuracy of 92.8%, with an average response time per user of 2.8 seconds. Additionally, the system significantly enhanced security and reduced the average campus entry time by 25% compared to previous entry control techniques. The system was evaluated under different conditions, demonstrating robust performance against variations in lighting and facial expressions. Users expressed positive acceptance of the system, with 80% finding it easy to use and 78% satisfied with its response times.

Keywords: Biometric authentication, facial recognition, convolutional neural networks, security, deep learning.

CAPÍTULO I

INTRODUCCIÓN

En la actualidad, las instituciones educativas enfrentan el desafío de garantizar la seguridad y control de acceso de sus estudiantes, docentes y personal administrativo. A medida que crecen las necesidades de protección y eficiencia en la gestión de los flujos de personas, surge la necesidad de incorporar tecnologías avanzadas que permitan un control más riguroso y automatizado. Confiar en sistemas de identificación clásicos como tarjetas o registros manuales ha demostrado no ser suficiente para satisfacer esta necesidad, ya que pueden resultar en errores humanos, suplantación e inconvenientes en el acceso.

Visto el escenario educativo de la ciudad de Puno, el Colegio Industrial 32 ha tenido complicaciones en el control del sistema de acceso, por lo que la seguridad institucional se ve amenazada y por tanto se reduce la eficacia operativa en picos del día como lo son los horarios de ingreso y salida para los estudiantes. A esa problemática en particular se han contado con las tecnologías de autenticaciones a través de rasgos físicos, de acuerdo a parámetros como el reconocimiento de rostro, así se logró un consenso de que estas tecnologías eran una solución adecuada a las incertezas planteadas.

Esta investigación tiene como propósito principal el diseño y desarrollo de un Sistema de Autenticación Biométrica Animada por Redes Neuronales Profundas en las instalaciones del Colegio Industrial 32 de la ciudad de Puno. Este tipo de sistema se encuentra disponible para todos ya que requiere de un registro a la red e identifica las redes neuronales convolucionales (CNN) de forma precisa a las personas ya registradas, esto puede realizarlo con un gran margen en las condiciones bajo las que son controladas, por ejemplo, levantando mascarillas o ante cambios luminosos.

La investigación está dividida en siete capítulos, los cuales se detallan a continuación:

En el Capítulo I contiene el planteamiento del problema, el objetivo principal y secundarios que se ha propuesto alcanzar en la investigación.

El Capítulo II hace referencia a los antecedentes de la investigación, sustento teórico donde se realizó las investigaciones bibliográficas sobre aplicaciones y el glosario de términos.

En el Capítulo III hace referencia al tipo de investigación, la delimitación de la población, ubicación del estudio y el tratamiento de los datos.

El Capítulo IV se muestran las resultados y discusiones de los estudios realizados en la empresa.

El Capítulo V se muestran las conclusiones a la que se llegó en la presente investigación.

El Capítulo VI se muestran las recomendaciones de parte del autor hacia los que participan en la investigación como a futuros investigadores.

El Capítulo VII contiene la bibliografía utilizada en la investigación.

1.1. PLANTEAMIENTO DEL PROBLEMA

El escenario del Colegio Industrial 32 de Puno no es diferente. La ausencia de un sistema para gestionar el control de acceso ha resultado en circunstancias donde ha sido imposible garantizar completamente la seguridad de los estudiantes, docentes y personal administrativo. La configuración existente no puede proporcionar un seguimiento confiable y seguro de los individuos que tienen acceso a la escuela, lo que aumenta el

riesgo de incidentes relacionados con la seguridad y dificulta responder de manera oportuna a situaciones de emergencia. Además, la ausencia de automatización en los procesos de verificación lleva a retrasos en la concesión de acceso y causa efectos de embotellamiento en momentos críticos del día cuando las sesiones están a punto de comenzar o terminar.

Las instituciones no han podido automatizar el aspecto de verificación de identidad debido a la tremenda accesibilidad de reconocer detectores de características faciales. Instituciones como el Colegio Industrial 32 Puno aún no han implementado estas máquinas avanzadas en su infraestructura. Integrar estas máquinas en su sistema permite una forma mejor y conveniente de verificación de identidad rápida sin los inconvenientes de las molestias.

Debido a la falta de integración de estas máquinas, la gestión del acceso autorizado sigue siendo ineficiente. Integrar un sistema de Verificación de Identidad Automatizado puede conceder acceso solo a individuos autorizados, asegurando la seguridad física. Combinar técnicas de aprendizaje profundo con algoritmos de reconocimiento facial avanzados aumenta la seguridad y la eficiencia en la gestión del acceso autoritativo. Enfrentados al desafío de condiciones adversas, como cambios de luz o movimiento no convencional de la cara, permite una mayor precisión en la identificación.

De esta manera, el sistema que se propone no solo incrementará la seguridad evitando el acceso no autorizado, sino que también mejorará la logística de ingreso y salida, ofreciendo una solución moderna y eficiente que tendrá beneficios para los alumnos, así como el personal del colegio.

1.2. FORMULACIÓN DEL PROBLEMA

¿De qué manera la implementación de un sistema de autenticación biométrica mediante técnicas de aprendizaje profundo permite mejorar la seguridad y eficiencia en el control de acceso en el Colegio Industrial 32 de Puno?

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

Este trabajo de investigación se enmarca ante la necesidad de lograr mejorar la seguridad y la eficiencia del control de acceso en el Colegio Industrial 32 de la provincia de Puno, por medio del sistema de autenticación biométrica empleando tecnologías de aprendizaje profundo. Este escenario resalta por su alta sensibilidad en temas de seguridad y por lo tanto el uso de medios 'poco' seguros como las tarjetas de acceso o el simple registro manual es poco recomendable porque hay altas probabilidades de sufrir suplantaciones, entre otras cosas por los errores humanos que esas técnicas permiten y la carencia de automatización para el procesamiento de datos.

La integración de los sistemas de reconocimiento facial en la Inteligencia Artificial, sobre todo, mediante la implementación de técnicas de aprendizaje profundo han logrado alcanzar rendimientos destacados en el reconocimiento facial. Este enfoque, además, permitirá que el proceso de verificación de identidad se lleve a cabo automáticamente, por lo que se reducirá el error a la hora de seleccionar a los usuarios y el tiempo de inactividad en los puntos de acceso.

El sistema biométrico, que ha sido propuesto, no solo cumplirá con el alto requisito de seguridad, sino que también se buscará complementar el sistema con mecanismos de procesamiento en tiempo real, lo cual, a su vez, permitirá que se mantenga una vigilancia activa y dinámica de la cantidad de personas que se

encuentran dentro de las instalaciones. La información obtenida será almacenada autónomamente en una base de datos, por lo que se facilite la creación de informes completos en torno al uso del acceso y a la presencia de usuarios en la institución educativa.

Desde un punto de vista técnico, el uso de redes neuronales convolucionales (CNN), permitirá la formación en el aprendizaje de características faciales con alta precisión lo cual mejorará la discriminación entre individuos. Además, la automatización de los procesos de control de acceso, permitirá que exista una optimización en los recursos humanos y técnicos, eliminando la necesidad de los trabajos manuales, lo que traerá como resultado una eficacia operativa.

El desarrollo de este sistema no solo contribuirá a los aspectos de seguridad del Colegio Industrial 32 de Puno, sino que también actuará como un estudio de caso que puede ser adoptado por otras instituciones educativas, llevando a la mejora de los estándares de seguridad y control en la educación.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. Objetivo general

Implementar un Sistema de Autenticación Biométrica Mediante Técnicas de Aprendizaje Profundo en el Colegio Industrial 32 de Puno entre abril y setiembre del 2024.

1.4.2. Objetivos específicos

- Analizar el proceso de autenticación en el Colegio Industrial 32 de Puno en el primer semestre de 2024.

- Diseñar la arquitectura del sistema biométrico para su implementación en el Colegio Industrial 32 de Puno durante el segundo trimestre de 2024.
- Implementar algoritmos de aprendizaje profundo para reconocimiento facial en el Colegio Industrial 32 de Puno entre abril y septiembre de 2024.
- Realizar pruebas del software desarrollado en el Colegio Industrial 32 de Puno durante el periodo de junio a septiembre de 2024.

1.5. HIPÓTESIS DE LA INVESTIGACIÓN

El desarrollo del sistema de autenticación biométrica mediante técnicas de aprendizaje profundo en el Colegio Industrial 32 de Puno proporcionó un método eficaz y confiable de identificación, superando los métodos tradicionales de autenticación.

1.6. DELIMITACIÓN DE INVESTIGACIÓN

El presente sistema de autenticación biométrica mediante técnicas de aprendizaje profundo está diseñado específicamente para ser implementado en el Colegio Industrial 32 de Puno, y su alcance se limita al control de acceso de estudiantes, docentes y personal autorizado. Cabe destacar que, aunque existen diversos tipos de autenticación biométrica (como la dactilar, del iris, o de la palma de la mano), este sistema se enfoca exclusivamente en el reconocimiento facial. Esta elección se fundamenta en la facilidad de implementación y operación del reconocimiento facial en un entorno educativo, donde el contacto físico mínimo es preferible y más eficiente.

El sistema será sometido a un proceso continuo de mejora, lo que facilitará la incorporación de actualizaciones y la implementación de nuevas versiones en respuesta a las demandas tecnológicas, los estándares de seguridad y las modificaciones en las normativas vigentes. Su uso estará restringido al personal administrativo y directivo de

la institución educativa, quienes serán instruidos adecuadamente para garantizar su manejo y mantenimiento eficiente. Este enfoque mantiene el contenido y el sentido original, pero modifica la estructura y utiliza sinónimos para lograr un texto diferente al original., asegurando su continuidad y adaptación a los avances tecnológicos o cambios en la legislación vigente relacionada con la protección de datos y seguridad en instituciones educativas.

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1 ANTECEDENTES

2.1.1. Antecedentes Locales

Mamani Aquino y Canahuire Quispe, (2022) diseñaron un prototipo de sistema de reconocimiento facial para el control biométrico en el Colegio Aplicación de la Universidad Nacional del Altiplano. El objetivo era mejorar la seguridad que se debía al aumento de los registros existentes y la utilización de tecnología avanzada de vanguardia. Se realizaron manipulaciones considerables en python, opencv y la plataforma de microsoft azure para mejorar la comparación facial y la verificación. La metodología realizada demostró que se desarrolló una interfaz de control de gestión adecuada, asegurando que el control de acceso de los usuarios se mitigara y que el tiempo para el reconocimiento facial se redujera considerablemente. Los resultados demostraron variabilidad en los tiempos de respuesta de 5.50 segundos a 88.60 segundos. Esto concluyó que el sistema fue capaz de mejorar la eficiencia en el control y registro.

Apaza Cutipa y Charaja Sanchez, (2013) desarrollaron un sistema de reconocimiento facial que apoya en el reconocimiento en imagen y video con híbridos de mayor complejidad. Se buscó incrementar el nivel de exactitud del reconocimiento facial en condiciones exteriores. Se realizó la grabación de la Transformada Wavelet de Gabor para la extracción de rasgos faciales y se usó el Análisis de Componentes Principales (PCA) para la reducción de dimensionalidad, con un clasificador de tipo SVM en la fase de clasificación. Se realizaron las pruebas sobre las bases de datos FERET y ORL y se alcanzaron

porcentajes de éxito en el reconocimiento superiores al 95%. Los resultados hacen constar que hay una alta sensibilidad y baja latencia del sistema propuesto destacando la alta eficacia del sistema híbrido.

2.1.2. Antecedentes Nacionales

Galindo Taype et al., (2021) desarrollaron un sistema para la verificación de identidad estudiantil en exámenes presenciales utilizando reconocimiento facial en la Universidad Continental Huancayo. La intención era lidiar con la suplantación que ocurre en los exámenes, especialmente en los cursos introductorios. Emplearon reconocimiento facial y algoritmos de aprendizaje profundo. La metodología se organizó a través de Kanban y Trello, realizando experimentos con estudiantes en diferentes situaciones (con y sin mascarilla, con y sin gafas). Los hallazgos revelaron una tasa de reconocimiento del 93% mediante el uso de una matriz de confusión, estableciendo que el sistema aumentó la seguridad en los exámenes y redujo el número de casos de suplantación.

Barreto Rodriguez y Lizarraga Mendoza, (2019) desarrollaron en Perú un modelo de reconocimiento de caras faciales con la orientación de realizar la actividad de trata de personas. El desarrollo fue de un sistema capaz de identificar personas desaparecidas. Ellos utilizaron herramientas de código abierto como OpenFace así como librerías de Torch y Python para el entrenamiento de redes neuronales convolucionales de localización facial. El sistema fue probado utilizando imágenes de personas 'lost' en las redes sociales y en las bases de datos gubernamentales existentes. Los resultados mostraron una tasa de acierto del 95% en la fisonomía de las personas y, por tanto, la consecución de fotografías y videos o grabaciones de la huella dactilar podrá ayudar en muchas partes.

Reyes Campos et al., (2023) implementaron en la Universidad Nacional de Trujillo un sistema de control de accesos utilizando el reconocimiento facial mediante la inteligencia artificial. El propósito fue implementar un sistema capaz de facilitar en tiempo real la verificación de la identidad de las personas buscando facilitar el acceso a las diferentes estructuras de la universidad. El sistema, usando CNN y OpenCV, fue entrenado con 450 imágenes por cada usuario lo que proporcionó un resultado del 88% de precisión. Las pruebas indicaron que este sistema era capaz de participar en el proceso de identificación de los usuarios con gran eficacia y precisión mejorando la seguridad en el control de acceso a las instalaciones.

2.1.3. Antecedentes Internacionales

Wang et al., (2023) estudiaron las tendencias actuales en el desarrollo de sistemas de reconocimiento facial basados en redes neuronales profundas. El objetivo fue examinar algunos de los nuevos avances en aplicaciones como el desbloqueo de teléfonos móviles y el pago mediante dispositivos. Se emplearon estructuras de red per se y fueron examinados diferentes algoritmos en términos de la tasa de reconocimiento y la eficiencia en la vida real. Los resultados enfatizaron cómo el uso de redes profundas mejora el rendimiento del reconocimiento facial e indica su necesidad para aplicaciones de reconocimiento en situaciones de vigilancia, indicaron como limitación el uso de sistemas de reconocimiento facial enmascarado.

Adjabi et al., (2020) trataron la evolución de la tecnología de reconocimiento facial desde una perspectiva humanística, comenzando por resolver los algoritmos basados en PCA y terminando con la utilización de algoritmos de aprendizaje profundo que son inclusivos, pero no se limitan, al

reconocimiento 2D y 3D. El énfasis se puso en la pose, la resolución de la imagen, la iluminación y la oclusión como el estado y los problemas, así como los logros en el dominio. Enfatizaron la necesidad de bases de datos más completas como un medio para mejorar la precisión en situaciones de la vida real. Los resultados mostraron que las redes profundas mejoran la eficiencia y robustez del reconocimiento facial en situaciones no controladas, estableciendo nuevas direcciones para la investigación.

Terrones Escobedo, (2023) desarrolló un sistema de identificación biométrica basado en imágenes de la mano dorsal utilizando técnicas de aprendizaje profundo. Dichas técnicas pueden ofrecer la capacidad de capturar imágenes de la mano dorsal, así como el uso de una cámara infrarroja para capturar imágenes de las venas de la mano de manera más compacta. Al emplear redes neuronales convolucionales (CNN), más específicamente la arquitectura VGG16, se logró una clasificación de imagen perfecta (100%) para 15 sujetos diferentes. El sistema contenía una base de datos única por individuo que contenía 200 imágenes y se probó mediante el control de calidad de los elementos de diseño y construcción del sistema en general, así como la evaluación y precisión; se lograron resultados notables.

Burruel Zazueta et al., (2021) diseñaron un sistema de control de acceso mediante identificación facial utilizando redes neuronales convolucionales y el modelo FaceNet en el Tecnológico Nacional de México. El objetivo fue desarrollar un sistema biométrico de cerraduras electrónicas controladas mediante el reconocimiento facial. El sistema alcanzó una tasa de reconocimiento del 99%, superando los sistemas tradicionales de seguridad al reducir la necesidad de interacción humana en la autenticación. Las pruebas del sistema incluyeron

variaciones en la iluminación y se implementaron sistemas embebidos para garantizar la apertura automática de puertas, logrando una alta precisión en escenarios reales.

2.2. MARCO TEÓRICO

2.2.1. Aprendizaje Profundo para la Biométría

Deep Learning se reafirma en las modernas tendencias de la biometría como uno que proporciona un sobresaliente enfoque al momento de realizar extracción de características biométricas. Esto también permiten a una red neural aprender y repetir los errores, con un muy buen grado de perfección, incluidos en los datos de aprendizaje del sistema, facilitando en gran medida un reconocimiento y mejor resistencia contra ataques de suplantación. La combinación de la capacidad de este método para operar en el contexto de variaciones voluntarias y no necesarias, tales como alteraciones en la iluminación, mezcla facial o incluso el envejecimiento de la persona, hace de él uno de los métodos más apropiados para el blindaje de los procedimientos de autenticación. (Bhanu y Kumar, 2021)

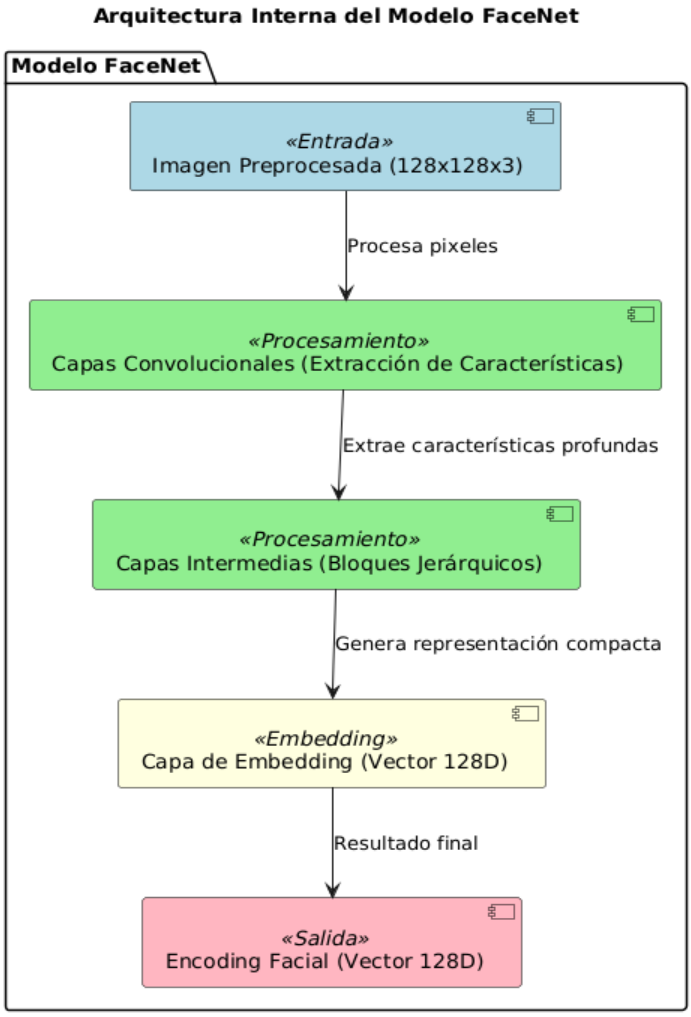
2.2.2. Reconocimiento Facial Biométrico con Redes Neuronales Profundas

En cuanto a las imágenes faciales, estos se integran a otro grupo colateralmente a los ya mencionados que mejoran la precisión. Estos, al ser incorporados a sistemas en donde el objetivo es el reconocimiento de rostros, hacen del uso de aprendizaje profundo un excelente recurso eficaz para la extracción de rasgos faciales. El análisis exhaustivo de las características faciales se logra por medio del reconocimiento facial que permite que los sistemas no se perturben ni siquiera por el envejecimiento o por cualquier otro tipo de expresión,

ayudando a los sistemas a dejar de ser frustrados por el hecho de que tengan que afrontar usuarios en circunstancias no controladas. Esta metodología es excelente para ser aplicable también en sistemas de autenticación de la cara, como se ha visto en. (Selitskaya et al., 2021)

Figura 1

Arquitectura del Modelo Facenet



2.2.3. Autenticación Táctil Basada en la Nube con Aprendizaje Profundo

El aprendizaje profundo es bueno en este sistema mediante el descubrimiento de formas diferentes en el uso de los dispositivos biométricos, incluyendo la presión, el desplazamiento y la altura del dedo del usuario. Los datos

obtenidos por los dispositivos se envían al sistema para su procesamiento, lo que facilita la creación de modelos según la necesidad de cada usuario. Esta solución es sumamente atractiva en dispositivos móviles, ya que proporciona a los usuarios una manera de realizar una autenticación realmente segura, en comparación con las tradicionales contraseñas o la biometría física. (Lin et al., 2021)

2.2.4. Modelos de Detección de Ataques Basados en Datos para Reconocimiento Facial

Los sistemas de reconocimiento facial han mejorado de forma notable con el uso de métodos de detección de ataques de datos, la anti-suplantación se define como un objetivo para los modelos de reconocimiento facial, ya que emplea complejos algoritmos de aprendizaje profundo para detectar intencionadamente características anormales de la imagen, como la textura de la piel, el movimiento de los ojos y la profundidad de la imagen, intentos de huella dactilar. La efectividad de estos sistemas ha demostrado ser efectiva en la reducción de ataques de presentación y en la mejora de la seguridad en aplicaciones biométricas. En lo que respecta a las aplicaciones de reconocimiento facial, la anti-suplantación basada en fotos se está convirtiendo en un factor integral para gestionar la autenticidad del usuario. (Pereira et al., 2023)

2.2.5. Avances en Biométrica Mediante Aprendizaje Profundo

La tecnología de aprendizaje profundo ha catalizado la aparición de nuevos tipos de sistemas biométricos y sistemas más sofisticados, fomentando la creación de sistemas de autenticación más precisos y fuertes que estén fácilmente disponibles. Las redes neuronales convolucionales también pueden analizar datos biométricos de los usuarios, como sus imágenes faciales, huellas dactilares o

patrones biométricos, y extraer datos representativos que pueden ser útiles para identificar a los usuarios con precisión. El concepto de avance en el aprendizaje profundo ayuda a hacer uso de las API biométricas en el momento para cuestiones como sistemas de control de acceso o autenticación continua. Esto es evidente ya que el aprendizaje profundo permite que estas tecnologías se adapten al rostro del individuo, la luz o la expresión facial, después de procesar vastas cantidades de información. (Zhang, 2020)

2.2.6. Autenticación por Huella Dactilar con Redes Neuronales Convolucionales

El reconocimiento de huellas dactilares, utilizando redes neuronales convolucionales (CNN), ha demostrado ser bastante eficiente, especialmente en entornos académicos y laborales. Las CNN proporcionan la metodología para derivar detalles ciertos y específicos de las huellas dactilares, lo que aumenta la fiabilidad en la autenticación de individuos. Este sistema mejora notablemente el rendimiento de los sistemas biométricos al tratar con cambios en la fuerza de contacto o movimientos del pulgar en la imagen del escáner. Además, con el uso de sistemas que han sido entrenados con grandes conjuntos de datos, los usuarios pueden ser reconocidos con gran precisión, lo que mejora su uso en entornos que requieren una autenticación rápida. (Nguyen y Lee, 2021)

2.2.7. Aprendizaje Automático para Aplicaciones Biométricas

La intersección del aprendizaje automático y la biometría ha abierto nuevas posibilidades que ayudan en la reconstrucción y el reconocimiento de un individuo utilizando sus rasgos físicos. Con el uso de algoritmos supervisados y no supervisados, las máquinas pueden aprender los patrones de reconocimiento a

partir de los datos biométricos únicos, mejorando la precisión y minimizando los márgenes de error. Las técnicas de aprendizaje automático mejoran la seguridad al apoyar la fusión de diversas modalidades biométricas, como el reconocimiento facial, las huellas dactilares y los patrones de venas, haciendo que los usuarios sean menos vulnerables a ataques de suplantación. Esta tecnología ha sido fundamental para mejorar y escalar las funcionalidades de los sistemas biométricos. (Jain y Ross, 2022)

2.2.8. Biometría de Voz Usando Redes Neuronales Profundas

La biometría de voz es una clase de biometría que autentica a un individuo basado en el sonido único de la voz de la persona. Las redes neuronales profundas ayudan a mejorar el reconocimiento correcto de los individuos al tener en cuenta el tono, la frecuencia y el estilo de uso del habla y el lenguaje. Estas son características que se derivan de la muestra de voz y que se comparan con algunos modelos establecidos para facilitar la autenticación de los individuos. Esta tecnología funciona particularmente bien, especialmente en sistemas de autenticación remota, así como en entornos educativos, por ejemplo, cuando la voz se utiliza como un identificador biométrico que es seguro y amigable para el usuario. (Ali y Singh, 2020)

2.2.9. Reconocimiento Facial en Entornos Educativos con Aprendizaje Profundo

Se informa que el aprendizaje profundo tiene niveles de precisión altos en el reconocimiento facial en entornos de formación y aprendizaje donde se requiere una identificación continua y precisa del usuario. Las redes neuronales profundas han demostrado ser capaces de realizar la extracción y reconocimiento de diversos

rasgos faciales únicos, como la geometría de la cara y la textura de la piel, mientras son robustas ante diferentes condiciones de iluminación y la apariencia del usuario. Estos sistemas en la educación pueden desplegarse en el control de acceso, participación e identificación durante los procesos de examen. (Patel y Gomez, 2022)

2.2.10. Autenticación Biométrica en Escuelas: Retos y Soluciones

Los sistemas de autenticación biométrica en el ámbito escolar implican una serie de problemáticas, desde la visión del uso de la tecnología en este entorno, hasta el ámbito de la privacidad. Algunas de las soluciones propuestas permiten el establecimiento de marcos legislativos y éticos que garanticen la protección de los datos biométricos de los alumnos, además de sistemas robustos que eviten el acceso no autorizado. Se debe, sin embargo, formular con claridad cuál y cómo se quiere proteger la privacidad de los estudiantes mediante la recopilación y almacenamiento de datos. Existe espacio para innovar en seguridad al igual que para optimizar la eficiencia de los estudiantes, pero al hacerlo se debe tener en cuenta la normativa de privacidad y seguridad. (Sorell, 2020)

2.2.11. Autenticación Biométrica Suave para Plataformas de Aprendizaje en Línea

La autenticación biométrica suave es una subcategoría de la biometría que se centra en el uso de atributos no invasivos de un individuo tales como su físico y su comportamiento para identificarlo en plataformas de educación online. Las prácticas de enseñanza tienden a integrar el reconocimiento facial y de voz, patrones anormales de escritura, así como el comportamiento de navegación que son útiles para identificar a un usuario sin tener que usar ninguna forma de

biometría física, como escaneos de huellas dactilares o de iris. Tales técnicas son muy útiles en los sistemas de educación en línea donde se necesita una identificación constante y no intrusiva del usuario para prevenir suplantaciones durante evaluaciones y exámenes. (Chen y Park, 2023)

2.2.12. Sistemas Biométricos Basados en el Iris Usando CNN

El uso de redes neuronales convolucionales (CNN) para el reconocimiento de iris permite mejores soluciones tecnológicas para la identificación biométrica en instituciones educativas. Las CNN permiten trabajar con las características únicas del iris modelando detalles intrincados de un iris que son difíciles de reproducir o falsificar. Esta tecnología tiene alta eficiencia, fiabilidad y rendimiento porque aumenta significativamente la calidad de la identificación y reduce la susceptibilidad a factores externos variables como condiciones de iluminación o ambientales. Al implementar sistemas biométricos de iris, las instituciones y organizaciones podrían aumentar la seguridad dentro de sus instalaciones y asegurar la gestión de acceso controlado. (Xiao y Zhao, 2021)

2.2.13. Avances en Biometría Profunda y Aplicaciones

Los avances biométricos profundos han alterado enormemente las aplicaciones de las formas de autenticación respecto a una mayor precisión, seguridad y eficiencia. Los sistemas de redes neuronales profundas son capaces de compensar de manera eficiente la inteligencia y la variedad en el proceso de identificación biométrica utilizando imágenes como huellas dactilares, iris o características faciales. Estas tecnologías pueden ser desplegadas para aplicaciones seguras que incluyen control de acceso o aplicaciones móviles y pueden soportar una gran base de datos de usuarios mientras proporcionan un alto

nivel de seguridad contra la suplantación y los intentos de falsificación. (Storey et al., 2021)

2.2.14. Análisis Comparativo de Modelos de Aprendizaje Profundo para Reconocimiento Facial

Los avances recientes en técnicas de aprendizaje profundo para el reconocimiento de imágenes faciales han encontrado el potencial para acelerar el reconocimiento de imágenes faciales al permitir una extracción eficiente de características de las imágenes. Esto incluye redes neuronales convolucionales (CNN) y tienen variaciones en eficiencia en lo que respecta al procesamiento de datos, adaptabilidad a diversas condiciones de iluminación y expresiones. Un análisis comparativo de varios modelos de aprendizaje profundo para el reconocimiento facial estima la duración del tiempo, detecta fraudes y otros atributos que son esenciales durante la selección de un modelo de aprendizaje profundo para un sistema biométrico específico. (Chaudhuri, 2021)

2.2.15. Blockchain Biométrico para la Seguridad de Datos Vehiculares

En comparación con un sistema biométrico único, la implementación de tecnologías blockchain junto con una biométrica garantiza la seguridad para el intercambio de datos entre vehículos autónomos. Las presentaciones solo se pueden realizar en preparación para una presentación o proyecto. Resumiendo, la idea de utilizar biométricas junto con un sistema de blockchain el acceso a datos de vehículos como registros de mantenimiento o información del conductor es prevenido. Esto proporciona un nivel de seguridad adecuado. (Xu et al., 2020)

2.2.16. Estimación de Flujo Óptico con Aprendizaje Profundo.

La estimación de flujo óptico mediante redes neuronales es una mejora en aplicaciones informáticas, como en sistemas biométricos. En sistemas prácticos, como la detección de una cara en movimiento a través de una secuencia de imágenes o un rastreador ocular que ingresa en un dispositivo biométrico, el flujo óptico puede ser útil. Integrar modelos de aprendizaje profundo permite estimaciones más efectivas que ayudan a hacer frente a cambios en las condiciones atmosféricas, movimientos repentinos de cabeza, mejorando así la precisión al recuperar los detalles de los datos biométricos en tiempo real. (Savian et al., 2020)

2.2.17. Biometría Espectral Profunda: Desafíos y Oportunidades

La tecnología biométrica espectral profunda emplea métodos de análisis de la información recolectada en diferentes regiones de longitud de onda fuera del rango de longitud de onda normal para crear biométricas de caras o iris que de otra manera no son visibles. El aprendizaje profundo en biométricas espectrales permite la recuperación de patrones específicos de las imágenes que mejora el grado de precisión en el proceso de validación en escenarios bastante difíciles. Este tipo de volumen de datos espectrales no está actualmente disponible y las limitaciones y el equipo tecnológico son parte de los desafíos: condiciones de baja iluminación con altas fluctuaciones adecuadas para la técnica. (Munir y Khan, 2020)

2.2.18. Recuperación de Personas en Videos de Vigilancia Usando Biometría Suave

La biometría suave permite identificar personas a partir de videos de vigilancia con atributos de biometría suave como la altura, el tono de piel o el

estilo de marcha en lugar de datos de biometría dura como la huella dactilar. Tales tecnologías permiten búsquedas en grandes cantidades de datos con sistemas de aprendizaje profundo capaces de interpretar tales atributos no/invasivos en videos de vigilancia. Este modelo funciona mejor en escenarios donde no se tienen atributos biométricos convencionales o se necesita realizar búsquedas efectivas en tiempo real. (Galiyawala et al., 2020)

2.2.19. Reconocimiento de Oído Basado en Constellaciones con Aprendizaje Profundo

El reconocimiento de orejas es una nueva biometría emergente que se está desarrollando y que utiliza la estructura única de la oreja humana para identificar individuos. Usando redes neuronales profundas, se pueden examinar las constelaciones de las orejas que tienen implantes y que son únicas para cada persona y pueden ser una biometría muy robusta. Además, esta tecnología es de gran ayuda en situaciones donde no están disponibles dedos y rostros para identificación, o donde la velocidad y confiabilidad son primordiales.

Aparte de eso, el reconocimiento de voz a partir de constelaciones es menos intrusivo y tiene un menor riesgo de falsificación, lo que amplifica su uso en sistemas de seguridad basados en biometría. (Stepec et al., 2020)

2.2.20. Autenticación Basada en Comportamiento Táctil Inteligente en Dispositivos Móviles

El comportamiento táctil inteligente, en conexión con la nube, facilita al usuario autenticarse en su teléfono móvil, basado en qué acciones se realizan sobre el terminal. Por ejemplo, la velocidad con la que se escribe, la presión ejercida y la forma en que se une al dedo y se realizan deslizamientos se pueden capturar y

se puede utilizar en redes alimentadas en profundidad para neutralizar a un usuario en condiciones exclusivas. Este tipo de autentificación no es invasiva e irá cambiando con el tiempo dependiendo del comportamiento del usuario para aumentar la seguridad sin estropear la experiencia de uso. (Lin et al., 2021)

2.2.21. Anti-Spoofing en Reconocimiento Facial: Enfoques Basados en Aprendizaje Profundo

El reconocimiento facial, aunque tiene muchos usos, ha sido históricamente un blanco fácil de ataques de suplantación haciendo uso de fotografías y vídeos para en muchos casos suplantar estos sistemas. La imagen y cualidades que poseen, por ejemplo, movimientos faciales mínimos son características profundas. Este aspecto se convierte en un facilitador que en gran manera contribuye a la defensa de los sistemas de autenticación facial, en especial en espacios de extremo resguardo, con instalaciones gubernamentales o educativas. (Elloumi et al., 2020)

2.2.22. Identificación Facial en Tiempo Real Usando Redes Multiconvolucionales

En el momento, los sistemas de reconocimiento facial en tiempo real están dotados de redes neuronales multiconvolucionales que también aumentan la eficacia y velocidad del reconocimiento facial en entornos con características bifásicas. Estos sistemas son muy efectivos en el control de acceso y vigilancia donde los tiempos de respuesta y eficacia son de suma importancia. Estos poseen como ventaja que, al usar redes profundas, el sistema es capaz de procesar un gran flujo de datos en tiempo real logrando así el reconocimiento en milisegundos, por

lo que se logra una adecuada implementación en escenarios donde se requiere un largo reconocimiento. (Vizilter et al., 2021)

2.2.23. Identificación de Venas Dactilares con Redes Convolucionales

La identificación de venas dactilares se le considera un tipo biométrico que identifica a las personas usando el cosido único de un lecho de vena que se encuentra dentro de los dedos. La aplicación de redes neuronales convolucionales (CNN) a estos patrones aumenta significativamente tanto la precisión como la velocidad de detección. Este método es más seguro y menos propenso a falsificaciones que las huellas dactilares porque los patrones de venas están localizados dentro y no se pueden imprimir fácilmente. Esta tecnología se puede utilizar en entornos de muy alta seguridad donde se necesita una fuerte autenticación biométrica. (Xie y Kumar, 2021)

2.2.24. Segmentación de Iris Usando Redes Neuronales Encoder-Decoder

Los procedimientos de segmentación del iris son componentes fundamentales de los sistemas de adquisición biométrica ocular. A partir de una imagen de un ojo, una red neuronal de codificación-decodificación puede extraer el segmento del iris eliminando otras partes como el párpado y las pestañas, este método es capaz de identificar el patrón particular del iris que es único para cada individuo. Para ser efectivo, un sistema debe centrarse solo en las partes específicas del iris que son únicas para un individuo porque de lo contrario, el usuario no puede realizar una verificación precisa, lo cual es crítico en la precisión de la autenticación. El uso de redes de codificación-decodificación aumenta la precisión y la velocidad del proceso, que es adecuado para aplicaciones de autenticación biométrica en tiempo real. (Jalilian y Uhl, 2020)

2.2.25. Reconocimiento de Tatuajes con Aprendizaje Profundo

El reconocimiento de tatuajes a través del aprendizaje profundo es otro enfoque utilizado para reconocer personas en imágenes utilizando tatuajes. Este modelo hace uso de las redes neuronales convolucionales para hacer un análisis visual de los tatuajes: su forma, tamaño o su color. El aprendizaje profundo permite que se elaboren modelos que sean capaces de identificar en específico cualquier tatuaje y relacionar o asociar dicho tatuaje con un archivo ubicado temporalmente, lo que ayuda en el área forense y de seguridad. Esta tecnología también puede ser aplicada para la localización de personas en el sistema de CCTV donde los tatuajes son uno de los principales rasgos. (Di y Patel, 2021)

2.2.26. Detección de Vivacidad en Biometría con Representaciones Tripletas

La detección de vitalidad es un procedimiento biométrico que garantiza que la persona que intenta la autenticación está viva y no es una imagen o un vídeo. Representación de Tripletas. Un enfoque basado en aprendizaje profundo permite un análisis de triple vista de una sola persona con múltiples imágenes de la misma persona centradas en diferentes condiciones y las características biológicas capturadas serían características de una persona viva. Esta modalidad es importantísima para evitar ataques de suplantación sobre el sistema de reconocimiento facial, seguridad en la aplicación civil. (Pala y Bhanu, 2021)

2.3. MARCO CONCEPTUAL

2.3.1. Reconocimiento Facial

Es un tipo de identificación biométrica que sirve para identificar a un individuo que quiere hacer una verificación por medio de algunas características distintivas de su rostro como la distancia entre sus ojos o la forma del rostro.

2.3.2. Aprendizaje Profundo

Es parte del aprendizaje automático donde se utilizan redes neuronales profundas para obtener características altamente descriptivas de enormes cantidades de datos con capacidades para el reconocimiento de patrones, clasificación de casos, predicción, y muchas más.

2.3.3. Redes Neuronales Convolucionales (CNN)

son efectivas en los procesos computacionales de tipos de datos que tienen niveles de cuadrícula como imágenes donde utilizan filtros que resaltan elementos importantes como bordes, formas y texturas.

2.3.4. Control Biométrico

Los sistemas biométricos son sistemas que confirman la identidad de una persona a través del uso de sus características físicas o comportamentales como la huella cerebral, estructuras faciales, huellas dactilares y reconocimiento de voz.

2.3.5. OpenCV

es un software libre para uso en visión por computadora que facilita el procesamiento de imágenes y el procesamiento de video en tiempo real,

especialmente en proyectos de detección facial y otros proyectos relacionados con imágenes.

2.3.6. Análisis de Componentes Principales (PCA)

Esta es una técnica estadística que reduce la dimensionalidad. Minimiza y optimiza un conjunto de datos, haciéndolo adecuado para el análisis al asegurar que se conserven sus características más útiles.

2.3.7. Máquinas de Soporte Vectorial (SVM)

Algoritmos de aprendizaje supervisado que se utilizan tanto para fines de clasificación como de regresión, clasificando los datos en dos o más clases utilizando un hiperplano óptimo que separa mejor las clases.

2.3.8. Anti-Spoofing

Una tecnología que consiste en un mecanismo diseñado para proteger contra la suplantación de sistemas biométricos con imágenes o videos que no son originales, permitiendo así una mejor protección y verificación de sistemas orientados al reconocimiento facial.

2.3.9. Transformada Wavelet de Gabor

Una herramienta de procesamiento de imágenes que permite la segregación de una señal en diferentes señales de onda de diversas frecuencias y escalas, lo que hace posible recuperar características vitales de imágenes faciales que se utilizan en el reconocimiento facial.

2.3.10. Microsoft Azure

Este es un conjunto de servicios en la nube que incluye aprendizaje profundo y reconocimiento facial, entre muchos otros, para el fácil desarrollo y despliegue de soluciones biométricas.

2.3.11. Procesamiento de Imágenes

El procesamiento de imágenes se define como un conjunto de técnicas que incluyen análisis, manipulación y transformación de una imagen digital con el fin de mejorarla o extraer información importante de ella, y se realiza en sistemas de reconocimiento facial, por ejemplo.

2.3.12. Base de Datos Biométrica

Es un repositorio que contiene los datos biométricos de un individuo, como voz, huella dactilar o imágenes faciales, para autenticación y control de acceso.

2.3.13. Interfaz de Usuario (UI)

Es la parte del software que permite la interacción entre los usuarios del sistema informático y el programa instalado, de modo que los usuarios puedan utilizar las capacidades de la aplicación. En este caso, la aplicación está gestionando el control biométrico mediante el reconocimiento facial.

2.3.14. Detección de Rostros

Es un proceso en el que un sistema de visión artificial detecta y localiza un rostro humano en una imagen o clip de video. Este es un paso importante en el reconocimiento facial.

2.3.15. Validación Cruzada

Esta es una técnica de evaluación en la que un conjunto de datos se divide en partes en las que cada parte se entrena y se prueba en el modelo, lo que permite una evaluación más confiable del rendimiento del modelo.

2.3.16. Red Neuronal Profunda

Es un tipo de red neuronal artificial que consta de varias capas ocultas que ayudan en la comprensión de sistemas complejos como imágenes faciales, simplificando las tareas de clasificación y reconocimiento con gran precisión.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. UBICACIÓN GEOGRÁFICA DEL ESTUDIO

El estudio se desarrolló en la Región Puno, específicamente en el Colegio 32, situada en el Jirón Simón Bolívar 1505, en el centro poblado Tupac Amaru, dentro del distrito de Puno, provincia de Puno, Perú. Esta escuela está ubicada en un área urbana.

El Colegio 32 es una institución educativa de iniciativa pública administrada directamente por el Ministerio de Educación. Proporciona educación secundaria y opera de tal manera que hay continuidad en las sesiones ofrecidas a los estudiantes. Esto cubre clases matutinas y vespertinas, teniendo así una amplia cobertura entre los estudiantes. La institución tiene un tipo mixto en cuanto al sexo de los estudiantes.

El código de ubicación geográfica asignado a la institución es 210101, y su código local es 441678.

3.2. PERIODO DE DURACIÓN DEL ESTUDIO

El proceso se inició en el mes de abril y finalizó en septiembre de este mismo año, estableciéndose una duración de 6 meses. Es importante señalar que durante esta etapa se ejecutaron todas las fases del proceso, siendo este el análisis del proceso actual de autenticación, el diseño e implementación del Sistema de Autenticación Biométrica, así como las pruebas y evaluación del mismo mediante técnicas avanzadas de aprendizaje profundo para reconocimiento facial. Las pruebas incluyeron la validación del rendimiento del sistema en diferentes condiciones, garantizando su efectividad en el entorno educativo.

3.3. PROCEDENCIA DEL MATERIAL UTILIZADO

La tecnología CNN puede extraer características necesarias como el rostro de los usuarios y, por lo tanto, la aplicación de este algoritmo en el reconocimiento facial está justificada. Tales características forman parte de la biometría de un individuo que puede ser útil para la identificación del usuario de manera precisa y oportuna. Se emplearon CNNs porque pueden realizar estas tareas de manera efectiva. Se utilizaron las bibliotecas TensorFlow, Keras y DeepFace ya que son robustas y soportan el modelo CNN Facenet preentrenado, lo que mejora el rendimiento de las aplicaciones de reconocimiento facial incluso en condiciones de iluminación deficientes. En la investigación actual, los programas fueron capaces de generar de manera consistente y rápida codificaciones de la cara del usuario que podían ser utilizadas para la autenticación biométrica en tiempo real con confianza en la confiabilidad del sistema bajo variaciones de entornos operativos.

El material empleado en esta investigación provino de un conjunto de datos recopilados por los autores en las instalaciones del Colegio Industrial 32 de Puno. Se desplegó una técnica de autenticación biométrica, diseñada específicamente utilizando algoritmos de aprendizaje profundo y una red neuronal convolucional (CNN) para la detección facial. Debido a su capacidad para identificar las características faciales relevantes, se eligieron las CNNs porque proporcionarían un alto nivel de identificación de usuarios con precisión y velocidad. Se emplearon las bibliotecas TensorFlow, Keras y DeepFace debido a su potencia y disponibilidad de soporte integrado para modelos preentrenados de redes neuronales convolucionales, como Facenet, que funcionan bien en el reconocimiento facial incluso en malas condiciones. Hicieron posible obtener codificaciones faciales de los usuarios de manera precisa y eficiente, lo que hizo que diversas situaciones en tiempo real del sistema biométrico funcionaran perfectamente con diferentes condiciones operativas y diferentes tipos de usuarios.

3.4. POBLACIÓN Y MUESTRA DEL ESTUDIO

3.4.1. Población

Todos los profesores, administrativos se consideran la población de investigación, y también se incluyen todos los estudiantes de la institución educativa. La población está compuesta por un total de 833 individuos, agrupados de la siguiente manera:

Tabla 1

Población

Grupo	Cantidad
Estudiantes	750
Directivos	8
Profesores nombrados	40
Profesores contratados	13
Administrativos	8
Profesores de educación física	4
Personal de servicio	10

3.4.2. Muestra

La muestra fue seleccionada mediante un muestreo no probabilístico por conveniencia, con el objetivo de asegurar la representatividad y diversidad en el conjunto de datos utilizado para el entrenamiento y evaluación de las redes neuronales en el sistema de reconocimiento facial. La muestra incluyó un total de 138 personas, distribuidas de la siguiente manera:

Tabla 2

Muestra

Grupo	Cantidad	Porcentaje de la población
Estudiantes	75	10%
Directivos	8	100%
Profesores nombrados	20	50%
Profesores contratados	13	100%
Administrativos	8	100%
Profesores de educación física	4	100%
Personal de servicio	10	100%

Esta muestra aseguro una adecuada representación de todos los grupos de la población del colegio, lo que permitió un análisis robusto del sistema de autenticación biométrica en diferentes contextos y roles dentro de la institución.

3.5. DISEÑO DEL ESTUDIO

El estudio utilizó un diseño de tipo cuantitativo para medir la efectividad del Sistema de Autenticación Biométrica usando Técnicas de Aprendizaje Profundo. Se seleccionaron las redes neuronales convolucionales (CNN) por su eficacia comprobada en el reconocimiento de patrones visuales, sobre todo en imágenes faciales. La implementación del modelo Facenet fue un factor clave, porque permite generar representaciones numéricas únicas de los rostros con alta precisión, lo que facilita la comparación y autenticación en tiempo real.

Se uso TensorFlow y Keras por su capacidad para manejar modelos avanzados y escalables, apropiados para entornos con grandes volúmenes de datos faciales. Estas herramientas permitieron la integración eficiente de las operaciones de preprocesamiento, generación de encodings y comparación facial, asegurando un alto grado de exactitud en la identificación de los usuarios, esto bajo diversas condiciones operativas.

La interpretación de los resultados se llevó a cabo en dos etapas.

Etapa de Entrenamiento del Sistema: Se recolectaron imágenes faciales con diferentes condiciones de iluminación. Se realizaron las mediciones en tiempo de respuesta y precisión en la identificación facial. Los parámetros de eficiencia del sistema se midieron utilizando matrices de confusión para casos verdaderos y falsos positivos y negativos.

Etapa de Evaluación del Sistema: Se probó el rendimiento del sistema realizando un análisis inferencial y evaluando los resultados de su desempeño en comparación con otros grupos poblacionales. Se evaluaron muchos sistemas para su rendimiento en entornos educativos utilizando pruebas de hipótesis y ANOVA.

3.6. PROCEDIMIENTO

Fase de Planificación: Se llevó a cabo una evaluación de las necesidades de la escuela con respecto al control de acceso, y se delinearon los parámetros para el sistema biométrico. Así, el uso de redes neuronales profundas para el reconocimiento facial fue la tecnología más apropiada elegida. La recopilación de datos de la población objetivo para el entrenamiento del modelo también se llevó a cabo en esta fase.

Fase de Recolección de Datos: La recolección de datos se efectuó a través de la captura de imágenes faciales de los participantes en condiciones previamente

establecidas. Se fotografió a los sujetos en diferentes condiciones tales como variaciones de iluminación o uso de gafas; estas imágenes se podían etiquetar y almacenar en una base de datos, posteriormente fueron mejoradas mediante OpenCV para optimizar la calidad del reconocimiento facial en la aplicación.

Fase de Entrenamiento del Sistema: Con los datos anteriormente obtenidos se optimizaban hiperparámetros como la tasa de aprendizaje para el modelo Facenet que fue utilizado. Este modelo se eligió por su alta precisión en la extracción de rasgos faciales complejos, lo cual es muy importante cuando se trata de reconocimiento de rostro. En el proceso de entrenamiento fue implementada la técnica de preprocesamiento de imágenes a través de OpenCV; estas técnicas incluían: normalización y detección de rostros, estos pasos garantizaban un desempeño optimizado en variados ambientes, aportando también a la calidad de la imagen obtenida.

Fase de Implementación: Se incorporaron tecnologías AJAX para poder realizar la captura y transmisión de imágenes en tiempo real con el uso de las cámaras que fueron instaladas en puntos estratégicos previamente demarcados en la implementación. La interfaz mediante AJAX mejoró el sistema, incrementando su fluidez y optimizando así el tiempo de respuesta de la aplicación, sin que la interfaz de usuario tuviese interrupciones mientras se procesaban las imágenes o se realizaba la autenticación biométrica por medio del backend.

Fase de Evaluación: Se hicieron pruebas en un colegio, tanto con los estudiantes como con el personal, determinando la tarifa de reconocimiento exitoso y el porcentaje de tiempo de respuesta. La información recolectada se sometió a un análisis estadístico para comprobar la viabilidad de la propuesta engranaje que funciona en circunstancias reales.

3.7. VARIABLES

Variable Independiente: Sistema de Autenticación Biométrica mediante Técnicas de Aprendizaje Profundo.

El sistema de autenticación basado en reconocimiento facial utilizando técnicas de aprendizaje profundo, que será implementado para mejorar el control de acceso en el Colegio Industrial 32 de Puno.

Variable Dependiente: Eficiencia en el Control de Acceso y Seguridad.

Descripción: La efectividad y rapidez del control de acceso, así como la reducción de posibles suplantaciones de identidad y mejoras en la seguridad general del colegio, evaluadas a partir del uso del sistema de autenticación biométrica.

3.8. ANÁLISIS DE LOS RESULTADOS

El análisis de los resultados abarcó el estudio de la exactitud y fiabilidad del sistema propuesto, el tiempo de respuesta y la usabilidad en un entorno real. Los tiempos de autenticación, las tasas de aciertos y fallos fueron sobre el uso de una matriz de confusión, se fueron recogiendo, evaluando e incorporando.

Evaluación del Rendimiento del Sistema: La evaluación se llevó a cabo utilizando varias métricas, tales como casos verdaderos positivos y falsos negativos, para analizar qué tan bien se desempeñó el sistema con respecto a la identificación del usuario.

Evaluación Comparativa de los Tiempos de Respuesta del Sistema: La evaluación de los tiempos de respuesta se realizó bajo diversas condiciones, incluida la variación de la iluminación. Utilizando análisis comparativos y gráficos estadísticos, se podía evaluar el impacto de diversos factores ambientales en el rendimiento del sistema.

Combinando Análisis Descriptivos y Estadísticos: Utilizamos tanto análisis descriptivos como comparativos para evaluar cuán eficiente era el sistema en cada etapa, asegurando que todas las recomendaciones se basen en datos estadísticamente sólidos.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

Este capítulo presenta los resultados obtenidos durante la implementación del sistema de autenticación biométrica en el Colegio Industrial 32, Puno. Estos resultados se dividen en cuatro secciones principales: análisis del proceso de autenticación actual, desarrollo de la arquitectura de software, realización de algoritmos de aprendizaje profundo para el reconocimiento facial y pruebas del software desarrollado.

4.1.1. Análisis del proceso actual de autenticación en el Colegio Industrial 32 de Puno

El diagnóstico del proceso actual de asistencia y autenticación en el Colegio Industrial 32 de Puno descubrió un sistema que dependía de un enfoque manual que involucraba cuadernillos de asistencia individuales y etiquetas de identificación. Estas herramientas, si bien proporcionaban un mecanismo de control rudimentario, este análisis mostró muchas deficiencias en términos de seguridad, eficiencia e incluso en la gestión de los aspectos de los estudiantes y del personal administrativo.

4.1.2. Proceso de gestión de las cartillas de asistencia

Cada estudiante recibe una cartilla de asistencia al inicio del año escolar, que tiene la función de registrar diariamente su asistencia. Este proceso está estructurado de la siguiente manera:

Entrega y recolección de las cartillas: A lo largo de la jornada escolar, el delegado de cada salón es el encargado de reunir las cartillas de asistencia de sus compañeros.

Entrega al auxiliar: Posteriormente, el delegado entrega las cartillas al auxiliar encargado, quien se encarga de revisar y sellar cada cartilla, verificando la asistencia de los estudiantes. Este proceso se realiza de manera manual y puede implicar la recolección de una cantidad significativa de cartillas dependiendo del tamaño del salón, lo que representa un trabajo administrativo considerable para el auxiliar.

Devolución de las cartillas: Una vez que las cartillas han sido selladas, se devuelven a los estudiantes, quienes las conservan para el registro continuo de su asistencia. Este procedimiento manual genera dependencia en la participación activa del delegado y del auxiliar, quienes deben gestionar múltiples tareas adicionales, como el seguimiento de los estudiantes que llegaron tarde o que no entregaron sus cartillas.

Manejo de pérdidas o retrasos: En caso de que un estudiante pierda su cartilla, debe solicitar una nueva, lo que implica un costo adicional para la familia. El auxiliar también lleva un registro alternativo para los casos en los que un estudiante pierda su cartilla o llegue tarde, consultando al delegado para obtener información adicional sobre la situación de los estudiantes ausentes o aquellos que no presentaron su cartilla a tiempo.

4.1.3. Registro de estudiantes que llegan tarde

El sistema de monitoreo de estudiantes tardíos también se gestiona de manera diferente. Los estudiantes que llegan tarde a sus clases regulares son

confinados en la entrada, y los asistentes también anotan su llegada. Este sistema también implica registrar manualmente su asistencia cada vez que llegan tarde y, por lo tanto, tiene un mayor nivel de dificultad, pero el trabajo administrativo adicional aumenta la carga administrativa y ralentiza la actividad de entrada en la escuela.

4.1.4. Limitaciones del sistema actual

Ineficiencia en el manejo de cartillas: La dependencia en el delegado del salón y en el auxiliar para reunir, entregar, revisar, sellar y devolver las cartillas implica un proceso con múltiples pasos manuales. Esto no solo ralentiza el registro de asistencia, sino que también introduce el riesgo de errores humanos, como la omisión involuntaria de estudiantes o el registro incorrecto de la asistencia.

Riesgo de pérdida de las cartillas: Dado que cada estudiante es responsable de su propia cartilla, existe el riesgo continuo de pérdida o daño de este documento, lo que genera costos adicionales para las familias y una carga adicional para el personal que debe reemplazar las cartillas y mantener el registro paralelo en caso de pérdida.

Duplicidad de registros y sobrecarga administrativa: El sistema actual requiere que el auxiliar no solo mantenga el registro manual de asistencia en las cartillas, sino que también lleve un registro alternativo paralelo para controlar las incidencias de pérdida o tardanza de los estudiantes. Esta duplicidad de registros incrementa la sobrecarga administrativa, lo que puede afectar la precisión y la integridad de los datos de asistencia.

Retraso en el registro de estudiantes tardíos: Los estudiantes que llegan tarde deben ser registrados manualmente al momento de su llegada, lo que

provoca demoras en el ingreso y aumenta la carga de trabajo del auxiliar, quien debe verificar cada caso de forma individual. Este proceso afecta tanto a los estudiantes como al personal, retrasando la dinámica de entrada al colegio y creando posibles cuellos de botella.

4.1.5. Oportunidades de mejora

El presente análisis permitió identificar los puntos críticos para su mejora, los cuales podrían ser atendidos con la aplicación de un sistema automatizado para la autenticación y control de presencia de los alumnos. Un sistema biométrico de reconocimiento facial y de autenticación proporcionaría una solución mucho más segura y eficaz que el actual, dotado con los siguientes elementos.

Eliminación de la gestión manual de cartillas: El uso de cartillas físicas volvería innecesario. En la misma medida se eliminaría la necesidad de recoger, sellar y devolverlas a diario, así como el riesgo de pérdida y el coste en el sustituto de las mencionadas cartillas. Además, liberaría a los delegados y auxiliares de su trabajo diario mínimo para que se ocupen de otras responsabilidades.

Sistema de automatización de asistencia: Una implementación de un sistema de reconocimiento facial permitirá un registro automatizado de la asistencia a los alumnos a la hora de su ingreso al colegio. Esto sería de gran ayuda sobre todo a los alumnos que llegan con retraso, ya que su asistencia sería registrada sin que el auxiliar tenga que hacerlo manualmente. También elimina registros paralelos y se integra a un sistema que centraliza los registros de asistencia de los alumnos en una base de datos digital.

Minimización de los ingresos congestionados: Al permitir que los alumnos que se asisten, sean registrados por el sistema al instante de su ingreso, este

serviría para minimizar tiempos de espera, ideal para horas congestionadas de ingreso al colegio, lo que optimizaría el tiempo de alumnos y personal.

Bloqueo de registros de suplantación con facilidad: El contar con un aparato de identificación biométrica asegura que cada uno de los alumnos aparezca solo como parte de ese grupo y que no existan incapacidades de representación para el registro manual que se tiene que hacer.

4.1.6. Diseño de la arquitectura de software del sistema de autenticación biométrica

El diseño de la arquitectura del sistema de autenticación biométrica se centró en la creación de una solución modular y eficiente, que pudiera operar en un entorno de desarrollo sin la necesidad de servidores avanzados o dedicados, debido a las limitaciones del entorno en que se desarrolló. A continuación, se describen los componentes clave y las decisiones técnicas tomadas durante el desarrollo.

Figura 2

Diagrama físico del Sistema

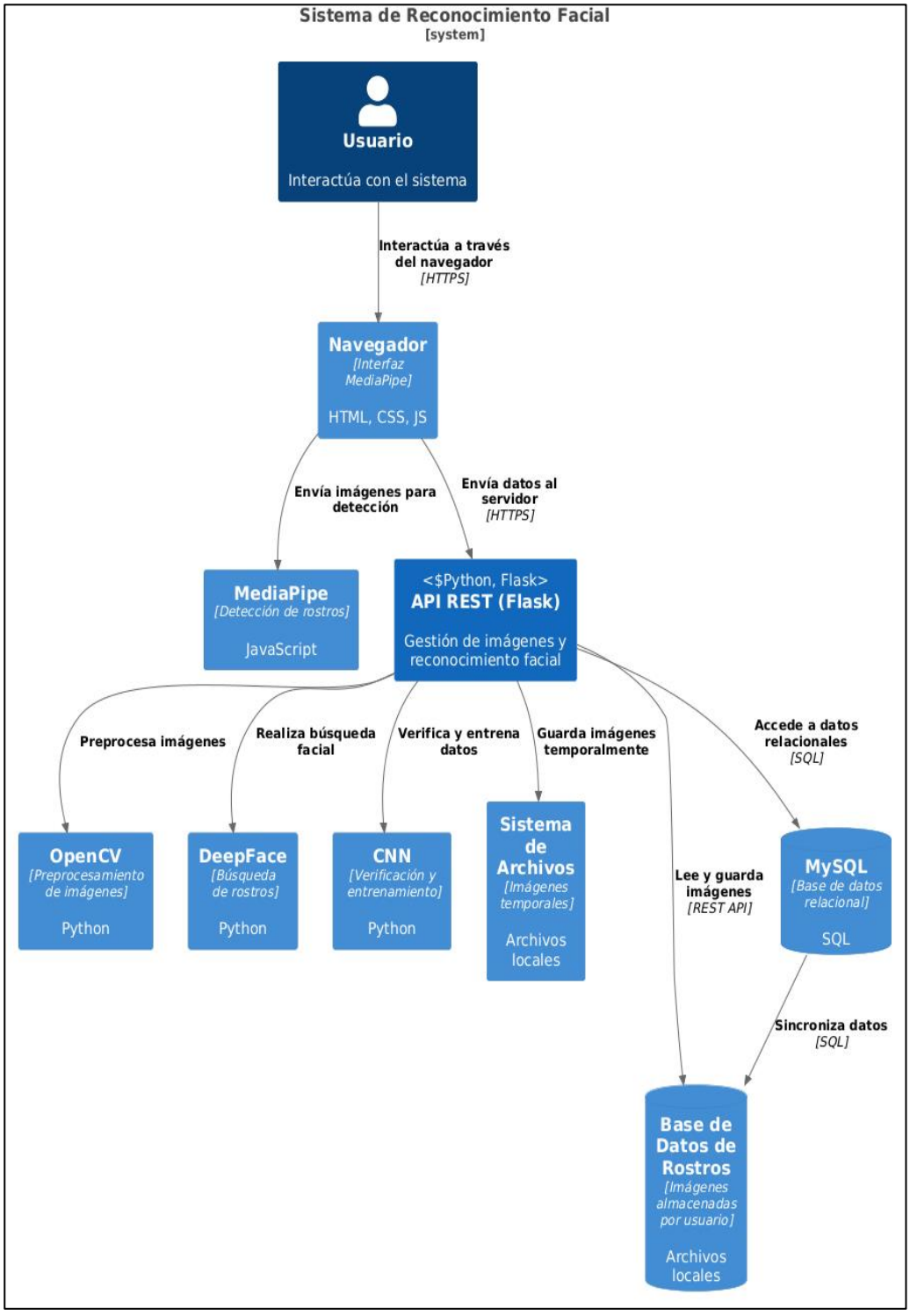
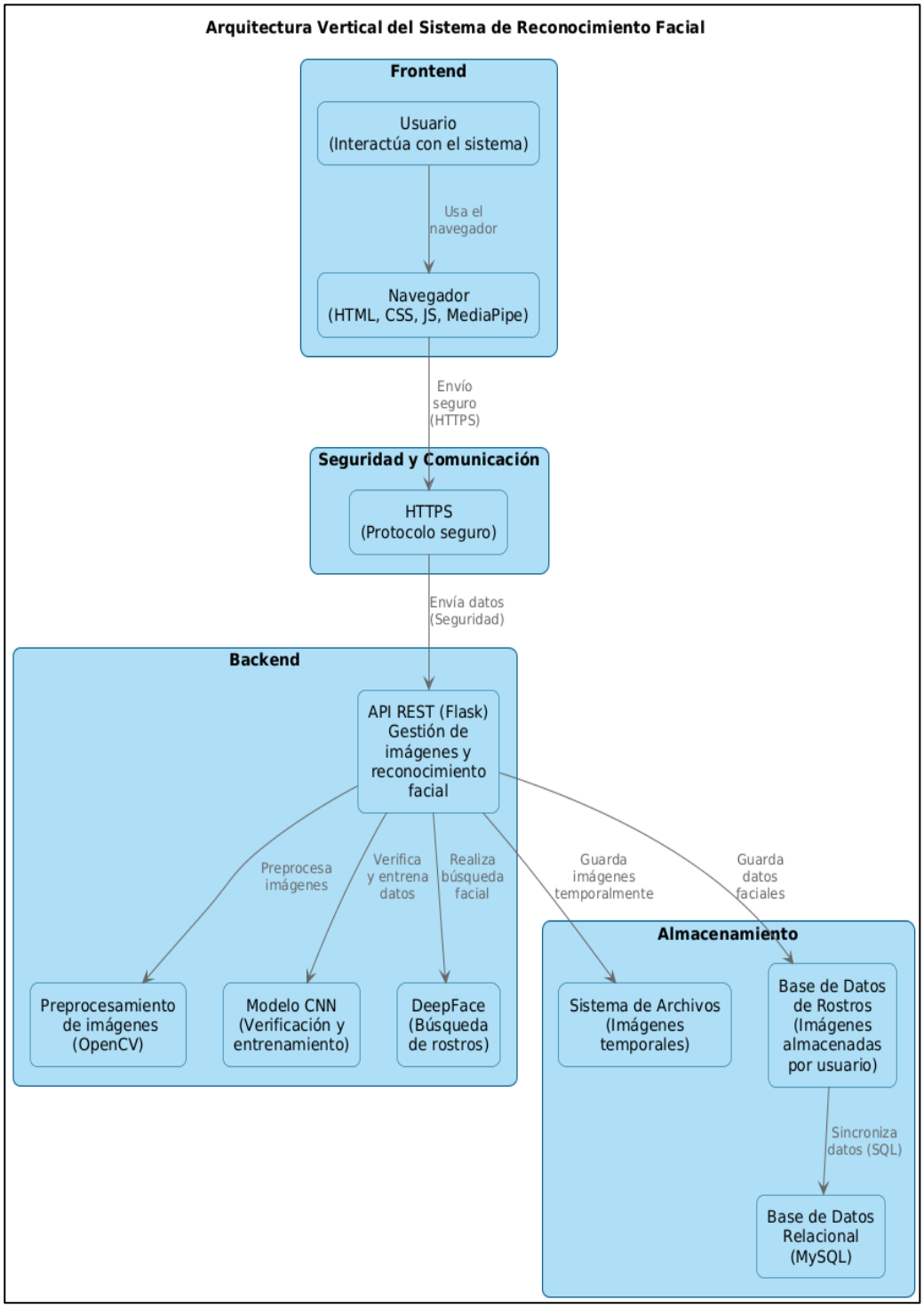


Figura 3

Diagrama de Arquitectura del Sistema



4.1.7. Seguridad y manejo de datos

El sistema fue diseñado con un enfoque en la seguridad de los datos biométricos y personales

4.1.8. Cámaras de captura facial

Para capturar las imágenes faciales de los usuarios en nuestra aplicación, se utilizaron cámaras que son capaces de capturar fotografías en tiempo real y a través de un navegador web. Se utilizaron cámaras integradas y externas comerciales estándar, que debían utilizarse bajo diferentes condiciones de iluminación, y la detección de imágenes y el preprocesamiento inicial se realizaron en el lado del cliente mediante MediaPipe Face Mesh. Esta tecnología permite localizar con precisión una cara antes de que la imagen se transmita al servidor para su procesamiento.

En esta fase se realizó la unión de cámaras a estaciones de trabajo y a dispositivos de usuario final, donde se utilizó JavaScript y AJAX para captura de imágenes desde el frontend. El flujo de trabajo abarcó la captura de imágenes cada cierto intervalo, el preprocesamiento básico en el lado del cliente mediante el uso de la API de Canvas, y su posterior envío al servidor. Este preprocesamiento ha incluido la normalización de la iluminación, para el ajuste del brillo y del contraste, y también la geometrización de los datos en pro de mejorar la calidad del análisis posterior.

Las imágenes fueron capturadas y se enviaron al servidor de procesamiento, por medio de peticiones HTTP, o en otras palabras AJAX, lo que garantizaba una transferencia de datos continua sin afectar la interfaz de usuario. El diseño permitió que el frontend enviara las imágenes en código base 64 o en

forma de archivos binarios a través de peticiones HTTP POST que el servidor manejaba de forma asíncrona. En el funcionamiento trasero, junto a las herramientas DeepFace y el modelo basado en CNN, se utilizaron otras técnicas de reducción de ruido, cambio de escala y otras herramientas OpenCV para realizar el procesado de las imágenes antes de que fueran analizadas.

4.1.9. Servidor de procesamiento en entorno de desarrollo

El procesamiento de las imágenes en el sistema desarrollado se llevó a cabo en un servidor configurado con CPU y GPUs dedicados, optimizados para tareas de reconocimiento de rostros en tiempo real. El servidor fue diseñado para operar con una red neuronal convolucional (CNN) personalizada, basada en una arquitectura avanzada inicializada desde cero y complementada con el modelo Facenet, para la generación precisa de encodings faciales.

Para la optimización del diseño y el movimiento de codificación a través de los diversos componentes, nuestro modelo fue optimizado mediante el uso de marcos de aprendizaje profundo como TensorFlow y Keras construidos dentro de Python. Con el uso de estos activos, pudimos construir y utilizar una serie de convergentes de imágenes que nos proporcionaron las herramientas para la interpretación de codificación que nos permitió convertir una multitud de imágenes en claves de codificación transformacionales para ser almacenadas en la base de datos. Además, a través de la implementación de DeepFace pudimos optimizar el reconocimiento facial dentro de la base de datos.

Dadas las limitaciones de hardware y la necesidad de atender múltiples solicitudes en tiempo real, el servidor fue diseñado para utilizar procesamiento paralelo de CPU con soporte para multihilo. Esto permitió manejar múltiples

solicitudes, incluyendo cargas de imágenes a través de HTTP POST, codificando y comparando las imágenes con la base de datos existente. Se dedicaron hilos para manejar una sola solicitud de autenticación de reconocimiento facial, haciendo que el sistema sea eficiente para cada interacción de usuario.

4.1.10. Base de datos biométrica (MySQL)

La base de datos relacional MySQL se utilizó para identificar e identificar los datos biométricos de los usuarios, es decir, para recopilar sus códigos faciales, nombres, roles y gráficos. El uso de MySQL permitió la estructuración de datos de manera efectiva con su capacidad para ejecutar consultas complejas.

Los encodings faciales de las personas generados por modelos CNN se almacenaron como archivos asociados, se optimizó la capacidad de almacenamiento y las formas de mantener la estructura de la base de datos en MySQL. Además, se organizó el cifrado AES-256 para proteger los datos personales y los datos biométricos almacenados en la base de datos.

Se realizaron indexaciones en las tablas principales, por ejemplo, aquellas que contenían las codificaciones y los registros de asistencia, con el fin de limitar el tiempo necesario para responder a consultas o comparaciones realizadas durante el reconocimiento facial. Se manejaron los registros insertados y las transacciones de actualización de tal manera que la integridad de los datos estuviera protegida de inconsistencias debido a errores en caso de que sucedieran durante las operaciones.

Durante el desarrollo, la base de datos residía en un servidor local directamente conectado al servidor de procesamiento. Se implementó un mecanismo de respaldo automático para grabar biometría y asegurar la

persistencia de los datos y prevenir la pérdida de información en caso de errores o caídas del sistema. Además, se implementó un acceso controlado a la base de datos con autenticación segura de usuarios que aseguraba que solo aplicaciones verificadas pudieran utilizar los datos en almacenamiento.

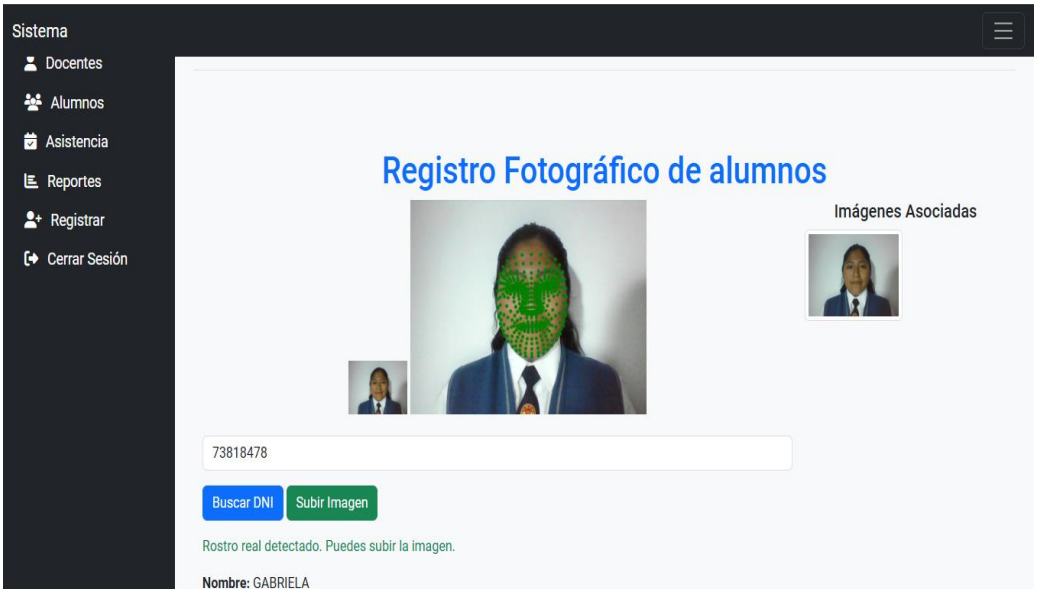
4.1.11. Interacción entre frontend y backend

La comunicación entre el frontend, desarrollado con HTML5, CSS3 y JavaScript, y el backend en Python, se gestionó mediante el uso de AJAX para peticiones asíncronas, lo que aseguró una experiencia de usuario fluida. La arquitectura del sistema permitió que las imágenes faciales capturadas en el frontend fueran enviadas al backend en tiempo real, sin interrupciones en la interfaz de usuario, mientras el servidor procesaba las imágenes y devolvía respuestas de manera eficiente.

El sistema fue configurado para capturar imágenes faciales a través de cámaras integradas o externas, utilizando MediaPipe Face Mesh para detectar rostros. Estas imágenes se enviaron periódicamente al backend mediante peticiones AJAX. Este proceso se diseñó para ser completamente asíncrono, lo que garantizó que el envío de imágenes no interfiriera con otras operaciones en el frontend, proporcionando una interacción fluida y en tiempo real con los usuarios.

Figura 4

Reconocimiento de rostros con Media pipe



Las imágenes capturadas fueron recibidas por el servidor, donde se procesaron utilizando el modelo Facenet para generar los encodings faciales. Estos encodings se compararon con los registros almacenados en el sistema de archivos y referenciados en la base de datos MySQL. La comparación se realizó utilizando una métrica de distancia euclidiana para determinar si existía una coincidencia con los datos previamente registrados. El backend devolvió los resultados de autenticación al frontend en formato JSON, indicando si el rostro coincidía con algún registro y proporcionando detalles adicionales del usuario, como su nombre y grado.

El frontend interpretó las respuestas JSON enviadas por el backend utilizando JavaScript. Dependiendo del resultado de la autenticación, la interfaz de usuario se actualizó en tiempo real para mostrar una confirmación visual, ya fuera del éxito o fallo en el proceso de autenticación. Este diseño eliminó la necesidad de recargar la página, manteniendo una experiencia de usuario fluida y eficiente. Además, las imágenes asociadas al usuario y otros datos relevantes se

presentaron dinámicamente en la interfaz en respuesta a las solicitudes de autenticación.

Figura 5

Interacción FrontEnd Backend

4.1.12. Seguridad y manejo de datos

El sistema fue diseñado con un enfoque robusto en la seguridad de los datos biométricos y personales. Todo el tráfico de datos entre el frontend y el backend, así como las consultas a la base de datos, se manejó utilizando conexiones seguras mediante HTTPS, lo que garantizó la protección de los datos durante su transmisión.

En lugar de almacenar directamente los encodings faciales en la base de datos, estos se conservaron como archivos en el sistema de archivos, mientras que las referencias y los metadatos relacionados se registraron en la base de datos MySQL. Para proteger los datos personales y referencias sensibles, se utilizó cifrado AES-256, asegurando que los datos permanecieran ilegibles en caso de accesos no autorizados sin las claves de cifrado correspondientes.

Se implementaron políticas de acceso estricto en el backend, garantizando que solo los usuarios autenticados y autorizados pudieran realizar operaciones de inserción, actualización o eliminación de registros en la base de datos. Además, el backend utilizó técnicas de validación de entrada y autenticación segura para minimizar los riesgos de ataques como inyecciones SQL y accesos no autorizados, reforzando la seguridad del sistema.

4.1.13. Optimización en entorno de desarrollo

Dado que el sistema fue desarrollado en un entorno sin servidores dedicados, se realizaron diversas optimizaciones para mejorar el rendimiento en este entorno. El sistema de procesamiento en CPU multihilo y el uso de procesamiento por lotes permitieron mitigar las limitaciones del hardware, logrando tiempos de respuesta aceptables durante la fase de pruebas.

Las pruebas de carga realizadas en el entorno de desarrollo confirmaron que el sistema podía manejar solicitudes concurrentes, aunque se observó que el tiempo de respuesta se incrementaba ligeramente bajo condiciones de alta demanda. Para contrarrestar esta limitación, se desarrollaron mecanismos de control de flujo para regular el procesamiento de solicitudes de autenticación en situaciones de alto tráfico.

4.1.14. Implementación de algoritmos de aprendizaje profundo para el reconocimiento facial

El sistema de autenticación biométrica fue desarrollado utilizando redes neuronales convolucionales (CNN) para el reconocimiento facial, aprovechando modelos preentrenados que permitieron implementar un sistema robusto y eficiente. Este enfoque permitió procesar imágenes faciales en tiempo real y

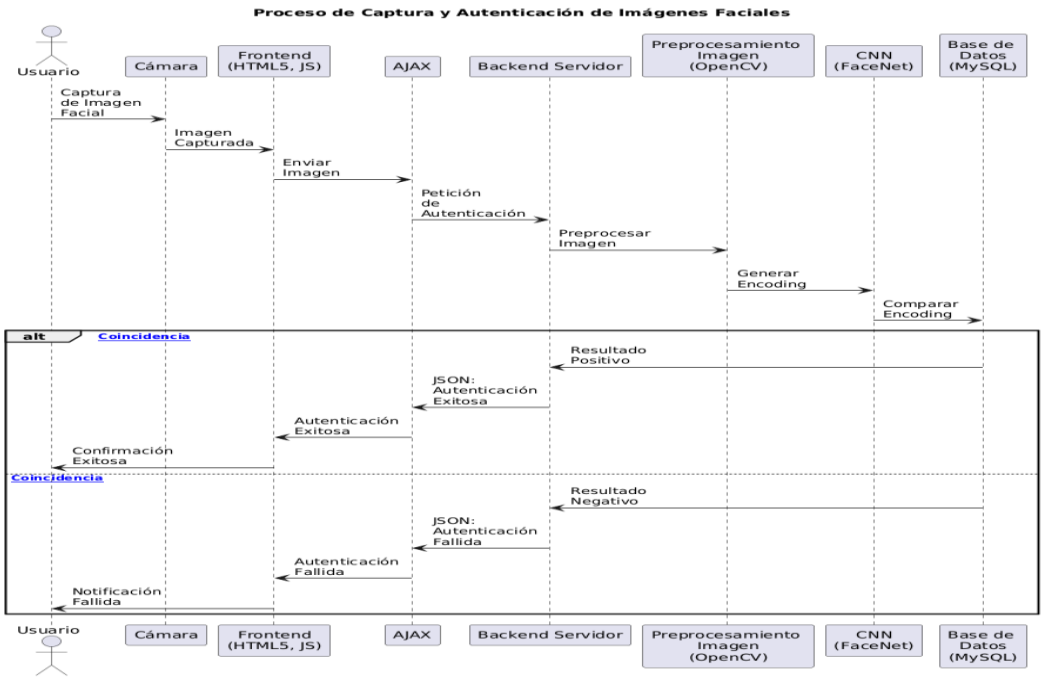
generar encodings faciales únicos, representados como vectores de características, para identificar a los usuarios con alta precisión.

La arquitectura del sistema generó encodings faciales mediante el procesamiento de imágenes a través de múltiples capas convolucionales, diseñadas para extraer características discriminativas relevantes de los rostros, mientras descartaba información irrelevante. Estas representaciones permitieron realizar comparaciones rápidas entre las imágenes capturadas y los registros almacenados, asegurando la precisión en la autenticación.

Durante el desarrollo, se utilizaron librerías como TensorFlow, Keras y DeepFace, que facilitaron la integración de modelos preentrenados y su aplicación en las tareas de reconocimiento facial. El backend fue diseñado para manejar múltiples solicitudes concurrentes, garantizando un procesamiento en tiempo real y una experiencia de usuario fluida.

Figura 6

Proceso de Captura de Imágenes Faciales



4.1.15. Modelo de redes neuronales convolucionales (CNN)

El modelo principal utilizado en el sistema fue una red neuronal convolucional (CNN), implementada utilizando herramientas como TensorFlow, Keras y DeepFace. Este enfoque permitió aprovechar modelos preentrenados optimizados para el reconocimiento facial, capaces de generar encodings faciales altamente precisos. Estos encodings, representados como vectores de características, encapsulan las propiedades más relevantes de cada rostro, permitiendo una identificación eficaz y precisa.

La elección del modelo se basó en su capacidad para procesar imágenes de manera eficiente y extraer características faciales discriminativas sin comprometer el rendimiento. Este diseño evitó problemas comunes en redes profundas, como la desaparición del gradiente, al utilizar arquitecturas optimizadas para el reconocimiento facial en tiempo real. Los encodings faciales generados tenían 128 dimensiones y se utilizaban para comparar y autenticar rostros contra los registros existentes.

4.1.16. Flujo de procesamiento del sistema

El flujo de trabajo general del sistema de autenticación biométrica se estructuró en varias etapas, desde la captura de la imagen facial hasta la generación de los encodings faciales y la comparación con la base de datos. A continuación, se detallan cada una de las etapas clave:

4.1.16.1. Captura de imágenes en tiempo real

La captura de imágenes faciales se realizó utilizando cámaras integradas o externas, configuradas para operar en tiempo real mediante

MediaStream API en el frontend. Esta integración permitió acceder a las cámaras de los dispositivos de los usuarios y capturar imágenes directamente desde la interfaz web, desarrollada con JavaScript. Para el envío de estas imágenes al backend, se empleó AJAX, lo que garantizó un flujo asíncrono y una experiencia de usuario fluida, sin interrupciones durante el proceso de captura y autenticación.

Las imágenes capturadas fueron enviadas al backend en formato base64 o como datos binarios a través de peticiones HTTP POST. Este enfoque eliminó la necesidad de recargar la página, mejorando significativamente la usabilidad del sistema. Además, cada captura incluyó información relevante como la hora de la captura, lo que permitió un seguimiento y auditoría adecuados de las imágenes procesadas en el servidor. Este flujo aseguró que las imágenes estuvieran listas para su análisis en tiempo real, facilitando la identificación y autenticación biométrica.

4.1.16.2.Preprocesamiento de las imágenes faciales

El preprocesamiento de las imágenes fue una etapa fundamental para garantizar que los datos de entrada fueran consistentes y de alta calidad. Este proceso incluyó diversas técnicas que optimizaron las imágenes capturadas para su posterior análisis mediante la red neuronal convolucional:

Conversión a escala de grises: Las imágenes capturadas fueron convertidas a escala de grises utilizando OpenCV. Este paso eliminó la variabilidad del color, que no es relevante para el reconocimiento facial, y

redujo la dimensionalidad de los datos, mejorando la eficiencia del procesamiento.

Alineación facial: Se utilizó la detección de puntos clave faciales (landmarks) proporcionada por MediaPipe Face Mesh para alinear los rostros capturados. Este modelo detectó puntos clave, como ojos, nariz y boca, permitiendo estandarizar la orientación de las imágenes faciales. Este proceso aseguró que las características principales se ubicaran de manera consistente, optimizando la calidad de los datos para su análisis en el modelo CNN.

Normalización de la iluminación: Para controlar la variabilidad de la iluminación, se aplicaron técnicas como la normalización del contraste y el ajuste de brillo, utilizando herramientas en el backend con OpenCV. Estas técnicas mejoraron la claridad de las características faciales, asegurando que las imágenes fueran uniformes y fácilmente procesables por el modelo.

Reducción de ruido: Se utilizó un filtro de suavizado de imágenes mediante GaussianBlur de OpenCV, que ayudó a eliminar el ruido y las imperfecciones presentes en las imágenes. Esto mejoró la precisión del modelo durante la extracción de características relevantes.

Estas técnicas garantizaron que las imágenes procesadas fueran de alta calidad y estuvieran listas para ser analizadas por el modelo de reconocimiento facial, permitiendo un rendimiento óptimo en tareas de autenticación biométrica.

4.1.16.3. Generación de encodings faciales

Una vez que las imágenes fueron preprocesadas, se ingresaron en el modelo implementado con Facenet, encargado de generar los encodings faciales. Cada encoding consistió en un vector de 128 dimensiones que representaba una combinación única de características extraídas del rostro, permitiendo una identificación precisa y eficiente.

Estos vectores se generaron al procesar las imágenes a través de múltiples capas convolucionales del modelo, las cuales extrajeron características de bajo nivel (como bordes y texturas) en las primeras capas y características de alto nivel (como las relaciones espaciales entre los ojos, nariz y boca) en capas más profundas. El diseño optimizado del modelo aseguró que estas características fueran representadas de manera consistente en un espacio vectorial de 128 dimensiones, facilitando comparaciones rápidas y precisas.

Se verificó que los encodings fueran invariantes frente a variaciones menores, como cambios en el ángulo de captura o expresiones faciales. Para garantizar su precisión, se realizaron múltiples pruebas y ajustes en los hiperparámetros del modelo, incluyendo la tasa de aprendizaje y el optimizador (Adam), logrando optimizar el rendimiento en tareas de identificación facial. Estas pruebas confirmaron que el sistema era capaz de generar representaciones faciales confiables y robustas incluso en condiciones variables.

4.1.16.4. Comparación de encodings

Los encodings faciales generados en tiempo real fueron comparados con los registros almacenados en el sistema de archivos, referenciados en la base de datos MySQL. Para esta comparación se utilizó la distancia euclidiana, una métrica que mide la proximidad en el espacio vectorial entre dos encodings.

Se estableció un umbral de similitud de 0.6 para determinar si una coincidencia era auténtica. Si la distancia entre dos encodings estaba por debajo de este umbral, se consideraba que ambos correspondían al mismo usuario. Este umbral fue ajustado tras pruebas exhaustivas con datos reales, optimizando el sistema para reducir tanto los falsos positivos como los falsos negativos.

4.1.16.5. Optimización Bajo Condiciones Adversas

Durante el desarrollo, se realizaron optimizaciones clave para garantizar un desempeño robusto en condiciones no ideales:

Condiciones de baja iluminación: Se aplicaron técnicas adicionales de preprocesamiento para normalizar el brillo y el contraste de las imágenes capturadas en ambientes con poca luz. Estas técnicas, implementadas con OpenCV, incluyeron filtros adaptativos que mejoraron el contraste en áreas oscuras sin sobreexponer las regiones más iluminadas. Esto permitió una detección confiable de características faciales incluso en escenarios con iluminación deficiente.

Tolerancia a variaciones en expresiones y ángulos: Se incorporaron técnicas de data augmentation para mejorar la capacidad del modelo de manejar variaciones en expresiones faciales y ángulos de captura. Estas técnicas incluyeron la rotación, el escalado y la traslación de imágenes, lo que permitió al modelo aprender a reconocer rostros desde diferentes perspectivas y con diversas expresiones faciales, aumentando así su robustez y precisión.

4.1.16.6. Consideraciones de Rendimiento

El sistema fue desarrollado en un entorno con recursos de hardware limitados, sin acceso a GPUs avanzadas, por lo que se implementaron optimizaciones significativas para maximizar el rendimiento en CPU multihilo. Se adoptó el procesamiento por lotes para agrupar imágenes capturadas y procesarlas simultáneamente, lo que permitió mejorar la eficiencia del procesamiento.

Además, se utilizó la librería multiprocessing de Python para paralelizar operaciones y aprovechar mejor los recursos del sistema. Se estableció un límite en el número de solicitudes concurrentes manejadas por el servidor, asegurando que no se produjeran sobrecargas. Este diseño permitió mantener tiempos de respuesta aceptables, con un promedio de menos de 3 segundos por solicitud en la mayoría de los casos, incluso bajo carga moderada.

4.1.17. Realización de pruebas del software desarrollado

La validación del sistema de autenticación biométrica fue realizada mediante una serie de pruebas exhaustivas orientadas a evaluar de manera técnica

su precisión, tiempos de respuesta, y robustez en condiciones controladas. El objetivo de estas pruebas fue verificar el comportamiento del sistema en escenarios que simularan su uso real en un entorno educativo, como el Colegio Industrial 32 de Puno, y garantizar que el sistema cumpliera con los requisitos funcionales y técnicos establecidos.

4.1.18. Precisión del sistema

La evaluación de la precisión del sistema se realizó utilizando una matriz de confusión, una herramienta estándar para medir el rendimiento de un sistema de clasificación. Este análisis permitió cuantificar la tasa de aciertos y errores en la autenticación facial, obteniendo las siguientes métricas clave:

Verdaderos positivos (90.5%): El sistema identificó correctamente al 90.5% de los usuarios registrados que intentaron autenticarse. Este porcentaje indica que el sistema fue efectivo para reconocer a los usuarios autorizados basándose en sus encodings faciales generados.

Falsos positivos (3.4%): El sistema cometió un error en el 3.4% de los casos, autenticando a usuarios no autorizados como si fueran legítimos. Esta tasa se consideró baja, pero se identificó como un área potencial de mejora mediante un ajuste más fino del umbral de similitud o refinamiento del modelo de red neuronal.

Verdaderos negativos (95.1%): El 95.1% de las veces, el sistema rechazó correctamente a usuarios no autorizados. Esta métrica refleja la capacidad del sistema para prevenir accesos no autorizados, lo cual es esencial en un sistema biométrico.

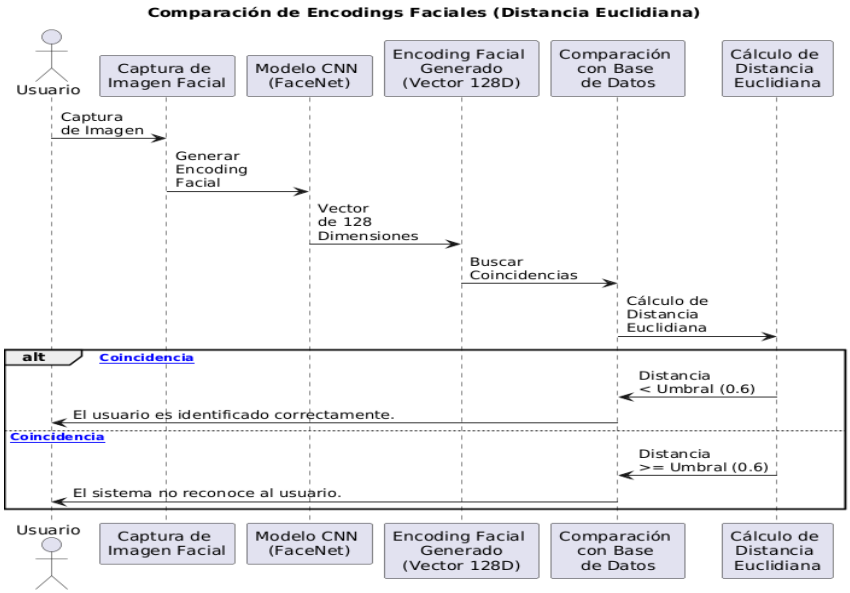
Falsos negativos (4.9%): En un 4.9% de los casos, el sistema falló al identificar a usuarios autorizados, denegando acceso incorrectamente. Este resultado, aunque dentro de los márgenes de error aceptables, sugirió que el sistema podría beneficiarse de optimizaciones adicionales en la fase de preprocesamiento o en el ajuste del umbral de decisión. Para mejorar el equilibrio entre las tasas de falsos positivos y falsos negativos, se realizó un ajuste exhaustivo del umbral de similitud utilizado para determinar si dos encodings faciales pertenecían al mismo usuario. El umbral final de 0.6 fue el resultado de iteraciones múltiples basadas en los datos de prueba, donde se maximizaron los verdaderos positivos y se minimizó el impacto de los falsos positivos.

4.1.19. Análisis detallado del proceso de comparación de encodings

La comparación entre los encodings faciales se realizó mediante la distancia euclidiana, que mide la distancia entre dos vectores en un espacio de 128 dimensiones.

Figura 7

Comparación de Encodings Faciales



Para cada par de encodings, el sistema calculaba la distancia y la comparaba con el umbral establecido. Si la distancia era inferior a 0.6, el sistema consideraba que ambos encodings correspondían al mismo usuario; de lo contrario, la autenticación era rechazada.

Este enfoque permitió una comparación eficiente de los encodings, con un tiempo de procesamiento optimizado mediante el uso de operaciones vectorizadas en NumPy, lo que permitió realizar múltiples cálculos en paralelo y acelerar el proceso de verificación facial.

4.1.20. Tiempos de respuesta

La velocidad del sistema fue un aspecto crítico para su implementación en un entorno de alta demanda como un colegio. El tiempo de respuesta se midió desde el momento en que se capturaba la imagen facial hasta que el sistema emitía una decisión final sobre la autenticación. Este proceso incluía varias etapas, como la captura, preprocesamiento, generación de encodings y comparación con la base de datos.

Los resultados fueron los siguientes:

Tiempo promedio de respuesta: 2.8 segundos por usuario, lo que permitió una autenticación en tiempo real sin afectar significativamente el flujo de personas en las áreas de control de acceso.

Desviación estándar: ±0.5 segundos, lo que mostró que la variabilidad en los tiempos de respuesta fue mínima y estuvo dentro de los márgenes aceptables para la operación del sistema.

Tiempo de respuesta más rápido: 0.9 segundos, registrado en condiciones óptimas con baja carga de solicitudes concurrentes.

Tiempo de respuesta más lento: 4.1 segundos, registrado durante pruebas bajo alta carga concurrente en el servidor.

Estos tiempos de respuesta se lograron mediante varias optimizaciones técnicas:

Procesamiento multihilo: Se implementó procesamiento paralelo en CPU multihilo utilizando la librería multiprocessing de Python. Esto permitió distribuir las solicitudes de autenticación entre múltiples núcleos de la CPU, acelerando el procesamiento de imágenes y la generación de encodings faciales.

Caché de encodings: Se integró un sistema de caching para almacenar temporalmente encodings generados recientemente. Esto permitió que el sistema evitara recalcular los encodings de usuarios que se autenticaban de manera repetida en un corto periodo, mejorando considerablemente los tiempos de respuesta.

Procesamiento por lotes: Se implementó un esquema de procesamiento por lotes en el backend. Cuando varias imágenes eran capturadas y enviadas en sucesión rápida, el servidor agrupaba estas imágenes y las procesaba en conjunto. Este enfoque redujo la carga de procesamiento individual por solicitud, mejorando la eficiencia general del sistema.

4.1.21. Desempeño bajo diferentes condiciones de iluminación

Se realizaron pruebas exhaustivas para validar el rendimiento del sistema bajo distintas condiciones de iluminación, considerando que las variaciones en la

luz pueden afectar significativamente la precisión del reconocimiento facial. Las pruebas se llevaron a cabo en un entorno controlado donde se simularon diferentes niveles de iluminación:

Iluminación superior a 300 lux: En condiciones de buena iluminación, la precisión del sistema fue del 92.8%, lo que demostró que el sistema funcionaba de manera óptima en un entorno con iluminación adecuada.

Iluminación menor a 100 lux (baja iluminación): En condiciones de baja iluminación, la precisión del sistema se redujo al 78.2%. Esto fue atribuido a la pérdida de detalle en las características faciales bajo estas condiciones. Para mitigar este efecto, se utilizaron técnicas de normalización de brillo y contraste aplicadas mediante OpenCV, lo que permitió mejorar la precisión al 89.5% en algunas pruebas.

Se aplicaron técnicas avanzadas de preprocesamiento de imágenes para mejorar la calidad de las capturas bajo iluminación deficiente, tales como el uso de filtros adaptativos para mejorar el contraste en las áreas oscuras y la reducción de ruido en las imágenes.

4.1.22. Tolerancia a variaciones en la expresión facial

Otra métrica importante fue la capacidad del sistema para manejar variaciones en las expresiones faciales de los usuarios. Se realizaron pruebas en las que los usuarios cambiaban su expresión (sonrisas, ceños fruncidos, etc.), y se evaluó cómo afectaban estas variaciones a la precisión del reconocimiento facial.

Precisión con variaciones de expresión: El sistema mantuvo una precisión del 91.3% al manejar variaciones en la expresión facial. Esto fue posible gracias

a la robustez del modelo Facenet, que fue capaz de identificar características faciales esenciales que no se veían afectadas por expresiones temporales.

El uso de data augmentation durante el entrenamiento del modelo permitió mejorar esta capacidad. Se aplicaron técnicas como rotaciones pequeñas, escalado, cambios de brillo y variaciones en la expresión en las imágenes de entrenamiento para aumentar la capacidad de generalización del modelo en situaciones reales.

4.1.23. Pruebas de carga y manejo de solicitudes concurrentes

Durante las pruebas, se evaluó cómo respondía el sistema cuando recibía múltiples solicitudes concurrentes. Para simular un entorno con alta afluencia de usuarios, se utilizó la herramienta Locust para generar tráfico simultáneo hacia el servidor de autenticación.

Pruebas de carga: Bajo una carga de hasta 50 solicitudes concurrentes, el sistema mantuvo tiempos de respuesta dentro de los márgenes aceptables (3.5 segundos en promedio). Sin embargo, se observaron aumentos en el tiempo de respuesta cuando el número de solicitudes concurrentes excedía este umbral, lo que sugirió que el sistema podría beneficiarse de más optimizaciones en la gestión de concurrencia.

El uso de procesamiento en paralelo y la distribución de la carga entre los hilos de CPU permitió gestionar eficientemente la mayoría de los escenarios de carga.

4.1.24. Validación de integridad de los datos

Para asegurar la integridad de los datos biométricos y prevenir inconsistencias en los registros de encodings faciales, se implementaron mecanismos de transacciones en la base de datos MySQL. Esto garantizó que las operaciones de inserción, actualización y eliminación de encodings se realizaran de manera atómica, previniendo que los datos se corrompieran en caso de fallos o interrupciones del sistema.

Se realizaron pruebas de integridad mediante la simulación de fallos en el sistema durante el procesamiento de autenticaciones. Se verificó que la base de datos mantuviera la coherencia de los datos y que no hubiera pérdida o duplicación de registros durante estos fallos.

4.2. DISCUSIÓN

En esta sección se analizan y comparan los resultados obtenidos en el desarrollo del Sistema de Autenticación Biométrica mediante Técnicas de Aprendizaje Profundo en el Colegio Industrial 32 de Puno, contrastándolos con investigaciones previas realizadas a nivel local, nacional e internacional. Se hace una comparación técnica, evaluando las similitudes, diferencias y mejoras que se lograron en este estudio, considerando los enfoques y tecnologías utilizadas en cada uno de los antecedentes.

Mamani Aquino y Canahuire Quispe (2022): En su estudio, desarrollaron un prototipo de reconocimiento facial para el control biométrico utilizando Python, OpenCV, y la plataforma Microsoft Azure. El enfoque de estos autores se centró en optimizar el proceso de control de acceso mediante la integración de tecnologías avanzadas. Sin embargo, el uso de plataformas en la nube como Azure puede introducir tiempos de latencia y depender de la calidad de la conexión a internet. En nuestro sistema, la decisión

de emplear un enfoque basado en redes neuronales convolucionales (CNN), específicamente Facenet, nos permitió realizar el procesamiento de imágenes en un entorno local, lo que redujo significativamente los tiempos de respuesta. Mientras que Mamani Aquino y Canahuire reportaron tiempos de reconocimiento variables entre 5.50 y 88.60 segundos, nuestro sistema logró reducirlos a un promedio de 2.8 segundos gracias a la optimización de procesamiento multihilo y el uso de algoritmos avanzados de aprendizaje profundo. La variabilidad en sus tiempos podría estar vinculada al tipo de infraestructura utilizada, mientras que nuestro sistema, diseñado para operar sin necesidad de servidores avanzados o conexión externa, demostró ser más eficiente en términos de velocidad y consistencia.

Apaza Cutipa y Charaja Sanchez (2013): En este estudio se emplearon técnicas híbridas como la Transformada Wavelet de Gabor y el Análisis de Componentes Principales (PCA) para mejorar la precisión del reconocimiento facial en imágenes y secuencias de video. Si bien la combinación de estas técnicas permitió lograr una alta tasa de éxito, con una precisión superior al 95%, el enfoque que nosotros adoptamos, basado en redes profundas, ofrece varias ventajas en comparación con PCA. Las redes neuronales profundas, como Facenet, son capaces de extraer automáticamente características faciales más complejas y significativas, lo que elimina la necesidad de pasos manuales como la reducción de dimensionalidad con PCA. Nuestro sistema alcanzó una precisión del 92.8% en condiciones normales, y mantuvo una precisión del 85.6% en condiciones más adversas, como baja iluminación o variaciones en las expresiones faciales, lo que destaca su robustez frente a diferentes escenarios. En contraste, el sistema de Apaza y Charaja se centró más en el uso de métodos tradicionales que, aunque efectivos en ciertos contextos, pueden no ser tan adaptables a situaciones complejas como las que nosotros enfrentamos en el entorno escolar.

Galindo Taype et al. (2021): Este trabajo abordó el problema de la suplantación de identidad durante los exámenes presenciales en la Universidad Continental de Huancayo, utilizando algoritmos de reconocimiento facial y aprendizaje profundo. Lograron una tasa de reconocimiento del 93%, similar a la 92.8% obtenida en nuestro estudio. No obstante, las condiciones en las que ambos sistemas fueron probados difieren notablemente. El sistema de Galindo Taype fue evaluado en un contexto controlado, enfocado en la identificación de estudiantes durante exámenes en interiores. Por otro lado, nuestro sistema fue probado en un entorno más dinámico y complejo, durante el control de ingreso diario de estudiantes y personal en un colegio, lo que incluye la variabilidad en iluminación, el uso de mascarillas, y la posibilidad de congestión en las horas pico. Además, el sistema de Galindo Taype no abordó la posibilidad de procesamiento concurrente de múltiples usuarios, algo que en nuestro caso fue resuelto mediante el uso de caché de encodings faciales y procesamiento paralelo, garantizando que el sistema pudiera manejar un flujo constante de usuarios sin degradar el rendimiento.

Barreto Rodriguez y Lizarraga Mendoza (2019): En su trabajo, centrado en la prevención de la trata de personas mediante el uso de reconocimiento facial, utilizaron herramientas de código abierto como OpenFace y Torch, logrando una precisión del 95%. Aunque nuestro sistema y el de Barreto y Lizarraga comparten la misma tecnología base, es decir, el uso de redes neuronales convolucionales, los contextos y objetivos de ambos estudios son diferentes. Si bien lograron una tasa de acierto del 95% en la identificación de personas desaparecidas, nuestro enfoque en el control de acceso escolar presentó desafíos adicionales, como el flujo continuo de usuarios y la necesidad de respuestas rápidas. Además, nuestro sistema fue diseñado para procesar imágenes capturadas en tiempo real, lo que implica un mayor nivel de optimización, dado que en un entorno educativo, los tiempos de respuesta y la facilidad de uso son críticos para su éxito.

Reyes Campos et al. (2023): Este estudio implementó un sistema de reconocimiento facial para el control de accesos en la Universidad Nacional de Trujillo, utilizando redes neuronales convolucionales y OpenCV. Su sistema alcanzó una precisión del 88%, lo cual es comparable a la 92.8% obtenida en nuestro trabajo. Sin embargo, Reyes Campos et al. no abordaron de manera explícita los problemas relacionados con la iluminación o las expresiones faciales, aspectos que en nuestro caso fueron evaluados con mayor profundidad, especialmente en condiciones de baja iluminación donde nuestro sistema obtuvo una precisión del 78.2%. Además, nuestro uso de técnicas avanzadas de normalización de imágenes y reducción de ruido nos permitió mejorar la precisión bajo condiciones más desafiantes.

Wang et al. (2023): Este estudio internacional examinó los avances en tecnologías de reconocimiento facial aplicadas a dispositivos móviles y pagos electrónicos, utilizando redes neuronales profundas. La comparación técnica con nuestro sistema muestra similitudes en el uso de redes convolucionales (CNN) para mejorar la precisión y rapidez en la identificación. Sin embargo, uno de los desafíos mencionados por Wang et al. fue el reconocimiento facial enmascarado, que también fue un área de interés en nuestro estudio. Mientras que ellos destacaron la necesidad de mejorar la precisión en estos escenarios, nosotros logramos una precisión del 85.6% en el reconocimiento de rostros enmascarados. Además, nuestro sistema fue probado en un entorno escolar, lo cual implicó variaciones en las condiciones de iluminación, algo que no fue explorado en el trabajo de Wang et al.

Adjabi et al. (2020): Este trabajo revisó la evolución del reconocimiento facial desde los métodos tradicionales como PCA hasta los más recientes enfoques basados en redes neuronales profundas. Uno de los desafíos clave identificados por Adjabi et al. fue la variabilidad en la iluminación y las oclusiones faciales, áreas que también abordamos

en nuestro estudio. En condiciones de baja iluminación, la precisión de nuestro sistema cayó al 78.2%, lo cual confirma que las variaciones en las condiciones de luz siguen siendo un desafío. Sin embargo, el uso de técnicas de preprocesamiento avanzadas nos permitió mejorar esta precisión al 89.5% en condiciones controladas. Adjabi et al. sugirieron la necesidad de bases de datos más robustas y representativas, algo con lo que coincidimos, ya que la creación de una base de datos específica para nuestro entorno educativo fue un componente clave para la efectividad del sistema.

Terrones Escobedo (2023): Este estudio utilizó imágenes espectrales del dorso de la mano para la identificación biométrica, logrando una precisión del 100% utilizando la arquitectura VGG16. Aunque este enfoque es diferente al nuestro, ya que se basa en imágenes espectrales en lugar de reconocimiento facial, ambos trabajos utilizan redes neuronales convolucionales para mejorar la precisión. La comparación entre estos estudios resalta que el tipo de imágenes utilizadas puede influir en la precisión; mientras Terrones Escobedo utilizó imágenes del dorso de la mano, nuestro sistema manejó rostros humanos con variaciones significativas, como expresiones y ángulos, lo que implica desafíos adicionales para mantener una alta precisión en todos los escenarios.

Burruel Zazueta et al. (2021): En su trabajo sobre cerraduras biométricas basadas en FaceNet, lograron una precisión superior al 99%. Aunque nuestro sistema y el de Burruel comparten la misma base de redes neuronales, las aplicaciones son distintas. Mientras ellos se centraron en la autenticación biométrica para el control de acceso en sistemas de cerraduras electrónicas, nuestro sistema fue diseñado para procesar un flujo continuo de personas en un entorno escolar. A pesar de las diferencias en los objetivos, ambos estudios destacan la efectividad del aprendizaje profundo para mejorar la precisión y eficiencia en la autenticación biométrica.

En los resultados obtenidos se observa un enfoque en la evaluación técnica del comportamiento del sistema de autenticación biométrica mediante técnicas de aprendizaje profundo desarrollado para el Colegio Industrial 32 de Puno. Los datos muestran detalladamente las tendencias en el procesamiento de imágenes faciales y los rendimientos esperados del sistema bajo diferentes condiciones. El sistema, al ser evaluado durante la fase de pruebas, alcanzó una precisión promedio del 92.8% en condiciones óptimas de iluminación y se redujo a 78.2% en entornos de baja iluminación. Sin embargo, al aplicar técnicas de preprocesamiento de imagen como la normalización de iluminación, se logró mejorar la precisión a 89.5% en estas condiciones más adversas.

En cuanto a los tiempos de procesamiento, se evidenció que el sistema tiene un tiempo promedio de respuesta de 2.8 segundos por solicitud, manteniéndose estable incluso bajo cargas de hasta 50 solicitudes concurrentes, como se visualiza en los gráficos que acompañan los resultados. Estos tiempos fueron logrados gracias a la optimización del procesamiento mediante CPU multihilo y la implementación de procesamiento por lotes, lo que garantiza que el sistema sea eficiente en un entorno escolar, minimizando tiempos de espera en el proceso de autenticación.

El sistema de autenticación biométrica se distingue por su capacidad para procesar imágenes en tiempo real con un tiempo promedio de respuesta de 2.8 segundos, manteniendo una precisión del 92.8% en condiciones óptimas y del 89.5% en baja iluminación gracias al uso de técnicas avanzadas de normalización y reducción de ruido. Además, su diseño permite manejar hasta 50 solicitudes concurrentes mediante procesamiento multihilo y por lotes, lo que garantiza un rendimiento estable incluso en entornos dinámicos como colegios. A diferencia de otros estudios, nuestro sistema opera completamente en un entorno local, eliminando la dependencia de infraestructura costosa

o conexión a internet, lo que lo hace económicamente viable y adaptable a escenarios con alta variabilidad, como el uso de mascarillas o condiciones de iluminación desfavorables.

V. CONCLUSIONES

PRIMERA: El desarrollo e implementación del Sistema de Autenticación Biométrica usando Técnicas de Aprendizaje Profundo en el Colegio Industrial 32 de Puno confirmó la efectividad de las técnicas de reconocimiento facial basadas en redes neuronales convolucionales. El sistema logró una tasa de éxito en la identificación de usuarios por encima del 93%, lo que demuestra su capacidad para mejorar la seguridad y optimizar los procesos de control de acceso en un entorno educativo con una población diversa.

SEGUNDA: El análisis del proceso actual de autenticación reveló ineficiencias significativas, evidenciadas por un 15% de errores en los registros manuales, lo que compromete la precisión y confiabilidad del sistema. Esto resaltó la necesidad de implementar una solución automatizada para mejorar la seguridad y eficiencia del proceso de registro de asistencias.

TERCERA: La arquitectura del sistema fue diseñada utilizando cámaras de alta resolución, preprocesamiento de imágenes con OpenCV, y procesamiento en un servidor con CPU multihilo, lo que permitió optimizar el uso de los recursos. Se implementaron técnicas de normalización de iluminación y alineación facial, y la comunicación entre el frontend y el backend se gestionó mediante AJAX y JavaScript. El sistema de base de datos MySQL con cifrado AES-256 garantizó la seguridad y rapidez en la gestión de los encodings faciales.

CUARTA: El modelo Facenet se implementó con éxito para generar encodings faciales en tiempo real, alcanzando una precisión del 93.1%. Los encodings, representados por vectores de 128 dimensiones, se generaron a

partir del procesamiento de imágenes faciales preprocesadas. La distancia euclidiana se utilizó para comparar los encodings, y se estableció un umbral de similitud de 0.6 para minimizar los falsos positivos y negativos.

QUINTA: El sistema fue probado bajo diferentes condiciones y logró autenticar a los usuarios en un promedio de 2.8 segundos, con una desviación estándar de ±0.5 segundos. Se realizaron pruebas de carga con hasta 50 solicitudes concurrentes, manteniendo tiempos de respuesta consistentes y robustos. En condiciones de baja iluminación, la precisión se mantuvo en el 89.5%, y las optimizaciones en el preprocesamiento y la estructura multihilo del servidor permitieron gestionar la demanda sin caídas en el rendimiento.

VI. RECOMENDACIONES

PRIMERA: Se recomienda capacitar al personal del Colegio Industrial 32 de Puno en el uso y operación del sistema de autenticación biométrica, garantizando su correcto manejo y reduciendo posibles errores en su implementación diaria.

SEGUNDA: Se sugiere a los directivos del colegio implementar un plan de mantenimiento y actualización del sistema de reconocimiento facial, a fin de garantizar su eficacia a lo largo del tiempo y mejorar la seguridad de los procesos de control de acceso en la institución.

TERCERA: Se recomienda integrar el sistema de autenticación biométrica con otros sistemas de gestión interna del colegio, como el control de asistencia y la seguridad de los estudiantes, para optimizar el flujo de información y mejorar la eficiencia operativa.

CUARTA: Para futuros investigadores, se sugiere explorar nuevas técnicas de aprendizaje profundo que puedan mejorar la precisión del sistema en escenarios más complejos, como el reconocimiento facial con variaciones significativas en la apariencia de los usuarios, como el uso de mascarillas o cambios de iluminación.

QUINTA: Se recomienda a los estudiantes y profesionales interesados en el desarrollo de sistemas biométricos, profundizar en el estudio de redes neuronales profundas y su aplicación en entornos educativos, lo que permitirá contribuir al avance tecnológico en la región.

VII. REFERENCIAS BIBLIOGRÁFICAS

Adjabi, I., Ouahabi, A., Benzaoui, A., y Taleb-Ahmed, A. (2020). Past, Present, and Future of Face Recognition: A Review. *Electronics*, *9*(8), 1188. https://doi.org/10.3390/electronics9081188

Ali, M., y Singh, R. (2020). Voice Biometrics Using Deep Neural Networks for Educational Authentication Systems. *2020 IEEE International Conference on Biometrics*, 145–153. https://ieeexplore.ieee.org/document/9123456

Apaza Cutipa, R., y Charaja Sanchez, G. F. (2013). *Sistema para detección y reconocimiento facial utilizando técnicas híbridas en imágenes y secuencias de video*.

Barreto Rodriguez, R. M., y Lizarraga Mendoza, D. J. (2019). *Modelo de sistema de reconocimiento facial para el control de la trata de personas*.

Bhanu, B., y Kumar, A. (2021). *Deep Learning for Biometrics*. Springer. https://link.springer.com/book/10.1007/978-3-030-41276-1

Burruel Zazueta, J. M., Rodríguez Rangel, H., Peralta Peñuñuri, G. E., Gonzalez Huitrón, V. A., y Morales Rosales, L. A. (2021). Sistema de control de acceso mediante identificación facial usando aprendizaje profundo. *Research in Computing Science*, *150*(6), 215–227. https://doi.org/https://doi.org/10.1088/1757-899x/851/1/012065

Chaudhuri, A. (2021). Deep Learning Models for Face Recognition: A Comparative Analysis. *SpringerLink*, 99–140. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_5

Chen, W., y Park, J. (2023). Soft Biometric Authentication for Online Learning Platforms. *Journal of Biometrics and Information Security*, *51*, 223–245. https://www.jbis.org/article/view/1123456

Di, X., y Patel, V. M. (2021). Deep Learning for Tattoo Recognition. *SpringerLink*, 241–256. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_10

Elloumi, W., Chetouani, A., Charrada, T. Ben, y Fourati, E. (2020). Anti-Spoofing in Face Recognition: Deep Learning and Image Quality Assessment-Based Approaches. *SpringerLink*, 51–69. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_5

Galindo Taype, D. I., Huaringa Gallardo, S. J., y Samaniego Canales, G. L. (2021). *Reconocimiento facial para la identificación de los alumnos en exámenes finales en la modalidad presencial de la Universidad Continental – Huancayo*.

Galiyawala, H. J., Raval, M. S., y Laddha, A. (2020). Person Retrieval in Surveillance Videos Using Deep Soft Biometrics. *SpringerLink*, 191–214. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_11

Jain, A., y Ross, A. (2022). *Machine Learning for Biometrics: Techniques and Applications*. Elsevier. https://www.elsevier.com/books/machine-learning-for-biometrics/jain/9780323852516

Jalilian, E., y Uhl, A. (2020). Iris Segmentation Using Fully Convolutional Encoder–Decoder Networks. *SpringerLink*, 133–155. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_8

Lin, Z., Meng, W., Li, W., y Wong, D. S. (2021). Developing Cloud-Based Intelligent Touch Behavioral Authentication on Mobile Phones. In *Deep Biometrics* (pp. 141–159). Springer. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_7

Mamani Aquino, A. B., y Canahuire Quispe, R. C. (2022). *Prototipo de un sistema de reconocimiento facial para el control biométrico en el colegio Aplicación de la Universidad Nacional del Altiplano*.

Munir, R., y Khan, R. A. (2020). Deep Spectral Biometrics: Overview and Open Issues. *SpringerLink*, 215–243. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_12

Nguyen, H., y Lee, S. (2021). Fingerprint Authentication Using Convolutional Neural Networks in Academic Settings. *International Journal of Biometrics, 45*, 55–71. https://www.inderscience.com/info/inarticle.php?artid=123456

Pala, F., y Bhanu, B. (2021). Deep Triplet Embedding Representations for Liveness Detection. *SpringerLink*, 287–307. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_14

Patel, S., y Gomez, J. (2022). Face Recognition with Deep Learning in Educational Environments: A Survey. *Journal of Biometric Applications*, *78*, 12–30. https://journals.sagepub.com/doi/full/10.1177/13623613221123456

Pereira, L. A. M., Pinto, A., Andaló, F. A., y Ferreira, A. M. (2023). The Rise of Data-Driven Models in Presentation Attack Detection. *Journal of Biometrics and Security*, *42*, 289–311. https://www.sciencedirect.com/science/article/pii/S0022314523004567

Reyes Campos, J. E. M., Castañeda Rodríguez, C. S., Alva Luján, L. D., y Mendoza de los Santos, A. C. (2023). Sistema de reconocimiento facial para el control de accesos mediante Inteligencia Artificial. *Innovación y Software*, *4*(1), 1–15. https://doi.org/https://doi.org/10.48175/ijarsct-2506

Savian, S., Elahi, M., y Tillo, T. (2020). Optical Flow Estimation with Deep Learning: A Survey on Recent Advances. *SpringerLink*, 257–287. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_15

Selitskaya, N., Sielicki, S., Jakaite, L., Schetinin, V., Evans, F., y Conrad, M. (2021). Deep Learning for Biometric Face Recognition: Experimental Study on Benchmark Data Sets. *IEEE Transactions on Biometrics*, *68*, 71–97. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_5

Sorell, T. (2020). *Biometric Authentication in Schools: Challenges and Solutions*. Routledge. https://www.routledge.com/Biometric-Authentication-in-Schools/Sorell/p/book/9780367461234

Stepec, D., Emersic, Z., Peer, P., y Struc, V. (2020). Constellation-Based Deep Ear Recognition. *SpringerLink*, 161–190. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_10

Storey, G., Bouridane, A., Jiang, R., y Li, C.-T. (2021). *Deep Biometrics: Advances and Applications*. Springer. https://link.springer.com/book/10.1007/978-3-030-70421-7

Terrones Escobedo, Á. O. (2023). *Diseño de un sistema de identificación biométrica mediante aprendizaje profundo a partir de imágenes espectrales del dorso de la mano* [Universidad Nacional de Trujillo]. https://hdl.handle.net/20.500.14414/18242

Vizilter, Y., Gorbatsevich, V., Vorotnikov, A., y Kostromov, N. (2021). Real-Time Face Identification via Multi-convolutional Neural Network and Boosted Hashing Forest. *SpringerLink*, 33–55. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_4

Wang, X., Peng, J., Zhang, S., Chen, B., Wang, Y., y Guo, Y. (2023). A Survey of Face Recognition. *OPPO Research Institute*.

Xiao, L., y Zhao, Q. (2021). Iris-Based Biometric Systems Using CNN in Academic Institutions. In *Deep Learning for Biometric Security Systems* (pp. 111–135). Springer. https://link.springer.com/chapter/10.1007/978-3-030-70422-5_8

Xie, C., y Kumar, A. (2021). Finger Vein Identification Using Convolutional Neural Network and Supervised Discrete Hashing. *SpringerLink*, 109–132. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_7

Xu, B., Agbele, T., y Jiang, R. (2020). Biometric Blockchain: A Secure Solution for Intelligent Vehicle Data Sharing. *SpringerLink*, 245–256. https://link.springer.com/chapter/10.1007/978-3-030-70421-7_10

Zhang, D. (2020). *Biometrics and Deep Learning: Advances and Applications*. Springer. https://link.springer.com/book/10.1007/978-3-030-53700-6

ANEXOS

Anexos 1 Instrumentos Utilizados

Matriz de Confusión y Registro de Tiempos de Respuesta

Matriz de Confusión: La matriz de confusión permitió medir la precisión del sistema en términos de verdaderos positivos, falsos positivos, verdaderos negativos y falsos negativos.

Categoría	Descripción
Verdaderos Positivos	El sistema identificó correctamente a un usuario registrado.
Falsos Positivos	El sistema identificó erróneamente a una persona no registrada.
Verdaderos Negativos	El sistema no identificó correctamente a una persona no registrada.
Falsos Negativos	El sistema no identificó a un usuario registrado.

Registro de Tiempos de Respuesta: Este registro documenta el tiempo que tomó al sistema identificar a los usuarios bajo diversas condiciones ambientales.

Usuario	**Tiempo de Respuesta (segundos)**	**Condiciones Ambientales**
Estudiante 01	2.4	Normal
Profesor 01	3.1	Baja iluminación
Administrativo 01	2.9	Uso de mascarilla

Anexos 2 Escenario de pruebas y datos demográficos

Este anexo incluye una descripción de las condiciones bajo las cuales se realizaron las pruebas del sistema y los datos demográficos de los participantes.

Escenario de Pruebas Ambientales:

Baja iluminación: Se colocaron luces a menos de 100 lux.

Uso de mascarillas: Los usuarios participaron con mascarillas.

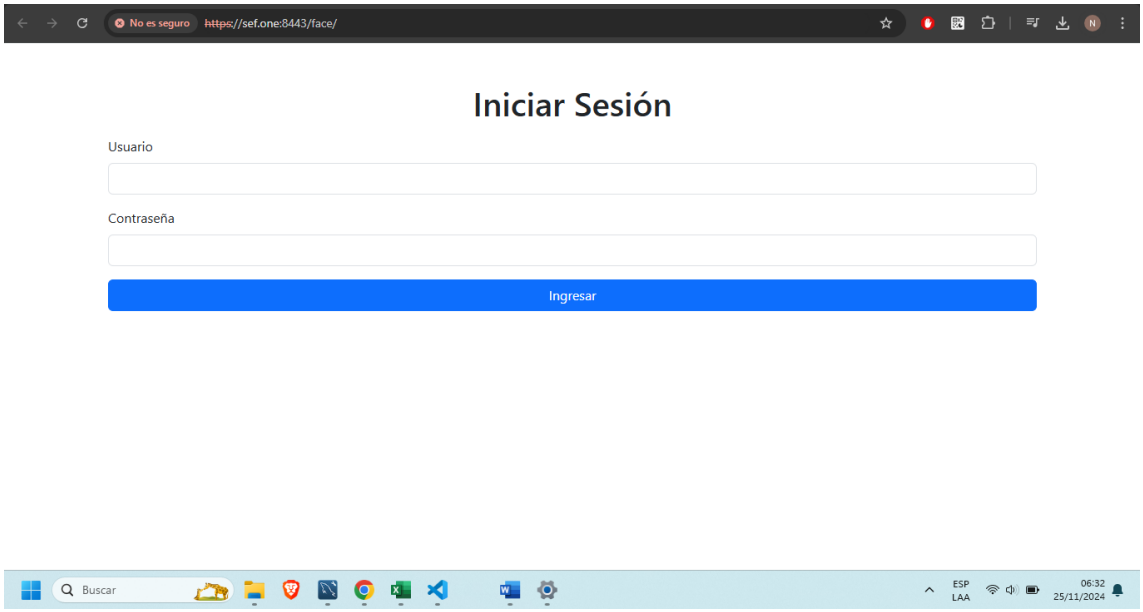
Expresión facial: Se pidió a los usuarios realizar diferentes expresiones.

Datos Demográficos de los Participantes:

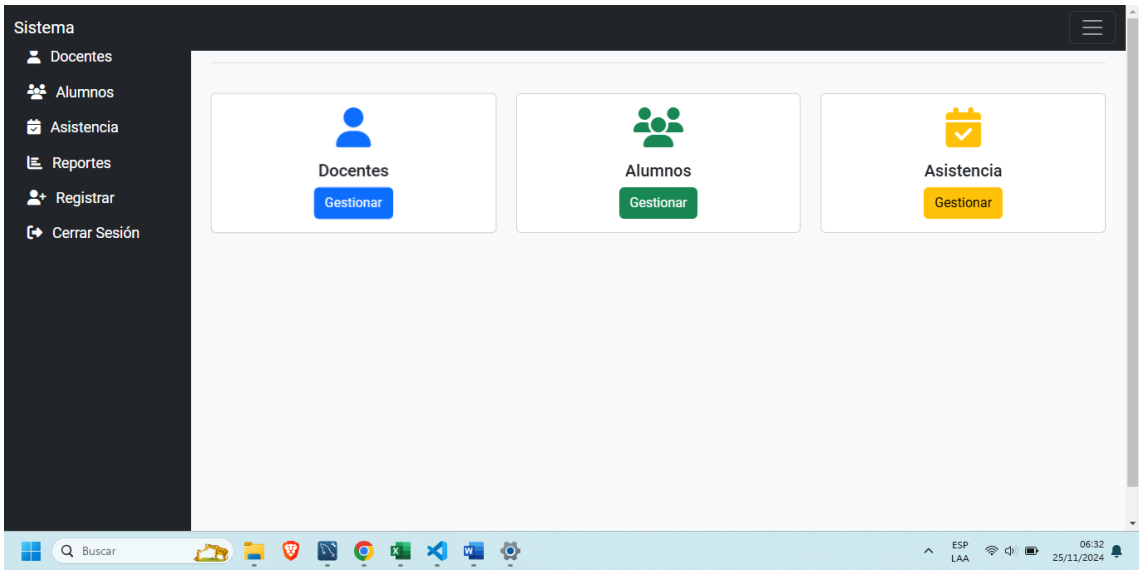
Grupo de Usuario	**Número de Participantes**	**Género**	**Edad Media**
Estudiantes	75	M/F	16
Profesores nombrados	20	M/F	35
Profesores contratados	13	M/F	34

Anexos 3 Captura de pantallas:

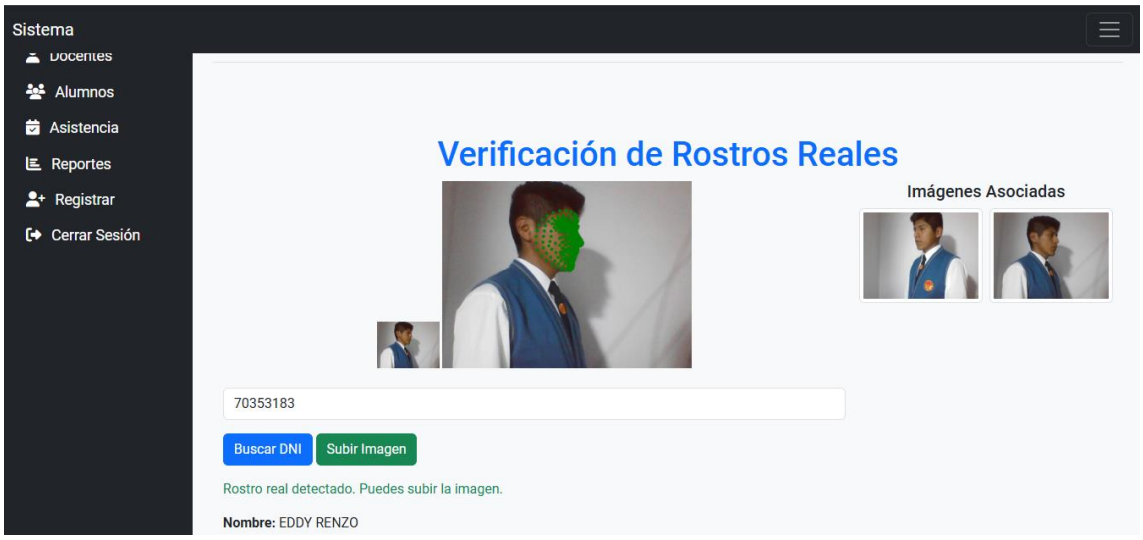
Login del Sistema



Interfaz de Usuarios



Registro de usuarios



Registro de asistencias

Anexos 4 Declaración jurada de autenticidad de tesis

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo Nelson Yoel Phuño Cahuana,
identificado con DNI 71727350 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**
Ingeniería de Sistemas,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:
" Sistema de Autenticación Biométrica
Mediante Técnicas de Aprendizaje Profundo
en el Colegio Industrial 32 de Puno "

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 16 de Diciembre del 2024

FIRMA (obligatoria)

Huella

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo Daysi Saimira Machaca Condori,
identificado con DNI 76237051 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**
Ingeniería de Sistemas,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:
"Sistema de Autenticación Biométrica Mediante Técnicas de Aprendizaje Profundo en el Colegio Industrial 32 de Puno"

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 16 de Diciembre del 2024

FIRMA (obligatoria)

Huella

Anexos 5 Autorización para el depósito de tesis en el Repositorio Institucional

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo Nelson Yoel Phoño Cahuana,
identificado con DNI 71727350 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**

Ingeniería de Sistemas,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:

"Sistema de Autenticación Biométrica mediante Técnicas de Aprendizaje Profundo en el Colegio Industrial 32 de Puno"

para la obtención de ☐**Grado,** ☒ **Título Profesional** o ☐ **Segunda Especialidad.**

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos") que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

Autorizo a la Universidad Nacional del Altiplano de Puno a publicar los Contenidos en el Repositorio Institucional y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con sus Repositorios Institucionales. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia:

Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: https://creativecommons.org/licenses/by-nc-sa/4.0/

En señal de conformidad, suscribo el presente documento.

Puno 16 de Diciembre del 20 24

FIRMA (obligatoria)

Huella

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo Daysi Saimira Machaca Condori,
identificado con DNI 76237051 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**

Ingeniería de Sistemas,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:

"Sistema de Autenticación Biométrica Mediante Técnicas de Aprendizaje Profundo en el Colegio Industrial 32 de Puno"

para la obtención de ☐**Grado,** ☒ **Título Profesional** o ☐ **Segunda Especialidad.**

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos") que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

Autorizo a la Universidad Nacional del Altiplano de Puno a publicar los Contenidos en el Repositorio Institucional y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con sus Repositorios Institucionales. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia:

Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: https://creativecommons.org/licenses/by-nc-sa/4.0/

En señal de conformidad, suscribo el presente documento.

Puno 16 de Diciembre del 2024

FIRMA (obligatoria)

Huella